Avaya G450

CLI Reference

03-602056
Issue 2
June 2008

© 2008 Avaya Inc.
All Rights Reserved.

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document may be incorporated in future releases.

For full legal page information, please see the complete document, Avaya Legal Page for Software Documentation, Document number 03-600758.

To locate this document on the website, simply go to http://www.avaya.com/support and search for the document number in the search box.

Documentation disclaimer

Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. Customer and/or End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation to the extent made by the Customer or End User.

Link disclaimer

Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all of the time and we have no control over the availability of the linked pages.

Warranty

Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available through the following Web site:

http://www.avaya.com/support

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Avaya support

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

http://www.avaya.com/support

Contents

About this Book 33

Overview 33
Audience 33
Using this book 33
Conventions 34
Downloading this book and updates from the Web 34
Downloading this book 35
Related resources 35
Technical assistance 36
Within the US 36
International 36
Trademarks 36
Sending us comments 37

Chapter 1: User Levels and Contexts 39

User levels 39
Contexts 40
Interface contexts 40
Entering an interface 41
Command line prompts 41
Available contexts 42

Chapter 2: Roadmap 45

Analog testing - Test and Heal 45
Announcement files 46
ARP table 47
ASG authentication 48
Auxiliary files 50
Backing up the gateway to a USB device 50
Backup interfaces 51
Broadcast relay 51
CAM table 52
CDR file 52
CLI sessions 53
CNA test plugs 53
Configuration files 54
Connectivity 56
Contact closure 56
Counters 57
CSU loopbacks 57
Date and time setting 57
Default gateway 58
Default settings 58
Device status 58
DHCP and BOOTP relay 60
DHCP binding file 60

DHCP client . . . 61
DHCP server . . . 62
Dialer interface . . . 65
Display . . . 66
DNS resolver . . . 66
Dynamic CAC . . . 68
Dynamic trap manager . . . 68
E1/T1 interfaces . . . 69
Echo cancellation configuration . . . 70
Ethernet port configuration . . . 71
ETR . . . 72
Fans . . . 72
Firmware management . . . 72
Fragmentation . . . 74
Frame relay encapsulation . . . 74
GRE tunneling . . . 76
HTTP server . . . 77
ICC configuration . . . 77
ICMP errors . . . 78
ICMP keepalive . . . 78
IP interface configuration . . . 79
IP phone upgrades . . . 80
IP unnumbered . . . 82
IPHC header compression . . . 82
License file of CM . . . 83
License file of gateway . . . 84
Link status . . . 85
LLDP . . . 85
Logging . . . 86
Master key configuration . . . 87
MGC (Media Gateway Controller) configuration . . . 87
Modem configuration – Console port . . . 88
Modem configuration – USB modem port . . . 89
MSS notifications 526 . . . 90
Object tracking . . . 91
OSPF . . . 93
Packet sniffing . . . 94
Platform information . . . 97
PMI . . . 98
Policy - access control lists . . . 98
Policy - QoS lists . . . 103
Policy-based routing . . . 108
Port classification . . . 111
Port mirroring . . . 111
Port redundancy . . . 111
Port status . . . 112
PPP encapsulation . . . 112

PPPoE (PPP over Ethernet) . . . 113
Priority queueing . . . 115
Proxy ARP . . . 115
QoS . . . 116
RADIUS authentication . . . 116
Recovery password . . . 117
Restoring gateway configuration . . . 117
RIP . . . 117
RMON monitoring . . . 119
Route redistribution . . . 120
Routing table configuration . . . 120
RSVP . . . 121
RTCP . . . 121
RTP statistics . . . 122
SAT . . . 123
SLS survivability . . . 123
SNMP access configuration . . . 135
SNMP trap configuration . . . 137
Spanning tree . . . 138
SSH protocol . . . 139
Synchronization . . . 139
SYN-cookies . . . 140
Syslog files . . . 140
System identification . . . 141
Telnet access . . . 141
TFTP server . . . 142
Traffic shaping . . . 142
USB mass storage device . . . 143
User accounts . . . 144
USP configuration . . . 145
Van Jacobson header compression . . . 145
VLAN configuration . . . 146
VoIP . . . 147
VoIP testing . . . 148
VPN . . . 148
VRRP . . . 154
WAN configuration, verifying . . . 155
WAN Ethernet port configuration . . . 156
WFVQ (Weighted Fair VoIP Queuing) . . . 156

Chapter 3: CLI Commands . . . 159

About the CLI . . . 159
Logging in to the CLI . . . 159
Using the CLI . . . 160
Using Help . . . 160
Using auto-complete . . . 160
Abbreviating commands . . . 160

Analog testing - Test and Heal . . . 161
analog-test . . . 161
cancel . . . 161
clear profile . . . 162
launch . . . 163
profile . . . 164
set crosstalk-destination . . . 165
set crosstalk-port . . . 166
set crosstalk-responder . . . 167
set destination . . . 168
set port . . . 169
set responder . . . 170
set responder-type . . . 171
set type . . . 172
show (profile) . . . 173
show result (profile) . . . 174
set balance . . . 175
set receive-gain . . . 176
set transmit-gain . . . 177
show correction . . . 178
show profile . . . 179
show result . . . 180
Announcement files . . . 182
copy announcement-file ftp . . . 182
copy announcement-file scp . . . 183
copy announcement-file usb . . . 184
copy ftp announcement-file . . . 185
copy scp announcement-file . . . 186
copy usb announcement-file . . . 187
erase announcement-file . . . 188
rename announcement-file . . . 189
show announcements files . . . 190
show download announcement-file status . . . 191
show upload announcement-file status . . . 192
ARP table . . . 194
arp . . . 194
arp timeout . . . 195
clear arp-cache . . . 196
ip max-arp-entries . . . 197
show ip arp . . . 198
show ip reverse-arp . . . 199
ASG authentication . . . 200
copy auth-file ftp . . . 200
copy auth-file scp . . . 201
copy auth-file tftp . . . 202
copy auth-file usb . . . 203
copy ftp auth-file . . . 204

copy scp auth-file . . . 205
copy tftp auth-file . . . 206
copy usb auth-file . . . 207
erase auth-file . . . 208
login authentication lockout . . . 209
login authentication local-craft-password . . . 210
login authentication response-time . . . 211
login authentication services-login . . . 212
ppp authentication . . . 213
show auth-file info . . . 214
show download auth-file status . . . 215
show login authentication . . . 216
show upload auth-file status . . . 217
username . . . 218
Auxiliary files . . . 219
set web aux-files-url . . . 219
show web aux-files-url . . . 220
Backing up the gateway to a USB device . . . 221
backup config usb . . . 221
show backup status . . . 222
Backup interfaces . . . 223
backup delay . . . 223
backup interface . . . 224
Broadcast relay . . . 225
ip directed-broadcast . . . 225
ip netbios-rebroadcast . . . 225
CAM table . . . 227
clear cam . . . 227
show cam . . . 227
show cam mac . . . 228
CDR file . . . 229
copy cdr-file ftp . . . 229
copy cdr-file scp . . . 230
copy cdr-file tftp . . . 231
copy cdr-file usb . . . 232
show upload cdr-file status . . . 233
CLI sessions . . . 234
exit . . . 234
reset . . . 235
retstatus . . . 236
set logout . . . 236
show logout . . . 237
tech . . . 238
tree . . . 238
CNA test plugs . . . 239
cna testplug . . . 239
clear counters (CNA test plugs) . . . 240

control-port . . . 241
fingerprint . . . 241
rtp-echo-port . . . 242
rtp-test-port . . . 243
scheduler . . . 244
shutdown (CNA test plugs) . . . 245
test-rate-limit . . . 246
cna-testplug-service . . . 247
show cna testplug . . . 247
Configuration files . . . 251
copy ftp startup-config . . . 251
copy running-config ftp . . . 252
copy running-config scp . . . 253
copy running-config startup-config . . . 254
copy running-config tftp . . . 255
copy scp startup-config . . . 256
copy startup-config ftp . . . 257
copy startup-config scp . . . 258
copy startup-config tftp . . . 259
copy startup-config usb . . . 260
copy tftp startup-config . . . 261
copy usb startup-config . . . 262
erase startup-config . . . 262
nvram initialize . . . 263
show copy status . . . 264
show download status . . . 265
show erase status . . . 266
show running-config . . . 266
show startup-config . . . 267
show upload status . . . 268
Connectivity . . . 269
ping . . . 269
Contact closure . . . 270
set contact-closure admin . . . 270
set contact-closure pulse-duration . . . 271
show contact-closure . . . 272
Counters . . . 273
clear counters (interface) . . . 273
clear ip traffic . . . 274
show ip traffic . . . 275
CSU loopbacks . . . 277
show csu loopbacks . . . 277
show csu status . . . 278
Date and time setting . . . 279
set date . . . 279
set time . . . 280
Default gateway . . . 281

ip default-gateway . . . 281
Default settings . . . 283
zeroize . . . 283
Device status . . . 284
clear utilization cpu . . . 284
set utilization cpu . . . 284
show download . . . 285
show faults . . . 286
show mg list_config . . . 287
show mgc . . . 288
show mm . . . 289
show module . . . 290
show recovery . . . 291
show restart-log . . . 292
show system . . . 293
show temp . . . 294
show timeout . . . 295
show upload . . . 296
show utilization . . . 297
show voltages . . . 297
test led . . . 298
DHCP and BOOTP relay . . . 299
ip bootp-dhcp network . . . 299
ip bootp-dhcp relay . . . 300
ip bootp-dhcp server . . . 300
DHCP binding file . . . 301
copy dhcp-binding ftp . . . 301
copy dhcp-binding scp . . . 302
copy dhcp-binding tftp . . . 303
copy dhcp-binding usb . . . 304
show upload dhcp-binding-file status . . . 305
DHCP client . . . 306
clear ip dhcp-client statistics . . . 306
ip address dhcp . . . 306
ip dhcp client client-id . . . 307
ip dhcp client hostname . . . 308
ip dhcp client lease . . . 309
ip dhcp client request . . . 310
ip dhcp client route track . . . 311
release dhcp . . . 312
renew dhcp . . . 313
show ip dhcp-client . . . 314
show ip dhcp-client statistics . . . 318
DHCP server . . . 320
clear ip dhcp-server binding . . . 320
clear ip dhcp server statistics . . . 321
ip dhcp activate pool . . . 321

ip dhcp ping packets . . . 322
ip dhcp ping timeout . . . 323
ip dhcp pool . . . 324
bootfile . . . 325
client-identifier . . . 326
default-router . . . 327
dns-server . . . 327
domain-name . . . 328
end-ip-addr . . . 329
lease . . . 330
name . . . 331
next-server . . . 332
option . . . 333
name . . . 334
value . . . 335
server-name . . . 336
show ip dhcp-pool . . . 337
start-ip-addr . . . 341
subnet-mask . . . 342
vendor-specific-option . . . 343
class-identifier . . . 343
name . . . 344
value . . . 345
ip dhcp-server . . . 347
show ip dhcp-server bindings . . . 347
show ip dhcp-server statistics . . . 348
Dialer interface . . . 350
interface dialer . . . 350
dialer modem-interface . . . 351
dialer order . . . 352
dialer persistent . . . 353
dialer persistent delay . . . 353
dialer persistent initial delay . . . 354
dialer persistent max-attempts . . . 355
dialer persistent re-enable . . . 356
dialer string . . . 356
dialer wait-for-ipcp . . . 357
ip address negotiated . . . 358
Display . . . 359
banner login . . . 359
banner post-login . . . 360
clear screen . . . 360
hostname . . . 361
line . . . 362
show banner login . . . 363
show banner post-login . . . 363
terminal length . . . 364

terminal width . . . 365
DNS resolver . . . 366
clear ip domain statistics . . . 366
ip domain list . . . 366
ip domain lookup . . . 367
ip domain name-server-list . . . 368
description (DNS resolver) . . . 369
name-server . . . 369
ip domain retry . . . 370
ip domain timeout . . . 371
nslookup . . . 372
ppp ipcp dns request . . . 373
show ip domain . . . 373
show ip domain statistics . . . 375
show protocol . . . 377
Dynamic CAC . . . 379
dynamic-cac . . . 379
show dynamic-cac . . . 380
Dynamic trap manager . . . 380
clear dynamic-trap-manager . . . 380
snmp-server dynamic-trap-manager . . . 381
E1/T1 interfaces . . . 383
clear controller counters . . . 383
controller . . . 384
cablelength long . . . 385
cablelength short . . . 386
channel-group . . . 387
clock source . . . 388
fdl . . . 389
framing . . . 390
linecode (E1) . . . 391
linecode (T1) . . . 392
loopback . . . 393
remote . . . 394
ds-mode . . . 395
interface serial . . . 396
ip address . . . 397
show controllers . . . 398
show controllers remote . . . 399
show ds-mode . . . 400
Echo cancellation . . . 401
set echo-cancellation analog . . . 401
set echo-cancellation config analog . . . 402
set echo-cancellation config voip . . . 405
set echo-cancellation voip . . . 407
show echo-cancellation . . . 408
Ethernet port configuration . . . 410

set port auto-negotiation-flowcontrol-advertisement . . . 410
set port duplex. . . . 411
set port edge admin state . . . 412
set port enable | disable . . . 413
set port flowcontrol . . . 414
set port level. . . . 416
set port name . . . 417
set port negotiation . . . 418
set port point-to-point admin status . . . 419
set port speed . . . 420
show port auto-negotiation-flowcontrol-advertisement . . . 421
show port edge state . . . 422
show port flowcontrol . . . 423
ETR . . . 425
set etr . . . 425
show etr . . . 426
Fans . . . 427
show platform fans . . . 427
Firmware management . . . 428
copy ftp EW_archive . . . 428
copy ftp module . . . 429
copy ftp SW_imageA . . . 430
copy ftp SW_imageB . . . 431
copy tftp EW_archive . . . 432
copy tftp module. . . . 433
copy tftp SW_imageA . . . 434
copy tftp SW_imageB . . . 435
copy usb EW_archive . . . 436
copy usb module . . . 437
copy usb SW_image . . . 438
dir . . . 439
set boot bank . . . 441
show boot bank . . . 442
show download software status . . . 442
show image version . . . 443
Fragmentation . . . 444
clear fragment . . . 444
fragment chain . . . 445
fragment size . . . 446
fragment timeout . . . 447
show fragment. . . . 447
Frame relay encapsulation . . . 448
clear frame-relay counters . . . 448
interface serial. . . . 449
encapsulation . . . 451
frame-relay class-dlci . . . 452
frame-relay interface-dlci . . . 453

frame-relay lmi-n391dte . . . 454
frame-relay lmi-n392dte . . . 455
frame-relay lmi-n393dte . . . 456
frame-relay lmi-type . . . 457
frame-relay priority-dlci-group . . . 458
frame-relay traffic-shaping . . . 459
ip address . . . 460
map-class frame-relay . . . 461
bc out . . . 462
be out . . . 463
cir out . . . 464
fragment . . . 465
show frame-relay map . . . 466
show frame-relay pvc brief . . . 467
show interfaces . . . 467
show map-class frame-relay . . . 470
show traffic-shape . . . 471
show traffic-shape-queue . . . 473
show traffic-shape-statistics . . . 475
GRE tunneling . . . 477
interface tunnel . . . 477
keepalive (GRE tunnel) . . . 478
tunnel checksum . . . 479
tunnel destination . . . 479
tunnel dscp . . . 480
tunnel key . . . 481
tunnel mode . . . 482
tunnel path-mtu-discovery . . . 483
tunnel source . . . 484
tunnel ttl . . . 485
show interfaces . . . 486
HTTP server . . . 489
ip http . . . 489
ICC configuration . . . 490
icc-vlan . . . 490
show icc-vlan . . . 490
ICMP errors . . . 491
ip icmp-errors . . . 491
show ip icmp . . . 492
ICMP keepalive . . . 492
keepalive-icmp . . . 492
keepalive-icmp failure-retries . . . 493
keepalive-icmp interval . . . 494
keepalive-icmp source-address . . . 495
keepalive-icmp success-retries . . . 496
keepalive-icmp timeout . . . 497
show keepalive-icmp . . . 497

IP interface configuration . . . 498
interface console . . . 498
interface dialer . . . 499
interface fastethernet . . . 500
interface loopback . . . 501
interface serial . . . 502
interface tunnel . . . 503
interface USB-modem . . . 504
interface vlan . . . 505
description (interface) . . . 506
ip address . . . 507
ip admin-state . . . 508
ip broadcast-address . . . 509
load-interval . . . 509
show ip interface . . . 510
show ip interface brief . . . 513
shutdown (interface) . . . 514
IP phone upgrades . . . 515
clear ip tftp-server statistics . . . 515
copy ftp phone-image . . . 516
copy ftp phone-script . . . 517
copy phone-script ftp . . . 518
copy phone-script scp . . . 519
copy phone-script tftp . . . 520
copy phone-script usb . . . 521
copy scp phone-script . . . 522
copy tftp phone-image . . . 523
copy tftp phone-script . . . 524
copy usb phone-image . . . 525
copy usb phone-script . . . 526
erase phone-image . . . 527
erase phone-script . . . 527
ip tftp-server file-system size . . . 528
show application-memory . . . 529
show download phone-image-file status . . . 530
show download phone-script-file status . . . 531
show ip tftp-server files . . . 532
show ip tftp-server statistics . . . 533
show upload phone-script-file status . . . 534
IP unnumbered . . . 535
ip unnumbered . . . 535
IPHC header compression . . . 537
clear ip rtp header-compression . . . 537
clear ip tcp header-compression . . . 538
ip rtp compression-connections . . . 539
ip rtp header-compression . . . 540
ip rtp max-period . . . 541

ip rtp max-time . . . 542
ip rtp non-tcp-mode . . . 543
ip rtp port-range . . . 544
ip tcp compression-connections . . . 545
show ip rtp header-compression . . . 546
show ip rtp header-compression brief . . . 548
show ip tcp header-compression . . . 549
show ip tcp header-compression brief . . . 551
License file of CM . . . 552
ip license-server . . . 552
License file of gateway . . . 553
copy ftp license-file . . . 553
copy license-file ftp . . . 554
copy license-file scp . . . 555
copy license-file tftp . . . 556
copy license-file usb . . . 556
copy scp license-file . . . 557
copy tftp license-file . . . 558
copy usb license-file . . . 559
show download license-file status . . . 560
show license status . . . 561
show upload license-file status . . . 562
Link status . . . 563
show isdn bri link . . . 563
show isdn link summary . . . 564
show isdn pri link . . . 565
LLDP . . . 566
set lldp re-init-delay . . . 566
set lldp system-control . . . 567
set lldp tx-delay . . . 567
set lldp tx-hold-multiplier . . . 568
set lldp tx-interval . . . 569
set port lldp . . . 570
set port lldp tlv . . . 571
show lldp . . . 573
show lldp config . . . 575
show port lldp config . . . 576
show port lldp vlan-name config . . . 578
Logging . . . 579
clear logging file . . . 579
clear logging server . . . 580
set logging file . . . 581
set logging server . . . 583
set logging server access-level . . . 584
set logging server condition . . . 585
set logging server enable | disable . . . 586
set logging server facility . . . 587

set logging session . . . 588
show dev log file . . . 590
show logging file condition . . . 590
show logging file content . . . 591
show logging server condition . . . 592
show logging session condition . . . 593
Master key configuration . . . 594
key config-key password-encryption . . . 594
MGC (Media Gateway Controller) configuration . . . 596
clear mgc list . . . 596
session . . . 597
set icc-monitoring . . . 598
set mediaserver . . . 598
set mgc list . . . 599
set reset-times . . . 600
show icc-monitoring . . . 601
show mediaserver . . . 602
show mgc . . . 603
show mgc list . . . 604
show recovery . . . 605
Modem configuration – Console port . . . 606
interface console . . . 606
async mode interactive . . . 607
async mode terminal . . . 607
async modem-init-string . . . 608
async reset-modem (Console port) . . . 609
ip peer address . . . 609
ppp authentication . . . 610
ppp chap-secret . . . 611
ppp timeout authentication . . . 612
show ppp authentication . . . 613
shutdown (interface) . . . 614
speed (PPP) . . . 615
timeout absolute . . . 615
Modem configuration – USB modem port . . . 616
interface usb-modem . . . 616
async modem-init-string . . . 617
async reset-modem (USB port) . . . 618
ip peer address . . . 619
ppp authentication . . . 620
ppp chap-secret . . . 621
ppp timeout authentication . . . 622
show ppp authentication . . . 623
shutdown (USB modem) . . . 624
timeout absolute . . . 624
MSS notifications . . . 625
DoS-classification . . . 625

icmp in-echo-limit . . . 627
set mss-notification rate . . . 627
show mss-notification rate . . . 628
Object tracking . . . 629
rtr . . . 629
type . . . 630
dscp (object tracking) . . . 631
fail-retries . . . 632
frequency . . . 633
interface-keepalive bypass-logic . . . 634
next-hop (object tracking) . . . 634
source-address . . . 636
success-retries . . . 637
wait-interval . . . 638
rtr-schedule . . . 639
show rtr configuration . . . 640
show rtr operational-state . . . 642
show track . . . 643
track . . . 645
description (object tracking) . . . 647
object . . . 648
threshold count . . . 649
OSPF . . . 650
bandwidth . . . 650
ip ospf authentication . . . 651
ip ospf authentication-key . . . 652
ip ospf cost . . . 653
ip ospf dead-interval . . . 654
ip ospf hello-interval . . . 655
ip ospf message-digest-key . . . 656
ip ospf network point-to-multipoint . . . 657
ip ospf priority . . . 657
ip ospf router-id . . . 658
router ospf . . . 659
area . . . 660
default-metric (OSPF) . . . 661
network (OSPF) . . . 661
passive-interface . . . 662
redistribute (OSPF) . . . 663
timers spf . . . 664
show ip ospf . . . 665
show ip ospf database . . . 666
show ip ospf interface . . . 667
show ip ospf neighbor . . . 668
show ip protocols . . . 669
Packet sniffing . . . 670
capture buffer-mode . . . 670

capture buffer-size . . . 671
capture filter-group . . . 672
capture interface . . . 673
capture ipsec . . . 674
capture max-frame-size . . . 675
capture start . . . 675
capture stop . . . 676
capture-service . . . 677
clear capture-buffer . . . 678
copy capture-file ftp . . . 679
copy capture-file scp . . . 680
copy capture-file tftp . . . 681
copy capture-file usb . . . 682
ip capture-list . . . 683
cookie . . . 683
ip-rule (policy, policy-based routing, packet sniffing) . . . 684
composite-operation . . . 685
destination-ip . . . 686
dscp (policy-based routing, packet sniffing, VPN) . . . 688
fragment . . . 689
icmp . . . 690
ip-protocol . . . 692
show ip-rule . . . 693
source-ip . . . 695
tcp destination-port . . . 696
tcp source-port . . . 698
udp destination-port . . . 700
udp source-port . . . 702
name . . . 704
owner . . . 705
show capture . . . 706
show capture-buffer hex . . . 707
show ip capture-list . . . 708
Password management . . . 710
Platform information . . . 710
show platform fans . . . 710
show platform power . . . 711
show platform mainboard . . . 712
PMI . . . 714
pmi . . . 714
show pmi . . . 715
Policy - access control lists . . . 716
ip access-control-list . . . 716
cookie . . . 717
ip-fragments-in . . . 718
ip-option-in . . . 719
ip-rule (policy, policy-based routing, packet sniffing) . . . 719

composite-operation . . . 720
destination-ip . . . 721
dscp (policy) . . . 723
fragment . . . 724
icmp . . . 725
ip-protocol . . . 727
show composite-operation . . . 728
show ip-rule . . . 729
source-ip . . . 731
tcp destination-port . . . 732
tcp established . . . 734
tcp source-port . . . 735
udp destination-port . . . 737
udp source-port . . . 739
name . . . 741
owner . . . 742
show composite-operation . . . 743
show ip-rule . . . 744
show list . . . 745
ip access-group . . . 746
ip policy-list-copy . . . 747
ip simulate . . . 748
show ip access-control-list . . . 750
Policy - QoS lists . . . 752
ip policy-list-copy . . . 752
ip qos-group . . . 753
ip qos-list . . . 754
composite-operation . . . 755
cos . . . 756
dscp (policy) . . . 757
name . . . 758
show composite-operation . . . 759
cookie . . . 760
dscp-table . . . 761
composite-operation . . . 762
name . . . 763
show dscp-table . . . 764
ip-rule (policy, policy-based routing, packet sniffing) . . . 765
composite-operation . . . 766
destination-ip . . . 767
dscp (policy) . . . 769
fragment . . . 770
icmp . . . 771
ip-protocol . . . 772
show composite-operation . . . 774
show dscp-table . . . 775
show ip-rule . . . 776

source-ip . . . 778
tcp destination-port . . . 779
tcp source-port . . . 781
udp destination-port . . . 783
udp source-port . . . 785
name . . . 787
owner . . . 788
pre-classification . . . 789
show composite-operation . . . 790
show dscp-table . . . 791
show ip-rule . . . 792
show list . . . 794
ip simulate . . . 795
show ip qos-list . . . 796
Policy-based routing . . . 798
ip next-hop-list . . . 798
next-hop-interface . . . 799
next-hop-ip . . . 801
show next-hop . . . 802
ip pbr-group . . . 802
ip pbr-list . . . 803
cookie . . . 804
icmp . . . 805
ip-rule (policy, policy-based routing, packet sniffing) . . . 806
destination-ip . . . 807
dscp (policy-based routing, packet sniffing, VPN) . . . 809
fragment . . . 810
ip-protocol . . . 811
next-hop (policy-based routing) . . . 813
show ip next-hop-list . . . 814
show ip-rule . . . 815
source-ip . . . 816
tcp destination-port . . . 818
tcp source-port . . . 820
udp destination-port . . . 822
udp source-port . . . 824
name . . . 826
owner . . . 827
show ip-rule . . . 828
show list . . . 830
show ip active-lists . . . 831
show ip active-pbr-lists . . . 833
show ip pbr-list . . . 833
Port classification . . . 834
set port classification . . . 834
show port classification . . . 835
Port mirroring . . . 836

clear port mirror . . . 836
set port mirror . . . 837
show port mirror . . . 838
Port redundancy . . . 839
set port redundancy . . . 839
set port redundancy enable|disable . . . 841
set port redundancy-intervals . . . 842
show port redundancy . . . 843
Port status . . . 843
show port . . . 843
PPP encapsulation . . . 845
interface serial . . . 845
encapsulation . . . 846
ip address . . . 848
keepalive (PPP) . . . 849
ppp timeout ncp . . . 850
ppp timeout retry . . . 851
show interfaces . . . 851
PPPoE (PPP over Ethernet) . . . 854
interface FastEthernet . . . 854
encapsulation pppoe . . . 855
ip address negotiated . . . 856
mtu . . . 857
ppp chap hostname . . . 858
ppp chap password . . . 859
ppp chap refuse . . . 860
ppp ipcp dns request . . . 860
ppp pap refuse . . . 861
ppp pap sent-username . . . 862
pppoe-client persistent delay . . . 863
pppoe-client persistent max-attempts . . . 864
pppoe-client service-name . . . 865
pppoe-client wait-for-ipcp . . . 866
Priority queueing . . . 867
priority-queue . . . 867
queue-limit . . . 868
show queueing . . . 869
voip-queue . . . 871
voip-queue-delay . . . 872
Proxy ARP . . . 873
ip proxy-arp . . . 873
QoS . . . 874
set qos bearer . . . 874
set qos control . . . 875
set qos signal . . . 876
show qos-rtcp . . . 877
show voip-parameters . . . 878

RADIUS authentication . . . 879
clear radius authentication server . . . 879
set radius authentication . . . 880
set radius authentication retry-number . . . 881
set radius authentication retry-time . . . 882
set radius authentication secret . . . 882
set radius authentication server . . . 883
set radius authentication udp-port . . . 884
show radius authentication . . . 885
Recovery password . . . 886
set terminal recovery password . . . 886
Restoring gateway configuration . . . 887
restore usb . . . 887
show restore status . . . 888
RIP . . . 889
ip distribution access-default-action . . . 889
ip distribution access-list . . . 890
ip distribution access-list-cookie . . . 891
ip distribution access-list-copy . . . 892
ip distribution access-list-name . . . 892
ip distribution access-list-owner . . . 893
ip rip authentication key . . . 894
ip rip authentication mode . . . 895
ip rip default-route-mode . . . 896
ip rip poison-reverse . . . 897
ip rip rip-version . . . 897
ip rip send-receive-mode . . . 898
ip rip split-horizon . . . 899
router rip . . . 900
default-metric (RIP) . . . 901
distribution-list . . . 901
network (RIP) . . . 902
redistribute (RIP) . . . 903
timers basic . . . 904
show ip distribution access-lists . . . 905
show ip protocols . . . 905
RMON monitoring . . . 907
clear rmon statistics . . . 907
rmon alarm . . . 907
rmon event . . . 909
rmon history . . . 910
show rmon alarm . . . 911
show rmon event . . . 912
show rmon history . . . 913
show rmon statistics . . . 914
Route redistribution . . . 915
default-metric (interface route metric value) . . . 915

default-metric (OSPF) . . . 915
default-metric (RIP) . . . 916
redistribute (OSPF) . . . 917
redistribute (RIP) . . . 918
Routing table configuration . . . 919
clear ip route . . . 919
ip default-gateway . . . 920
ip netmask-format . . . 921
ip redirects . . . 922
ip route . . . 922
ip routing . . . 924
show ip route . . . 925
show ip route best-match . . . 926
show ip route static . . . 927
show ip route summary . . . 928
show ip route track-table . . . 929
traceroute . . . 929
RSVP . . . 932
set qos rsvp . . . 932
show qos-rtcp . . . 933
RTCP . . . 934
set qos rtcp . . . 934
show qos-rtcp . . . 935
RTP statistics . . . 937
rtp-stat clear . . . 937
rtp-stat event-threshold . . . 938
rtp-stat fault . . . 940
rtp-stat min-stat-win . . . 941
rtp-stat qos-trap . . . 942
rtp-stat qos-trap-rate-limit . . . 943
rtp-stat-service . . . 944
rtp-stat threshold . . . 944
show rtp-stat config . . . 947
show rtp-stat detailed . . . 948
show rtp-stat sessions . . . 949
show rtp-stat summary . . . 952
show rtp-stat thresholds . . . 953
show rtp-stat traceroute . . . 954
SAT . . . 956
sat . . . 956
SLS survivability . . . 957
sls . . . 957
set sls . . . 958
show sls . . . 959
bri . . . 960
set bearer-capability . . . 961
set country-protocol . . . 962

set directory-number-a . . . 964
set directory-number-b . . . 965
set endpoint-init . . . 966
set interface . . . 967
set interface-companding . . . 968
set layer1-stable . . . 969
set name . . . 970
set side . . . 971
set spid-a . . . 973
set spid-b . . . 974
set tei-assignment . . . 975
show (bri) . . . 976
clear attendant . . . 978
clear bri . . . 978
clear dial-pattern . . . 979
clear ds1 . . . 980
clear extension . . . 980
clear fac . . . 981
clear incoming-routing . . . 982
clear sig-group . . . 983
clear slot-config . . . 984
clear station . . . 985
clear survivable-config . . . 986
clear trunk-group . . . 986
dial-pattern . . . 987
set delete-digits . . . 989
set deny . . . 990
set insert-digits (dial-pattern) . . . 990
set max-length . . . 991
set min-length . . . 992
set tgnum . . . 993
set type (dial-pattern) . . . 994
show (dial-pattern) . . . 997
ds1 . . . 998
set bearer-capability . . . 1000
set bit-rate . . . 1001
set channel-numbering . . . 1002
set connect . . . 1003
set country-protocol . . . 1004
set interface . . . 1005
set interface-companding . . . 1007
set long-timer . . . 1008
set name . . . 1009
set protocol-version . . . 1010
set side . . . 1012
set signaling-mode . . . 1013
show (ds1) . . . 1014

incoming-routing . . . 1017
set delete-digits . . . 1018
set insert-digits (incoming-routing) . . . 1019
set length . . . 1020
set match-pattern . . . 1021
show (incoming-routing) . . . 1022
set attendant . . . 1023
set date-format . . . 1024
set fac . . . 1025
set ip-codec-set . . . 1026
set max-ip-registrations . . . 1027
set pim-lockout . . . 1027
set slot-config . . . 1028
show attendant . . . 1030
show bri . . . 1030
show date-format . . . 1032
show dial-pattern . . . 1032
show ds1 . . . 1034
show extension . . . 1035
show fac . . . 1037
show incoming-routing . . . 1038
show ip-codec-set . . . 1039
show last-pim-update . . . 1040
show max-ip-registrations . . . 1040
show pim-lockout . . . 1041
show sig-group . . . 1041
show slot-config . . . 1042
show station . . . 1043
show trunk-group . . . 1045
sig-group . . . 1047
add nfas-interface . . . 1049
remove nfas-interface . . . 1050
set associated-signaling . . . 1051
set primary-dchannel . . . 1052
set trunk-group-chan-select . . . 1053
show (sig-group) . . . 1054
station . . . 1055
set cor . . . 1056
set expansion-module . . . 1059
set name . . . 1059
set password . . . 1061
set port . . . 1062
set swhook-flash . . . 1063
set trunk-destination . . . 1064
set type (station) . . . 1065
show (station) . . . 1067
trunk-group . . . 1068

add port . . . 1072
Analog trunks . . . 1072
Digital trunks . . . 1073
clear tac . . . 1075
remove port . . . 1075
set busy-disconnect . . . 1076
set cbc . . . 1077
set cbc-parameter . . . 1079
set cbc-service-feature . . . 1080
set channel-preference . . . 1081
set codeset-display . . . 1082
set codeset-national . . . 1083
set dial . . . 1084
set digit-handling . . . 1084
set digits . . . 1086
set digit-treatment . . . 1087
set incoming-destination . . . 1088
set incoming-dialtone . . . 1089
set japan-disconnect . . . 1090
set name . . . 1091
set numbering-format . . . 1092
set send-name . . . 1093
set send-number . . . 1095
set supervision . . . 1096
set tac . . . 1097
set trunk-hunt . . . 1098
show (trunk-group) . . . 1099
SNMP access configuration . . . 1102
ip snmp . . . 1102
set snmp community . . . 1103
set snmp retries . . . 1104
set snmp timeout . . . 1105
show snmp . . . 1106
show snmp engineID . . . 1107
show snmp group . . . 1108
show snmp retries . . . 1109
show snmp timeout . . . 1110
show snmp user . . . 1111
show snmp usertogroup . . . 1112
show snmp view . . . 1113
snmp-server community . . . 1114
snmp-server engineID . . . 1115
snmp-server group . . . 1117
snmp-server remote-user . . . 1119
snmp-server user . . . 1120
snmp-server view . . . 1122
SNMP trap configuration . . . 1123

set port trap . . . 1123
set snmp trap enable | disable auth . . . 1125
set snmp trap enable | disable frame-relay . . . 1125
show port trap . . . 1126
show snmp . . . 1127
snmp trap link-status . . . 1128
snmp-server enable notifications . . . 1129
snmp-server host . . . 1130
snmp-server informs . . . 1133
Spanning tree . . . 1135
set port edge admin state . . . 1135
set port point-to-point admin status . . . 1136
set port spantree . . . 1137
set port spantree cost . . . 1138
set port spantree force-protocol-migration . . . 1139
set port spantree priority . . . 1140
set spantree default-path-cost . . . 1141
set spantree enable | disable . . . 1142
set spantree forward-delay . . . 1143
set spantree hello-time . . . 1143
set spantree max-age . . . 1144
set spantree priority . . . 1145
set spantree tx-hold-count . . . 1146
set spantree version . . . 1147
show port edge state . . . 1148
show port point-to-point status . . . 1149
show spantree . . . 1149
SSH protocol . . . 1152
clear ssh-client known-hosts . . . 1152
crypto key generate . . . 1152
disconnect ssh . . . 1153
hostname . . . 1154
ip ssh . . . 1155
show ip ssh . . . 1156
Synchronization . . . 1157
clear sync interface . . . 1157
set sync interface . . . 1158
set sync source . . . 1159
set sync switching . . . 1160
show sync timing . . . 1161
SYN-cookies . . . 1162
clear tcp syn-cookies counters . . . 1162
show tcp syn-cookies . . . 1163
tcp syn-cookies . . . 1164
Syslog files . . . 1165
copy syslog-file ftp . . . 1165
copy syslog-file scp . . . 1166

copy syslog-file tftp . . . 1167
copy syslog-file usb . . . 1167
show upload syslog-file status . . . 1168
System identification . . . 1170
set system contact . . . 1170
set system location . . . 1171
set system name . . . 1171
Telnet access . . . 1172
ip telnet . . . 1172
ip telnet-client . . . 1173
ip telnet-services . . . 1174
show ip telnet . . . 1174
telnet . . . 1175
TFTP server . . . 1176
clear ip tftp-server statistics . . . 1176
ip tftp-server . . . 1177
ip tftp-server file-system size . . . 1177
show application-memory . . . 1178
Traffic shaping . . . 1179
interface serial . . . 1179
frame-relay traffic-shaping . . . 1181
map-class frame-relay . . . 1181
bc out . . . 1183
be out . . . 1184
cir out . . . 1185
fragment . . . 1186
show map-class frame-relay . . . 1187
show traffic-shape . . . 1188
show traffic-shape-queue . . . 1190
show traffic-shape-statistics . . . 1191
traffic-shape rate . . . 1193
USB mass storage device . . . 1194
backup config usb . . . 1194
dir . . . 1195
erase usb . . . 1197
restore usb . . . 1197
safe-removal usb . . . 1198
show backup status . . . 1199
show restore status . . . 1200
show usb . . . 1201
User accounts . . . 1203
login authentication inactivity-period . . . 1203
login authentication lockout . . . 1204
login authentication min-password-digit-chars . . . 1205
login authentication min-password-length . . . 1206
login authentication min-password-lower-chars . . . 1207
login authentication min-password-special-chars . . . 1208

login authentication min-password-upper-chars . . . 1209
login authentication password-expire . . . 1210
password . . . 1212
show login authentication . . . 1213
show username . . . 1214
username . . . 1215
USP configuration . . . 1217
interface serial . . . 1217
bandwidth . . . 1218
idle-character . . . 1219
ignore dcd . . . 1220
invert txclock . . . 1221
nrzi-encoding . . . 1221
transmitter-delay . . . 1222
Van Jacobson header compression . . . 1223
clear ip tcp header-compression . . . 1223
ip tcp compression-connections . . . 1224
ip tcp header-compression . . . 1225
show ip tcp header-compression . . . 1226
show ip tcp header-compression brief . . . 1227
VLAN configuration . . . 1229
clear port static-vlan . . . 1229
clear vlan . . . 1230
interface vlan . . . 1231
icc-vlan . . . 1232
set port static-vlan . . . 1233
set port vlan . . . 1234
set port vlan-binding-mode . . . 1235
set trunk . . . 1236
set vlan . . . 1237
show cam vlan . . . 1238
show port vlan-binding-mode . . . 1239
show trunk . . . 1240
show vlan . . . 1241
VoIP . . . 1243
campon-busyout voip-dsp . . . 1243
reset voip-dsp . . . 1244
show voip-dsp . . . 1244
show voip-parameters . . . 1246
VoIP testing . . . 1247
busyout voip-dsp . . . 1247
release voip-dsp . . . 1248
show voip-parameters . . . 1249
test voip-dsp . . . 1250
VPN . . . 1251
clear crypto isakmp . . . 1251
clear crypto sa . . . 1252

clear crypto sa counters . . . 1254
crypto ipsec df-bit . . . 1254
crypto ipsec minimal-pmtu . . . 1255
crypto ipsec nat-transparency udp-encapsulation . . . 1256
crypto ipsec transform-set . . . 1257
mode . . . 1259
set pfs . . . 1260
set security-association lifetime . . . 1261
crypto isakmp invalid-spi-recovery . . . 1262
crypto isakmp nat keepalive . . . 1262
crypto isakmp peer . . . 1263
continuous-channel . . . 1264
description (ISAKMP peer) . . . 1265
initiate mode . . . 1266
isakmp-policy . . . 1267
keepalive (VPN) . . . 1268
keepalive-track . . . 1269
pre-shared-key . . . 1270
self-identity . . . 1271
suggest-key . . . 1272
crypto isakmp peer-group . . . 1273
description (ISAKMP peer group) . . . 1274
set peer (peer group) . . . 1275
crypto isakmp policy . . . 1276
authentication . . . 1277
description (ISAKMP policy) . . . 1278
encryption . . . 1279
group . . . 1280
hash . . . 1280
lifetime . . . 1281
crypto isakmp suggest-key . . . 1282
crypto map . . . 1283
continuous-channel . . . 1284
description (crypto map) . . . 1285
set dscp . . . 1286
set peer (crypto map) . . . 1287
set peer-group . . . 1288
set transform-set . . . 1289
ip crypto-group . . . 1290
ip crypto-list . . . 1291
ip-rule (VPN) . . . 1292
description (ip rule) . . . 1292
destination-ip . . . 1293
protect crypto map . . . 1295
source-ip . . . 1296
local-address . . . 1297
show crypto ipsec sa . . . 1298

show crypto ipsec transform-set . . . 1306
show crypto isakmp peer . . . 1308
show crypto isakmp peer-group . . . 1309
show crypto isakmp policy . . . 1310
show crypto isakmp sa . . . 1311
show crypto map . . . 1313
show ip active-lists . . . 1314
show ip crypto-list . . . 1316
VRRP . . . 1319
ip vrrp . . . 1319
ip vrrp address . . . 1320
ip vrrp auth-key . . . 1321
ip vrrp override addr owner . . . 1322
ip vrrp preempt . . . 1323
ip vrrp primary . . . 1324
ip vrrp priority . . . 1325
ip vrrp timer . . . 1325
router vrrp . . . 1326
show ip vrrp . . . 1327
WAN configuration, verifying . . . 1329
show controllers . . . 1329
show frame-relay fragment . . . 1330
show frame-relay lmi . . . 1331
show frame-relay map . . . 1333
show frame-relay pvc . . . 1334
show frame-relay traffic . . . 1335
show interfaces . . . 1336
show map-class frame-relay . . . 1339
WAN Ethernet port configuration . . . 1340
interface FastEthernet . . . 1340
autoneg . . . 1341
duplex . . . 1341
keepalive-track . . . 1342
speed (interface) . . . 1343
traffic-shape rate . . . 1344
WFVQ (Weighted Fair VoIP Queueing) . . . 1345
fair-queue-limit . . . 1345
fair-voip-queue . . . 1346
priority-queue . . . 1347
show queue . . . 1348
show queueing . . . 1349
voip-queue . . . 1351

Alphabetical Index of Commands . . . 1353

Topical Index of Commands . . . 1363

About this Book

Overview

The *Avaya G450 CLI Reference* describes the commands used to configure and manage the Avaya G450 Media Gateway after it is already installed. For instructions on using these commands to configure and manage the G450, refer to *Administration for the Avaya G450 Media Gateway*, 03-602055.

Audience

The information in this book is intended for use by Avaya technicians, provisioning specialists, business partners, and customers.

Using this book

This book describes how to use the G450 Command Line Interface (CLI) and provides a reference to the CLI commands. Each command description contains:

- The command name
- A short description of the purpose of the command
- The following sections:
  - **Syntax** - This section describes the correct syntax for the command.
  - **Parameters** - This section lists and describes elements of the command syntax, such as parameters, their definitions, and allowed values.
  - **User Level** - This section shows the lowest access level for which the command is accessible. There are three access levels: User (read-only), Configure (read-write), and Supervisor (admin).
  - **Context** - This section shows the contexts from which the command can be executed.
  - **Example** - This section provides an example of the use of a command, and, where applicable, the output display. This section does not appear if the syntax and output are simple.
  - **Output Fields** - This section describes the fields in the command output, if applicable.

In addition, the Roadmap chapter provides quick reference tables organized by topic for all the commands.

Conventions

The following are the conventions used in this book to represent syntax and examples:

Display Type	Description
Screen Display text	Text represented in this format is displayed by the CLI.
`User entered text`	Text represented in this format is entered by the user.
`Variable`	This format indicates a variable argument as it is entered by the user.
`Variable in text`	This format indicates a variable argument discussed in the Parameters section.
`[]`	Syntax elements grouped by square brackets are optional.
|	Syntax elements separated by a pipe are mutually exclusive. Choose one of the elements separated by the pipe.
`{}`	These braces are used to group syntax elements, where necessary, to eliminate ambiguity in the syntax. For example, if a keyword and an argument together constitute one of a set of mutually exclusive elements, the keyword and argument are grouped with braces and separated from the other options with a pipe.

Downloading this book and updates from the Web

You can download the latest version of the *Avaya G450 CLI Reference* from the Avaya Web site. You must have access to the Internet, and a copy of Acrobat Reader must be installed on your personal computer.

Avaya makes every effort to ensure that the information in this book is complete and accurate. However, information can change after we publish this book. Therefore, the Avaya Web site

might also contain new product information and updates to the information in this book. You can also download these updates from the Avaya Web site.

Downloading this book

1. Access the Avaya Web site at http://www.avaya.com/support/.
2. Click **FIND DOCUMENTATION and TECHNICAL INFORMATION by PRODUCT NAME**.
3. Type this book's document number (03-602056) in the **Search** box.
4. Click **GO**.

   The search results appear.
5. Locate the latest version of the book.
6. Click the book title. Your browser downloads the book.

Related resources

For more information on the Avaya G450 Media Gateway and related features, see the following books:

Title	Number
Overview for the Avaya G450 Media Gateway	03-602058
Quick Start for Hardware Installation for the Avaya G450 Media Gateway	03-602053
Installing and Upgrading the Avaya G450 Media Gateway	03-602054
Administration for the Avaya G450 Media Gateway	03-602055
Maintenance Alarms for Avaya Communication Manager, Media Gateways and Servers	03-300430
Maintenance Commands for Avaya Communication Manager, Media Gateways and Servers	03-300431
Maintenance Procedures for Avaya Communication Manager, Media Gateways and Servers	03-300432

Technical assistance

Avaya provides the following resources for technical assistance.

Within the US

For help with:

- Feature administration and system applications, call the Avaya DEFINITY Helpline at 1-800-225-7585
- Maintenance and repair, call the Avaya National Customer Care Support Line at 1-800-242-2121
- Toll fraud, call Avaya Toll Fraud Intervention at 1-800-643-2353

International

For all international resources, contact your local Avaya authorized dealer for additional help.

Trademarks

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners.

Sending us comments

Avaya welcomes your comments about this book. To reach us by:

- Mail, send your comments to:

  Avaya Inc.

  Product Documentation Group

  Room B3-H13

  1300 W. 120th Ave.

  Westminster, CO 80234 USA

- E-mail, send your comments to:

  document@avaya.com

- Fax, send your comments to:

  1-303-538-1741

Ensure that you mention the name and number of this book, *Avaya G450 CLI Reference*, 03-602056.

Chapter 1: User Levels and Contexts

The G450 Command Line Interface (CLI) consists of commands that are divided into logical contexts. These contexts enable you to view and configure the Avaya G450 Media Gateway more efficiently. A context can be a particular interface of the media gateway, or it can be a specific function with all its related commands.

The contexts you can enter and the commands you can access, depend on the user level from which you log in to the CLI.

For example, you can use all **`show`** commands in User mode. To configure the Avaya G450 Media Gateway, you must be in Supervisor or Privileged mode.

After logging in, type **`tree`** to see a list of all the commands that are accessible at your user level. Type **`help`** to see the list of commands available in the current context.

User levels

The following are the user levels that control access to the various parts of the CLI:

Level	Access	Description
User	read-only	User level is a general access level used to display system parameter values. This level complies with the Read Only restrictions level.
Privileged	read-write	Privileged level is used to access configuration options. This level complies with the Read and Write restrictions level.
Supervisor	admin	Supervisor level is used for highly secured operations, such as adding a new user account, showing the PPP chap secret, and setting the device policy manager source.
Services	admin	Services includes the craft and dadmin logins and other remote services logins. Except for the dadmin login, these accounts are protected with the use of an authentication file and the use of a challenge/response algorithm for generating the appropriate password.

Contexts

The CLI is divided into various contexts from which sets of related commands can be entered. Contexts are nested in a hierarchy, with each context accessible from another context, called the parent context. The top level of the CLI tree is called the root context. Commands that can be executed from any context in the system are listed as having the *general* context.

Interface contexts

Each interface has its own context in the CLI, which you use to manage the interface. The set of commands related to an interface are only accessible from its interface context. For example, in order to configure the Loopback interface, you must first enter the Loopback context. You enter the Loopback context using the interface command with an interface identifier such as **`interface loopback 1`**.

When an interface has only one sub-interface, the commands for the sub-interface are available from the context of the parent interface. This is called unified configuration. When there are multiple sub-interfaces, you must enter the context of a particular sub-interface in order to configure the sub-interface.

For example, when you create a new VLAN interface 1, the sub-interface VLAN 1.0 is also created. In this case, you can execute sub-interface context commands such as **`ip admin-state`** from the parent context. If you add a second sub-interface VLAN 1.1, then you can only execute sub-interface commands from the context of the sub-interface.

If you are in Supervisor or Privileged mode, you can enter any of the following interface contexts:

- Interface Console
- Interface USB-modem
- Interface Dialer
- Interface FastEthernet
- Interface VLAN
- Interface Serial
- Interface Loopback
- Interface Tunnel

Entering an interface

You enter an interface context using the **interface** command, followed by the type of interface, and the interface specification. For the Console and USB interfaces there is no interface specification.

Interface types include:

- FastEthernet
- Serial
- VLAN
- Loopback
- Console
- USB
- Tunnel
- Dialer

An interface is specified with the following syntax:

interface_num[.ip_interface] [if_link_type]

For a complete discussion of the **interface** command syntax, see IP interface configuration on page 498.

Command line prompts

The command line prompt is always prefixed with the hostname of the media gateway. If the media gateway is registered, then the prompt is **hostname-media_gateway_number**. Otherwise, the prompt is **hostname-???**.

The root context prompt reflects the logged-in user level:

- The Supervisor level prompt always ends with **(super)#**
- The Privileged level prompt ends with **#**
- The User level prompt ends with **>**

Note:

For the sake of consistency, this CLI Reference uses the prompt **(super)#** in examples. This does not mean that the command is only available at the Supervisor level.

As you change contexts, the command line prompt changes to reflect the context path. For example, when you enter the **access-control-list** configuration context, the prompt reads **(ACL 330)#**.

To enter a context from another context:

- Enter the name of the context. The prompt changes to indicate the context entered.

To leave a context:

- Enter **exit**. The user returns to the parent context.

Available contexts

The following table describes all the contexts in the CLI. The Context column provides the command to type in order to enter the context. The CLI prompt column is the prompt that you see once you have entered the context.

Table 1: List of CLI Contexts

Context	Description	CLI prompt
(Log in as User)	Root Read Only context	**>**
(Log in as Privileged User)	Root Read Write context	**#**
(Log in as Supervisor)	Root Admin context	**(super)#**
CNA testplug	Configuring a CNA testplug	**(cna-testplug 1)#**
Interface Console	Configuring the Console interface	**(if:Console)#**
Interface USB	Configuring the USB interface	**(if:USB-Modem)#**
Interface Serial	USP, E1/T1	**(if:serial 2/1)#**
Interface Loopback	The loopback virtual interface	**(if:loopback 1.0)#**
Interface VLAN	G450 interfaces to VLANs	**(if:vlan 1)#**
Interface FastEthernet	An Ethernet port connected directly to the router	**(if:fastEthernet 20/1)#**
Interface Tunnel	A GRE Tunnel interface. A GRE tunnel is a virtual point-to-point link between two routers at two ends of an Internet cloud.	**(if:Tunnel 1)#**
Interface DIaler	A Dialer interface	**(if:Dialer 1)#**

1 of 3

Table 1: List of CLI Contexts (continued)

Context	Description	CLI prompt
Banner login	For editing a text message that appears before users login	**(login)#**
Banner post login	For editing a text message that appears after users login	**(post-login)#**
Router OSPF	OSPF routing protocol configuration	**(router:ospf)#**
Router RIP	RIP routing protocol configuration	**(router:rip)#**
ip QoS-list	QoS policy list	**(QoS 401)#**
rule	QoS policy list entry	**(QoS 401/rule 4)#**
composite-operation	QoS policy list match action	**(QoS 401/CompOp 2)#**
dscp-table	QoS policy list DSCP to CoS map	**(QoS 401/dscp 63)#**
ip Access-Control-List	Security Access list	**(ACL 301)#**
ip-rule	Security ACL list entry	**(ACL 301/ip rule 4)#**
composite-operation	Security ACL match action	**(ACL 301/CompOp 2)#**
ip capture-list	Configure a capture list	**(Cap 501)#**
ip capture-list/ip-rule	Configure a capture list rule	**(Cap 501/ip rule 22)#**
ip dhcp pool	Configure a DHCP pool	**(DHCP 5)#**
ip dhcp pool/option	Configure a DHCP option	**(DHCP 5/option 19)#**
ip dhcp pool/vendor-specific-option	Configure a vendor specific DHCP option	**(DHCP 5/vendor specific 1)#**
ip next-hop-list	Configure a next hop list	**(next hop list 1)#**
ip pbr-list	Configure a PBR list	**(PBR 801)#**
ip pbr-list/ip-rule	Configure a PBR list rule	**(PBR 801/ip rule 22)#**
map-class frame-relay	Create a QoS template	**(map-class)#**
rtr	Enter RTR configuration mode	**(rtr icmp 1)#**
track	Configure an object tracker	**(track rtr 1)#**

2 of 3

Table 1: List of CLI Contexts (continued)

Context	Description	CLI prompt
crypto isakmp policy	Create an ISAKMP policy (VPN)	**(config-isakmp:1)#**
crypto ipsec transform-set	Create an IPSec transform set (VPN)	**(transform:ts1)#**
crypto isakmp peer	Create an ISAKMP peer (VPN)	**(peer:149.49.70.1)#**
crypto isakmp peer-group	Create an ISAKMP peer group (VPN)	**(peer-grp:vpn.avaya.com)#**
crypto map	Create a crypto map (VPN)	**(crypto:1)#**
sls	Configure Standard Local Survivability (SLS)	**(sls)**
sls/station	Configure SLS stations	**(sls-station <extension>)**
sls/trunk-group	Configure SLS trunks	**(sls-trunk-group-<tgnum>)**
sls/ds1	Configure SLS DS1 parameters	**(sls-ds1-<port-address>)**
sls/sig-group	Configure SLS signaling-group parameters	**(sls-sig-group <sgnum>)**
sls/bri	Configure SLS BRI parameters	**(sls-bri <slot-address>)**
sls/dial-pattern	Configure SLS dial-pattern parameters	**(sls-dial-pattern <dialed-string>)**
sls/incoming-routing	Configure SLS incoming-routing parameters	**(sls-incoming-routing <tgnum>)**

3 of 3

Chapter 2: Roadmap

This chapter provides quick-reference tables for all the CLI commands, arranged alphabetically by topic, and alphabetically within each topic.

Analog testing - Test and Heal

Table 2: Analog testing CLI commands

Root Level Commands	First level command	Second level command	Description
analog-test			Enter the analog-test context
	cancel		Abort an analog test if it is already running
	clear profile		Clear a test profile
	launch		Launch a specific test
	profile		Enter the analog-test-profile context
		set crosstalk-destination	Set the Local Exchange Carrier number destination of the call from the crosstalk port
		set crosstalk-port	Specify the crosstalk port
		set crosstalk-responder	Specify the responder port for the crosstalk port
		set destination	Set the Local Exchange Carrier number destination of the measurement call
		set port	Specify the port target of the test
		set responder	Specify the responder port
		set responder-type	Specify the responder type

Table 2: Analog testing CLI commands (continued)

Root Level Commands	First level command	Second level command	Description
		set type	Specify what type of test to run
		show (profile)	Display a test profile
		show result (profile)	Display the results of the latest measurement obtained by this test
	set balance		Set the balance on a specific port
	set receive-gain		Set the receive-gain on a specific port
	set transmit-gain		Set the transmit-gain on a specific port
	show correction		Display the balance, receive-gain and transmit-gain corrections applied to each port
	show profile		Display the details of a test profile
	show result		Display the result of the last measurement performed for a particular profile

Announcement files

Table 3: Announcement files CLI commands

Command	Description
copy announcement-file ftp	Upload an announcement file to a remote FTP server
copy announcement-file scp	Upload an announcement file to a remote SCP server
copy announcement-file usb	Upload an announcement file to a USB mass storage device

Table 3: Announcement files CLI commands (continued)

Command	Description
copy ftp announcement-file	Download an announcement file from an FTP server to the G450 announcement directory
copy scp announcement-file	Download an announcement file from a remote SCP server to the G450 announcement directory
copy usb announcement-file	Download an announcement file from a USB mass storage device to the G450 announcement directory
erase announcement-file	Erase an announcement file from the G450 announcement directory
rename announcement-file	Rename an announcement file in the G450 announcement directory
show announcements files	Display the announcements files stored in the G450 announcement directory
show download announcement-file status	Display the status of a download process of announcement files from the remote SCP server
show upload announcement-file status	Display the status of an upload process of announcement files to the remote SCP server

ARP table

Table 4: ARP table CLI commands

Command	Description
arp	Add a permanent entry to the ARP table
arp timeout	Configure the amount of time, in seconds, that an entry remains in the ARP table
clear arp-cache	Delete all dynamic entries from the ARP table and the IP route cache
ip max-arp-entries	Specify the maximum number of ARP table entries allowed in the ARP table

Table 4: ARP table CLI commands (continued)

Command	Description
show ip arp	Display a list of the ARP resolved MAC to IP addresses in the ARP table
show ip reverse-arp	Display the IP address of a host, based on a known MAC address

ASG authentication

Table 5: ASG authentication CLI commands

Command	Description
copy auth-file ftp	Upload the authentication file from the gateway to an FTP server
copy auth-file scp	Upload the authentication file from the gateway to an SCP server
copy auth-file tftp	Upload the authentication file from the gateway to a TFTP server
copy auth-file usb	Upload the authentication file from the gateway to a USB mass storage device
copy ftp auth-file	Download an ASG authentication file from a remote FTP server
copy scp auth-file	Download an ASG authentication file from a remote SCP server
copy tftp auth-file	Download an ASG authentication file from a remote TFTP server
copy usb auth-file	Download an ASG authentication file from a USB mass storage device
erase auth-file	Erase the gateway's ASG authentication file
login authentication lockout	Set a policy for locking out access to the gateway after successive failed login attempts
	1 of 2

Table 5: ASG authentication CLI commands (continued)

Command	Description
login authentication local-craft-password	Enable password authentication of Avaya Services local connections to the Console port with the "craft" login. Use the **no** form to disable password authentication for Avaya Services local connections to the Console port. When password authentication is disabled, ASG authentication is activated.
login authentication response-time	Set the time the gateway waits for user response to authentication requests before timing out a connection
login authentication services-login	Activate all Avaya Services logins, including local login to Console port with "craft" login. Use the **no** form to deactivate all Avaya Services logins.
ppp authentication	Set modem operation mode. Setting the mode to `ras` enables ASG authentication for Avaya Services remote login through a dial-up modem connection.
show auth-file info	Display ASG authentication file information
show download auth-file status	Display download status of ASG authentication file, after using **copy ftp**|**scp**|**tftp auth-file** to download an authentication file to the gateway
show login authentication	Display login authentication settings and information
show upload auth-file status	Display upload status of ASG authentication file, after using **copy auth-file ftp**|**scp**|**tftp** to upload an authentication file from the gateway
username	Add a local user account or remove a user account from the system

Auxiliary files

Table 6: Auxiliary files CLI commands

Command	Description
set web aux-files-url	Specify the URL of the Web server containing the online help files and Java plug-in
show web aux-files-url	Display the URL of the Web server containing online help files and the Java plug-in

Backing up the gateway to a USB device

Table 7: USB backup CLI commands

Command	Description
backup config usb	Back up the gateway configuration to a USB mass storage device
show backup status	Display information regarding the status of a backup of the gateway configuration to a USB mass storage device

Backup interfaces

Table 8: Backup interfaces CLI commands

Root level command	First level command	Description
interface {FastEthernet|loopback|serial|tunnel} see **IP interface configuration**		Enter interface configuration mode for the FastEthernet, Loopback, Serial, or Tunnel interface
	backup delay	Set the time to wait before switching to the backup interface, in case of failure
	backup interface	Set a backup interface for the current interface

Broadcast relay

Table 9: Broadcast relay CLI commands

Root level command	First level command	Description
interface {dialer|FastEthernet|serial|tunnel|VLAN} see **IP interface configuration**		Enter the context of a Dialer, FastEthernet, Serial, Tunnel, or VLAN interface
	ip directed-broadcast	Enable or disable directed broadcast forwarding on the interface
	ip netbios-rebroadcast	Enable or disable NetBIOS rebroadcasts on the interface

CAM table

Table 10: CAM table CLI commands

Command	Description
clear cam	Delete all entries from the Contents Address Memory (CAM) table
show cam	Display the CAM table entries for a specific module and port
show cam mac	Display a specific mac entry in the CAM table

CDR file

Table 11: CDR file CLI commands

Command	Description
copy cdr-file ftp	Upload a Call Detail Recording (CDR) file to a remote server using FTP
copy cdr-file scp	Upload a Call Detail Recording (CDR) file to a remote server using FTP
copy cdr-file tftp	Upload a Call Detail Recording (CDR) file to a remote server using FTP
copy cdr-file usb	Upload a Call Detail Recording (CDR) file from the gateway to the USB mass storage device
show upload cdr-file status	View the status of the upload of a CDR file

CLI sessions

Table 12: CLI sessions commands

Command	Description
exit	Exit the current context. If you are in the root context, the **exit** command logs you out of the system.
reset	Reset a specified system resource
retstatus	Show whether or not the last CLI command you performed was successful
set logout	Set the number of minutes until the system automatically disconnects an idle session
show logout	Display the amount of time in minutes the terminal remains idle before timing out. If the logout value is 0, there is no timeout limit.
tech	Enter tech mode, where additional tech-related commands are available
tree	Display an alphabetical list of commands that are available at your current location in the CLI hierarchy

CNA test plugs

Table 13: CNA test plugs CLI commands

Root level command	First level command	Description
cna testplug		Enter the CNA test plug configuration context
	clear counters (CNA test plugs)	Clear the CNA test plug counters
	control-port	Set or reset the UDP port on which the CNA test plug listens for test requests from schedulers

1 of 2

Table 13: CNA test plugs CLI commands (continued)

Root level command	First level command	Description
	fingerprint	Configure the certificate fingerprint used by the CNA Agent to authenticate the CNA Server
	rtp-echo-port	Set or reset the UDP port used by the CNA test plug to listen for RTP streams sent by other test plugs running RTP tests
	rtp-test-port	Set or reset the UDP port used by the CNA test plug to send an RTP stream to another test plug in an RTP test
	scheduler	Add a scheduler's IP address to the list of schedulers with which the test plug can attempt to register
	shutdown (CNA test plugs)	Disable the CNA test plug
	test-rate-limit	Configure the CNA test rate limiter
cna-testplug-service		Enable or disable the CNA test plug service on the gateway
show cna testplug		Display CNA test plug configuration and statistics

Configuration files

Table 14: Configuration files CLI commands

Command	Description
copy ftp startup-config	Download a G450 configuration file from an FTP server to the Startup Configuration NVRAM
copy running-config ftp	Upload the current G450 configuration to a file on an FTP server
copy running-config scp	Upload the current G450 configuration to a file on a SCP server

Table 14: Configuration files CLI commands (continued)

Command	Description
copy running-config startup-config	Commit the current configuration, including Standard Local Survivability (SLS) data, to NVRAM
copy running-config tftp	Upload the current G450 configuration to a file on a TFTP server
copy scp startup-config	Download a G450 configuration from a SCP server to the Startup Configuration NVRAM
copy startup-config ftp	Upload the current G450 configuration to a file on an FTP server
copy startup-config scp	Upload the current G450 configuration to a file on a SCP server
copy startup-config tftp	Upload the current G450 configuration to a file on a TFTP server
copy startup-config usb	Upload the current G450 configuration to a file on a USB mass storage device
copy tftp startup-config	Download a G450 configuration file from a TFTP server to the Startup Configuration NVRAM
copy usb startup-config	Download a G450 configuration file from a USB mass storage device to the Startup Configuration NVRAM
erase startup-config	Reset the NVRAM parameters to the factory default values. This command is an alias for **nvram initialize**.
nvram initialize	reset the NVRAM parameters to the factory default values. This command is an alias for **erase startup-config**.
show copy status	Display the status of the **copy running-config startup-config** operation
show download status	Display the status of the current G450 configuration file download process, as the file is being loaded into the device
show erase status	Display the status of the **erase startup-config** operation
show running-config	Display the G450's current configuration

2 of 3

Table 14: Configuration files CLI commands (continued)

Command	Description
show startup-config	Display the NVRAM based configuration loaded automatically at startup
show upload status	Display status information regarding the upload of a configuration file for a specific module or for all modules
	3 of 3

Connectivity

Table 15: Connectivity CLI commands

Command	Description
ping	Check host reachability and network connectivity

Contact closure

Table 16: Contact closure CLI commands

Command	Description
set contact-closure admin	Specify how the contact closure relay is controlled
set contact-closure pulse-duration	Set the length of time for the relay to return to normal after the call controller triggers it
show contact-closure	Display the status of one or all contact closure relays

Counters

Table 17: Counters CLI commands

Command	Description
clear counters (interface)	Clear counters for the selected interface or the entire device
clear ip traffic	Clear the IP counters
show ip traffic	Display IP counters information for a given protocol or for all protocols

CSU loopbacks

Table 18: CSU loopbacks CLI commands

Command	Description
show csu loopbacks	View the state of the server SAT-controlled CSU loopbacks on a media module
show csu status	View the status of the CSU on a media module

Date and time setting

Table 19: Date and time setting CLI commands

Command	Description
set date	Set the current date
set time	Set the current time

Default gateway

Table 20: Default gateway CLI commands

Command	Description
ip default-gateway	Define or remove a default gateway (router)

Default settings

Table 21: Default gateway CLI commands

Command	Description
zeroize	Clear all secret parameters and initialize the NVRAM to its factory defaults

Device status

Table 22: Device status commands

Command	Description
clear utilization cpu	Disable CPU utilization measurements
set utilization cpu	Enable CPU utilization measurements
show download	Display the status of the current file copy process to the device
show faults	Display information about currently active faults
show mg list config	Display the current hardware and firmware configurations for the installed media gateway equipment
	1 of 2

Table 22: Device status commands (continued)

Command	Description
show mgc	Display information about the Media Gateway Controller with which the G450 is registered
show mm	Display information about media modules that are installed on the G450
show module	Display brief information about the media modules installed in the G450
show recovery	Display the G450 monitoring and recovery setup
show restart-log	Display information about the last time that the G450 was reset
show system	Display information about the G450
show temp	Display the device temperature
show timeout	Display the amount of time in minutes the terminal remains idle before timing out
show upload	Display the status of the current file copy process from the device
show utilization	Display information about CPU and memory usage on the G450
show voltages	Display power supply voltages
test led	Test the system ALM, MDM and CPU LEDs on the front panel of the G450

2 of 2

DHCP and BOOTP relay

Table 23: DHCP and BOOTP relay CLI commands

Root level command	First level command	Description
interface {FastEthernet | VLAN} see IP interface configuration		Enter configuration mode for the FastEthernet or VLAN interface
	ip bootp-dhcp network	Select the network from which the BOOTP/DHCP server should allocate an address
	ip bootp-dhcp server	Add or remove a BOOTP/DHCP server to handle BOOTP/DHCP requests received by the current interface
ip bootp-dhcp relay		Enable or disable relaying of BOOTP and DHCP requests to the BOOTP/DHCP server

DHCP binding file

Table 24: DHCP binding file CLI commands

Command	Description
copy dhcp-binding ftp	Upload the DHCP bindings file to a remote server using FTP
copy dhcp-binding scp	Upload the DHCP bindings file to a remote server using SCP
copy dhcp-binding tftp	Upload the DHCP bindings file to a remote server using TFTP
copy dhcp-binding usb	Upload the DHCP bindings file to a USB mass storage device
show upload dhcp-binding-file status	Display the upload status of a DHCP binding file

DHCP client

Table 25: DHCP client configuration CLI commands

Root level command	First level command	Description
clear ip dhcp-client statistics		Clear the DHCP client statistics counters
interface fastethernet		Enter interface FastEthernet configuration mode
	clear ip dhcp-client statistics	Clear the DHCP client statistics counters
	ip address dhcp	Enable or disable IP address negotiation via DHCP (applies to WAN FastEthernet interface only)
	ip dhcp client client-id	Set the client-identifier for the DHCP client
	ip dhcp client hostname	Set the client host name for the DHCP client
	ip dhcp client lease	Set the lease requested by the DHCP client
	ip dhcp client request	Specify which DHCP options the DHCP client requests from the DHCP server
	ip dhcp client route track	Apply object tracking in order to monitor the DHCP client's default route
	show ip dhcp-client	Display the configuration of the DHCP client
	show ip dhcp-client statistics	Display the DHCP client statistics counters
release dhcp		Release a DHCP lease for an interface
renew dhcp		Renew a DHCP lease for an interface

1 of 2

Table 25: DHCP client configuration CLI commands (continued)

Root level command	First level command	Description
show ip dhcp-client		Display the configuration of the DHCP client
show ip dhcp-client statistics		Display the DHCP client statistics counters
		2 of 2

DHCP server

Table 26: DHCP server CLI commands

Root level command	First level command	Second level command	Description
clear ip dhcp-server binding			Delete IP address binding
clear ip dhcp server statistics			Clear the statistics of the DHCP server
ip dhcp activate pool			Activate configured DHCP pools
ip dhcp ping packets			Enable the sending of a ping packet by the DHCP server to check if the IP address it is about to allocate is already in use by another client
ip dhcp ping timeout			Set the time the DHCP server waits for a reply to a sent ping packet before allocating an IP address to a DHCP client
ip dhcp pool			Create a DHCP pool
			1 of 3

Table 26: DHCP server CLI commands (continued)

Root level command	First level command	Second level command	Description
	bootfile		Provide startup parameters for the DHCP client device
	client-identifier		Reserve the pool's IP address for assignment to a specific client
	default-router		Set up to eight default router IP addresses in order of preference
	dns-server		Set up to eight Domain Name Server (DNS) IP addresses
	domain-name		Set a domain name string for the client
	end-ip-addr		Set the end IP address of the range of available IP addresses that the DHCP server may assign to clients
	lease		Configure the lease period for IP address assignment
	name		Configure the pool's name
	next-server		Specify the IP address of the next server in the boot process of a DHCP client
	option		Enter the context of a DHCP option
		name	Configure a name for the DHCP option
		value	Enter the option data type and the option data
	Announcement files		Specify the optional server name in the boot process of a DHCP client
	show ip dhcp-pool		Display DHCP pool configurations

Table 26: DHCP server CLI commands (continued)

Root level command	First level command	Second level command	Description
	start-ip-addr		Set the start IP address of the range of available IP addresses that the DHCP server may assign to clients
	subnet-mask		Configure the subnet mask of the pool
	vendor-specific-option		Create a vendor-specific option with a unique index
		class-identifier	Set a vendor-specific identifier
		name	Name the vendor-specific option
		value	Set the data type and value of the vendor-specific option
ip dhcp-server			Activate DHCP server
show ip dhcp-server bindings			Display bindings
show ip dhcp-server statistics			Display DHCP server statistic

Dialer interface

Table 27: Dialer interface CLI commands

Root level command	First level command	Description
interface dialer		Enter the interface Dialer configuration context
	dialer modem-interface	Associate a Dialer with a modem interface
	dialer order	Set which dial strings are used upon a new dial trigger event
	dialer persistent	Force the Dialer to attempt to reconnect every second
	dialer persistent delay	Set the redial interval
	dialer persistent initial delay	Set the minimum delay from boot to persistent dialing
	dialer persistent max-attempts	Set the number of consecutive dial attempts for the dial list
	dialer persistent re-enable	Set the persistent re-enable timer after the maximum number of dial attempts has been reached
	dialer string	Add a phone number to the dial list
	dialer wait-for-ipcp	Set the maximum time the Dialer waits between dialing a number to successfully establishing PPP/IPCP
	ip address negotiated	Enable obtaining an IP address via PPP/IPCP negotiation

Display

Table 28: Banner CLI commands

Command	Description
banner login	Enter the login banner configuration mode
banner post-login	Enter the post-login banner configuration mode
clear screen	Clear the current terminal display
hostname	Change the Command Line Interface (CLI) prompt
line	Add a line to the current banner message
show banner login	Display the banner that appears before the login prompt
show banner post-login	Display the banner that appears after a user logs in successfully
terminal length	Set the length of the terminal display, in characters
terminal width	Set the width of the terminal display, in characters

DNS resolver

Table 29: DNS Resolver configuration commands

Root level command	First level command	Description
clear ip domain statistics		Clear the DNS Resolver's statistics counters
interface {dialer|serial console| FastEthernet| USB-modem} see IP interface configuration		Enter the interface configuration mode for a Dialer, Serial, Console, FastEthernet, or USB-modem interface

1 of 2

Table 29: DNS Resolver configuration commands

Root level command	First level command	Description
	ppp ipcp dns request	Enable or disable requesting DNS information from the remote peer during the PPP/IPCP session
ip domain list		Specify static domain names (suffixes) to complete non-FQDN names (host names that do not end with a dot)
ip domain lookup		Enable or disable the DNS Resolver.
ip domain name-server-list		Enter the context of the DNS servers list, or set up the list
	description (DNS resolver)	Set a name for the DNS servers list.
	name-server	Add a DNS server to the list of up DNS servers
ip domain retry		Set the number of retries for a DNS query
ip domain timeout		Set the timeout for a DNS query
nslookup		Resolve a host name to an IP address
show ip domain		Display the DNS Resolver's configuration
show ip domain statistics		Display the DNS Resolver's statistics counters
show protocol		Display the status of a specific management protocol, or all protocols

2 of 2

Dynamic CAC

Table 30: Dynamic CAC CLI commands

Root level command	First level command	Description
interface {dialer | serial loopback | FastEthernet | tunnel | VLAN} see **IP interface configuration**		Enter the interface configuration mode for a Dialer, Serial, Loopback, FastEthernet, Tunnel, or VLAN interface
	dynamic-cac	Enable the ICMP keepalive mechanism on the current interface
show dynamic-cac		Display information about the most recent dynamic CAC event

Dynamic trap manager

Table 31: Dynamic trap manager CLI commands

Command	Description
clear dynamic-trap-manager	Remove administration of the dynamic trap manager
snmp-server dynamic-trap-manager	Modify the SNMP settings of the dynamic trap manager, or restore the dynamic trap manager to its default settings and remove all notification type filters

E1/T1 interfaces

Table 32: E1/T1 port configuration CLI commands

Root level command	First level command	Description
clear controller counters		Reset the controller counters
controller		Enter configuration mode for a specific controller
	cablelength long (T1)	Set transmit and receive levels for a cable longer than 655 feet
	cablelength short (T1)	Set transmit levels for a cable of length 655 feet or shorter
	channel-group	Create a channel group logical interface for a PPP or Frame Relay session
	clock source	Set the clock source for an E1 or T1 controller
	fdl	Define the type of Facility Data Link loopback that the remote line is requested to enter
	framing	Set the frame type for an E1 or T1 data line
	linecode (E1)	Set the type of line-code transmission for the E1 line
	linecode (T1)	Set the type of line-code transmission for the T1 line
	loopback	Activate or deactivate loopback mode for an E1 or T1 line
	remote	Reset the far end counters on a T1 line
ds-mode		Set the mode of the controller to `e1` or `t1`
interface serial		Enter Serial interface or sub-interface configuration mode
	ip address	Configure the IP address and subnet mask of the interface
show controllers		Display status information about a controller interface

1 of 2

Table 32: E1/T1 port configuration CLI commands (continued)

Root level command	First level command	Description
show controllers remote		Display controller statistics from a peer station
show ds-mode		Display the current mode of the controller
		2 of 2

Echo cancellation configuration

Table 33: Echo cancellation configuration CLI commands

Command	Description
set echo-cancellation analog	Control echo cancellation on analog lines and trunks
set echo-cancellation config analog	Configure echo cancellation on analog lines and trunks
set echo-cancellation config voip	Configure echo cancellation on the VoIP engine
set echo-cancellation voip	Control echo cancellation on the VoIP engine
show echo-cancellation	Display echo cancellation settings and configuration information

Ethernet port configuration

Table 34: Ethernet port configuration CLI commands

Command	Description
set port auto-negotiation-flowcontrol-advertisement	Set the flowcontrol advertisement for the specified Gigabit Ethernet port when performing auto-negotiation
set port duplex	Configure the duplex type (full or half duplex) of an Ethernet or FastEthernet port or range of ports
set port edge admin state	Determine whether the port is an edge port, for the purposes of Rapid Spanning Tree Protocol (RSTP)
set port enable | disable	Enable or disable a port or a range of ports
set port flowcontrol	Set the send/receive mode for flowcontrol frames (IEEE 802.3x or proprietary) for a full duplex port
set port level	Set the default packet priority level for untagged packets
set port name	Configure a name for a port
set port negotiation	Enable or disable auto-negotiation on the port
set port point-to-point admin status	Set the connection type of the port: `force-true`, `force-false`, or `auto`
set port speed	Set the speed of a port or range of ports
show port auto-negotiation-flowcontrol-advertisement	Display the flowcontrol advertisement for a Gigabit port used to perform auto-negotiation
show port edge state	Display the edge state of a port
show port flowcontrol	Display port flow control information

ETR

Table 35: ETR configuration CLI commands

Command	Description
set etr	Enable Emergency Transfer Relay (ETR) mode, or allow the gateway to control ETR mode automatically
show etr	Display the status of Emergency Transfer Relay (ETR) mode

Fans

Table 36: Fans CLI commands

Command	Description
show platform fans	Display information about the fan tray unit

Firmware management

Table 37: Firmware management CLI commands

Command	Description
copy ftp EW_archive	Upgrade the Java applet for Avaya G450 Manager software from an FTP server
copy ftp module	Upgrade the firmware on a media module from an FTP server
copy ftp SW_imageA	Upgrade the G450 firmware into Bank A from an FTP server
copy ftp SW_imageB	Upgrade the G450 firmware into Bank B from an FTP server
	1 of 2

Table 37: Firmware management CLI commands (continued)

Command	Description
copy tftp EW_archive	Upgrade the Java applet for Avaya G450 Manager software from a TFTP server
copy tftp module	Upgrade the firmware on a media module from a TFTP server
copy tftp SW_imageA	Upgrade the G450 firmware into Bank A from a TFTP server
copy tftp SW_imageB	Upgrade the G450 firmware into Bank B from a TFTP server
copy usb EW_archive	Upgrade the Java applet for Avaya G450 Manager software from the USB mass storage device
copy usb module	Upgrade the firmware on a media module from the USB mass storage device
copy usb SW_image	Upgrade the G450 firmware into Bank A or into Bank B, from the USB mass storage device
dir	List all files in the USB mass storage device connected to the G450
set boot bank	Set the default bank from which firmware is loaded during startup
show boot bank	Display the bank from which the G450 is currently set to load its firmware upon startup or reset
show download software status	Display the status of the firmware download process
show image version	Display the software version of the image on both memory banks of the device

2 of 2

Fragmentation

Table 38: Fragmentation CLI commands

Command	Description
clear fragment	Clear the fragment database and restore its default values
fragment chain	Set the maximum number of fragments that can comprise a single IP packet destined to the router
fragment size	Set the maximum number of fragmented IP packets destined to the router which should be reassembled at any given time
fragment timeout	Set the maximum number of seconds allocated for reassembling a fragmented IP packet destined to the router
show fragment	Display information regarding fragmented IP packets that are destined to a router

Frame relay encapsulation

Table 39: Frame relay CLI commands

Root level command	First level command	Description
clear frame-relay counters		Clear the frame relay counters
interface serial		Enter Serial interface or sub-interface configuration mode
	encapsulation	Set the encapsulation mode for a Serial interface
	frame-relay class-dlci	Associate a Virtual Channel with a named QoS or Traffic shaping template (map-class)
	frame-relay interface-dlci	Associate a frame relay Virtual Channel with the current interface

1 of 3

Table 39: Frame relay CLI commands (continued)

Root level command	First level command	Description
	frame-relay lmi-n391dte	Set the number of status enquiry intervals that pass before issuing a full status enquiry message
	frame-relay lmi-n392dte	Set the maximum number of unanswered status enquiries the equipment accepts before declaring the interface down
	frame-relay lmi-n393dte	Set the number of status polling intervals over which the error threshold is counted (the monitored event count)
	frame-relay lmi-type	Manually define the type of the Local Management Interface (LMI) to use
	frame-relay priority-dlci-group	Assign Virtual Channels to priority classifications, for supporting traffic separation
	frame-relay traffic-shaping	Turn on or turn off traffic shaping and frame relay fragmentation
	ip address	Configure an IP address and mask for the interface
map-class frame-relay		Create a QoS template which can later be assigned to DLCIs
	bc out	Configure the committed burst size in bits, for the outbound direction
	be out	Configure the excess burst size in bits, for the outbound direction
	cir out	Configure the Committed Information Rate in bits per second, for the outbound direction
	fragment	Enable FRF.12 fragmentation and configure the fragment size, or disable FRF.12 fragmentation
show frame-relay map		Display a summary table of frame relay sub-interfaces and DLCIs associated with the sub-interfaces
show frame-relay pvc brief		Display information on all PVCs known to the device, in table form

Table 39: Frame relay CLI commands (continued)

Root level command	First level command	Description
show interfaces		Display interface configuration and statistics for a particular interface or all interfaces
show map-class frame-relay		Display the map-class frame relay table
show traffic-shape		Display traffic shaping and Frame Relay Traffic Shaping configuration information
show traffic-shape-queue		Display information about the real-time status of traffic-shaping and Frame Relay Traffic Shaping queues
show traffic-shape-statistics		Display traffic shaping and Frame Relay Traffic Shaping statistics

3 of 3

GRE tunneling

Table 40: GRE tunneling CLI commands

Root level command	First level command	Description
interface tunnel		Enter interface tunnel configuration mode, create an interface tunnel if it does not exist, or delete an interface tunnel or sub-interface
	keepalive (GRE tunnel)	Enable the tunnel keepalive feature
	tunnel checksum	Add a checksum to the GRE header of packets traveling through the tunnel
	tunnel destination	Set the destination address of the tunnel
	tunnel dscp	Assign a DSCP value to packets traveling through the tunnel
	tunnel key	Enable and set an ID key for the tunnel

1 of 2

Table 40: GRE tunneling CLI commands (continued)

Root level command	First level command	Description
	tunnel mode	Specify the encapsulation method of the tunnel. This command is only included for future development, and for conformity with other systems. Currently, the tunnel can only perform GRE encapsulation.
	tunnel path-mtu-discovery	Enable dynamic MTU discovery by the tunnel
	tunnel source	Set the source address of the tunnel
	tunnel ttl	Assign a TTL value to packets traveling through the tunnel
show interfaces		Show interface configuration and statistics for a particular tunnel or all GRE tunnels

HTTP server

Table 41: HTTP server CLI commands

Command	Description
ip http	Enable or disable the HTTP server

ICC configuration

Table 42: ICC configuration CLI commands

Root level command	First level command	Description
interface vlan		Create a VLAN interface, enter interface VLAN configuration mode, or delete a VLAN interface
	icc-vlan	Set the current VLAN as the ICC-VLAN
show icc-vlan		Display the current ICC VLAN

ICMP errors

Table 43: ICMP errors CLI commands

Command	Description
ip icmp-errors	Set ICMP error messages to ON or OFF
show ip icmp	Display the status (enabled or disabled) of ICMP error messages

ICMP keepalive

Table 44: ICMP keepalive CLI commands

Root level command	First level command	Description
interface fastethernet		Enter the configuration context for the FastEthernet interface
	keepalive-icmp	Enable the ICMP keepalive mechanism on an interface
	keepalive-icmp failure-retries	Set the number of consecutive failed keepalive packets necessary to set the interface's keepalive status as down
	keepalive-icmp interval	Set the interval (in seconds) between keepalive packets
	keepalive-icmp source-address	Set the source IP address of the keepalive packets
	keepalive-icmp success-retries	Set the number of consecutive successful keepalive packets necessary to set the interface's keepalive status as up
	keepalive-icmp timeout	Set the timeout (in seconds) for receiving the keepalive response
	show keepalive-icmp	Display information about the extended keepalive settings

IP interface configuration

Table 45: IP interface configuration CLI commands

Root level command	First level command	Description
interface console		Enter the Console interface configuration mode, create the interface if it does not exist, or delete the Console interface
interface dialer		Enter the interface Dialer context, create the Dialer interface if it does not exist, or delete the Dialer interface
interface fastethernet		Enter interface FastEthernet configuration mode, create a FastEthernet interface if it does not exist, or delete a FastEthernet interface
interface loopback		Enter interface Loopback configuration mode, create a Loopback interface if it does not exist, or delete a Loopback interface or sub-interface
interface serial		Enter Serial interface or sub-interface configuration mode, create a Serial interface if it does not exist, or delete a Serial interface or sub-interface
interface tunnel		Enter interface tunnel configuration mode, create an interface tunnel if it does not exist, or delete an interface tunnel or sub-interface
interface USB-modem		Enter the configuration context for the USB-modem interface, or reset the USB-modem interface settings to their factory defaults
interface vlan		Enter interface VLAN configuration mode, create a VLAN interface if it does not exist, or delete a VLAN interface
interface {console|dialer|FastEthernet|loopback|serial|tunnel|USB-modem|VLAN} see IP interface configuration		Enter interface configuration mode for the Console, Dialer, FastEthernet, Loopback, Serial, Tunnel, USB-modem, or VLAN interface

Table 45: IP interface configuration CLI commands (continued)

Root level command	First level command	Description
	description (interface)	Configure a description for the current interface
	ip address	Assign an IP address and mask to an interface or delete an interface
	ip admin-state	Set the administrative state of an IP interface
	ip broadcast-address	Update the interface broadcast address
	load-interval	Set the load calculation interval for an interface
show ip interface		Display information about an IP interface
show ip interface brief		Display a summary of the information for a specific interface or for all the interfaces
shutdown (interface)		Set the administrative status of the current interface to down, or restore the administrative status of the interface to up

IP phone upgrades

Table 46: IP phone upgrades CLI commands

Command	Description
clear ip tftp-server statistics	Clear TFTP server statistics
copy ftp phone-image	Download a file from a remote FTP server to phone image bank A, B, C, or D in the local G450 TFTP directory
copy ftp phone-script	Download a file from a remote FTP server to phone script bank A or B on the local G450 TFTP directory
copy phone-script ftp	Upload a phone script file from the local G450 TFTP directory to a remote server, using FTP

Table 46: IP phone upgrades CLI commands (continued)

Command	Description
copy phone-script scp	Upload a phone script file from the local G450 TFTP directory to a remote server, using SCP
copy phone-script tftp	Upload a phone script file from the local G450 TFTP directory to a remote server, using TFTP
copy phone-script usb	Upload a phone script file from the local G450 TFTP directory to the USB mass storage device
copy scp phone-script	Download a file from a remote SCP server to phone script bank A or B in the local G450 TFTP directory
copy tftp phone-image	Download a file from a remote TFTP server to phone image bank A, B, C, or D in the local G450 TFTP directory
copy tftp phone-script	Download a file from a remote TFTP server to phone script bank A or B in the local G450 TFTP directory
copy usb phone-image	Download a file from the external USB mass storage device to phone image bank A, B, C, or D in the local gateway TFTP directory
copy usb phone-script	Download a phone script file from the external USB mass storage device to phone script bank A or B on the local gateway's TFTP directory
erase phone-image	Delete phone-image A, B, C, D, E, or F
erase phone-script	Delete phone-script A, B, C, or D
ip tftp-server file-system size	Set the TFTP file system size
show application-memory	Display the configured and allocated application memory
show download phone-image-file status	Display the status of the download of a phone-image file
show download phone-script-file status	Display the status of a download of a phone-script file
show ip tftp-server files	Display the phone image and script files
show ip tftp-server statistics	Display TFTP server error counters
show upload phone-script-file status	Display the uploaded phone-script file

IP unnumbered

Table 47: IP unnumbered CLI commands

Command	Description
ip unnumbered	Configure an interface to borrow an IP address from another interface, or delete an unnumbered IP configuration on the interface

IPHC header compression

Table 48: IPHC configuration CLI commands

Root level command	First level command	Description
clear ip rtp header-compression		Clear IP RTP header compression statistics for all enabled interfaces or for a specific interface
clear ip tcp header-compression		Clear TCP header compression statistics for all enabled interfaces or for a specific interface
interface {dialer|serial} see IP interface configuration		Enter the context of the Dialer or Serial interface
	ip rtp compression-connections	Control the number of Real-Time Transport Protocol (RTP) connections supported on the current interface
	ip rtp header-compression	Enable both RTP and TCP header compression on the current interface
	ip rtp max-period	Set the maximum number of compressed headers that can be sent between full headers
	ip rtp max-time	Set the maximum number of seconds between full headers

1 of 2

Table 48: IPHC configuration CLI commands (continued)

Root level command	First level command	Description
	ip rtp non-tcp-mode	Set the type of IP header compression: ietf or non-ietf
	ip rtp port-range	Set the range of UDP ports considered as RTP on the current interface
	ip tcp compression-connections	Set the total number of TCP header compression connections supported on the current interface
show ip rtp header-compression		Display header compression statistics for a specific interface
show ip rtp header-compression brief		Display a subset of header compression statistics in the form of a table
show ip tcp header-compression		Display TCP header compression statistics for a specific interface
show ip tcp header-compression brief		Display a subset of TCP header compression statistics in the form of a table

2 of 2

License file of CM

Table 49: License file of CM, CLI commands

Command	Description
ip license-server	Enable the gateway to supply a hardware serial number on behalf of an S8500 local survivable processor (LSP)

License file of gateway

Table 50: License file of gateway, CLI commands

Command	Description
copy ftp license-file	Download a VPN license from an FTP server to the gateway
copy license-file ftp	Upload the license file from the gateway to a remote server using FTP
copy license-file scp	Upload the license file from the gateway to a remote server using SCP
copy license-file tftp	Upload the license file from the gateway to a remote server using TFTP
copy license-file usb	Upload the license file from the gateway to a USB mass storage device
copy scp license-file	Download a VPN license from an SCP server to the gateway
copy tftp license-file	Download a VPN license from a TFTP server to the gateway
copy usb license-file	Download a VPN license from a USB mass storage device to the gateway
show download license-file status	Display the status of the download process of the VPN license to the gateway
show license status	Display the status of the VPN license file
show upload license-file status	Display the status of the upload operation of a VPN license file

Link status

Table 51: Link status CLI commands

Command	Description
show isdn bri link	View the status of all BRI links on a media module
show isdn link summary	View a summary of all ISDN links
show isdn pri link	View the status of all PRI links on a media module

LLDP

Table 52: LLDP configuration CLI commands

Command	Description
set lldp re-init-delay	Set the delay from when an LLDP is disabled on a port until re-initialization is attempted
set lldp system-control	Enable or disable the LLDP application globally per device or stack
set lldp tx-delay	Set the minimal delay in seconds between successive LLDP frame transmissions, on each port
set lldp tx-hold-multiplier	Set the multiplier on the interval that determines the actual TTL value sent in an LLDP frame
set lldp tx-interval	Set the interval at which the device transmits LLDP frames
set port lldp	Change the administrative LLDP status of a port
set port lldp tlv	Enable or disable the transmission of the optional TLVs on a per port basis
show lldp	Display the LLDP information received on each port
show lldp config	Display the global LLDP configuration

1 of 2

Table 52: LLDP configuration CLI commands

Command	Description
show port lldp config	Display port-level LLDP configuration
show port lldp vlan-name config	Show the VLANs that are being transmitted on a specific port
	2 of 2

Logging

Table 53: Logging CLI commands

Command	Description
clear logging file	Delete the message log file being stored in non-volatile memory (NVRAM), including the history log, and open a new, empty log file
clear logging server	Delete the specified Syslog message server from the Syslog server table
set logging file	Manage the logging of system messages to non-volatile memory (NVRAM)
set logging server	Define a new Syslog output server for remote logging of system messages
set logging server access-level	Set the access level associated with a Syslog server sink
set logging server condition	Set a filter for messages sent to the specified Syslog server. Messages can be filtered by source system, severity, or both.
set logging server enable | disable	Enable or disable a specific Syslog server
set logging server facility	Define an output facility for the specified Syslog server
set logging session	Manage message logging for the current Console session
show dev log file	Display the encrypted device's log file
show logging file condition	Display all conditions that have been defined for the file output sink
	1 of 2

Table 53: Logging CLI commands (continued)

Command	Description
show logging file content	Output the messages in the log file to the CLI Console
show logging server condition	Display the filter conditions defined for the Syslog output sink
show logging session condition	Display the filter conditions defined for message logging to the current Console session
	2 of 2

Master key configuration

Table 54: Master configuration key CLI commands

Command	Description
key config-key password-encryption	Set the default Master Configuration Key of the gateway

MGC (Media Gateway Controller) configuration

Table 55: MGC list CLI commands

Command	Description
clear mgc list	Remove one or more MGCs from the MGC list
session	Open a telnet connection to the MGC
set icc-monitoring	Enable or disable heartbeat monitoring of an MGC in ICC or LSP mode
set mediaserver	Set the MGC management address and ports
set mgc list	Create a list of valid Media Gateway Controller(s)
	1 of 2

Table 55: MGC list CLI commands (continued)

Command	Description
set reset-times	Set the time-out for the G450's search for the primary MGC, or search for the other MGC's on the MGC list, or configure the point at which the primary MGCs in the list end and the LSPs begin
show icc-monitoring	Display the status of the ICC/LSP monitoring process
show mediaserver	Display MGC configuration information
show mgc	Display the state and setup parameters of the currently active MGC
show mgc list	Display the IP addresses of the MGCs on the MGC list
show recovery	Show the media gateway monitoring and recovery setup

2 of 2

Modem configuration – Console port

Table 56: Console port configuration for modem use, CLI commands

Root level command	First level command	Description
interface console		Enter configuration context for the Console interface
	async mode interactive	Enter modem mode every time the proprietary modem cable is plugged into the Console port
	async mode terminal	Disable interactive mode on the Console
	async modem-init-string	Change the default modem initialization string
	async reset-modem (Console port)	Reset the connected modem
	ip address	Assign an IP address and mask to an interface

1 of 2

Table 56: Console port configuration for modem use, CLI commands (continued)

Root level command	First level command	Description
	ip peer address	Change the IP address offered to a requesting calling host during PPP/IPCP connection establishment
	ppp authentication	Configure the authentication method used when starting a client session on the PPP server
	ppp chap-secret	Configure the shared secret used in PPP sessions with CHAP authentication
	ppp timeout authentication	Set the maximum time to wait for an authentication response
	show ppp authentication	Display PPP authentication status
	shutdown (interface)	Disconnect an active PPP session and shut down the modem
	speed (PPP)	Set the PPP baud rate to be used by asynchronous PPP ports
	timeout absolute	Set the number of minutes until the system automatically disconnects an idle PPP incoming session

Modem configuration – USB modem port

Table 57: USB port configuration for modem use, CLI commands

Root level command	First level command	Description
interface usb-modem		Enter configuration context for the USB-modem interface
	async modem-init-string	Change the default modem initialization string
	async reset-modem (USB port)	Reset the connected modem

Table 57: USB port configuration for modem use, CLI commands (continued)

Root level command	First level command	Description
	ip address	Assign an IP address and mask to an interface
	ip peer address	Change the IP address offered to a requesting calling host during PPP/IPCP connection establishment
	ppp authentication	Configure the authentication method used when starting a client session on the PPP server
	ppp chap-secret	Configure the shared secret used in PPP sessions with CHAP authentication
	ppp timeout authentication	Set the maximum time to wait for an authentication response
	show ppp authentication	Display PPP authentication status
	shutdown (USB modem)	Disconnect an active PPP session and shut down the modem
	timeout absolute	Set the number of minutes until the system automatically disconnects an idle PPP incoming session

2 of 2

MSS notifications 526

Table 58: MSS notifications CLI commands

Command	Description
DoS-classification	Set a label for a user-defined DoS attack classification to be reported in MSS notifications
icmp in-echo-limit	Set the maximum number of echo requests that can be received in one second

1 of 2

Table 58: MSS notifications CLI commands (continued)

Command	Description
set mss-notification rate	Set the rate at which the gateway sends Managed Security Services (MSS) notifications
show mss-notification rate	Show the interval time, in seconds, between MSS notifications
	2 of 2

Object tracking

Table 59: Object tracking CLI commands

Root level command	First level command	Second level command	Description
rtr			Enter Respond Time Reports (RTR) configuration mode. RTRs are the basic building blocks of object tracking.
	type		Set the type of operation an RTR should employ in its probes, and specify the address of the remote device being probed
		dscp (object tracking)	Set the DSCP value for the packets of the RTR probes
		fail-retries	Set how many consecutive unanswered probes change the status of an RTR operation device from up to down
		frequency	Set the frequency of the RTR probes
		interface-keepalive bypass-logic	Provide support for an alternative internal path for RTR probes, in cases where next-hop is configured for the RTR probes
			1 of 2

Table 59: Object tracking CLI commands (continued)

Root level command	First level command	Second level command	Description
		next-hop (object tracking)	Specify the next hop for the RTR probes, bypassing normal routing
		source-address	Set the source IP address for RTR operations
		success-retries	Set how many consecutive answered probes change the status of an RTR operation device from down to up
		wait-interval	Set how long to wait for a device to answer an RTR probe
rtr-schedule			Activate or stop an RTR operation
show rtr configuration			Display RTR configuration values
show rtr operational-state			Display the global operational status of the RTR feature
show track			Display tracking information
track			Configure an object tracker
	description (object tracking)		Set a description for the object tracker
	object		Add an object tracker to a track list
	threshold count		Set the upper and lower thresholds in the track list command

OSPF

Table 60: OSPF CLI commands

Root level command	First level command	Description
interface {dialer|FastEthernet |loopback|serial| tunnel|VLAN} see **IP interface configuration**		Enter the context of a Dialer, FastEthernet, Loopback, Serial, Tunnel, or VLAN interface
	bandwidth	Set the bandwidth parameter manually for this interface
	ip ospf authentication	Specify the authentication type for an interface
	ip ospf authentication-key	Configure the interface authentication password
	ip ospf cost	Configure the cost of an OSPF interface, for the purpose of determining the shortest path
	ip ospf dead-interval	Configure the interval before declaring the neighbor as dead
	ip ospf hello-interval	Specify the time interval between hello packets sent by the router
	ip ospf message-digest-key	Specify the message-digest key for the interface and enable OSPF MD5 authentication
	ip ospf network point-to-multipoint	Specify the network type for the interface
	ip ospf priority	Configure interface priority used in DR election
ip ospf router-id		Configure the router ID
router ospf		Enable OSPF protocol on the system and to enter the router configuration context
	area	Configure the OSPF area ID of the router
	default-metric (OSPF)	Set the interface OSPF route metric value

1 of 2

Table 60: OSPF CLI commands (continued)

Root level command	First level command	Description
	network (OSPF)	Enable OSPF in a network
	passive-interface	Suppress OSPF routing updates on an interface
	redistribute (OSPF)	Redistribute routing information from other protocols into OSPF
	timers spf	Configure the delay between runs of OSPF's (SPF) calculation
show ip ospf		Display general information about OSPF routing
show ip ospf database		Display lists of information related to the OSPF database for a specific router
show ip ospf interface		Display the OSPF-related interface information
show ip ospf neighbor		Display OSPF neighbor information on a per-interface basis
show ip protocols		Display parameters and statistics of a given IP routing protocol

2 of 2

Packet sniffing

Table 61: Packet sniffing CLI commands

Root level command	First level command	Second level command	Description
capture buffer-mode			Set the capture buffer to cyclic mode
capture buffer-size			Change the size of the capture file
capture filter-group			Activate a capture list

1 of 4

Table 61: Packet sniffing CLI commands (continued)

Root level command	First level command	Second level command	Description
capture interface			Specify a capture interface (by default, the service captures from all interfaces simultaneously)
capture ipsec			Set whether to capture IPSec VPN packets, handled by the internal VPN process, decrypted (plaintext) or encrypted (cyphertext)
capture max-frame-size			Set the maximum octets that are captured from each frame
capture start			Start capturing packets
capture stop			Stop capturing packets
capture-service			Enable or disable the capture service
clear capture-buffer			Clear the capture buffer (useful in case it holds sensitive information)
copy capture-file ftp			Upload the packet sniffing buffer to a file on a remote FTP server
copy capture-file scp			Upload the packet sniffing buffer to a file on a remote SCP server
copy capture-file tftp			Upload the packet sniffing buffer to a file on a remote TFTP server
copy capture-file usb			Upload the capture file to a USB mass storage device
ip capture-list			Enter the capture list configuration context, create a capture list, or delete a capture list

Table 61: Packet sniffing CLI commands (continued)

Root level command	First level command	Second level command	Description
	cookie		Set a number to identify a list (used by the rule-manager application)
	ip-rule (policy, policy-based routing, packet sniffing)		Enter an ip-rule context or erase an ip-rule
		composite-operation	Create or edit a composite operation
		destination-ip	Define an equation on the destination IP
		dscp (policy-based routing, packet sniffing, VPN)	Specify the DSCP value to be set by the current IP rule
		fragment	Apply the current rule to non-initial fragments only
		icmp	Set the IP protocol to ICMP and an equation on the types of ICMP messages
		ip-protocol	Set the IP protocol
		show ip-rule	Display the attributes of a specific rule
		source-ip	Set the current rule to apply to packets from the specified source IP address
		tcp destination-port	Set the IP protocol to TCP and an equation on the destination port
		tcp source-port	Set the IP protocol to TCP and an equation on the source port
		udp destination-port	Set the IP protocol to UDP and an equation on the destination port

Table 61: Packet sniffing CLI commands (continued)

Root level command	First level command	Second level command	Description
		udp source-port	Set the IP protocol to UDP and an equation on the source port
	name		Name a capture list
	owner		Set the name of the person or application that has created the list
show capture			Show the sniffer status
show capture-buffer hex			Show a hex-dump of the captured frames
show ip capture-list			Show capture list(s)
			4 of 4

Platform information

Table 62: Platform configuration CLI commands

Command	Description
show platform fans	Display information on the fan tray unit
show platform power	Display the power supply configuration and parameters
show platform mainboard	Display the supervisor board parameters and the list of media gateway equipment installed in the sockets on the supervisor board.

PMI

Table 63: PMI configuration CLI commands

Root level command	First level command	Description
interface {FastEthernet | serial | tunnel | VLAN | loopback | dialer} see **IP interface configuration**		Enter configuration mode for the FastEthernet, Serial, Tunnel, VLAN, Loopback, or Dialer interface
	pmi	Set the current interface as the Primary Management Interface for the system
show pmi		Display the current Primary Management Interface

Policy - access control lists

Table 64: Access control list CLI commands

Root level command	First level command	Second level command	Description
interface {dialer | serial | loopback | FastEthernet | tunnel | VLAN} see **IP interface configuration**			Enter the interface configuration mode for a Dialer, Serial, Loopback, FastEthernet, Tunnel, or VLAN interface
	ip access-group		Activate a specific Access Control list, for a specific direction, on the current interface

Table 64: Access control list CLI commands (continued)

Root level command	First level command	Second level command	Description
	ip simulate		Test the action of a policy on a simulated packet
	show ip access-control-list		Display the attributes of a specific access control list or of all access control lists on the current interface
ip access-control-list			Enter configuration mode for the specified policy access control list, and create the list if it does not exist
	cookie		Set the cookie for the current list
	ip-fragments-in		Specify the action taken on incoming IP fragmentation packets for the current access control list
	ip-option-in		Drop incoming packets that contain IP options

Table 64: Access control list CLI commands (continued)

Root level command	First level command	Second level command	Description
	ip-rule (policy, policy-based routing, packet sniffing)		Enter configuration mode for a specified policy rule or, if the rule does not exist, create it and enter its configuration mode
		composite-operation	Assign the specified composite operation to the current rule
		destination-ip	Apply the current rule to packets with the specified destination IP address
		dscp (policy)	Apply the current rule to packets with the specified DSCP value
		fragment	Apply the current rule for non-initial fragments only
		icmp	Apply the current rule to a specific type of ICMP packet
		ip-protocol	Apply the current rule to packets with the specified IP protocol

Table 64: Access control list CLI commands (continued)

Root level command	First level command	Second level command	Description
		show composite-operation	Display the parameters of the composite operation assigned to the current rule
		show ip-rule	Display the attributes of the current rule
		source-ip	Apply the current rule to packets from the specified source IP address
		tcp destination-port	Apply the current rule to TCP packets with the specified destination port
		tcp established	Apply the current rule only to packets that are part of an established TCP session
		tcp source-port	Apply the current rule to TCP packets from ports with specified source port
		udp destination-port	Apply the rule to UDP packets with the specified destination port
		udp source-port	Apply the rule to UDP packets from the specified source port

Table 64: Access control list CLI commands (continued)

Root level command	First level command	Second level command	Description
	name		Assign a name to the current list
	owner		Specify the owner of the current list
	show composite-operation		Display the composite operations configured for the list
	show ip-rule		Display the rules configured for the current list attributes of a specific rule
	show list		Display the attributes of the current list, including its rules
ip policy-list-copy			Copy an existing policy list to a new list
show ip access-control-list			Display the attributes of a specific access control list or of all access control lists
			5 of 5

Policy - QoS lists

Table 65: QoS list CLI commands

Root level command	First level command	Second level command	Description
interface {dialer|serial|loopback|FastEthernet|tunnel|VLAN} see **IP interface configuration**			Enter the interface configuration mode for a Dialer, Serial, Loopback, FastEthernet, Tunnel, or VLAN interface
	ip qos-group		Activate a specific QoS list, for a specific direction, on the current interface
	ip simulate		Test the action of a policy on a simulated packet
	show ip qos-list		Display the attributes of a specific QoS list or all QoS lists for the current interface
ip policy-list-copy			Copy an existing policy list to a new list
ip qos-list			Enter configuration mode for the specified QoS list, and create the list if it does not exist

Table 65: QoS list CLI commands (continued)

Root level command	First level command	Second level command	Description
	composite-operation		Enter the configuration mode for one of the current list's composite operations
		cos	Set the CoS priority value for the current composite operation
		dscp (policy)	Set the DSCP value for the current composite operation
		name	Assign a name to the current composite operation
		show composite-operation	Display the attributes of the current composite operation
	cookie		Set the cookie for the current list
	dscp-table		Enter the DSCP table entry context for a particular DSCP value for the current QoS list
		composite-operation	Specify the composite operation to execute for packets with the specified DSCP value

Table 65: QoS list CLI commands (continued)

Root level command	First level command	Second level command	Description
		name	Assign a name to the current DSCP table entry
		show dscp-table	Display the parameters of the current DSCP table entry
	ip-rule (policy, policy-based routing, packet sniffing)		Enter configuration mode for a specified policy rule or, if the rule does not exist, create it and enter its configuration mode
		composite-operation	Assign the specified composite operation to the current rule
		destination-ip	Apply the current rule to packets with the specified destination IP address
		dscp (policy)	Apply the current rule to packets with the specified DSCP value
		fragment	Apply the current rule for non-initial fragments only

Table 65: QoS list CLI commands (continued)

Root level command	First level command	Second level command	Description
		icmp	Apply the current rule to a specific type of ICMP packet
		ip-protocol	Apply the current rule to packets with the specified IP protocol
		show composite-operation	Display the parameters of the composite operation assigned to the current rule
		show dscp-table	Display the current list's DSCP table
		show ip-rule	Display the attributes of the current rule
		source-ip	Apply the current rule to packets from the specified source IP address
		tcp destination-port	Apply the current rule to TCP packets with the specified destination port
		tcp source-port	Apply the current rule to TCP packets from ports with specified source port

4 of 6

Table 65: QoS list CLI commands (continued)

Root level command	First level command	Second level command	Description
		udp destination-port	Apply the rule to UDP packets with the specified destination port
		udp source-port	Apply the rule to UDP packets from the specified source port
	name		Assign a name to the current list
	owner		Specify the owner of the current list
	pre-classification		Specify which priority tag the current QoS list uses for data flows
	show composite-operation		Display all composite operations configured for the list
	show dscp-table		Display the current list's DSCP table
	show ip-rule		Display the rules configured for the current list attributes of a specific rule

Table 65: QoS list CLI commands (continued)

Root level command	First level command	Second level command	Description
	show list		Display the attributes of the current list, including its rules
show ip qos-list			Display the attributes of a specific QoS list or all QoS lists
			6 of 6

Policy-based routing

Table 66: Policy-based routing CLI commands

Root level command	First level command	Second level command	Description
interface {dialer|serial|loopback|FastEthernet|tunnel|VLAN} see IP interface configuration			Enter the interface configuration mode for a Dialer, Serial, Loopback, FastEthernet, Tunnel, or VLAN interface
	ip pbr-group		Apply the specified PBR list to the current interface. The PBR list is applied to ingress packets only.
ip next-hop-list			Enter the context of the specified next hop list. If the list does not exist, it is created.
	next-hop-interface		Add the specified interface to the next hop path for this next-hop list
			1 of 3

Table 66: Policy-based routing CLI commands (continued)

Root level command	First level command	Second level command	Description
	next-hop-ip		Add the specified ip address to the next hop path for this next-hop list
	show next-hop		Display the next-hop entries in the current list
ip pbr-list			Enter the context of the specified PBR list. If the list does not exist, it is created.
	cookie		Set the cookie for the current list
	ip-rule (policy, policy-based routing, packet sniffing)		Enter configuration mode for the specified rule. If the specified rule does not exist, the system creates it and enters its configuration mode.
		destination-ip	Specify the destination IP address of packets to which the current rule applies
		dscp (policy-based routing, packet sniffing, VPN)	Specify the DSCP value that is set by the current policy operation
		fragment	Apply the current rule for non-initial fragments only
		icmp	Apply the current rule to a specific type of ICMP packet
		ip-protocol	Apply the current rule to packets with the specified IP protocol
		next-hop (policy-based routing)	Specify the next-hop policy to use when the current rule is applied

Table 66: Policy-based routing CLI commands (continued)

Root level command	First level command	Second level command	Description
		show ip next-hop-list	Display the details of the next-hop list or of all next-hop lists
		show ip-rule	Display the attributes of a specific rule or all rules
		source-ip	Apply the current rule to packets from the specified source IP address
		tcp destination-port	Apply the current rule to TCP packets with the specified destination port
		tcp source-port	Apply the current rule to TCP packets from ports with specified source port
		udp destination-port	Apply the rule to UDP packets with the specified destination port
		udp source-port	Apply the rule to UDP packets from the specified source port
	name		Assign a name to the specified list or operation
	owner		Specify the owner of the current list
	show ip-rule		Display the attributes of a specific rule or all rules
	show list		Display information about the specified list
show ip active-lists			Display information about a specific policy list or all lists
show ip active-pbr-lists			Display details about a specific PBR list or all PBR lists
show ip pbr-list			Display information about the specified PBR list

3 of 3

Port classification

Table 67: Port classification CLI commands

Command	Description
set port classification	Set the port classification to either regular or valuable (any change in the spanning tree state from forwarding for a valuable port will erase all learned MAC addresses in the switch)
show port classification	Display port classification for a specified port or all ports

Port mirroring

Table 68: Port mirroring CLI commands

Command	Description
clear port mirror	Delete a port mirroring pair
set port mirror	Define a port mirroring source-destination pair
show port mirror	Display mirroring information for a specified port or for all ports

Port redundancy

Table 69: Port redundancy CLI commands

Command	Description
set port redundancy enable|disable	Globally enable or disable port redundancy pairs defined on the media gateway
set port redundancy	Define or remove redundancy pairs

Table 69: Port redundancy CLI commands (continued)

Command	Description
set port redundancy-intervals	Configure the two time constants that determine redundancy switchover parameters
show port redundancy	Display information about software port redundancy pairs defined on the media gateway

Port status

Table 70: Port status CLI commands

Command	Description
show port	Display port status on I/O modules. If no port is specified, information for all ports is displayed.

PPP encapsulation

Table 71: PPP encapsulation CLI commands

Root level command	First level command	Description
interface serial		Enter Serial interface or sub-interface configuration mode
	encapsulation	Set the encapsulation mode for a Serial interface: PPP or frame-relay
	ip address	Configure the IP address and subnet mask of the interface
	keepalive (PPP)	Enable PPP keepalive, in order to maintain a persistent connection
	ppp timeout ncp	Set the maximum time, in seconds, that PPP allows for negotiation of a network layer protocol

1 of 2

Table 71: PPP encapsulation CLI commands (continued)

Root level command	First level command	Description
	ppp timeout retry	Set the maximum time to wait for a response during PPP negotiation
show interfaces		Display interface configuration and statistics for a particular interface or all interfaces
		2 of 2

PPPoE (PPP over Ethernet)

Table 72: PPPoE CLI commands

Root level command	First level command	Description
interface fastethernet		Enter the context of the FastEthernet interface
	encapsulation pppoe	Change the encapsulation to PPPoE
	ip address	Configure an IP address and subnet mask for the interface
	ip address negotiated	Obtain an IP address via PPP/IPCP negotiation
	keepalive-track	Bind interface status to an object tracker to check whether the interface is up
	mtu	Set the interface's MTU to 1492 which ensures that overall packet size for the PPPoE interface does not exceed 1500, which is the MTU for Ethernet
	ppp chap hostname	Override the device hostname for PPP CHAP authentication
	ppp chap password	Set the CHAP password for authentication with a remote peer
	ppp chap refuse	Prevent the device from authenticating with CHAP after the device is requested by the remote peer
		1 of 2

Table 72: PPPoE CLI commands (continued)

Root level command	First level command	Description
	ppp ipcp dns request	Request the list of available DNS servers from the remote peer during the PPP/IPCP session
	ppp pap refuse	Prevent the device from authenticating with PAP after the device is requested by the remote peer
	ppp pap sent-username	Set the Password Authentication Protocol (PAP) password for authentication with the remote peer
	pppoe-client persistent delay	Set the interval between PPPoE client dial attempts
	pppoe-client persistent max-attempts	Limit the number of consecutive connection establishment retries
	pppoe-client service-name	Set the PPPoE client service-name
	pppoe-client wait-for-ipcp	Set the amount of time (in seconds) between establishment of the PPPoE tunnel and establishment of the IPCP tunnel. If this time is exceeded, the PPPoE client terminates the PPPoE tunnel.
	shutdown (interface)	Shut down the port, and the PPPoE client, if configured

2 of 2

Priority queueing

Table 73: Priority queueing CLI commands

Root level command	First level command	Description
interface {serial | FastEthernet | dialer} see **IP interface configuration**		Enter interface configuration mode for either a Serial, FastEthernet, or Dialer interface
	priority-queue	Enable or disable priority queuing mode in a Serial or FastEthernet interface. If you disable priority queuing, WFVQ is re-enabled.
	queue-limit	Set the size of any of the four priority queues, in packets, for a given interface or interface type
	voip-queue	Enable or disable custom queueing for VoIP traffic. If you disable custom queueing, WFVQ is re-enabled.
	voip-queue-delay	Set the maximum query delay for which to estimate the high priority queue size necessary to meet the queuing delay
show queueing		Display the priority queue configuration

Proxy ARP

Table 74: Proxy ARP CLI commands

Root level command	First level command	Description
interface {FastEthernet | VLAN} see **IP interface configuration**		Enter the context of a FastEthernet or VLAN interface
	ip proxy-arp	Enable proxy ARP on a G450 interface

QoS

Table 75: QoS configuration CLI commands

Command	Description
set qos bearer	Permit the setting of VoIP QoS-bearer related parameters for the Media Gateway Processor and VoIP engines
set qos control	Define the source for QoS control parameters: `local` or `remote`
set qos signal	Set QoS signaling parameters (DSCP or 802.1Q) for the Media Gateway Processor
show qos-rtcp	Display QoS, RSVP, and RTCP parameters

RADIUS authentication

Table 76: RADIUS authentication configuration commands

Command	Description
clear radius authentication server	Clear the primary or secondary RADIUS server IP address
set radius authentication	Enable or disable RADIUS authentication
set radius authentication retry-number	Set the number of times to resend an access request when there is no response
set radius authentication retry-time	Set the time to wait before resending an access request
set radius authentication secret	Set the shared secret for RADIUS authentication
set radius authentication server	Set the IP address of the primary or secondary RADIUS Authentication server
set radius authentication udp-port	Set the RFC 2138 approved UDP port number
show radius authentication	Display all RADIUS authentication configurations (shared secrets are not displayed)

Recovery password

Table 77: Recovery password CLI commands

Command	Description
set terminal recovery password	Enable or disable the recovery password

Restoring gateway configuration

Table 78: Restore gateway configuration CLI commands

Command	Description
restore usb	Restore gateway files from a USB mass storage device
show restore status	Display information regarding the status of a restore operation of gateway files from a USB mass storage device

RIP

Table 79: RIP CLI commands

Root level command	First level command	Description
interface {dialer|FastEthernet|loopback|serial|VLAN|tunnel} see IP interface configuration		Enter the context of a Dialer, FastEthernet, Loopback, Serial, VLAN, or Tunnel interface
	ip rip authentication key	Set the authentication string used on the interface
		1 of 3

Table 79: RIP CLI commands (continued)

Root level command	First level command	Description
	ip rip authentication mode	Specify the type of authentication used in RIP v2 packets
	ip rip default-route-mode	Enable learning of the default route received by the RIP protocol. The default state is talk-listen.
	ip rip poison-reverse	Enable or disable split-horizon with poison-reverse on an interface
	ip rip rip-version	Specify the RIP version running on the interface
	ip rip send-receive-mode	Set the RIP send and receive modes on an interface
	ip rip split-horizon	Enable or disable the split-horizon mechanism
ip distribution access-default-action		Set the default action for a specific RIP distribution access list
ip distribution access-list		Create a RIP distribution access list
ip distribution access-list-cookie		Set the access list cookie
ip distribution access-list-copy		Copy the distribution access list
ip distribution access-list-name		Set the name of the distribution list
ip distribution access-list-owner		Set the owner of the distribution list
router rip		Enable the RIP and enter the router configuration context or disable the RIP
	default-metric (RIP)	Set or reset the interface RIP route metric value
	distribution-list	Apply a distribution policy rule for incoming or outgoing routing information in route updates or deactivate the rule

2 of 3

Table 79: RIP CLI commands (continued)

Root level command	First level command	Description
	network (RIP)	Specify a list of networks on which the RIP is running
	redistribute (RIP)	Redistribute routing information from other protocols into RIP
	timers basic	Set RIP timers
show ip distribution access-lists		Display the contents of all current distribution lists or of a specific list
show ip protocols		Display parameters and statistics of a given IP routing protocol
		3 of 3

RMON monitoring

Table 80: RMON monitoring CLI commands

Command	Description
clear rmon statistics	Clear RMON statistic
rmon alarm	Create or delete an RMON alarm entry
rmon event	Create or delete an RMON event entry
rmon history	Create or delete an RMON history entry
show rmon alarm	Display information about a specific RMON alarm entry or all existing RMON alarm entries
show rmon event	Display a specific RMON event entry or all RMON event entries
show rmon history	Display a specific RMON history entry or all RMON history entries
show rmon statistics	Display RMON statistics for a specific interface or for all interfaces

Route redistribution

Table 81: Route redistribution CLI commands

Root level command	First level command	Description
router ospf		Enable OSPF and enter the router configuration context
	redistribute (OSPF)	Redistribute routing information from other protocols into OSPF
	default-metric (OSPF)	Configure the metric to be used in updates that are redistributed from one routing protocol to another
router rip		Enable RIP and enter the router configuration context
	redistribute (RIP)	Redistribute routing information from other protocols into RIP
	default-metric (RIP)	Configure the metric to be used in updates that are redistributed from one routing protocol to another

Routing table configuration

Table 82: Routing table CLI commands

Command	Description
clear ip route	Delete all the dynamic routing entries from the routing table
ip default-gateway	Define a default gateway for the router
ip netmask-format	Specify the format of netmasks in the **show** command output
ip redirects	Enable the sending of redirect messages on the current interface
ip route	Establish a static route

1 of 2

Table 82: Routing table CLI commands (continued)

Command	Description
ip routing	Enable IP routing
show ip route	Display information about the IP routing table
show ip route best-match	Display a routing table for a destination address
show ip route static	Display static routes
show ip route summary	Display the number of routes known to the device
show ip route track-table	Display all routes with configured object trackers
traceroute	Trace the route packets are taking to a particular IP address by displaying the hops along the path
	2 of 2

RSVP

Table 83: RTP statistics CLI commands

Command	Description
set qos rsvp	Set values for the RSVP parameters of the VoIP engines
show qos-rtcp	Display QoS, RSVP, and RTCP parameters

RTCP

Table 84: RTP statistics CLI commands

Command	Description
set qos rtcp	Set values for RTCP parameters
show qos-rtcp	Display QoS, RSVP, and RTCP parameters

RTP statistics

Table 85: RTP statistics CLI commands

Command	Description
rtp-stat clear	Reset the RTP statistics application
rtp-stat event-threshold	Set a QoS event-threshold for RTP streams
rtp-stat fault	Configure the RTP statistics application to send QoS fault and/or clear traps
rtp-stat min-stat-win	Set the RTP statistics minimum statistic window
rtp-stat qos-trap	Configure the RTP statistics application to automatically send a QoS trap upon the termination of an RTP stream in which one or more QoS event counters exceeded their configured threshold
rtp-stat qos-trap-rate-limit	Configure the QoS trap rate limiter
rtp-stat-service	Enable the RTP statistics application
rtp-stat threshold	Set thresholds for the RTP statistics applications
show rtp-stat config	Display the RTP statistics application configuration
show rtp-stat detailed	Display a detailed QoS log for a specific RTP session
show rtp-stat sessions	Display RTP sessions QoS statistics
show rtp-stat summary	Display a summary of the RTP statistics
show rtp-stat thresholds	Display the configured RTP statistic thresholds
show rtp-stat traceroute	Display the results of UDP traceroutes issued by the media gateway VoIP engine per active RTP session

SAT

Table 86: SAT CLI commands

Command	Description
sat	Provide a shortcut method to access the System Access Terminal (SAT) so that Avaya Communication Manager translation work can be performed

SLS survivability

Table 87: SLS survivability CLI commands

Root Level Commands	First level command	Second level command	Description
set sls			Enable or disable SLS
show sls			Display SLS status: enabled or disabled
sls			Enter the SLS context
	bri		Administer an ISDN Basic Rate Interface (BRI) port for SLS
		set bearer-capability	Set the Information Transfer Rate field of the Bearer Capability IE in SLS
		set country-protocol	Specify the ISDN Layer-3 country protocol type in SLS
		set directory-number-a	Assign a directory number to the B1 channel of the BRI interface in SLS
		set directory-number-b	Assign a directory number to the B2 channel of the BRI interface in SLS
			1 of 11

Table 87: SLS survivability CLI commands (continued)

Root Level Commands	First level command	Second level command	Description
		set endpoint-init	Determine whether or not the far-end supports endpoint initialization in SLS
		set interface	Specify the glare-handling convention for a BRI link in SLS
		set interface-companding	Set the interface to agree with the companding method used by the far-end of the DS1 circuit for SLS mode
		set layer1-stable	Determine whether or not to keep the physical layer active (stable) between calls in SLS
		set name	Identify the user name for an ISDN facility in SLS
		set side	Specify the glare-handling conditions when the **set interface** command has been administered as `peerMaster` or `peerSlave` for the ISDN link in SLS
		set spid-a	Assign a Service Profile Identifier (SPID) to the B1 channel of the BRI link in SLS
		set spid-b	Assign a Service Profile Identifier (SPID) to the B2 channel of the BRI link in SLS
		set tei-assignment	Select the method by which the Layer 2 (LAPD) protocol obtains its Terminal Endpoint Identification (TEI) address in SLS
		show (bri)	List all BRI SLS parameters for this BRI port
	clear attendant		Delete the administered attendant provisioning
	clear bri		Delete the administration for a given BRI channel in SLS

Table 87: SLS survivability CLI commands (continued)

Root Level Commands	First level command	Second level command	Description
	clear dial-pattern		Delete a single dialed string pattern entry in the SLS data set
	clear ds1		Delete the administration for a specific DS1 channel in SLS
	clear extension		Delete a particular extension number in the SLS data set. **Note:** It is preferable to use the **clear station** command.
	clear fac		Delete an administered Feature Access Code for SLS
	clear incoming-routing		Delete an entry for a particular incoming routed string that is associated with a given trunk group in SLS
	clear sig-group		Delete the administration for a given ISDN signaling group in SLS
	clear slot-config		Delete the slot and the board administration in the G450 for SLS
	clear station		Delete a particular extension number in the SLS data set
	clear survivable-config		Set the SLS parameters to their default values
	clear trunk-group		Delete a trunk group entry from the SLS data set
	dial-pattern		Administering ARS dial patterns for SLS
		set delete-digits	Specify the number of digits to be deleted from the beginning of the dialed string for an outbound call in SLS
		set deny	Permit or deny access to an outbound trunk in SLS

Table 87: SLS survivability CLI commands (continued)

Root Level Commands	First level command	Second level command	Description
		set insert-digits (dial-pattern)	Specify the number of digits to be inserted at the beginning of the dialed string for an outbound call in SLS
		set max-length	Establish the maximum length of the dialed string in SLS
		set min-length	Establish the minimum length of the dialed string in SLS
		set tgnum	Designate the trunk-group number in SLS
		set type (dial-pattern)	Administer the type of outbound call in SLS
		show (dial-pattern)	List all dial-pattern SLS parameters
	ds1		Administer DS1 trunks for SLS
		set bearer-capability	Set the Information Transfer Rate field of the Bearer Capability IE in SLS
		set bit-rate	Set the maximum transmission rate for the DS1 facility in SLS
		set channel-numbering	Select the channel-numbering method for B-channels on an E1 interface in SLS
		set connect	Specify the equipment at the far-end of the DS1 link in SLS
		set country-protocol	Specify the ISDN Layer-3 country protocol type in SLS
		set interface	Specify the glare-handling convention for a DS1 link in SLS
		set interface-companding	Set the interface to agree with the companding method used by the far-end of the DS1 circuit for SLS mode
		set long-timer	Increase the duration of the T303 (call establishment) timer in SLS

Table 87: SLS survivability CLI commands (continued)

Root Level Commands	First level command	Second level command	Description
		set name	Identify the user name for a DS1 facility in SLS
		set protocol-version	Specify country protocol for countries whose public networks allow for multiple ISDN Layer-3 country protocols for ISDN Primary Rate service in SLS
		set side	Specify the glare-handling conditions when the **set interface** command has been administered as `peerMaster` or `peerSlave` for the ISDN link in SLS
		set signaling-mode	Set the signaling mode for the DS1 facility in SLS
		show (ds1)	List all SLS parameters for this DS1 interface
	incoming-routing		Administer digit-treatment for incoming routed calls in SLS
		set delete-digits	Specify number of digits to be deleted from the beginning of the dialed string for an inbound trunk call in SLS
		set insert-digits (incoming-routing)	Specify number of digits to be inserted at the beginning of the dialed string for an inbound trunk call in SLS
		set length	Specify the length of the dialed string in SLS
		set match-pattern	Specify the beginning digit pattern of the incoming alphanumeric dial string to be matched against in SLS
		show (incoming-routing)	List all incoming-routing SLS parameters

Table 87: SLS survivability CLI commands (continued)

Root Level Commands	First level command	Second level command	Description
	set attendant		Set the dial access code which the SLS dial plan manager recognizes as the attendant feature
	set date-format		Set a date format for the SLS data set
	set fac		Administer the Feature Access Code for SLS
	set ip-codec-set		Configure an IP codec set within the SLS data set
	set max-ip-registrations		Configure the maximum number of IP registrations allowed in the SLS data set
	set pim-lockout		Prevent PIM updates while working on SLS administration of the G450
	set slot-config		Define the slot and the board type in the G450 for SLS
	show attendant		Display the administered attendant provisioning
	show bri		List the administered BRI parameters for SLS
	show date-format		Display the current date format for the SLS data set
	show dial-pattern		List all dial-pattern strings in the SLS data set
	show ds1		List the administered DS1 parameters for SLS
	show extension		Display extension-specific SLS data parameters. **Note:** It is preferable to use the **show station** command
	show fac		List the administered Feature Access Codes for SLS

Table 87: SLS survivability CLI commands (continued)

Root Level Commands	First level command	Second level command	Description
	show incoming-routing		Show all of the administered dial patterns in SLS for trunk groups
	show ip-codec-set		List the codec set entries for SLS
	show last-pim-update		Display when the last PIM update of SLS data occurred
	show max-ip-registrations		Display the maximum IP registration administration in the SLS data set
	show pim-lockout		Display the current status of the setting for the PIM lockout feature
	show sig-group		List all administered signaling groups in SLS
	show slot-config		Define the slot and the board administration in the G450 for SLS
	show station		Display extension-specific SLS data parameters
	show trunk-group		Display trunk group administration in SLS
	sig-group		Administer signaling groups for SLS
		add nfas-interface	Identify a list of DS1 modules that are controlled by the primary D-channel in SLS
		remove nfas-interface	Remove a member from a NFAS-managed DS1 group in SLS
		set associated-signaling	Specify whether the D-channel is physically present in the DS1 interface in SLS
		set primary-dchannel	Identify the D-channel number in SLS

Table 87: SLS survivability CLI commands (continued)

Root Level Commands	First level command	Second level command	Description
		set trunk-group-chan-select	Specify the trunk-group number that can accept incoming calls in cases where the Information Channel Selection field does not specify a preferred channel for bearer transport in SLS
		show (sig-group)	List all SLS parameters for this signaling-group
	station		Administer stations for SLS
		set cor	Administer the class-of-restriction values for each station that uses SLS
		set expansion-module	Administer a DCP or IP station for an expansion module in SLS
		set name	Identify the user name for a station in SLS
		set password	Administer a station password in SLS for DCP and IP station sets
		set port	Administer the port on a station for SLS
		set swhook-flash	Enable SLS to recognize the switchhook flash signal from a particular analog station and to provide a subsequent transfer service
		set trunk-destination	Administer a station extension to be included in a pool of stations that can receive incoming analog loop-start trunk calls in circular queuing in SLS
		set type (station)	Administer specific phone models for SLS
		show (station)	List all Station SLS parameters for this station
	trunk-group		Administer trunks for SLS

Table 87: SLS survivability CLI commands (continued)

Root Level Commands	First level command	Second level command	Description
		add port	Administer the port appropriate for SLS
		clear tac	Remove a trunk access code (TAC) assignment from a trunk group in SLS
		remove port	Remove the port assignment from a trunk group in SLS
		set busy-disconnect	Specify whether the SLS analog trunk call state machine will monitor the trunk for the presence of a busy tone, and disconnect the call if a busy tone is detected
		set cbc	Specify whether the ISDN trunk group will operate by declaring the service type explicitly on a call-by-call basis
		set cbc-parameter	Specify the type of service or feature being declared in the Network Services Facility information element
		set cbc-service-feature	Define what class of service is being specified, as part of the ***scocs*** service declared in the Network Services Facility information element
		set channel-preference	Define how the Channel Identification IE field is encoded in SLS
		set codeset-display	Specify which Q.931 codesets are allowed to send display information to the user phone in SLS
		set codeset-national	Specify which Q.931 codesets are allowed to send National Information Elements to the user phone in SLS

Table 87: SLS survivability CLI commands (continued)

Root Level Commands	First level command	Second level command	Description
		set dial	Define the method for sending outbound digits in SLS
		set digit-handling	Define how the inbound/outbound calls handle the transmission/reception of the dialed pattern in SLS
		set digits	Define the inserted dial string that is added to the beginning of the received DID incoming dial string for analog DID trunks or for DS1 TIE trunks using in-band signaling in SLS
		set digit-treatment	Define the incoming digit treatment for analog DID trunks or for DS1 TIE trunks using in-band signaling in SLS
		set incoming-destination	Identify an extension to directly receive an incoming trunk call in SLS
		set incoming-dialtone	Provide a dial tone in response to far-end trunk group seizures in SLS
		set japan-disconnect	Perform a disconnect sequence (CONNECT message followed by a DISCONNECT message) in SLS
		set name	Identify the user name for a trunk group in SLS
		set numbering-format	Specify the numbering plan for this trunk in SLS
		set send-name	Define whether or not the calling, connected, called, or busy party's administered name is sent to the network on outgoing or incoming calls in SLS

Table 87: SLS survivability CLI commands (continued)

Root Level Commands	First level command	Second level command	Description
		set send-number	Define whether or not the calling, connected, called, or busy party's administered number is sent to the network on outgoing or incoming calls in SLS
		set supervision	Define the incoming signaling supervision mode for analog DID trunks or DS1 tie trunks only in SLS
		set tac	Administer the trunk-access codes for SLS
		set trunk-hunt	Specify the trunk-hunting search within a facility in an ISDN trunk group or through a non-ISDN digital trunk group in SLS
		show (trunk-group)	List all trunk-group SLS parameters for this trunk-group

SNMP access configuration

Table 88: SNMP access configuration CLI commands

Root level command	Description
ip snmp	Enable or disable the SNMP agent for the G450
set snmp community	Create or modify an SNMPv1 community
set snmp retries	Set the number of times to attempt to communicate with a particular node
set snmp timeout	Specify the time to wait for a response before retrying the communication
show snmp	Display SNMP configuration information, including a list of SNMP notification receivers
show snmp engineID	Display the SNMPv3 engine ID for the G450

Table 88: SNMP access configuration CLI commands (continued)

Root level command	Description
show snmp group	Display a list of SNMPv3 groups
show snmp retries	Display the number of retry attempts to make when attempting to communicate with a node
show snmp timeout	Display the time to wait before resending a communication
show snmp user	Display configuration information for a specified SNMP user
show snmp usertogroup	Display a table of SNMPv3 users and the groups to which they are mapped
show snmp view	Display configuration information for all SNMP views
snmp-server community	Enable or disable SNMP access to the G450
snmp-server engineID	Specify the SNMP Engine ID for the G450
snmp-server group	Define a new SNMPv3 group, or to configure settings for the group
snmp-server remote-user	Configure settings for a remote SNMPv3 user. If the user does not exist, it is created.
snmp-server user	Configure settings for an SNMPv3 user. If the user does not exist, it is created.
snmp-server view	Configure settings for an SNMP MIB view. If the view does not exist, it is created.

2 of 2

SNMP trap configuration

Table 89: SNMP trap configuration CLI commands

Root level command	First level command	Description
set port trap		Enable or disable SNMP Link Up and Link Down traps notifications and traps on a port
set snmp trap enable | disable auth		Enable or disable authentication failure traps for all managers
set snmp trap enable | disable frame-relay		Enable or disable frame relay traps for all managers
show port trap		Display information on SNMP generic Link Up and Link Down traps sent for a specific port or for all ports
show snmp		Display SNMP configuration information
interface {console|dialer|FastEthernet|serial|tunnel|USB-modem} see IP interface configuration		Enter the context of the Console, Dialer, FastEthernet, Serial, Tunnel, or USB-modem interface
	snmp trap link-status	Enable or disable Link Up and Link Down traps on an interface
snmp-server enable notifications		Enable or disable the sending of all traps and notifications from the G450
snmp-server host		Identify an SNMP management server, and specify the kind of messages it receives. Use the **no** form of the command to remove the specified server, or to disable a particular set of notification types.
snmp-server informs		Configure the SNMPv3 timeout and retries for notifications

Spanning tree

Table 90: Spanning tree CLI commands

Command	Description
set port edge admin state	Assign or unassign RSTP edge-port admin state to a port for Rapid Spanning Tree Protocol (RSTP) treatment
set port point-to-point admin status	Specify a port's connection type
set port spantree	Enable or disable spanning tree for specific ports
set port spantree cost	Set the spanning tree default path cost used by a port
set port spantree force-protocol-migration	Force the port to send a rapid spanning tree hello packet (Bridge Protocol Data Unit)
set port spantree priority	Set the spanning tree priority level of a port
set spantree default-path-cost	Set the version of the spanning tree default path cost used by the current bridge
set spantree enable | disable	Enable or disable the spanning-tree algorithm for the media gateway
set spantree forward-delay	Specify the time used when transferring the state of a port to the forwarding state
set spantree hello-time	Specify the time interval between the generation of configuration BPDUs by the root
set spantree max-age	Specify the time to keep an information message before it is discarded
set spantree priority	Set the bridge priority for the spanning tree
set spantree tx-hold-count	Set the value in packets used by the spanning tree in order to limit the maximum number of BPDU's transmitted during a hello-time period
set spantree version	Set the version of the spanning tree protocol used by the device
show port edge state	Display the edge state of a specified port
show port point-to-point status	Display the point-to-point status of a specific port or all ports
show spantree	Display spanning-tree information

SSH protocol

Table 91: SSH protocol CLI commands

Command	Description
clear ssh-client known-hosts	Clear the SSH known-host file content
crypto key generate	Generate an SSH host key pair
disconnect ssh	Disconnect an existing SSH session
hostname	Assign host name identification to the gateway
ip ssh	Enable or disable the Secure Shell (SSH) service
show ip ssh	Display general SSH information and information about the currently active connections that are using SSH

Synchronization

Table 92: Synchronization CLI commands

Command	Description
clear sync interface	Disassociate an interface previously specified as the primary or secondary clock synchronization source
set sync interface	Define the specified module and port as a potential source for clock synchronization for the media gateway
set sync source	Specify which clock source is the active clock source. The identity of the current synchronization source is not stored in persistent storage.
set sync switching	Toggle automatic sync source switching
show sync timing	Display the status of the primary, secondary, and local clock sources

SYN-cookies

Table 93: SYN-cookies CLI commands

Command	Description
clear tcp syn-cookies counters	Clear the SYN cookies counters
show tcp syn-cookies	Show SYN cookies statistics for inbound TCP connections
tcp syn-cookies	Enable or disable the TCP SYN cookies defense mechanism against SYN attacks

Syslog files

Table 94: Syslog file CLI commands

Command	Description
copy syslog-file ftp	Copy the Syslog file to a remote server using FTP
copy syslog-file scp	Copy the Syslog file to a remote server using SCP
copy syslog-file tftp	Copy the Syslog file to a remote server using TFTP
copy syslog-file usb	Upload the Syslog file from the gateway to the USB mass storage device
show upload syslog-file status	View the status of the upload operation of a Syslog file

System identification

Table 95: System identification CLI commands

Command	Description
set system contact	Set the contact information for this media gateway system
set system location	Set the location information for this media gateway system
set system name	Specify the name of the media gateway system

Telnet access

Table 96: Telnet access configuration CLI commands

Command	Description
ip telnet	Enable the G450 to establish an incoming telnet connection, or disable its ability to establish an incoming telnet connection
ip telnet-client	Enable the G450 to establish an outgoing telnet connection, or disable its ability to establish an outgoing telnet connection
ip telnet-services	Enable the Telnet server on the Services interface
show ip telnet	Display the status of the Telnet server and the current Telnet connections
telnet	Initiate a login session via Telnet to a network host

TFTP server

Table 97: TFTP server CLI commands

Command	Description
clear ip tftp-server statistics	Clear TFTP server statistics
ip tftp-server	Enable the TFTP server
ip tftp-server file-system size	Set the TFTP file system size
show application-memory	Show the configured and allocated application memory

Traffic shaping

Table 98: Traffic shaping CLI commands

Root level command	First level command	Description
interface serial		Enter Serial interface or sub-interface configuration mode
	frame-relay traffic-shaping	Turn on or turn off traffic shaping and frame relay fragmentation
map-class frame-relay		Create a QoS template which can later be assigned to DLCIs
	bc out	Configure the committed burst size in bits, for the outbound direction
	be out	Configure the excess burst size in bits, for the outbound direction
	cir out	Configure the Committed Information Rate in bits per second, for the outbound direction
	fragment	Enable FRF.12 fragmentation and configure the fragment size, or disable FRF.12 fragmentation

1 of 2

Table 98: Traffic shaping CLI commands (continued)

Root level command	First level command	Description
show map-class frame-relay		Display the map-class frame relay table
show traffic-shape		Display traffic shaping and Frame Relay Traffic Shaping configuration information
show traffic-shape-queue		Display information about the real-time status of traffic-shaping and Frame Relay Traffic Shaping queues
show traffic-shape-statistics		Display traffic shaping and Frame Relay Traffic Shaping statistics
traffic-shape rate		Configure traffic shaping for outbound traffic on the current interface

2 of 2

USB mass storage device

Table 99: USB mass storage CLI commands

Command	Description
backup config usb	Back up the gateway configuration to a USB mass storage device
dir	Display information regarding the status of a restore operation of gateway files from a USB mass storage device
erase usb	Erase a file or directory on the USB mass storage device
restore usb	Restore gateway files from a USB mass storage device
safe-removal usb	Safely remove the USB mass storage device
show backup status	Display information regarding the status of a backup of the gateway configuration to a USB mass storage device

1 of 2

Table 99: USB mass storage CLI commands (continued)

Command	Description
show restore status	Display information regarding the status of a restore operation of gateway files from a USB mass storage device
show usb	Display the USB devices connected to the gateway
	2 of 2

User accounts

Table 100: User accounts CLI commands

Command	Description
login authentication inactivity-period	Disable a local user account after a specified inactivity period
login authentication lockout	Lockout or disable an account after successive failed login attempts
login authentication min-password-digit-chars	Set the minimum number of digit characters that a password must contain
login authentication min-password-length	Set the minimum password length
login authentication min-password-lower-chars	Set the minimum number of lowercase characters that a password must contain
login authentication min-password-special-chars	Set the minimum number of special characters that a password must contain
login authentication min-password-upper-chars	Set the minimum number of uppercase characters that a password must contain
login authentication password-expire	Cause all local user passwords to expire after a specified number of days
password	Change the password of a user account
show login authentication	View the login authentication settings and information
show username	Display information about the local user accounts
username	Add or remove a local user account

USP configuration

Table 101: USP port configuration CLI commands

Root level command	First level command	Description
interface serial		Enter Serial interface or sub-interface configuration mode
	bandwidth	Set the bandwidth parameter manually for this interface
	idle-character	Set the bit pattern used to indicate an idle line
	ignore dcd	Specify how the system monitors the line to determine if it is up or down
	invert txclock	Invert the transmit clock signal from the data communications equipment (DCE)
	nrzi-encoding	Enable or disable the non-return-to-zero inverted (NRZI) line coding format on the interface
	transmitter-delay	Set the minimum number of flags to be sent between successive packets

Van Jacobson header compression

Table 102: Van Jacobson header compression CLI commands

Root level command	First level command	Description
clear ip tcp header-compression		Clear TCP header compression statistics for all enabled interfaces or for a specific interface
interface {dialer|serial} see IP interface configuration		Enter the context of the Dialer or Serial interface

Table 102: Van Jacobson header compression CLI commands (continued)

Root level command	First level command	Description
	ip tcp compression-connections	Set the total number of TCP header compression connections supported on the current interface
	ip tcp header-compression	Enable TCP header compression on the current interface
show ip tcp header-compression		Display TCP header compression statistics for a specific interface
show ip tcp header-compression brief		Display a subset of TCP header compression statistics in the form of a table

2 of 2

VLAN configuration

Table 103: VLAN CLI commands

Root level command	First level command	Description
clear port static-vlan		Delete statically configured VLANs from the port
clear vlan		Delete an existing VLAN and its interface, remove the entry from the VLAN table, and return ports from this VLAN to the default VLAN 1
interface vlan		Create a VLAN interface, enter interface VLAN configuration mode, or delete a VLAN interface
	icc-vlan	Set the current VLAN as the ICC-VLAN
set port static-vlan		Assign a static VLAN to a port
set port vlan		Set the port VLAN ID (PVID)
set port vlan-binding-mode		Define the binding method used by ports
set trunk		Configure the VLAN tagging mode of a port
set vlan		Create or modify a VLAN

1 of 2

Table 103: VLAN CLI commands (continued)

Root level command	First level command	Description
show cam vlan		Display all MAC entries in the CAM table for a specific VLAN
show port vlan-binding-mode		Display port VLAN binding mode information
show trunk		Display VLAN tagging information for all or some ports
show vlan		Display the VLANs configured in the media gateway

VoIP

Table 104: VoIP CLI commands

Command	Description
campon-busyout voip-dsp	Put the entire VoIP engine or individual DSP childboard in busyout (not available) state for maintenance or firmware upgrade
reset voip-dsp	Reset a VoIP DSP childboard on the motherboard
show voip-dsp	Display information about the DSP and DSP cores parameters, status and occupancy
show voip-parameters	Display information about the VoIP engine

VoIP testing

Table 105: VoIP testing CLI commands

Command	Description
busyout voip-dsp	Put the VoIP engine in busyout (not available) state. This is recommended before starting a Bit Transfer Rate (BTR) test.
release voip-dsp	Release the VoIP entity from a busyout (not available) state. This command also ends a running Bit Transfer Rate test.
show voip-parameters	Display information about the VoIP engine
test voip-dsp	Start a BTR test on the VoIP engine or a VoIP subsystem

VPN

Table 106: VPN CLI commands

Root level command	First level command	Second level command	Description
clear crypto isakmp			Flush a specific ISAKMP SA or all the ISAKMP SAs
clear crypto sa			Clear all or specific IPSec SAs
clear crypto sa counters			Clear the crypto SA counters
crypto ipsec nat-transparency udp-encapsulation			Re-enable NAT Traversal if it was disabled
crypto ipsec transform-set			Enter the IKE phase 2 (IPSec) transform-set context and create or edit IPSec parameters for the VPN tunnel

Table 106: VPN CLI commands (continued)

Root level command	First level command	Second level command	Description
	mode		Set security-association lifetime
	set pfs		Specify whether each IKE phase 2 negotiation will employ PFS and, if yes, which Diffie-Hellman group to employ
	set security-association lifetime		Set the IKE phase 2 (IPSec) SA lifetime
crypto isakmp invalid-spi-recovery			Enable invalid SPI recovery (default setting)
crypto isakmp nat keepalive			Re-enable NAT Traversal keepalive if it was disabled, and configure the keepalive interval. This command keeps the NAT devices tables updated.
crypto isakmp peer			Enter the crypto ISAKMP peer context and create or edit an ISAKMP peer
	continuous-channel		Enable continuous-channel IKE, which keeps the IKE phase1 session always up and running, even if there is no traffic
	description (ISAKMP peer)		Enter a description for the ISAKMP peer
	initiate mode		Specify which IKE Phase-1 mode to use when communicating with the peer: `aggressive` or `none`

Table 106: VPN CLI commands (continued)

Root level command	First level command	Second level command	Description
	isakmp-policy		Set the ISAKMP policy for the ISAKMP peer
	keepalive (VPN)		Enable DPD keepalives that check whether the remote peer is up
	keepalive-track		Bind an object tracker to a remote VPN peer or to an interface, to check whether the remote peer or the interface is up
	pre-shared-key		Configure the IKE pre-shared key
	self-identity		Set the identity of this device
	suggest-key		Generate a cryptographic-grade random string which you can use as a pre-shared key for IKE. You must use the same key on both peers.
crypto isakmp peer-group			Enter the crypto ISAKMP peer-group context and create or edit an ISAKMP peer group
	description (ISAKMP peer group)		Enter a description for the ISAKMP peer group
	set peer (peer group)		Add a peer to the peer-group
crypto isakmp policy			Enter the crypto ISAKMP policy context and create or edit IKE Phase 1 parameters

Table 106: VPN CLI commands (continued)

Root level command	First level command	Second level command	Description
	authentication		Set the authentication of ISAKMP policy pre-shared secret
	description (ISAKMP policy)		Enter a description for the ISAKMP policy
	encryption		Set the encryption algorithm for an ISAKMP policy
	group		Set the Diffie-Hellman group for an ISAKMP policy
	hash		Set the hash method for an ISAKMP policy
	lifetime		Set the lifetime of the ISAKMP SA in seconds
crypto isakmp suggest-key			Generate a random string which you can use as a pre-shared key for IKE. You must use the same key on both peers.
crypto map			Enter crypto map context and create or edit a crypto map
	continuous-channel		In a crypto ISAKMP peer context, enable continuous-channel IKE, which keeps the IKE phase1 session always up and running, even if there is no traffic
	description (crypto map)		Enter a description for the crypto map
	set dscp		Set the DSCP value in the tunneled packet

Table 106: VPN CLI commands (continued)

Root level command	First level command	Second level command	Description
	set peer (crypto map)		Attach a peer to a crypto map
	set peer-group		Attach a peer-group to a crypto map
	set transform-set		Configure the transform-set
interface {FastEthernet|dialer|serial|VLAN} see IP interface configuration			Enter the context of the FastEthernet, Dialer, Serial, or VLAN interface
	crypto ipsec df-bit		Set the Don't-Fragment bit to clear mode or copy mode
	crypto ipsec minimal-pmtu		Set the minimal PMTU value that can be applied to an SA when the G450 participates in PMTUD for the tunnel pertaining to that SA
	ip crypto-group		Activate a crypto-list in the context of the interface on which the crypto-list is activated
ip crypto-list			Enter crypto-list context and create or edit a crypto-list
	ip-rule (VPN)		Enter ip-rule context and create or modify a specific rule
		description (ip rule)	Enter a description for the ip-rule in the ip crypto-list
		destination-ip	Specify the destination IP address of packets to which the current rule applies

Table 106: VPN CLI commands (continued)

Root level command	First level command	Second level command	Description
		protect crypto map	Protect traffic that matches this rule by applying the IPSec processing configured by the specific crypto map
		source-ip	Indicate that the current rule applies to packets from the specified source IP address
	local-address		Set the local IP address for the IPSec tunnels derived from this crypto-list
show crypto ipsec sa			Display the IPSec SA database and related runtime, statistical, and configuration information
show crypto ipsec transform-set			Display the configuration for the specified transform-set or all transform-sets
show crypto isakmp peer			Display crypto ISAKMP peer configuration
show crypto isakmp peer-group			Display crypto ISAKMP peer-group configuration
show crypto isakmp policy			Display ISAKMP policy configuration
show crypto isakmp sa			Display the ISAKMP SA database status
show crypto map			Display all or specific crypto map configurations

Table 106: VPN CLI commands (continued)

Root level command	First level command	Second level command	Description
show ip active-lists			Display information about a specific policy list or all lists
show ip crypto-list			Display all or specific crypto-list configurations
			7 of 7

VRRP

Table 107: VRRP CLI commands

Root level command	First level command	Description
interface {FastEthernet | VLAN} see IP interface configuration		Enter the configuration context for the FastEthernet or VLAN interface
	ip vrrp	Create a virtual router on an interface
	ip vrrp address	Assign an IP address to a virtual router
	ip vrrp auth-key	Set the virtual router simple password authentication key for the virtual router ID
	ip vrrp override addr owner	Accept packets addressed to the IP addresses associated with the virtual router, such as ICMP, SNMP, and telnet (if it is not the IP address owner)
	ip vrrp preempt	Configure a router to preempt a lower priority master for the virtual router ID
	ip vrrp primary	Set the primary address used as the source address of VRRP packets for the virtual router ID
	ip vrrp priority	Set the virtual router priority value used when selecting a master router
		1 of 2

Table 107: VRRP CLI commands (continued)

Root level command	First level command	Description
	ip vrrp timer	Set the virtual router advertisement timer value for the virtual router ID
router vrrp		Enable or disable VRRP routing globally
show ip vrrp		Display VRRP information
		2 of 2

WAN configuration, verifying

Table 108: WAN configuration verification CLI commands

Command	Description
show controllers	Display status information about a controller interface
show frame-relay fragment	Display frame-relay fragmentation statistics and configuration on all PVCs, all PVCs associated with an interface, or a specific PVC
show frame-relay lmi	Display LMI statistics for a particular interface or for all interfaces. The output displayed differs depending on the type of interface.
show frame-relay map	Display a summary table of frame relay sub-interfaces and DLCIs associated with the sub-interfaces
show frame-relay pvc	Display detailed PVC information
show frame-relay traffic	Display frame-relay protocol statistics, including ARP requests and replies sent and received over frame relay interfaces
show interfaces	Display interface configuration and statistics for a particular interface or all interfaces
show map-class frame-relay	Display the map-class frame relay table

WAN Ethernet port configuration

Table 109: WAN Ethernet port configuration CLI commands

Root level command	First level command	Description
interface FastEthernet		Enter interface FastEthernet configuration mode
	autoneg	Set the port speed and duplex to auto-negotiation mode
	duplex	Set the duplex setting (full or half) for the interface
	keepalive-track	Bind an object tracker to the interface to check whether it is up
	speed (interface)	Set the speed for the interface
	traffic-shape rate	Configure traffic shaping for outbound traffic on the current interface

WFVQ (Weighted Fair VoIP Queuing)

Table 110: WFVQ configuration CLI commands

Root level command	Command	Description
interface {serial | FastEthernet | dialer} see IP interface configuration		Enter interface configuration mode for either a Serial, FastEthernet, or Dialer interface
	fair-queue-limit	Set the maximum number of packets that can be queued in the weighted fair queue
	fair-voip-queue	Enable Weighted Fair VoIP Queuing (WFVQ) on the current interface

1 of 2

Table 110: WFVQ configuration CLI commands (continued)

Root level command	Command	Description
	priority-queue	Enable or disable priority queuing mode in a Serial or FastEthernet interface. If you disable priority queuing, WFVQ is re-enabled.
	show queue	Display information about the real-time status of output queues for the current interface
	voip-queue	Enable or disable custom queueing for VoIP traffic. If you disable custom queueing, WFVQ is re-enabled.
show queueing		Display the priority queue size, in packets

2 of 2

Chapter 3: CLI Commands

About the CLI

The Avaya G450 Media Gateway CLI is accessible directly via the serial console port, remotely via Secure Shell (SSH), or via the modem PPP interface. The CLI is command-line driven and does not have any menus. The CLI commands available, and the functions of those commands, depend on the context you are in when you issue the command. For a complete discussion of contexts, refer to Contexts on page 40.

This chapter lists all the CLI commands for the Avaya G450 Media Gateway, arranged alphabetically within topics.

Logging in to the CLI

To login to the CLI, you need a username and a password. Initially, there is only one user, named **root** (with password **root**), on the system. It is recommended to change the root user password to prevent unauthorized entry into the system. The root user has Administrative privileges. You can add more users with the **`username`** command.

When you open the CLI interface, you are prompted for a username. Enter the username and press **Enter**. Enter your password at the password prompt, and press **Enter**. Once you have logged in, you can execute all the CLI commands that are permitted at your user level. For a full discussion of user levels, refer to User levels on page 39.

Using the CLI

To use a command, type the desired command at the prompt and press **Enter**.

Using Help

You can use the built-in Help feature to display the list of commands that are available to you. Type **`help`** to see the list of available commands in the present context. Type **`help`** followed by a word or part of a word to see a list of all commands starting with that word. For example, type **`help show`** to see a list of all commands using **`show`**. Type **`tree`** to see the full list of commands available at the current permission level.

Using auto-complete

If you are unsure of the spelling of a command, use the auto-complete feature. Type the first few letters of the command and then press the **tab** key. The system completes the command automatically. If more than one command begins with those letters, pressing the tab key twice displays a list of commands matching those letters. Pressing the tab key twice automatically populates the next part of the command when only one option is available.

Abbreviating commands

You can abbreviate commands or parts of commands in the CLI. As long as the abbreviation uniquely identifies a command, the system executes that command. If the abbreviation is ambiguous, the system displays a list of possible matches.

For example, typing **`sh ban login`** is the same as typing **`show banner login`**. However, typing **`show m`** matches more than one command and is not executed. Instead the system displays a list such as:

```
Ambiguous Command.  Possible commands are:
map-class mediaserver mg mgc mm module
```

Analog testing - Test and Heal

analog-test

Use the **analog-test** command to enter the analog-test context, which enables running analog testing and correction procedures.

Syntax

analog-test

User level

admin

Context

general

Example

To enter the analog-test context:

```
G450-001(super)# analog-test
G450-001(analog-test)#
```

Related commands

analog-test, cancel, clear profile, launch, profile, set crosstalk-destination, set crosstalk-port, set crosstalk-responder, set destination, set port, set responder, set responder-type, set type, show (profile), show result (profile), set balance, set receive-gain, set transmit-gain, show correction, show profile, show result

cancel

Use the **cancel** command to abort an analog test if it is already running.

Syntax

cancel ***id***

Parameters

Parameter	Description	Possible Values	Default Value
id	The ID of the test profile		

User level

admin

Context

analog-test

Example

To cancel the `measure3` analog test:

```
G450-001(analog-test)# cancel measure3
```

Related commands

analog-test, clear profile, launch, profile, set crosstalk-destination, set crosstalk-port, set crosstalk-responder, set destination, set port, set responder, set responder-type, set type, show (profile), show result (profile), set balance, set receive-gain, set transmit-gain, show correction, show profile, show result

clear profile

Use the **`clear profile`** command to delete a test profile.

Syntax

`clear profile {`*`id`*` | all}`

Parameters

Parameter	Description	Possible Values	Default Value
id	The ID of the test profile		
`all`	A keyword indicating to clear all test profiles		

User level

admin

Context

analog-test

Example

To clear the profile of the `measure3` test:

```
G450-001(analog-test)# clear profile measure3
```

Related commands

analog-test, cancel, launch, profile, set crosstalk-destination, set crosstalk-port, set crosstalk-responder, set destination, set port, set responder, set responder-type, set type, show (profile), show result (profile), set balance, set receive-gain, set transmit-gain, show correction, show profile, show result

launch

Use the **`launch`** command to launch a specific test. The results of previous measurements on the target are cleared as soon as this command is issued.

Note:

The port(s) specified in the test profile must be busied out from Communication Manager before the test is launched.

Syntax

`launch` ***`id`***

Parameters

Parameter	Description	Possible Values	Default Value
`id`	The ID of the test profile		

User level

admin

Context

analog-test

Example

To launch the `mesure3` test:

```
G450-001(analog-test)# launch measure3
```

Related commands

analog-test, cancel, clear profile, profile, set crosstalk-destination, set crosstalk-port, set crosstalk-responder, set destination, set port, set responder, set responder-type, set type, show (profile), show result (profile), set balance, set receive-gain, set transmit-gain, show correction, show profile, show result

profile

Use the **`profile`** command to enter the `analog-test-profile` context, for configuring a specific test profile. Each profile pertains to a particular set of defined ports. You can define up to 30 profiles.

Note:

You must at least set a port for the profile before exiting the `analog-test-profile` context, otherwise the profile will not be saved.

Syntax

`profile` ***`id`***

Parameters

Parameter	Description	Possible Values	Default Value
`id`	The ID of the test profile	alphanumerical string of up to 10 characters	

User level

analog-test

Context

general

Example

```
G450-001(analog-test)# profile measure3
G450-001(analog-test-profile-measure3)#
```

Related commands

analog-test, cancel, clear profile, launch, set crosstalk-destination, set crosstalk-port, set crosstalk-responder, set destination, set port, set responder, set responder-type, set type, show (profile), show result (profile), set balance, set receive-gain, set transmit-gain, show correction, show profile, show result

set crosstalk-destination

Use the **set crosstalk-destination** command to set the Local Exchange Carrier number destination of the call from the crosstalk port.

Syntax

set crosstalk-destination {*number* | none}

Parameters

Parameter	Description	Possible Values	Default Value
number	The Local Exchange Carrier number destination of the call from the crosstalk port. **Note**: You can specify a number only if the type of the current profile is `crosstalk`.	A string of 1-14 characters, composed of digits **0**-**9**	
none	A keyword specifying that the crosstalk port will not attempt to make a call toward any destination but will expect an incoming call		

User level

admin

Context

analog-test-profile

Example

```
G450-001(analog-test-measure3)# set crosstalk-destination 7771234
```

Related commands

analog-test, cancel, clear profile, launch, profile, set crosstalk-port, set crosstalk-responder, set destination, set port, set responder, set responder-type, set type, show (profile), show result (profile), set balance, set receive-gain, set transmit-gain, show correction, show profile, show result

set crosstalk-port

Use the **set crosstalk-port** command to specify the crosstalk port. The port must be on the same board as the port target of the test, but it must be a different port from the port under test.

Syntax

set crosstalk-port {***slot port***}

Parameters

Parameter	Description	Possible Values	Default Value
slot	Number of the slot, represented as a number preceded by the letter **v**. For example, slot 1 is represented as **v1**.	A slot with an analog media module	
port	Number of the port on the module, represented as two digits. For example, port 2 is represented as **02**	Any analog trunk port, including DID trunk ports	

User level

admin

Context

analog-test-profile

Example

```
G450-001(analog-test-measure3)# set crosstalk-port v405
```

Related commands

analog-test, cancel, clear profile, launch, profile, set crosstalk-destination, set crosstalk-responder, set destination, set port, set responder, set responder-type, set type, show (profile), show result (profile), set balance, set receive-gain, set transmit-gain, show correction, show profile, show result

set crosstalk-responder

Use the **set crosstalk-responder** command to specify the responder port for the crosstalk port. A responder answers an incoming call and then plays a sequence of tones. The tones are used by test equipment at the other end of the loop to make measurements. The responder can be a port in the media module, or the Local Exchange Carrier (LEC).

Note:

Once you specify a responder port on the gateway, the crosstalk responder type is `test 100` and cannot be modified.

Syntax

set crosstalk-responder {{*slot port*} | none}

Parameters

Parameter	Description	Possible Values	Default Value
slot	Number of the slot, represented as a number preceded by the letter **v**. For example, slot 1 is represented as **v1**.	A slot with an analog media module	
port	Number of the port on the module, represented as two digits. For example, port 2 is represented as **02**. **Note**: If you set the crosstalk-port to be the responder port, the crosstalk port plays the role of the responder.	Any analog trunk port, including DID trunk ports	
none	A keyword specifying that the Local Exchange Carrier (LEC) plays the role of the responder		

User level

admin

Context

analog-test-profile

Example

```
G450-001(analog-test-measure3)# set crosstalk-responder v406
```

Related commands

analog-test, cancel, clear profile, launch, profile, set crosstalk-destination, set crosstalk-port, set destination, set port, set responder, set responder-type, set type, show (profile), show result (profile), set balance, set receive-gain, set transmit-gain, show correction, show profile, show result

set destination

Use the **set destination** command to set the Local Exchange Carrier number destination of the measurement call.

Syntax

set destination {***number*** | **none**}

Parameters

Parameter	Description	Possible Values	Default Value
number	The Local Exchange Carrier number destination of the call	A string of 1-14 characters, composed of digits **0**-**9**	
none	A keyword specifying that the trunk will not attempt to make a call toward any destination but will make the measurement on the current call		

User level

admin

Context

analog-test-profile

Example

```
G450-001(analog-test-measure3)# set destination 7775634
```

Related commands

analog-test, cancel, clear profile, launch, profile, set crosstalk-destination, set crosstalk-port, set crosstalk-responder, set port, set responder, set responder-type, set type, show (profile), show result (profile), set balance, set receive-gain, set transmit-gain, show correction, show profile, show result

set port

Use the **set port** command to specify the port target of the test.

Note:

The port target must belong to a media module with a firmware release that supports the Test & Heal feature. The following do not support the Test & Heal feature: an MM711 with a pre-30 hardware vintage, and an MM714 with a pre-10 hardware vintage.

Syntax

set port {***slot port***}

Parameters

Parameter	Description	Possible Values	Default Value
slot	Number of the slot, represented as a number preceded by the letter **v**. For example, slot 1 is represented as **v1**.	A slot with an analog media module	
port	Number of the port on the module, represented as two digits. For example, port 2 is represented as **02**.	Any analog trunk port	

User level

admin

Context

analog-test-profile

Example

```
G450-001(analog-test-measure3)# set port v401
```

Related commands

analog-test, cancel, clear profile, launch, profile, set crosstalk-destination, set crosstalk-port, set crosstalk-responder, set destination, set responder, set responder-type, set type, show (profile), show result (profile), set balance, set receive-gain, set transmit-gain, show correction, show profile, show result

set responder

Use the **set responder** command to specify the responder port. A responder answers an incoming call and then plays a sequence of tones. The tones are used by test equipment at the other end of the loop to make measurements. The responder can be a port in the media module, or the Local Exchange Carrier (LEC).

Syntax

set responder {{*slot port*} | **none**}

Parameters

Parameter	Description	Possible Values	Default Value
slot	Number of the slot, represented as a number preceded by the letter **v**. For example, slot 1 is represented as **v1**.	A slot with an analog media module	
port	Number of the port on the module, represented as two digits. For example, port 2 is represented as **02**. **Note**: If you set the test port to be the responder port, the test port plays the role of the responder.	Any analog trunk port, including DID trunk ports	
none	A keyword specifying that the Local Exchange Carrier (LEC) plays the role of the responder		

User level

admin

Context

analog-test-profile

Example

```
G450-001(analog-test-measure3)# set responder v402
```

Related commands

analog-test, cancel, clear profile, launch, profile, set crosstalk-destination, set crosstalk-port, set crosstalk-responder, set destination, set port, set responder-type, set type, show (profile), show result (profile), set balance, set receive-gain, set transmit-gain, show correction, show profile, show result

set responder-type

Use the **set responder-type** command to specify the responder type. The different types send different sequences of tones.

Syntax

set responder-type ***test***

Parameters

Parameter	Description	Possible Values	Default Value
test	The type of tone sequence to be sent by the responder: • **100** – Responder test type 100 • **102** – Responder test type 102 • **105** – Responder test type 105	• **100** • **102** • **105**	**100**

User level

admin

Context

analog-test-profile

Example

```
G450-001(analog-test-measure3)# set responder-type 100
```

Related commands

analog-test, cancel, clear profile, launch, profile, set crosstalk-destination, set crosstalk-port, set crosstalk-responder, set destination, set port, set responder, set type, show (profile), show result (profile), set balance, set receive-gain, set transmit-gain, show correction, show profile, show result

set type

Use the **set type** command to specify what type of test to run.

Note:

If type is set to **crosstalk**, you must specify the crosstalk port using the set crosstalk-port command before you exit the profile. Otherwise, the profile will not be saved.

Syntax

set type *type*

Parameters

Parameter	Description	Possible Values	Default Value
type	The type of test to run: • **noise** – noise test • **receive-loss** – receive-loss test • **crosstalk** – crosstalk test • **balance** – trans-hybrid loss test • **match** – hybrid balance match test • **passive** – indicates that the test measurements will be made by the LEC, not by the analog board	• **noise** • **receive-loss** • **crosstalk** • **balance** • **match** • **passive**	**noise**

User level

admin

Context

analog-test-profile

Example

```
G450-001(analog-test-measure3)# set type noise
```

Related commands

analog-test, cancel, clear profile, launch, profile, set crosstalk-destination, set crosstalk-port, set crosstalk-responder, set destination, set port, set responder, set responder-type, show (profile), show result (profile), set balance, set receive-gain, set transmit-gain, show correction, show profile, show result

show (profile)

Use the **show** command to display a test profile.

Syntax

show

User level

admin

Context

analog-test-profile

Examples

- To show the profile of a crosstalk test:

```
G450-001(analog-test-measure3)# show

Port State   Type          Destination      Resp. Resp. type
---- ------- ------------- ---------------- ----- ----------
v401 idle    crosstalk     7771234          v402  100

Crosstalk:
Port Destination      Responder Responder type
---- ---------------- --------- --------------
v403 7771235          v405      102
```

- To show the profile of a receive-loss test:

```
G450-001(analog-test-measure3)# show

Port State Type          Destination      Resp. Resp. type
---- ----- ------------- ---------------- ----- ----------
V401 Idle  receive-loss  7771234          v401  105
```

Related commands

analog-test, cancel, clear profile, launch, profile, set crosstalk-destination, set crosstalk-port, set crosstalk-responder, set destination, set port, set responder, set responder-type, set type, show result (profile), set balance, set receive-gain, set transmit-gain, show correction, show profile, show result

show result (profile)

Use the **show result** command to display the results of the latest measurements obtained by this test. If the test did not succeed, the output indicates the reason for the test failure.

Syntax

show result

User level

admin

Context

analog-test-profile

Example

- To show the results of a noise test:

```
G450-001(analog-test-noise)# show result
Noise: +4.56 dBrnC, +8.76 dBrn 3kHz flat
```

- To show the results of a loss test:

```
G450-001(analog-test-Loss)# show result
Loss: +4.43 dB
```

- To show the results of a balance test:

```
G450-001(analog-test-Balance)# show result

Trans-hybrid Loss vs. frequency (frequency in Hz, loss in dB):
( 200,+7.45) ( 300,+6.22) ( 400,+6.12) ( 500,+6.10) ( 600,+6.10)
( 700,+6.10) ( 800,+6.11) ( 900,+6.11) (1000,+6.10) (1100,+6.09)
(1200,+6.06) (1300,+6.04) (1400,+6.01) (1500,+5.98) (1600,+5.96)
(1700,+5.94) (1800,+5.92) (1900,+5.92) (2000,+5.92) (2100,+5.93)
(2200,+5.95) (2300,+5.97) (2400,+5.99) (2500,+6.01) (2600,+6.02)
(2700,+6.03) (2800,+6.04) (2900,+6.03) (3000,+6.02) (3100,+5.99)
(3200,+5.95) (3300,+5.98) (3400,+6.34)
```

- To show the results of a match test:

```
G450-001(analog-test-Match)# show result

Coefficient match, (coefficient table, ERL in dB):
( 1,+10.69) ( 2,+18.99) ( 0, +6.07) ( 3,+19.16) ( 4,+13.41)
( 5,+13.66) ( 6,+12.66) ( 7,+10.69) ( 8, +9.53)
Measurements are shown in the order of best match first.
Coefficient table 1 is the best match.
```

- To show the results of a crosstalk test:

```
G450-001(analog-test-Crosstalk)# show result

Crosstalk coupling vs. frequency (frequency in Hz, coupling in dB):
( 400,-88.12) (1200,-99.28) (3000,-76.48)
```

Related commands

analog-test, cancel, clear profile, launch, profile, set crosstalk-destination, set crosstalk-port, set crosstalk-responder, set destination, set port, set responder, set responder-type, set type, show (profile), set balance, set receive-gain, set transmit-gain, show correction, show profile, show result

set balance

Use the **set balance** command to set the balance on a specific port.

Syntax

set balance {***slot port***} ***value***

Parameters

Parameter	Description	Possible Values	Default Value
slot	Number of the slot, represented as a number preceded by the letter **v**. For example, slot 1 is represented as **v1**.	A slot with an analog media module	

Parameter	Description	Possible Values	Default Value
port	Number of the port on the module, represented as two digits. For example, port 2 is represented as **02**.	Any analog trunk port	
value	An index in the gateway's internal balance coefficient table, corresponding to a specific hybrid balance coefficient set	**0**-**15**	

User level

admin

Context

analog-test

Example

To set the balance on port v401 to 7:

```
G450-001(analog-test)# set balance v401 7
```

Related commands

analog-test, cancel, clear profile, launch, profile, set crosstalk-destination, set crosstalk-port, set crosstalk-responder, set destination, set port, set responder, set responder-type, set type, show (profile), show result (profile), set receive-gain, set transmit-gain, show correction, show profile, show result

set receive-gain

Use the **set receive-gain** command to set the receive-gain on a specific port.

Syntax

set receive-gain {***slot port***} ***value***

Parameters

Parameter	Description	Possible Values	Default Value
slot	Number of the slot, represented as a number preceded by the letter **v**. For example, slot 1 is represented as **v1**.	A slot with an analog media module	
port	Number of the port on the module, represented as two digits. For example, port 2 is represented as **02**.	Any analog trunk port	
value	The receive-gain	**-6.00** - **+3.00**	

User level

admin

Context

analog-test

Example

To set the receive-gain on port v201 to 1:

```
G450-001(analog-test)# set receive-gain v201 1.00
```

Related commands

analog-test, cancel, clear profile, launch, profile, set crosstalk-destination, set crosstalk-port, set crosstalk-responder, set destination, set port, set responder, set responder-type, set type, show (profile), show result (profile), set balance, set transmit-gain, show correction, show profile, show result

set transmit-gain

Use the **set transmit-gain** command to set the transmit-gain on a specific port.

Syntax

set transmit-gain {***slot port***} ***value***

Parameters

Parameter	Description	Possible Values	Default Value
slot	Number of the slot, represented as a number preceded by the letter **v**. For example, slot 1 is represented as **v1**.	A slot with an analog media module	
port	Number of the port on the module, represented as two digits. For example, port 2 is represented as **02**.	Any analog trunk port	
value	The transmit-gain	**-6.00** - **+3.00**	

User level

admin

Context

analog-test

Example

To set the transmit-gain on port v201 to -2:

```
G450-001(analog-test)# set transmit-gain v201 -2.00
```

Related commands

analog-test, cancel, clear profile, launch, profile, set crosstalk-destination, set crosstalk-port, set crosstalk-responder, set destination, set port, set responder, set responder-type, set type, show (profile), show result (profile), set balance, set receive-gain, show correction, show profile, show result

show correction

Use the **show correction** command to display the balance, receive-gain, and transmit-gain corrections applied to each port.

Syntax

show correction

User level

admin

Context

analog-test

Example

To show the corrections entered for all ports:

```
G450-001(analog-test)# show correction
Port balance receive-gain transmit-gain
---- ------- ------------ -------------
v201 2       -            -
v302 -       +1.25        -0.5
```

Note:

A dash indicates 0 or no correction.

Related commands

analog-test, cancel, clear profile, launch, profile, set crosstalk-destination, set crosstalk-port, set crosstalk-responder, set destination, set port, set responder, set responder-type, set type, show (profile), show result (profile), set balance, set receive-gain, set transmit-gain, show profile, show result

show profile

Use the **show profile** command to display the details of a test profile.

Syntax

show profile {*id* | **all**}

Parameters

Parameter	Description	Possible Values	Default Value
id	The ID of a test profile		
all	A keyword specifying to display the details of all profiles		

User level

admin

Context

analog-test

Example

To show the details of the test profile `measure3`:

```
G450-001(analog-test)# show profile measure3
Port State Type          Destination      Resp. Resp. type
---- ----- ------------- ---------------- ----- ----------
v401 Idle  receive-loss  7771234          v401  105
```

Related commands

analog-test, cancel, clear profile, launch, profile, set crosstalk-destination, set crosstalk-port, set crosstalk-responder, set destination, set port, set responder, set responder-type, set type, show (profile), show result (profile), set balance, set receive-gain, set transmit-gain, show correction, show result

show result

Use the show result command to display the result of the last measurement performed for a particular profile. If the test did not succeed, the output indicates the reason for the test failure.

Syntax

show result *id*

Parameters

Parameter	Description	Possible Values	Default Value
id	The ID of the test profile		

User level

admin

Context

analog-test

Examples

- To show the results of a noise test:

```
G450-001(analog-test)# show result Noise
Noise: +4.56 dBrnC, +8.76 dBrn 3kHz flat
```

- To show the results of a loss test:

```
G450-001(analog-test)# show result Loss
Loss: +4.43 dB
```

- To show the results of a balance test:

```
G450-001(analog-test)# show result Balance

Trans-hybrid Loss vs. frequency (frequency in Hz, loss in dB):
( 200,+7.45) ( 300,+6.22) ( 400,+6.12) ( 500,+6.10) ( 600,+6.10)
( 700,+6.10) ( 800,+6.11) ( 900,+6.11) (1000,+6.10) (1100,+6.09)
(1200,+6.06) (1300,+6.04) (1400,+6.01) (1500,+5.98) (1600,+5.96)
(1700,+5.94) (1800,+5.92) (1900,+5.92) (2000,+5.92) (2100,+5.93)
(2200,+5.95) (2300,+5.97) (2400,+5.99) (2500,+6.01) (2600,+6.02)
(2700,+6.03) (2800,+6.04) (2900,+6.03) (3000,+6.02) (3100,+5.99)
(3200,+5.95) (3300,+5.98) (3400,+6.34)
```

- To show the results of a match test:

```
G450-001(analog-test)# show result Match

Coefficient match, (coefficient table, ERL in dB):
( 1,+10.69) ( 2,+18.99) ( 0, +6.07) ( 3,+19.16) ( 4,+13.41)
( 5,+13.66) ( 6,+12.66) ( 7,+10.69) ( 8, +9.53)
Measurements are shown in the order of best match first.
Coefficient table 1 is the best match.
```

- To show the results of a crosstalk test:

```
G450-001(analog-test)# show result Crosstalk

Crosstalk coupling vs. frequency (frequency in Hz, coupling in dB):
( 400,-88.12) (1200,-99.28) (3000,-76.48)
```

Related commands

analog-test, cancel, clear profile, launch, profile, set crosstalk-destination, set crosstalk-port, set crosstalk-responder, set destination, set port, set responder, set responder-type, set type, show (profile), show result (profile), set balance, set receive-gain, set transmit-gain, show correction, show profile

Announcement files

copy announcement-file ftp

Use the **copy announcement-file ftp** command to upload an announcement file from the G450 announcement directory to a remote FTP server. The files can then be downloaded from the FTP server to Avaya Voice Announcements Manager (VAM).

Syntax

copy announcement-file ftp *source-filename ip* [*destination-filename*]

Parameters

Parameter	Description	Possible Values	Default Value
source-filename	The name of the announcement file in the G450 announcement directory. If the file name includes spaces, use quotes.		
ip	The IP address of the remote FTP server		
destination-filename	The destination file name, including full path, if a name change is required. If the file name includes spaces, use quotes.	up to 32 characters for the file name	

User Level

read-write

Context

general

Example

To upload `local_announcement2.wav` from the announcements directory to a remote FTP server with IP address 192.168.49.10, place it in the C drive, and name it `remote_announcement2.wav`:

```
G450-001(super)# copy announcement-file ftp local_announcement2.wav
192.168.49.10 c:\remote_announcement2.wav
```

Related Commands

copy announcement-file usb, copy announcement-file scp, copy ftp announcement-file, copy scp announcement-file, copy usb announcement-file, erase announcement-file, rename announcement-file, show announcements files, show download announcement-file status, show upload announcement-file status

copy announcement-file scp

Use the **copy announcement-file scp** command to upload an announcement file from the G450 announcement directory to a remote SCP server, using SCP. The files can then be downloaded from the SCP server to Avaya Voice Announcements Manager (VAM).

Syntax

copy announcement-file scp *source-filename ip* [*destination-filename*]

Parameters

Parameter	Description	Possible Values	Default Value
source-filename	The file name of the announcement file in the G450 announcement directory. If the file name includes spaces, use quotes.		
ip	The IP address of the remote SCP server		
destination-filename	The destination file name, including full path, if a name change is required. If the file name includes spaces, use quotes.	Up to 32 characters, not including the path	

User Level

read-write

Context

general

Example

To upload the file `local_announcement2.wav` from the announcements directory to the location c:\ on a remote SCP server with IP address 192.168.49.10, and name the destination file `remote_announcement2.wav`:

```
G450-001(super)# copy announcement-file scp local_announcement2.wav
192.168.49.10 c:\remote_announcement2.wav
```

Related Commands

copy announcement-file usb, copy announcement-file ftp, copy ftp announcement-file, copy scp announcement-file, copy usb announcement-file, erase announcement-file, rename announcement-file, show announcements files, show download announcement-file status, show upload announcement-file status

copy announcement-file usb

Use the **`copy announcement-file usb`** command to upload an announcement file from the gateway to the USB mass storage device.

Syntax

`copy announcement-file usb` ***`source-filename destination-usb-device`*** **`[`*** ***`destination-filename`*** **`]`**

Parameters

Parameter	Description	Possible Values	Default Value
`source-filename`	The logical name for the source file		
`destination usb-device`	The destination USB mass storage device	**usb-device0**	
`destination-filename`	The destination file name and path		

User Level

read-write

Context

general

Example

To upload `local_announcement2.wav` from the gateway to usb-device0 and call it `remote_announcement2.wav`:

```
G450-001(super)# copy announcement-file usb local_announcement2.wav
usb-device0 remote_announcement2.wav
```

Related Commands

backup config usb, copy usb announcement-file, erase usb, restore usb, safe-removal usb, show backup status, show restore status, show usb

copy ftp announcement-file

Use the **`copy ftp announcement-file`** command to download a file from an FTP server to the gateway's announcement directory. The FTP command prompts for the username and password after the command is entered.

Syntax

`copy ftp announcement` ***`filename ip`*** **[***`destination-filename`***]**

Parameters

Parameter	Description	Possible Values	Default Value
`filename`	The file name on the FTP server		
`ip`	The IP address of the FTP server		
`destination-filename`	The file name in the gateway's announcement directory	string of up to 32 characters	

User Level

read-write

Context

general

Example

To download `announcement_file2.wav` from the FTP server at IP address 192.168.49.10 and save it in the gateway's announcement directory as `local_announcement_file2`, using login dan:

```
G450-001cp(super)# copy ftp announcement-file c:\temp\announcement_file2.wav
```

```
192.168.49.10 local_announcement_file2
Username: dan
Password:
```

Related Commands

copy announcement-file ftp, copy announcement-file scp, copy announcement-file usb, copy scp announcement-file, copy usb announcement-file, erase announcement-file, rename announcement-file, show announcements files, show download announcement-file status, show upload announcement-file status

copy scp announcement-file

Use the **copy scp announcement-file** command to download an announcement file from the Voice Announcements Manager to the G450 announcement directory using SCP. A maximum of 256 announcement files can be stored in the announcement directory.

Syntax

copy scp announcement-file *source-filename ip* [*destination-filename*]

Parameters

Parameter	Description	Possible Values	Default Value
source-filename	The filename of the announcement file on the Voice Announcements Manager host with the full path. If the file name includes spaces, use quotes.		
ip	The IP address of the Voice Announcements Manager host		
destination-filename	The destination filename, if a name change is required. If the file name includes spaces, use quotes.		

User Level

read-write

Context

general

Example

To download `announcement_file1.wav` from the Voice Announcements Manager on host 192.168.49.10, and change the name to `local announcement file2`:

```
G450-001(super)# copy scp announcement-file c:\temp\announcement_file2.wav
192.168.49.10 "local announcement file2"
```

Related Commands

copy announcement-file ftp, copy announcement-file scp, copy announcement-file usb, copy ftp announcement-file, copy usb announcement-file, erase announcement-file, rename announcement-file, show announcements files, show download announcement-file status, show upload announcement-file status

copy usb announcement-file

Use the **`copy usb announcement-file`** command to download an announcement file from the external USB mass storage device to the gateway.

Syntax

copy usb announcement-file ***`source-usb-device source-filename`*** [***`destination-filename`***]

Parameters

Parameter	Description	Possible Values	Default Value
`source usb-device`	The source USB mass storage device	**usb-device0**	
`source-filename`	The full name and path of the file to be downloaded		
`destination-filename`	The destination file name (no path)		

User Level

read-write

Context

general

Example

To download `announcement_file1.wav` from usb-device0 to the gateway and name it `local_announcement_file2.wav`:

```
G450-001(super)# copy usb announcement-file usb-device0 \temp\
announcement_file1.wav local_announcement_file2.wav
```

Related Commands

backup config usb, copy announcement-file usb, erase usb, restore usb, safe-removal usb, show backup status, show restore status, show usb

erase announcement-file

Use the **`erase announcement-file`** command to erase an announcement file in the G450 announcement directory.

Syntax

`erase announcement-file` ***`source-filename`***

Parameters

Parameter	Description	Possible Values	Default Value
`source-filename`	The name of the announcement file to delete		

User Level

read-write

Context

general

Example

To erase the announcement file `local_announcement1.wav` from the G450 announcement directory:

```
G450-001# erase announcement-file local_announcement1.wav
```

Related Commands

copy announcement-file scp, copy announcement-file usb, copy ftp announcement-file, copy scp announcement-file, copy usb announcement-file, rename announcement-file, show announcements files, show download announcement-file status, show upload announcement-file status

rename announcement-file

Use the **rename announcement-file** command to rename an announcement file in the G450 announcement directory.

Syntax

rename announcement-file *source-filename destination-filename*

Parameters

Parameter	Description	Possible Values	Default Value
source-filename	The name of the announcement file to be renamed		
destination-filename	The new name for the announcement file		

User Level

read-write

Context

general

Example

To change the name of the announcement file from `from_local_announcement1.wav` to `to_local_announcement1.wav`:

```
G450-001# rename announcement-file from_local_announcement1.wav
to_local_announcement1.wav
```

Related Commands

copy announcement-file scp, copy announcement-file usb, copy ftp announcement-file, copy scp announcement-file, copy usb announcement-file, erase announcement-file, show announcements files, show download announcement-file status, show upload announcement-file status

show announcements files

Use the **show announcements files** command to display the announcements files stored in the G450 announcement directory.

Syntax

show announcements files [brief]

Parameters

Parameter	Description	Possible Values	Default Value
brief	Keyword indicating to display less detail		

User Level

read-only

Context

general

Example

To display the announcements files in full detail:

```
G450-001(super)# show announcements files
Mode: FTP-SERVER/SCP-CLIENT
ID   File              Description  Size (Bytes) Date
---- ---------------- ------------ ------------ -----------------
5     46xxupgrade.scr  Announcement1  4000        09:54:55 04 APR 2005
8     4601dbte1_82.bin Announcement2  8000        09:55:55 04 APR 2005
9     4602dbte1_82.bin Announcement3  16000       09:56:55 04 APR 2005
Nv-Ram:
Total bytes used: 28000
Total bytes free: 7344800
Total bytes capacity(fixed) 7372800
G450-001(super)# show announcements files brief
Mode: FTP-SERVER/SCP-CLIENT
ID     File
----  ----------------
5     46xxupgrade.scr
8     4601dbte1_82.bin
9     4602dbte1_82.bin
Nv-Ram:
Total bytes used: 28000
Total bytes free: 7344800
Total bytes capacity(fixed) 7372800
```

Related Commands

copy announcement-file scp, copy announcement-file usb, copy ftp announcement-file, copy scp announcement-file, copy usb announcement-file, erase announcement-file, rename announcement-file, show download announcement-file status, show upload announcement-file status

show download announcement-file status

Use the **show download announcement-file status** command to display the status of the download process of announcement files from the Voice Announcements Manager to the G450 announcement directory.

Syntax

show download announcement-file status

User Level

read-only

Context

general

Example

To display the status of the download process of announcement files:

(In this example, no download command has been issued.)

```
G450-001(super)# show download announcement-file status
Module #9
===========
No dest file for download operation - no download operation was done.
```

(In this example, a download command has been issued.)

```
G450-001(super)# show download announcement-file status
Module #9
===========
Module           : 9
Source file      : hellosource.wav
Destination file : hellodestination.wav
Host             : 135.64.102.64
Running state    : Idle
Failure display  : (null)
Last warning     : No-warning
Bytes Downloaded   : 7825
===========
```

Related Commands

copy announcement-file scp, copy announcement-file usb, copy ftp announcement-file, copy scp announcement-file, copy usb announcement-file, erase announcement-file, rename announcement-file, show announcements files, show upload announcement-file status

show upload announcement-file status

Use the **show upload announcement-file status** command to display the status of the upload process of announcement files from the G450 announcement directory to the Voice Announcements Manager.

Syntax

show upload announcement-file status

User Level

read-only

Context

general

Example

To display the status of the upload process of announcement files:

(In this example, an upload command has been issued and the upload succeeds.)

```
G450-001(super)# show upload announcement-file status
Module #9
===========
Module           : 9
Source file      : hellosource.wav
Destination file : d:\hellodestination.wav
Host             : 135.64.102.64
Running state    : Idle
Failure display  : (null)
Last warning     : No-warning
===========
```

(In this example, an upload command has been issued, but the upload fails.)

```
G450-001(super)# show upload announcement-file status
Module #9
===========
Module           : 9
Source file      : hellosource.wav
Destination file : d:\hellodestination.wav
Host             : 135.64.102.64
Running state    : Idle
Failure display  : SCP- Permission denied
Last warning     : No-warning
===========
```

(In this example, no upload command has been issued.)

```
G450-001(super)# show upload announcement-file status
Module #9
===========
No source file for upload operation - no upload operation was done.
```

Related Commands

copy announcement-file scp, copy announcement-file usb, copy ftp announcement-file, copy scp announcement-file, copy usb announcement-file, erase announcement-file, rename announcement-file, show announcements files, show download announcement-file status

ARP table

arp

Use the **arp** command to add a permanent entry to the Address Resolution Protocol (ARP) cache. Use the **no** form of this command to remove either a static entry or a dynamically learned entry from the ARP cache.

Syntax

arp *ip_address mac_address*

no arp *ip_address*

Parameters

Parameter	Description	Possible Values	Default Value
ip_address	IP address of the station		
mac_address	Corresponding MAC address for this station		

User Level

read-write

Context

general

Example

To add a permanent entry for station 192.168.7.8 to the ARP cache:

```
G450-001(super)# arp 192.168.7.8 00:40:0d:8c:2a:01
```

To remove an entry from the ARP cache for the station 192.168.13.76:

```
G450-001(super)# no arp 192.168.13.76
```

Related Commands

arp timeout, clear arp-cache, ip max-arp-entries, ip proxy-arp, show ip arp, show ip reverse-arp

arp timeout

Use the **arp timeout** command to configure the amount of time, in seconds, that an entry remains in the ARP cache. Entering the **arp timeout** command without a ***seconds*** parameter will display the current timeout value. Use the **no** form of this command to restore the default value (four hours).

Syntax

arp timeout [*seconds*]

no arp timeout

Parameters

Parameter	Description	Possible Values	Default Value
seconds	The number of seconds that an entry remains in the ARP cache	**60-604800**	**14400**

User Level

read-write

Context

general

Example

To set the ARP timeout to one hour:

```
G450-001(super)# arp timeout 3600
```

To restore the default value for ARP timeout:

```
G450-001(super)# no arp timeout
```

Related Commands

arp, clear arp-cache, ip max-arp-entries, ip proxy-arp, show ip arp, show ip reverse-arp

clear arp-cache

Use the **clear arp-cache** command to delete all dynamic entries from the ARP cache.

Syntax

clear arp-cache [*interface*|*vlan_id*|*ip_address*[*mask*]]

Parameters

Parameter	Description	Possible Values	Default Value
interface	The interface name for which to delete entries		
vlan_id	The VLAN ID for which to delete entries	**1-4090**	
ip_address	The host IP address to clear		
mask	The IP mask of the subnet to clear		

User Level

read-write

Context

general

Example

To flush all ARP entries:

```
G450-001(super)# clear arp-cache
Flushing all arp entries
Flushed 22 ARP entries.
```

To flush ARP entries for an interface named FastEthernet 10/2:

```
G450-001(super)# clear arp-cache "fastethernet 10/2"
Flushing ARP cache entries on ifName fastethernet 10/2
Flushed 1 ARP entries.
```

To flush ARP entries for one host address:

```
G450-001(super)# clear arp-cache 156.16.11.32
Flushing ARP cache entry of host 156.16.11.32
Flushed 0 ARP entries.
```

To flush a range of ARP entries belonging to one subnet:

```
G450-001(super)# clear arp-cache 156.3.2.33 255.255.255.0
Flushing ARP cache entries in the range [156.3.2.33, 255.255.255.0]
Flushed 0 ARP entries.
```

Related Commands

arp, arp timeout, ip max-arp-entries, ip proxy-arp, show ip arp, show ip reverse-arp

ip max-arp-entries

Use the **ip max-arp-entries** command to specify the maximum number of ARP cache entries allowed in the ARP cache. Use the **no** form of this command to restore the default value. In order for this command to take effect, you must copy the running configuration to the startup configuration and reset the device.

Syntax

ip max-arp-entries *value*

no ip max-arp-entries

Parameters

Parameter	Description	Possible Values	Default Value
value	The maximum number of entries allowed in the IP address table. When you decrease the number of entries, it may cause the table to be relearned more frequently. If you do not enter a value, the current ARP Cache size is displayed.	**128-16384**	**4096**

User Level

read-write

Context

general

Example

To set the maximum number of ARP cache entries to 8000:

```
G450-001(super)# ip max-arp-entries 8000
```

Related Commands

arp, arp timeout, clear arp-cache, ip proxy-arp, show ip arp, show ip reverse-arp

show ip arp

Use the **show ip arp** command to display the Address Resolution Protocol (ARP) cache.

Syntax

show ip arp [*interface*|*ip_interface*|*ip_addr*[*ip_mask*] | static]

Parameters

Parameter	Description	Possible Values	Default Value
interface	The interface name, in quotes	string (1-32 chars)	
ip_interface	The IP interface name, in quotes	string (1-32 chars)	
ip_addr	The IP address of the station(s)		
ip_mask	The IP mask of the routes		
static	Keyword that specifies to display static IP ARP information		

User Level

read-only

Context

general

Example

To display all ARP mappings:

```
G450-001(super)# show ip arp
```

To display one host ARP mapping:

```
G450-001(super)# show ip arp 192.168.49.1
```

To display a range of ARP mappings:

```
G450-001(super)# show ip arp 192.168.49.1 255.255.255.0
```

To display ARP mappings for the VLAN 1 interface:

```
G450-001(super)# show ip arp "Vlan 1"
```

To display static ARP mapping:

```
G450-001(super)# show ip arp static
```

Note:

When specifying an interface name that includes spaces, enclose the entire name in quotation marks (for example, “New York”).

Related Commands

arp, arp timeout, clear arp-cache, ip max-arp-entries, ip proxy-arp, show ip reverse-arp

show ip reverse-arp

Use the **show ip reverse-arp** command to display the IP address of a host, based on a known MAC address.

Syntax

show ip reverse-arp *mac_addr* [*match_len*]

Parameters

Parameter	Description	Possible Values	Default Value
mac_addr	The MAC address		
match_len	The number of bytes in the address to match		

User Level

read-only

Context

general

Example

To list IPs that match a specific MAC address:

```
G450-001(super)# show ip reverse-arp 00:10:a4:98:97:e0
Showing 1 rows
Address          MAC Address           I/F         Type      TTL
---------------- ----------------- ----------- ------- --------
149.49.70.68     00:10:a4:98:97:e0   e-70        Dynamic     14355
```

Related Commands

arp, arp timeout, clear arp-cache, ip max-arp-entries, ip proxy-arp, show ip arp

ASG authentication

copy auth-file ftp

Use the **copy auth-file ftp** command to copy the authentication file to a remote server using FTP.

Syntax

copy auth-file ftp *filename ip*

Parameters

Parameter	Description	Possible Values	Default Value
filename	File name with full path	string	
ip	IP address of the host	IP address	

User Level

admin

Context

general

Example

To copy the authorization file `auth-pass` to the host with IP address 192.168.49.10:

```
G450-001(super)# copy auth-file ftp auth-pass 192.168.49.10
```

Related Commands

copy auth-file scp, copy auth-file tftp, copy auth-file usb, copy ftp auth-file, copy scp auth-file, copy tftp auth-file, copy usb auth-file, erase auth-file, login authentication lockout, login authentication local-craft-password, login authentication response-time, login authentication services-login, ppp authentication, show auth-file info, show download auth-file status, show login authentication, show upload auth-file status

copy auth-file scp

Use the **copy auth-file scp** command to copy the authentication file to a remote server using SCP.

Syntax

copy auth-file scp *filename ip*

Parameters

Parameter	Description	Possible Values	Default Value
filename	File name with full path	string	
ip	IP address of the host	IP address	

User Level

admin

Context

general

Example

To copy the authorization file `auth-pass` to the host with IP address 192.168.49.10:

```
G450-001(super)# copy auth-file scp auth-pass 192.168.49.10
```

Related Commands

copy auth-file ftp, copy auth-file tftp, copy auth-file usb, copy ftp auth-file, copy scp auth-file, copy tftp auth-file, copy usb auth-file, erase auth-file, login authentication lockout, login authentication local-craft-password, login authentication response-time, login authentication services-login, ppp authentication, show auth-file info, show download auth-file status, show login authentication, show upload auth-file status

copy auth-file tftp

Use the **copy auth-file tftp** command to copy the authentication file to a remote server using TFTP.

Syntax

copy auth-file tftp *filename ip*

Parameters

Parameter	Description	Possible Values	Default Value
filename	File name with full path	string	
ip	IP address of the host	IP address	

User Level

admin

Context

general

Example

To copy the authorization file `auth-pass` to the host with IP address 192.168.49.10:

```
G450-001(super)# copy auth-file tftp auth-pass 192.168.49.10
```

Related Commands

copy auth-file ftp, copy auth-file scp, copy auth-file usb, copy ftp auth-file, copy scp auth-file, copy tftp auth-file, copy usb auth-file, erase auth-file, login authentication lockout, login authentication local-craft-password, login authentication response-time, login authentication services-login, ppp authentication, show auth-file info, show download auth-file status, show login authentication, show upload auth-file status

copy auth-file usb

Use the **copy auth-file usb** command to upload the authentication file from the gateway to the USB mass storage device.

Syntax

copy auth-file usb ***source-filename destination-usb-device*** **[*destination-filename*]**

Parameters

Parameter	Description	Possible Values	Default Value
source-filename	The logical name for the source file		
destination usb-device	The destination USB mass storage device	**usb-device0**	
destination-filename	The destination file name and path		

User Level

admin

Context

general

Example

To upload `auth-file.cfg` from the gateway to usb-device0:

```
G450-001(super)# copy auth-file usb auth-file.cfg usb-device0
```

Related Commands - ASG authentication

copy auth-file ftp, copy auth-file scp, copy auth-file tftp, copy ftp auth-file, copy scp auth-file, copy tftp auth-file, copy usb auth-file, erase auth-file, login authentication lockout, login authentication local-craft-password, login authentication response-time, login authentication services-login, ppp authentication, show auth-file info, show download auth-file status, show login authentication, show upload auth-file status

Related Commands

backup config usb, copy usb announcement-file, erase usb, restore usb, safe-removal usb, show backup status, show restore status, show usb

copy ftp auth-file

Use the **copy ftp auth-file** command to download an authentication file from a remote FTP server. The gateway prompts you for a username and password after you enter the command.

Syntax

copy ftp auth-file *filename ip*

Context

admin

Parameters

Parameter	Description	Possible Values	Default Value
filename	The name of the authentication file, including the full path		
ip	The IP address of the host		

User Level

read-write

Example

To download authentication file `AF-7000003638-06712-211123.xml` from the remote FTP server at IP address 195.123.49.54:

```
G450-001# copy ftp auth-file \firmware\AF-7000003638-060712-211123.xml
195.123.49.54
Confirmation - do you want to continue (Y/N)? y
Username: anonymous
Password:
Beginning download operation ...
This operation may take up to 20 seconds.
Please refrain from any other operation during this time.
```

Related Commands

copy auth-file ftp, copy auth-file scp, copy auth-file tftp, copy auth-file usb, copy scp auth-file, copy tftp auth-file, copy usb auth-file, erase auth-file, login authentication lockout, login authentication local-craft-password, login authentication response-time, login authentication services-login, ppp authentication, show auth-file info, show download auth-file status, show login authentication, show upload auth-file status

copy scp auth-file

Use the **copy scp auth-file** command to download an authentication file from a remote SCP server.

Syntax

copy scp auth-file *filename ip*

Context

general

Parameters

Parameter	Description	Possible Values	Default Value
filename	The name of the authentication file, including the full path		
ip	The IP address of the host		

User Level

admin

Example

To download authentication file `AF-7000003638-060712-211123.xml` from the host at IP address 195.123.49.54:

```
G450-001# copy scp auth-file \firmware\AF-7000003638-060712-211123.xml
195.123.49.54
Confirmation - do you want to continue (Y/N)? y
Username: anonymous
Password:
Beginning download operation ...
This operation may take up to 20 seconds.
Please refrain from any other operation during this time.
```

Related Commands

copy auth-file ftp, copy auth-file scp, copy auth-file tftp, copy auth-file usb, copy ftp auth-file, copy tftp auth-file, copy usb auth-file, erase auth-file, login authentication lockout, login authentication local-craft-password, login authentication response-time, login authentication services-login, ppp authentication, show auth-file info, show download auth-file status, show login authentication, show upload auth-file status

copy tftp auth-file

Use the **copy tftp auth-file** command to download an authentication file from a remote TFTP server.

Syntax

copy tftp auth-file *filename ip*

Context

general

Parameters

Parameter	Description	Possible Values	Default Value
filename	The name of the authentication file, including the full path		
ip	The IP address of the host		

User Level

admin

Example

To download authentication file `AF-70000036368-060712-211123.xml` from the host at IP address 195.123.49.54:

```
G450-001# copy tftp auth-file \firmware\AF-7000003638-060712-211123.xml
195.123.49.54
Confirmation - do you want to continue (Y/N)? y
Username: anonymous
Password:
Beginning download operation ...
This operation may take up to 20 seconds.
Please refrain from any other operation during this time.
```

Related Commands

copy auth-file ftp, copy auth-file scp, copy auth-file tftp, copy auth-file usb, copy ftp auth-file, copy scp auth-file, copy usb auth-file, erase auth-file, login authentication lockout, login authentication local-craft-password, login authentication response-time, login authentication services-login, ppp authentication, show auth-file info, show download auth-file status, show login authentication, show upload auth-file status

copy usb auth-file

Use the **copy usb auth-file** command to download an authentication file from the external USB mass storage device to the gateway.

Syntax

copy usb auth-file ***source-usb-device source-filename***

Parameters

Parameter	Description	Possible Values	Default Value
source usb-device	The source USB mass storage device	**usb-device0**	
source-filename	The full name and path of the file to be downloaded		

User Level

Admin

Context

general

Example

To download `auth-file.cfg` from usb-device0 to the gateway:

```
G450-001(super)# copy usb auth-file usb-device0 \temp\auth-file.cfg
```

Related Commands

backup config usb, copy announcement-file usb, erase usb, restore usb, safe-removal usb, show backup status, show restore status, show usb

Related Commands - ASG authentication

copy auth-file ftp, copy auth-file scp, copy auth-file tftp, copy auth-file usb, copy ftp auth-file, copy scp auth-file, copy tftp auth-file, erase auth-file, login authentication lockout, login authentication local-craft-password, login authentication response-time, login authentication services-login, ppp authentication, show auth-file info, show download auth-file status, show login authentication, show upload auth-file status

erase auth-file

Use the **erase auth-file** command to erase the G450 ASG authentication file.

Use this command only if you need to replace the current ASG authentication file with a new ASG authentication file that has a different ID. This command can only be used when directly connecting to the Console or Services port. If you use this command and replace the authentication file with a new file that has a different ID, make sure that the authentication file label on the gateway chassis is also replaced.

Syntax

erase auth-file *source-filename*

Parameters

Parameter	Description	Possible Values	Default Value
source-filename	The name of the ASG authentication file to delete		

User Level

admin

Context

general

Example

To erase the ASG authentication file `auth_file g450.lac`:

```
G450-001# erase auth_file g450.lac
```

Related Commands

copy announcement-file scp, copy announcement-file usb, copy ftp announcement-file, copy scp announcement-file, copy usb announcement-file, rename announcement-file, show announcements files, show download announcement-file status, show upload announcement-file status

Related Commands - ASG authentication

copy auth-file ftp, copy auth-file scp, copy auth-file tftp, copy auth-file usb, copy ftp auth-file, copy scp auth-file, copy tftp auth-file, copy usb auth-file, login authentication lockout, login authentication local-craft-password, login authentication response-time, login authentication services-login, ppp authentication, show auth-file info, show download auth-file status, show login authentication, show upload auth-file status

login authentication lockout

Use the **login authentication lockout** command to set a policy for locking out access to device administration service policy after successive failed login attempts. Use the **no login authentication lockout** command to return the lockout time and lockout attempt threshold to their default values.

Note:

As soon as you use the **login authentication lockout** command, the new lockout settings immediately override previous settings, for all user accounts.

Syntax

[no] login authentication lockout *time* attempt *count*

Parameters

Parameter	Description	Possible Values	Default Value
time	The lockout time, in seconds	**30-3600** **0** disables the timeout function	**180**
count	The number of successive failed login attempts before account lockout is enforced	**1-10** **0** disables the timeout function	**3**

User Level

admin

Context

general

Example

To lockout Avaya Services access to the device for 360 seconds following 5 failed login attempts:

```
G450-001(super)# login authentication lockout 360 attempt 5
```

Related Commands

copy auth-file ftp, copy auth-file scp, copy auth-file tftp, copy auth-file usb, copy ftp auth-file, copy scp auth-file, copy tftp auth-file, copy usb auth-file, erase auth-file, login authentication local-craft-password, login authentication response-time, login authentication services-login, ppp authentication, show auth-file info, show download auth-file status, show login authentication, show upload auth-file status

login authentication local-craft-password

Use the **login authentication local-craft-password** command to enable Avaya Services login local craft authentication using a password (default). Use the **no** form of this command to disable Avaya Services login local craft authentication using a password.

Syntax

[no] login authentication local-craft-password

User Level

admin

Context

general

Example

To disable Avaya Services login local craft authentication using a password:

```
G450-001(super)# no login authentication local-craft-password
```

Related Commands

copy auth-file ftp, copy auth-file scp, copy auth-file tftp, copy auth-file usb, copy ftp auth-file, copy scp auth-file, copy tftp auth-file, copy usb auth-file, erase auth-file, login authentication lockout, login authentication response-time, login authentication services-login, ppp authentication, show auth-file info, show download auth-file status, show login authentication, show upload auth-file status

login authentication response-time

Use the **login authentication response-time** command to set the time the system waits for user response to authentication requests before timing out a connection.
The system aborts the connection if no response is received within the defined response time period. Use the **no** form of the command to return the response time value to the factory default.

The time value you enter is used for both:

- The response time interval between the user name prompt and the user name entry
- The response time interval between the challenge prompt and the challenge response

Note:

The authentication response timeout is ignored by the gateway for the Console interface.

Syntax

[no] login authentication response-time *time*

Parameters

Parameter	Description	Possible Values	Default Value
time	The authentication response time period, in seconds, before timing out a connection	**30-3600** **0** disables the timeout function	**120**

User Level

admin

Context

general

Example

To timeout a connection if no response arrives within 120 seconds after an authentication request:

```
G450-001(super)# login authentication response-time 120
```

Related Commands

copy auth-file ftp, copy auth-file scp, copy auth-file tftp, copy auth-file usb, copy ftp auth-file, copy scp auth-file, copy tftp auth-file, copy usb auth-file, erase auth-file, login authentication lockout, login authentication local-craft-password, login authentication services-login, ppp authentication, show auth-file info, show download auth-file status, show login authentication, show upload auth-file status

login authentication services-login

Use the **login authentication services-login** command to enable Avaya Services login access. Use the **no** form of the command to disable all Avaya Services logins, including local craft password-based authentication.

Note:

By default, Avaya Services login access is enabled as soon as the Authentication File is downloaded to the gateway.

Syntax

[no] login authentication services-login

User Level

admin

Context

general

Example

To enable Avaya Services login:

```
G450-001(super)# login authentication services-login
```

Related Commands

copy auth-file ftp, copy auth-file scp, copy auth-file tftp, copy auth-file usb, copy ftp auth-file, copy scp auth-file, copy tftp auth-file, copy usb auth-file, erase auth-file, login authentication lockout, login authentication local-craft-password, login authentication response-time, ppp authentication, show auth-file info, show download auth-file status, show login authentication, show upload auth-file status

ppp authentication

Use the **ppp authentication** command to select the authentication method used when closing a PPP server or client session.

Note:

The value set for **ppp authentication** affects both the USB interface and the Console interface, simultaneously.

Syntax

ppp authentication {pap|chap|none|ras}

Parameters

Parameter	Description	Possible Values	Default Value
pap	Keyword indicating the Password Authentication Protocol. An unencrypted password is sent for authentication. This is the default.		
chap	Keyword indicating the Challenge Handshake Authentication Protocol. An encrypted password is sent for authentication.		
ras	Keyword indicating Remote Access Service mode is being used for authentication		
none	Keyword indicating that no password is sent		

User Level

read-write

Context

Interface: Console, USB-modem

Example

To select the CHAP authentication protocol:

```
G450-001(if:CON)# ppp authentication chap
```

Related Commands - ASG authentication

copy auth-file ftp, copy auth-file scp, copy auth-file tftp, copy auth-file usb, copy ftp auth-file, copy scp auth-file, copy tftp auth-file, copy usb auth-file, erase auth-file, login authentication lockout, login authentication local-craft-password, login authentication response-time, login authentication services-login, show auth-file info, show download auth-file status, show login authentication, show upload auth-file status

Related Commands - Modem configuration - USB modem port

interface usb-modem, async modem-init-string, async reset-modem (USB port), ip peer address, ppp chap-secret, shutdown (USB modem), timeout absolute

Related Commands - Modem configuration - Console port

interface console, async mode interactive, async mode terminal, async modem-init-string, async reset-modem (Console port), ip peer address, ppp chap-secret, shutdown (interface), speed (PPP), timeout absolute

show auth-file info

Use the **show auth-file info** command to view information about the ASG authentication file.

Syntax

show auth-file info

User Level

admin

Context

general

Example

To view information about the ASG authentication file:

```
G450-001(super)# show auth-file info
Authentication File (AF) information:
AF-ID :7000012345
Date/time : 15:02:27 27-SEP-2005
Major release : 4
```

Related Commands

copy auth-file ftp, copy auth-file scp, copy auth-file tftp, copy auth-file usb, copy ftp auth-file, copy scp auth-file, copy tftp auth-file, copy usb auth-file, erase auth-file, login authentication lockout, login authentication local-craft-password, login authentication response-time, login authentication services-login, ppp authentication, show download auth-file status, show login authentication, show upload auth-file status

show download auth-file status

Use the **show download auth-file status** command to display the status of the download process of the authentication file to the device.

Syntax

show download auth-file status

User Level

read-only

Context

general

Example

To display the status of the download process of the authentication file to the device:

```
G450-001(super)# show download auth-file status
Module #10
===========
Module           : 10
Source file      : AF-7000003277-060926-211040.xml
Destination file : auth-file
Host             : 149.49.71.50
Running state    : Idle
Failure display  : (null)
Last warning     : No-warning
Bytes Downloaded : 1242
```

Related Commands

copy auth-file ftp, copy auth-file scp, copy auth-file tftp, copy auth-file usb, copy ftp auth-file, copy scp auth-file, copy tftp auth-file, copy usb auth-file, erase auth-file, login authentication lockout, login authentication local-craft-password, login authentication response-time, login authentication services-login, ppp authentication, show auth-file info, show login authentication, show upload auth-file status

show login authentication

Use the **show login authentication** command to view the login authentication settings and information.

Syntax

show login authentication

User Level

admin

Context

general

Example

To view the login authentication settings and information:

```
G450-001(super)# show login authentication
Services logins: On
Local craft: On
Lockout time: 180 seconds
Lockout attempt threshold: 3
Authentication response time: 120 seconds
CLI logout timeout: Off
Inactivity period:  90 days
Password expiration period Off
Min password length: 10
Min lower case chars: 1
Min upper case chars: 0 (default)
Min digit chars: 1
Min special chars: 0 (default)
```

Related Commands

copy auth-file ftp, copy auth-file scp, copy auth-file tftp, copy auth-file usb, copy ftp auth-file, copy scp auth-file, copy tftp auth-file, copy usb auth-file, erase auth-file, login authentication lockout, login authentication local-craft-password, login authentication response-time, login authentication services-login, ppp authentication, show auth-file info, show download auth-file status, show upload auth-file status

show upload auth-file status

Use the **show upload auth-file status** command to view the status of the upload operation of an authentication file.

Syntax

show upload auth-file status

User Level

read-only

Context

general

Example

To view the status of the upload operation of an authentication file:

(In this example, an upload command has been issued and the upload succeeds.)

```
G450-001(super)# Show upload auth-file status
Module #10
===========
Module           : 10
Source file      : auth-file
Destination file : 444
Host             : 135.64.102.114
Running state    : Idle
Failure display  : (null)
Last warning     : No-warning
```

(In this example, an upload command has been issued, but the upload fails.)

```
G450-001(super)# Show upload auth-file status
Module #10
===========
Module           : 10
Source file      : auth-file.
Destination file : d:\zion\run.cfg
Host             : 135.64.102.39
Running state    : Idle
Failure display  : SCP - Permission denied
Last warning     : No-warning
```

(In this example, no upload command has been issued.)

```
G450-001(super)# show upload auth-file status
Module #10
===========
No source file for upload operation - no upload operation was done.
```

Related Commands

copy auth-file ftp, copy auth-file scp, copy auth-file tftp, copy auth-file usb, copy ftp auth-file, copy scp auth-file, copy tftp auth-file, copy usb auth-file, erase auth-file, login authentication lockout, login authentication local-craft-password, login authentication response-time, login authentication services-login, ppp authentication, show auth-file info, show download auth-file status, show login authentication

username

Use the **username** command to add a local user account. Use the **no** form of the command to remove the user account from the system.

By default there is only a single user account, named **root**, with password **root**, which accesses the administrator level. You cannot delete this basic user account, nor modify its access level. However, you can modify its basic password.

Note:

For security reasons, you should change the **root** password immediately.

Syntax

username *name* [password *passwd* | asg-secret *secret*] access-type *access_type*

no username *name*

Parameters

Parameter	Description	Possible Values	Default Value
name	New user name or **dadmin**	minimum four character string	
passwd	User's password	minimum eight character string	
secret	ASG secret key of a dadmin user	32 hexadecimal characters	
access_type	Access type definition	**read-only**, **read-write**, **admin** **Note:** A dadmin user and a root user must be assigned an **admin** access type.	

User Level

admin

Context

general

Example

To create a new user account with username john, password johnnysm, and a read-write access:

```
G450-001(super)# username john password johnnysm access-type read-write
User account added.
```

To change the password of the root user:

```
G450-001(super)# username root password mysecret access-type admin
User account modified.
```

Note:

You cannot change the access type of the root user:

```
G450-001(super)# username root password verysecret access-type read-write
ERROR: User account root has always an administrator access type.
```

Note:

If you wish to define a username which includes spaces, you must enclose the entire name in quotation marks, for example “new york”.

Related Commands

login authentication lockout, show username

Auxiliary files

set web aux-files-url

Use the **set web aux-files-url** command to specify the URL of the Web server containing the online help files and Java plug-in.

Syntax

set web aux-files-url *url*

Parameters

Parameter	Description	Possible Values	Default Value
url	The IP address and directory name of the Web server		

User Level

read-write

Context

general

Example

To set the URL of the Web server to 176.2.3.66/DMweb:

```
G450-001(super)# set web aux-files-url http://176.2.3.66/DMweb
```

Related Commands

show web aux-files-url

show web aux-files-url

Use the **show web aux-files-url** command to display the URL of the Web server containing online help files and the Java plug-in.

Syntax

show web aux-files-url

User Level

read-only

Context

general

Example

To display the URL of the Web server:

```
G450-001(super)# show web aux-files-url
the web aux-files-url is http://176.2.3.66/DMweb
```

Related Commands

set web aux-files-url

Backing up the gateway to a USB device

backup config usb

Use the **backup config usb** command to back up the gateway configuration to a USB mass storage device.

Syntax

backup config usb *usb-device backup-name*

Parameters

Parameter	Description	Possible Values	Default Value
usb-device	The destination USB mass storage device	**usb-device0**	
backup-name	The destination backup database path and file name on the USB device	string of up to 64 characters	

User Level

read-write

Context

general

Example

To back up the gateway configuration in the form of file `gatewaybackup1` to usb-device0:

```
G450-001(super)# backup config usb usb-device0 gatewaybackup1
```

Related Commands

copy announcement-file usb, copy usb announcement-file, erase usb, restore usb, safe-removal usb, show backup status, show restore status, show usb

show backup status

Use the **show backup status** command to display information regarding the status of a backup of the gateway configuration to a USB mass storage device.

Syntax

show backup status

User Level

read-only

Context

general

Example

To display information regarding the status of a backup:

```
G450-001(super)# show backup status
```

Backup operation in progress. Do not remove usb mass storage device until the end of operation.

```
Files backup:
Type              FileName            Status
------            ----------------    -----------
Startup-config    startup-config.cfg  OK
```

Related Commands

backup config usb, copy announcement-file usb, copy usb announcement-file, erase usb, restore usb, safe-removal usb, show restore status, show usb

Backup interfaces

backup delay

Use the **backup delay** command to set the time to wait before switching to the backup interface, in case of failure.

Syntax

backup delay *failure_delay secondary_disable_delay*

Parameters

Parameter	Description	Possible Values	Default Value
failure_delay	The delay before switching to the backup interface, in seconds	**0-3600**	0
secondary_disable_delay	The delay before reverting to the primary interface, in seconds	**0-3600**	0

User Level

read-write

Context

interface:FastEthernet (L2, L2-L3), Serial (DS1 PPP L2, DS1 PPP L2-L3, DS1 FR L2, DS1 FR-SUB L2, DS1 FR-SUB L2-L3, USP FR L2, USP PPP L2, USP PPP L2-L3), Tunnel (L2, L2-L3)

Example

To switch over immediately to the backup interface, in case of failure, and pause 60 seconds before reverting to the primary interface:

```
G450-001(if:FastEthernet 10/2)# backup delay 0 60
```

Related Commands

backup interface

backup interface

Use the **backup interface** command to set a backup interface for the current interface.

Syntax

backup interface *interface_type interface_number*

Parameters

Parameter	Description	Possible Values	Default Value
interface_type	The type of interface	**Serial**, **FastEthernet**, **Dialer**	
interface_number	The interface number		

User Level

read-write

Context

interface:FastEthernet (L2, L2-L3), Serial (DS1 PPP L2, DS1 PPP L2-L3, DS1 FR L2, DS1 FR-SUB L2, DS1 FR-SUB L2-L3, USP FR L2, USP PPP L2, USP PPP L2-L3), Tunnel (L2, L2-L3), Loopback

Example

To specify that Serial interface 3/1:1 is a backup interface for the current interface:

```
G450-001(if:Serial 3/1:2)# backup interface Serial 3/1:1
```

Related Commands

backup delay

Broadcast relay

ip directed-broadcast

Use the **ip directed-broadcast** command to enable net-directed broadcast forwarding. Use the **no** form of this command to disable net-directed broadcasts on an interface.

Syntax

[no] ip directed-broadcast

User Level

read-write

Context

interface:Serial (DS1 PPP L2-L3, DS1 PPP L3, DS1 FR-SUB L2-L3, DS1 FR-SUB L3, USP PPP L2-L3, USP PPP L3), FastEthernet (L2-L3, L3, PPP L2, PPP L2-L3, PPP L3), Tunnel (L2-L3, L3), VLAN (L2-L3, L3), Dialer (L2, L2-L3, L3

Related Commands

interface fastethernet, interface serial, interface vlan, ip netbios-rebroadcast

ip netbios-rebroadcast

Use the **ip netbios-rebroadcast** command to enable the forwarding of NETBIOS packets on an interface. If no value is provided for ***direction***, the **both** option is applied as the default value.

Use the **no** form of this command to disable forwarding of NETBIOS packets on an interface.

Syntax

ip netbios-rebroadcast [*direction*]

no ip netbios-rebroadcast

Parameters

Parameter	Description	Possible Values	Default Value
direction	The NETBIOS rebroadcasts mode	**both** - NETBIOS packets received on the interface are rebroadcast to other interfaces and NETBIOS packets received on other interfaces are rebroadcast to this interface. **disable** - NETBIOS packets are not rebroadcast in or out of this interface.	**both**

User Level

read-write

Context

interface:Serial (DS1 PPP L2-L3, DS1 PPP L3, DS1 FR-SUB L2-L3, DS1 FR-SUB L3, USP PPP L2-L3, USP PPP L3), FastEthernet (L2-L3, L3, PPP L2, PPP L2-L3, PPP L3), Tunnel (L2-L3, L3), VLAN (L2-L3, L3), Dialer (L2, L2-L3, L3)

Example

To enable rebroadcasting of NETBIOS packets received by and sent from the FastEthernet interface:

```
G450-001(if:FastEthernet 10/2)# ip netbios-rebroadcast both
```

Related Commands

interface fastethernet, interface serial, interface vlan, ip directed-broadcast

CAM table

clear cam

Use the **clear cam** command to delete all entries from the Contents Address Memory (CAM) table.

Syntax

clear cam

User Level

read-write

Context

general

Example

To clear the CAM table:

```
G450-001(super)# clear cam
CAM table cleared.
```

Related Commands

show cam, show cam mac

show cam

Use the **show cam** command to display the CAM table entries for a specific module and port. If no module or port is specified, the system displays all CAM table entries.

Note:
MACs associated with LAGs appear under the LAG ID, not under the LAG port.

Syntax

show cam [*module*[/*port*]]

Parameters

Parameter	Description	Possible Values	Default Value
module	Number of the module		
port	Number of the port on the module		

User Level

read-only

Context

general

Example

To display the CAM table entries for module 3 of port 33:

```
G450-001(super)# show cam 3/33
Total Matching CAM Entries Displayed = 128
Dest MAC/Route Dest vlan Destination Ports
------------------- ---- -----------------
08:00:20:c6:98:5f    1     3/33
08:00:20:c4:c8:51    1     3/33
00:00:5e:00:01:02    1     3/33
00:01:02:de:96:2f    1     3/33
00:02:2d:47:18:67    1     3/33
00:02:2d:48:18:29    1     3/33
00:04:0d:01:b0:00    1     3/33
...
```

Related Commands

clear cam, show cam mac

---

show cam mac

Use the **show cam mac** command to display a specific mac entry in the CAM table.

Syntax

show cam mac ***mac_addressic***

Parameters

Parameter	Description	Possible Values	Default Value
mac_address	The MAC entry to display		

User Level

read-only

Context

general

Example

To display all entries that match the MAC address 00:40:c2:00:66:b0:

```
G450-001(super)# show cam mac 00:40:c2:00:66:b0
```

Related Commands

clear cam, show cam

CDR file

copy cdr-file ftp

Use the **copy cdr-file ftp** command to copy a Call Detail Recording (CDR) file to a remote server using FTP.

Syntax

copy cdr-file ftp *filename ip*

Parameters

Parameter	Description	Possible Values	Default Value
filename	File name with full path	string	
ip	IP address of the host	IP address	

User Level

admin

Context

general

Example

To copy the authorization file `cdr1` to the host with IP address 192.168.49.10:

```
G450-001(super)# copy cdr-file ftp cdr1 192.168.49.10
```

Related Commands

copy cdr-file scp, copy cdr-file tftp, copy announcement-file usb, show upload cdr-file status

copy cdr-file scp

Use the **`copy cdr-file scp`** command to copy a Call Detail Recording (CDR) file to a remote server using SCP.

Syntax

`copy cdr-file scp` ***`filename ip`***

Parameters

Parameter	Description	Possible Values	Default Value
`filename`	File name with full path	string	
`ip`	IP address of the host	IP address	

User Level

admin

Context

general

Example

To copy the authorization file `cdr1` to the host with IP address 192.168.49.10:

```
G450-001(super)# copy cdr-file scp cdr1 192.168.49.10
```

Related Commands

copy cdr-file ftp, copy cdr-file tftp, copy announcement-file usb, show upload cdr-file status

copy cdr-file tftp

Use the **copy cdr-file tftp** command to copy a Call Detail Recording (CDR) file to a remote server using TFTP.

Syntax

copy cdr-file tftp *filename ip*

Parameters

Parameter	Description	Possible Values	Default Value
filename	File name with full path	string	
ip	IP address of the host	IP address	

User Level

admin

Context

general

Example

To copy the authorization file `cdr1` to the host with IP address 192.168.49.10:

```
G450-001(super)# copy cdr-file tftp cdr1 192.168.49.10
```

Related Commands

copy cdr-file ftp, copy cdr-file scp, copy announcement-file usb, show upload cdr-file status

copy cdr-file usb

Use the **copy cdr-file usb** command to upload a Call Detail Recording (CDR) file from the gateway to the USB mass storage device.

Syntax

copy cdr-file usb ***source-filename destination-usb-device*** **[*destination-filename*]**

Parameters

Parameter	Description	Possible Values	Default Value
source-filename	The logical name for the source file		
destination usb-device	The destination USB mass storage device	**usb-device0**	
destination-filename	The destination file name and path		

User Level

admin

Context

general

Example

To upload cdr1 from the gateway to usb-device0:

```
G450-001(super)# copy cdr-file usb cdr1 usb-device0
```

Related Commands

backup config usb, copy usb announcement-file, erase usb, restore usb, safe-removal usb, show backup status, show restore status, show usb

show upload cdr-file status

Use the **show upload cdr-file status** command to view the status of the upload of a CDR file.

Syntax

show upload cdr-file status

User Level

read-only

Context

general

Example

To view the status of the upload of a CDR file:

(In this example, an upload command has been issued and the upload succeeds.)

```
G450-001(super)# Show upload cfr-file status
Module #10
===========
Module           : 10
Source file      : cdr file
Destination file : 444
Host             : 135.64.102.114
Running state    : Idle
Failure display  : (null)
Last warning     : No-warning
```

(In this example, an upload command has been issued, but the upload fails.)

```
G450-001(super)# Show upload cdr-file status
Module #10
===========
Module           : 10
Source file      : cdr file.
Destination file : d:\zion\run.cfg
Host             : 135.64.102.39
Running state    : Idle
Failure display  : SCP - Permission denied
Last warning     : No-warning
```

(In this example, no upload command has been issued.)

```
G450-001(super)# show upload cdr-file status
Module #10
===========
No source file for upload operation - no upload operation was done.
```

Related Commands

copy cdr-file ftp, copy cdr-file scp, copy cdr-file tftp, copy announcement-file usb

CLI sessions

exit

Use the **exit** command to exit the current context. If you are in the root context, the **exit** command logs you out of the system.

Syntax

exit

User Level

read-only

Context

all

Example

To exit the rule 22 configuration context, and then the access-control-list 330 context:

```
G450-001(ACL 330/ip rule 22)# exit
G450-001(ACL 330)# exit
G450-001(super)#
```

Related Commands

reset, set logout, show logout

reset

Use the **reset** command to reset a specified system resource. The command performs a hard reset of the specified entity, returning any selectable parameters to their startup configuration values and setting all hardware and firmware to a known state.

Note:

If the Supervisor modules are in Active/Standby configuration, resetting the active supervisor causes the standby supervisor to take over and become active.

Note:

The reset command does not work while the configuration is being saved.

Note:

If a reset command is issued while a backup or restore operation is in progress, a query displays, inquiring whether you wish to reset. If the gateway is reset while a backup or restore operation is in progress, the backup/restore operation fails.

Syntax

reset [module *module_number* | voip | chassis]

Parameters

Parameter	Description	Possible Values	Default Value
module	Keyword indicating to reset a module		
module_number	The module to reset		
voip	Keyword indicating to reset the VoIP engine		
chassis	Keyword indicating to reset the gateway and all its media modules		

User Level

read-write

Context

general

Example

To reset the VoIP engine:

```
G450-001(super)# reset voip
This command will perform a hard reset.
Do you want to continue (Y/N)? y
```

Related Commands

exit, set logout, show logout

retstatus

Use the **retstatus** command to show whether or not the last CLI command you performed was successful.

Syntax

retstatus

User Level

read-only

Context

general

Example

To display the status of the most recently executed command:

```
G450-001(super)# retstatus
Succeeded
G450-001(super)# retstatus
Failed
```

set logout

Use the **set logout** command to set the number of minutes until the system automatically disconnects an idle session.

Syntax

set logout [*timeout*]

Parameters

Parameter	Description	Possible Values	Default Value
timeout	Number of minutes until the system automatically disconnects an idle session. Setting the value to 0 disables the automatic disconnection of idle sessions.	**0-99**	**15**

User Level

read-write

Context

general

Example

To set the system to disconnect idle sessions automatically after 20 minutes:

```
G450-001(super)# set logout 20
```

To disable the automatic disconnection of idle sessions:

```
G450-001(super)# set logout 0
```

Related Commands

exit, reset, show logout

---

show logout

Use the **show logout** command to display the amount of time in minutes the terminal remains idle before timing out. If the logout value is 0, there is no timeout limit. The default logout value is 15 minutes.

Syntax

show logout

User Level

read-only

Context

general

Example

To display the timeout value:

```
G450-001(super)# show logout
CLI timeout is 15 minutes
```

Related Commands

exit, reset, set logout

---

tech

Use the **tech** command to enter tech mode, where additional tech-related commands are available.

Note:

This command is reserved for service personnel use only.

Syntax

tech

User Level

tech

Context

general

Example

To enter tech mode:

```
G450-001(super)# tech
Password:
G450-001(tech)#
```

---

tree

Use the **tree** command to display the commands that are available at your current location in the CLI hierarchy. All commands are listed alphabetically.

Syntax

tree *depth*

Parameters

Parameter	Description	Possible Values	Default Value
depth	The level of depth at which to display the list of CLI commands		

User Level

read-only

Context

general

Example

To display the list of available commands to two levels:

```
G450-001(super)# tree 2
> arp
> arp timeout
> banner login
  banner login > line
> banner post-login
  banner post-login > line
--type q to quit or space key to continue--
```

CNA test plugs

cna testplug

The G450 features one CNA test plug, which has its own CNA configuration context. Use the **cna testplug** command to enter the CNA test plug configuration context.

Syntax

cna testplug 1

User Level

read-write

Context

general

Example

To enter the test plug context:

```
G450-001# cna testplug 1
G450-001(cna-testplug 1)#
```

Related Commands

clear counters (CNA test plugs), cna-testplug-service, control-port, fingerprint, rtp-echo-port, rtp-test-port, scheduler, show cna testplug, shutdown (CNA test plugs), test-rate-limit

clear counters (CNA test plugs)

Use the **clear counters** command to clear the CNA test plug counters.

Syntax

clear counters

User Level

read-write

Context

cna-testplug

Example

To clear CNA test plug counters on testplug 1:

```
G450-001(cna-testplug 1)# clear counters
```

Related Commands

cna testplug, cna-testplug-service, control-port, fingerprint, rtp-echo-port, rtp-test-port, scheduler, show cna testplug, shutdown (CNA test plugs), test-rate-limit

control-port

Use the **control-port** command to set the UDP port on which the CNA test plug listens for test requests from schedulers. Use the **no** form of the command to return to the default control port.

Syntax

control-port ***port***

no control port

Parameters

Parameter	Description	Possible Values	Default Value
port	The UDP port number to be used as the control port	**1-65535**	**8888**

User Level

read-write

Context

cna-testplug

Example

To set the control port to port number 12843:

```
G450-001(cna-testplug 1)# control-port 12843
```

Related Commands

clear counters (CNA test plugs), cna testplug, cna-testplug-service, fingerprint, rtp-echo-port, rtp-test-port, scheduler, show cna testplug, shutdown (CNA test plugs), test-rate-limit

fingerprint

Use the **fingerprint** command to configure the certificate fingerprint used by the CNA test plug to authenticate the CNA scheduler.

Syntax

fingerprint ***string***

Parameters

Parameter	Description	Possible Values	Default Value
string	A 59 character string, consisting of 2-character hex values separated by ':'		

User Level

read-write

Context

cna-testplug

Example

To set the certificate fingerprint for the CNA test plug:

```
G450-001(cna-testplug 1)#
fingerprint A3:45:37:4D:CF:A3:45:37:4D:CF:A3:45:37:4D:CF:....
```

Related Commands

clear counters (CNA test plugs), cna testplug, cna-testplug-service, control-port, rtp-echo-port, rtp-test-port, scheduler, show cna testplug, shutdown (CNA test plugs), test-rate-limit

rtp-echo-port

Use the **rtp-echo-port** command to set the UDP port used by the CNA test plug to listen for RTP streams send by other test plugs running RTP tests. Use the **no** form of the command to return the RTP echo port to its default.

Syntax

rtp-echo-port ***port***

Parameters

Parameter	Description	Possible Values	Default Value
port	The UDP port number to be used as the RTP echo port number	**1-65535**	**8888**

User Level

read-write

Context

cna-testplug

Example

To set the RTP echo port to port 45230:

```
G450-001(cna-testplug 1)# rtp-echo-port 45230
```

Related Commands

clear counters (CNA test plugs), cna testplug, cna-testplug-service, control-port, fingerprint, rtp-test-port, scheduler, show cna testplug, shutdown (CNA test plugs), test-rate-limit

rtp-test-port

Use the **rtp-test-port** command to set the UDP port used by the CNA test plug to send an RTP stream to another test plug in an RTP test. Use the **no** form of the command to return to the default UDP port for RTP tests.

Syntax

rtp-test-port ***port***

no rtp-test-port

Parameters

Parameter	Description	Possible Values	Default Value
port	The UDP port number to be used as the RTP test port	**1-65535**	**8887**

User Level

read-write

Context

cna-testplug

Example

To set the RTP test port to 65120:

```
G450-001(cna-testplug 1)# rtp-test-port 65120
```

Related Commands

clear counters (CNA test plugs), cna testplug, cna-testplug-service, control-port, fingerprint, rtp-echo-port, scheduler, show cna testplug, shutdown (CNA test plugs), test-rate-limit

scheduler

Use the **scheduler** command to add a scheduler's IP address to the list of schedulers with which the test plug can attempt to register. You can list up to five schedulers. The test plug attempts to register with the scheduler highest on the list, and moves along the list if necessary until registration is successful.

You can specify the TCP registration port, the port used by the test plug to request registration and send registration parameters to a scheduler. By default, the TCP registration port is 8888.

Use the **no** form of the command to clear one of the scheduler addresses.

Syntax

scheduler *index scheduler-address*[:*port*]

no scheduler ***index***

Parameters

Parameter	Description	Possible Values	Default Value
index	An index in the scheduler list. Scheduler 1 is the first scheduler attempted by the test plug for registration.	**1-5**	
scheduler-address	The IP address of a scheduler		
port	The TCP registration port number	**1-65535**	**8888**

User Level

read-write

Context

cna-testplug

Example

To add the scheduler whose IP address is 124.12.221.43 to the fourth place in the scheduler list:

```
G450-001(cna-testplug 1)# scheduler 4 124.12.221.43
```

Related Commands

clear counters (CNA test plugs), cna testplug, cna-testplug-service, control-port, fingerprint, rtp-echo-port, rtp-test-port, show cna testplug, shutdown (CNA test plugs), test-rate-limit

shutdown (CNA test plugs)

Use the **shutdown** command to disable the CNA test plug. Use the **no** form of the command to enable the CNA test plug. By default, the test plug is enabled.

Syntax

[no] shutdown

User Level

read-write

Context

cna-testplug

Example

To enable the test plug:

```
G450-001(cna-testplug 1)# no shutdown
```

Related Commands

clear counters (CNA test plugs), cna testplug, cna-testplug-service, control-port, fingerprint, rtp-echo-port, rtp-test-port, scheduler, show cna testplug, test-rate-limit

test-rate-limit

Use the **test-rate-limit** command to configure the CNA test rate limiter. The CNA test rate limiter sets the maximum rate of tests that can be run by the CNA test plug embedded in the G450. Use the **no** form of the command to return the CNA test rate limiter to its default configuration.

Syntax

test-rate-limit *maxTests interval*

Parameters

Parameter	Description	Possible Values	Default Value
maxTests	The maximum number of tests allowed in an interval. Zero means no limit.	**0-10000**	**60**
interval	The rate limiter interval, in seconds	**1-1000**	**10**

User Level

read-write

Context

cna-testplug

Example

To set the CNA test rate limit to 70 tests every 20 seconds:

```
G450-001(cna-testplug 1)# test-rate-limit 70 20
```

Related Commands

clear counters (CNA test plugs), cna testplug, cna-testplug-service, control-port, fingerprint, rtp-echo-port, rtp-test-port, scheduler, show cna testplug, shutdown (CNA test plugs)

cna-testplug-service

Use the **cna-testplug-service** command to enable the CNA test plug service on the gateway. Use the **no** form of the command to disable CNA test plug service on the gateway. In order to enable the test plug, both the test plug and the test plug service must be enabled. Use the **shutdown** and **no shutdown** commands in the test plug context to disable/enable the test plug itself.

Syntax

cna-testplug-service

User Level

admin

Context

general

Example

To enable the CNA test plug service:

```
G450-001# cna-testplug-service
The Converged Network Analyzer test plug is enabled.
```

Related Commands

clear counters (CNA test plugs), cna testplug, control-port, fingerprint, rtp-echo-port, rtp-test-port, scheduler, show cna testplug, shutdown (CNA test plugs), test-rate-limit

show cna testplug

Use the **show cna testplug** command to display CNA test plug configuration and statistics.

Syntax

show cna testplug

User Level

read-only

Context

cna-testplug

Example

To display the CNA test plug configuration and statistics:

```
G450-001(cna-testplug 1)# show cna testplug
CNA testplug 1 is up, test-plug status is running a test
Address 149.49.54.114, bind to PMI, ID 00:04:0d:6d:30:48
Scheduler list:
   1: 135.64.102.76:50002 (current)
   5: 135.64.105.3:50002
Ports: Control 8889,  RTP-test 8888,  RTP-echo 8887
Test rate limiter: Maximum 60 tests in 10 seconds
Last Test: rtp to 149.49.54.114, scheduler: 135.64.102.76:50002
   Result: RTP echo started
Test                 Count        Failed       Cancelled
----------           ------       ------       ---------
traceroute           1            0            0
rtp                  66           0            0
ping                 0            0            0
tcpconnect           0            0            0
merge                0            0            0
```

Output fields

Name	Description
test plug 1 is...	The status of the test plug service. Possible values are: • **up**. The test plug is up. • **down**. The test plug is down due to lack of success registering or a configuration error. • **administratively down**. The test plug is configured as down.

1 of 3

Name	Description
test-plug status	The registration status of the test plug. Possible values are: • **test-plug is unregistered**. The test plug is attempting to register and is currently unregistered. • **test-plug is unregistered (scheduler list exhausted)**. The test plug has exhausted its scheduler list at least once, and is now attempting to register. • **test-plug is idle**. The test plug is registered but not currently running a test. • **test-plug is running a test**. The test plug is running a test. • **test-plug is suspended**. The test plug is suspended by its test rate limiter. • **test-plug configuration error (no IP address)**. No IP address is configured for the test plug interface. • **test-plug configuration error (bad IP address)**. The configured test plug address is not configured for the test plug interface. • **test-plug configuration error (scheduler list empty)**. The scheduler list is empty, and, therefore, the test plug is disabled. • **test-plug control port binding error**. The test plug cannot bind the UDP control port. • **test-plug RTP port binding error**. The test plug cannot bind the RTP test UDP port.
Address	The IP address of the test plug interface
bind to PMI	States that the PMI is the test plug's IP address
ID	The MAC address of the G450, used to identify the test plug
Scheduler list	The list of up to five IP addresses of schedulers with which the test plug can attempt to register
Ports:	
Control	The control port number. The UDP port on which the CNA test plug listens for test requests from the current scheduler.
RTP-test	The UDP port from which the CNA test plug send RTP streams to another test plug when running an RTP test
RTP-echo	The RTP echo port number. The UDP port on which the CNA test plug listens for RTP streams sent by other test plugs running RTP tests.

2 of 3

Name	Description
Test rate limiter	The configuration of the CNA test rate limiter
Last Test	The current or last test performed by the test plug. Possible values: • **none**. No test has been performed since the test plug was up. • **traceRoute**. The current/last test performed is/was a traceroute test. • **rtp**. The current/last test performed is/was an RTP test. • **ping**. The current/last test performed is/was a ping test. • **tcpConnect**. The current/last test performed is/was a TCPConnect test. • **merge**. The current/last test performed is/was a merge test.
Result	The results of the last test run
Test	The types of tests
Count	The number of tests of each type that was run since the test plug was up
Failed	The number of tests of each type that failed
Cancelled	The number of tests of each type that was cancelled

3 of 3

Related Commands

clear counters (CNA test plugs), cna testplug, cna-testplug-service, control-port, fingerprint, rtp-echo-port, rtp-test-port, scheduler, shutdown (CNA test plugs), test-rate-limit

Configuration files

copy ftp startup-config

Use the **copy ftp startup-config** command to download a configuration file from an FTP server. The command prompts for the username and password.

Note:

After you download the configuration file, the new configuration is not active until you reset the device.

Syntax

copy ftp startup-config *filename ip*

Parameters

Parameter	Description	Possible Values	Default Value
filename	The file name on the FTP server		
ip	The IP address of the FTP server		

User Level

read-write

Context

general

Example

To download the configuration file `G450.img` from the FTP server at IP address 135.64.10.33 using login dan:

```
G450-001(super)# copy ftp startup-config G450.img 135.64.10.33
Username: dan
Password:
G450-001(super)# reset
```

Related Commands

copy running-config ftp, copy running-config scp, copy running-config startup-config, copy running-config tftp, copy startup-config ftp, copy startup-config scp, copy startup-config tftp, copy tftp startup-config, erase startup-config, nvram initialize, show copy status, show download status, show erase status, show logging file condition, show running-config, show startup-config

copy running-config ftp

Use the **copy running-config ftp** command to upload the current configuration to a file on an FTP server. The command prompts for the username and password. Uncommitted changes to the configuration are included.

Note:

After you change the configuration, run the **copy running-config startup-config** command to save the changes. If you do not save the changes, the device loses the changes when you reset it.

Syntax

copy running-config ftp *filename ip*

Parameters

Parameter	Description	Possible Values	Default Value
filename	File name to create on the FTP server		
ip	IP address of the FTP server		

User Level

read-write

Context

general

Example

To upload the current configuration to `G450.cfg` on the ftp server at IP address 135.64.10.33 using login dan:

```
G450-001(super)# copy running-config ftp c:\config_files\router1.cfg
135.64.10.33
Username: dan
Password:
```

Related Commands

copy ftp startup-config, copy running-config scp, copy running-config startup-config, copy running-config ftp, copy running-config tftp, copy startup-config ftp, copy startup-config scp, copy startup-config tftp, copy tftp startup-config, erase startup-config, nvram initialize, show copy status, show download status, show erase status, show logging file condition, show running-config, show startup-config

copy running-config scp

Use the **copy running-config scp** command to upload the current configuration using the SCP secure protocol. The command prompts for the username and password. Uncommitted changes to the configuration are included.

Note:

After you change the configuration, run the **copy running-config startup-config** command to save the changes. If you do not save the changes, the device loses the changes when you reset it.

Syntax

copy running-config scp *filename ip*

Parameters

Parameter	Description	Possible Values	Default Value
filename	File name to create on the SCP server		
ip	IP address of the SCP server		

User Level

read-write

Context

general

Example

To upload `router.cfg` to the SCP at IP address 192.168.49.10 using login dan:

```
G450-001(super)# copy running-config scp c:\config_files\router1.cfg
192.168.49.10
Username: dan
Password:
```

Related Commands

copy ftp startup-config, copy running-config startup-config, copy running-config tftp, copy startup-config ftp, copy startup-config scp, copy startup-config tftp, copy tftp startup-config, erase startup-config, nvram initialize, show copy status, show download status, show erase status, show logging file condition, show running-config, show startup-config

copy running-config startup-config

Use the **copy running-config startup-config** command to commit the current configuration, including Standard Local Survivability (SLS) data, to NVRAM.

When a gateway powers up, SLS is disabled by default. However, if the gateway resets because of a CLI command, a software timeout, etc. and the **copy running-config startup-config** command has not been issued prior to the reset, any administrative changes made are lost. This command is equivalent to **save translation** in the Communication Manager.

Note:

Station passwords are stored in a special area of NVRAM to prevent them from being uploaded or downloaded through non-secure protocols.

Syntax

copy running-config startup-config

User Level

read-write

Context

general

Example

```
G450-001(super)# copy running-config startup-config
```

Related Commands

clear survivable-config, set sls, sls

copy running-config tftp

Use the **copy running-config tftp** command to upload the current configuration to a file on a TFTP server. Uncommitted changes to the configuration are included.

To use this command, you need to have an active TFTP server. If Avaya Network Manager is running, you do not require an additional TFTP server.

Note:

After you change the configuration, run the **copy running-config startup-config** command to save the changes. If you do not save the changes, the device loses the changes when you reset it.

Syntax

copy running-config tftp *filename ip*

Parameters

Parameter	Description	Possible Values	Default Value
filename	Name of file to create on TFTP server		
ip	IP address of TFTP server		

User Level

read-write

Context

general

Example

To upload the current configuration to `G450.cfg` on the TFTP server at IP address 135.64.10.33:

```
G450-001(super)# copy running-config tftp G450.cfg 135.64.10.33
```

Related Commands

copy ftp startup-config, copy running-config ftp, copy running-config scp, copy running-config startup-config, copy startup-config ftp, copy startup-config scp, copy startup-config tftp, copy tftp startup-config, erase startup-config, nvram initialize, show copy status, show download status, show erase status, show logging file condition, show running-config, show startup-config

copy scp startup-config

Use the **copy scp startup-config** command to download a startup-config file using the SCP secure protocol. The command prompts for the username and password. Uncommitted changes to the configuration are not included.

Note:

After you change the configuration, run the **copy running-config startup-config** command to save the changes. If you do not save the changes, the device loses the changes when you reset it.

Syntax

copy scp startup-config *filename ip*

Parameters

Parameter	Description	Possible Values	Default Value
filename	Name of file to create on SCP server		
ip	IP address of SCP server		

User Level

read-write

Context

general

Example

To download `router1.cfg` from the SCP server at IP address 192.168.49.10:

```
G450-001(super)# copy scp startup-config c:\config_files\router1.cfg
192.168.49.10
```

copy startup-config ftp

Use the **copy startup-config ftp** command to upload the current configuration to a file on an FTP server. The command prompts for the username and password. Uncommitted changes to the configuration are not included.

Note:

After you change the configuration, run the **copy running-config startup-config** command to save the changes. If you do not save the changes, the device loses the changes when you reset it.

Syntax

copy startup-config ftp *filename ip*

Parameters

Parameter	Description	Possible Values	Default Value
filename	Name of file to create on the FTP server		
ip	IP address of the FTP server		

User Level

read-write

Context

general

Example

To upload the current configuration to `G450.cfg` on the FTP server at IP address 135.64.10.33:

```
G450-001(super)# copy startup-config ftp G450.cfg 135.64.10.33
```

Related Commands

copy ftp startup-config, copy running-config scp, copy running-config startup-config, copy running-config tftp, copy startup-config scp, copy startup-config tftp, copy tftp startup-config, erase startup-config, nvram initialize, show copy status, show download status, show erase status, show logging file condition, show running-config, show startup-config

copy startup-config scp

Use the **copy startup-config scp** command to upload the current configuration to a file on an SCP server. The command prompts for the username and password. Uncommitted changes to the configuration are not included.

Note:

After you change the configuration, run the **copy running-config startup-config** command to save the changes. If you do not save the changes, the device loses the changes when you reset it.

Syntax

copy startup-config scp *filename ip*

Parameters

Parameter	Description	Possible Values	Default Value
filename	Name of file to create on the SCP server		
ip	IP address of the SCP server		

User Level

read-write

Context

general

Example

To upload the current configuration to `router1.cfg` on the SCP server at IP address 192.168.49.10:

```
G450-001(super)# copy startup-config scp c:\config_files\router1.cfg
192.168.49.10
```

Related Commands

copy ftp startup-config, copy running-config ftp, copy running-config scp, copy running-config startup-config, copy running-config tftp, copy startup-config ftp, copy startup-config tftp, copy tftp startup-config, erase startup-config, nvram initialize, show copy status, show download status, show erase status, show logging file condition, show running-config, show startup-config

copy startup-config tftp

Use the **copy startup-config tftp** command to upload the current configuration to a file on a TFTP server. Uncommitted changes to the configuration are not included.

To use this command, you need to have an active TFTP server. If Avaya Network Manager is running, you do not require an additional TFTP server.

Note:

After you change the configuration, run the **copy running-config startup-config** command to save the changes. If you do not save the changes, the device loses the changes when you reset it.

Syntax

copy startup-config tftp *filename ip*

Parameters

Parameter	Description	Possible Values	Default Value
filename	Name of file to create on TFTP server		
ip	IP address of TFTP server		

User Level

read-write

Context

general

Example

To upload the current configuration to `G450.cfg` on the TFTP server at IP address 135.64.10.33:

```
G450-001(super)# copy startup-config tftp G450.cfg 135.64.10.33
```

Related Commands

copy ftp startup-config, copy running-config ftp, copy running-config scp, copy running-config startup-config, copy running-config tftp, copy startup-config ftp, copy startup-config scp, copy tftp startup-config, erase startup-config, nvram initialize, show copy status, show download status, show erase status, show logging file condition, show running-config, show startup-config

copy startup-config usb

Use the **copy startup-config usb** command to upload the current configuration from the gateway to the USB mass storage device.

Syntax

copy startup-config usb ***source-filename destination-usb-device*** [***destination-filename***]

Parameters

Parameter	Description	Possible Values	Default Value
source-filename	The logical name for the source file		
destination usb-device	The destination USB mass storage device	**usb-device0**	
destination-filename	The destination file name and path		

User Level

read-write

Context

general

Examples

To upload `startup_config.cfg` from the gateway to usb-device0:

```
G450-001(super)# copy startup-config usb startup_config.cfg usb-device0
```

Related Commands

backup config usb, copy usb announcement-file, erase usb, restore usb, safe-removal usb, show backup status, show restore status, show usb

copy tftp startup-config

Use the **copy tftp startup-config** command to copy the media gateway configuration from the saved TFTP file to the Startup Configuration NVRAM.

To use this command, you need to have an active TFTP server, and to create a file into which to download the data. If Avaya Network Manager is running, an additional TFTP server is not required.

Syntax

copy tftp startup-config *filename ip*

Parameters

Parameter	Description	Possible Values	Default Value
filename	The file name, including the full path		
ip	The IP address of the host		

User Level

read-write

Context

general

Example

To copy the configuration file `router1.cfg` from the TFTP server 192.168.49.10 into the startup configuration:

```
G450-001(super)# copy tftp startup-config c:\G450\router1.cfg 192.168.49.10
```

Related Commands

copy ftp startup-config, copy running-config ftp, copy running-config scp, copy running-config startup-config, copy running-config tftp, copy startup-config ftp, copy startup-config scp, copy startup-config tftp, erase startup-config, nvram initialize, show copy status, show download status, show erase status, show logging file condition, show running-config, show startup-config

copy usb startup-config

Use the **copy usb startup-config** command to download a configuration file from the external USB mass storage device to the gateway.

Syntax

copy usb startup-config ***source-usb-device source-filename***

Parameters

Parameter	Description	Possible Values	Default Value
source usb-device	The source USB mass storage device	**usb-device0**	
source-filename	The full name and path of the file to be downloaded		

User Level

Admin

Context

general

Example

To download `startup_config.cfg` from usb-device0 to the gateway:

```
G450-001(super)# copy usb startup-config usb-device0 \temp\startup_config.cfg
```

Related Commands

backup config usb, copy announcement-file usb, erase usb, restore usb, safe-removal usb, show backup status, show restore status, show usb

erase startup-config

Use the **erase startup-config** command to reset the NVRAM parameters to the factory default values. This command is an alias for the command nvram initialize on page 263.

Syntax

erase startup-config

User Level

read-write

Context

general

Related Commands

copy ftp startup-config, copy running-config ftp, copy running-config scp, copy running-config startup-config, copy running-config tftp, copy startup-config ftp, copy startup-config scp, copy startup-config tftp, copy tftp startup-config, nvram initialize, show copy status, show download status, show erase status, show logging file condition, show running-config, show startup-config

nvram initialize

Use the **nvram initialize** command to reset the NVRAM parameters to the factory default values. This command is an alias for **erase startup-config** (refer to erase startup-config on page 262).

CAUTION:

This command erases all announcement files in the G450 announcement directory.

Syntax

nvram initialize

User Level

read-write

Context

general

Example

To reset the configuration parameters for the device:

```
G450-001(super)# nvram initialize
This command will restore factory defaults, and can disconnect your telnet
session
*** Reset *** - do you want to continue (Y/N)? Y
Connection closed by foreign host.
```

Related Commands - Configuration files

copy ftp startup-config, copy running-config ftp, copy running-config scp, copy running-config startup-config, copy running-config tftp, copy startup-config ftp, copy startup-config scp, copy startup-config tftp, copy tftp startup-config, erase startup-config, nvram initialize, show copy status, show download status, show erase status, show logging file condition, show running-config, show startup-config

Related Commands - USP configuration

bandwidth, idle-character, ignore dcd, interface serial, invert txclock, transmitter-delay

---

show copy status

Use the **`show copy status`** command to display the status of the **copy running-config startup-config** operation.

Syntax

`show copy status`

User Level

read-write

Context

general

Example

To display the status of the current copy operation:

```
G450-001(super)# show copy status
Module #10
===========
Module           : 10
Source file      : startup-config
Destination file : running-config
Host             : -
Running state    : Idle
Failure display  : (null)
Last warning     : No-warning
```

Related Commands

copy ftp startup-config, copy running-config ftp, copy running-config scp, copy running-config startup-config, copy running-config tftp, copy startup-config ftp, copy startup-config scp, copy startup-config tftp, copy tftp startup-config, erase startup-config, nvram initialize, show download status, show erase status, show logging file condition, show running-config, show startup-config

show download status

Use the **show download status** command to display the status of the current configuration file download process, as the file is being loaded into the device.

Syntax

show download status [*module_number*]

Parameters

Parameter	Description	Possible Values	Default Value
module_number	The number of the module for which to display information	**1-10**	

User Level

read-only

Context

general

Example

To display the status of a configuration file download for module 10:

```
G450-001(super)# show download status 10
```

Related Commands

copy ftp startup-config, copy running-config ftp, copy running-config scp, copy running-config startup-config, copy running-config tftp, copy startup-config ftp, copy startup-config scp, copy startup-config tftp, copy tftp startup-config, erase startup-config, nvram initialize, show copy status, show erase status, show logging file condition, show running-config, show startup-config

show erase status

Use the **show erase status** command to display the status of the **erase startup-config** operation.

Syntax

show erase status

User Level

read-write

Context

general

Related Commands

copy ftp startup-config, copy running-config ftp, copy running-config scp, copy running-config startup-config, copy running-config tftp, copy startup-config ftp, copy startup-config scp, copy startup-config tftp, copy tftp startup-config, erase startup-config, nvram initialize, show copy status, show download status, show logging file condition, show running-config, show startup-config

show running-config

Use the **show running-config** command to display the G450's current configuration.

Syntax

show running-config

User Level

read-only

Context

general

Example

To display the current configuration:

```
G450-001(super)# show running-config
G450-001(super)#
! version 0.0.13
!
!
!
ds-mode t1
!
interface Vlan 1
icc-vlan
ip address 172.16.1.139    255.255.255.240
pmi
!
interface FastEthernet 10/2
!
interface Console
ip address  10.3.0.1  255.255.255.0
!
```

Related Commands - Configuration files

copy ftp startup-config, copy running-config ftp, copy running-config scp, copy running-config startup-config, copy running-config tftp, copy startup-config ftp, copy startup-config scp, copy startup-config tftp, copy tftp startup-config, erase startup-config, nvram initialize, show copy status, show download status, show erase status, show logging file condition, show startup-config

---

show startup-config

Use the **show startup-config** command to show the NVRAM based configuration loaded automatically at startup.

Syntax

show startup-config

User Level

read-only

Context

general

Example

To display the startup configuration:

```
G450-001(super)# show startup-config
G450-001(super)#
! version 0.0.13
ds-mode t1
interface Vlan 1
icc-vlan
ip address 172.16.1.139    255.255.255.240
pmi
interface FastEthernet 10/2
interface Console
ip address  10.3.0.1  255.255.255.0
```

Related Commands

copy ftp startup-config, copy running-config ftp, copy running-config scp, copy running-config startup-config, copy running-config tftp, copy startup-config ftp, copy startup-config scp, copy startup-config tftp, copy tftp startup-config, erase startup-config, nvram initialize, show copy status, show download status, show erase status, show logging file condition, show running-config

show upload status

Use the **show upload status** command to display status information regarding the upload of a capture file or a configuration file, for a specific module or for all modules.

Syntax

show upload status [*module_number*]

Parameters

Parameter	Description	Possible Values	Default Value
module_number	The module number for which to display upload information	**0-10**	

User Level

read-only

Context

general

Example

To display upload status information for module 10:

```
G450-001(super)# show upload status 10

Module #10
==========
No source file for upload operation - no upload operation was done.
```

Related Commands

composite-operation, cookie, copy capture-file ftp, copy capture-file scp, copy capture-file tftp, ip-rule (policy, policy-based routing, packet sniffing), owner, show ip capture-list

Connectivity

ping

Use the **ping** command to send ICMP packets to a target system. The ping command is useful for checking host reachability and network connectivity.

Syntax

ping *host* [*interval* [*size*[*timeout*[*source_address*]]]]

Parameters

Parameter	Description	Possible Values	Default Value
host	The IP address of the target system		
interval	The number of seconds between successive ICMP packets	**1-256**	**1**
size	The size, in bytes, of the packet sent when pinging	**22-65500**	**50**
timeout	The timeout in seconds	**1-10**	
source_address	IP address from which to send the ICMP packets		

User Level

read-only

Context

general

Example

To send test 50-byte packets to IP address 192.168.49.1 from IP address 192.168.49.4 every 3 seconds, timing out after 5 seconds:

```
G450-001(super)# ping 192.168.49.1 3 50 5 192.168.49.4
```

Contact closure

set contact-closure admin

Use the **set contact-closure admin** command to specify how the contact closure relay is controlled.

Note:

The **set contact-closure pulse-duration** command does not affect the **set contact-closure admin manual** command.

Syntax

set contact-closure admin ***module/port*:*relay***
{mgc | manual-trigger | manual-off}

Parameters

Parameter	Description	Possible Values	Default Value
module	Module number of the contact closure port	**10**	
port	Port number of the contact closure port	**2**	
relay	Contact closure relay	**1**, **2**	
mgc	Contact closure is controlled by the call controller		

Parameter	Description	Possible Values	Default Value
manual-trigger	Contact closure relay is triggered		
manual-off	Contact closure relay is not triggered		

User Level

read-write

Context

general

Example

To specify that contact closure for relay 2 of port 1 on module 10 is controlled by the call controller:

```
G450-001(super)# set contact-closure admin 10/1:2 mgc
```

Related Commands

set contact-closure pulse-duration, show contact-closure

set contact-closure pulse-duration

Use the **set contact-closure pulse-duration** command to set the pulse duration for a contact closure relay. Pulse duration is the amount of time for the relay to return to normal after the call controller triggers it.

Syntax

set contact-closure pulse-duration ***module/port:relay time***

Parameters

Parameter	Description	Possible Values	Default Value
module	Module number of the contact closure port	**10**	
port	Port number of the contact closure port	**1**	
relay	Relay number	**1**, **2**	
time	Amount of time until the relay returns to normal, in seconds	**1-60**	

User Level

read-write

Context

general

Example

To set the pulse duration to 3 seconds for relay 2 of port 1 on module 10:

```
G450-001(super)# set contact-closure pulse-duration 10/1:2 3
```

Related Commands

set contact-closure admin, show contact-closure

show contact-closure

Use the **show contact-closure** command to view the status of a contact closure relay. If no relay is specified, the status of all relays is displayed.

Syntax

show contact-closure [module/port:*relay*]

Parameters

Parameter	Description	Possible Values	Default Value
module	Contact closure module to display	**10**	
port	Contact closure module port to display	**2**	
relay	Relay number	**1, 2**	

User Level

read-only

Context

general

Example

To display information about all contact closure relays:

```
G450-001(super)# show contact-closure
MODULE PORT RELAY ADMIN           PULSE DURATION   STATUS
------ ---- ----- --------------- ---------------  ------
10       2    1   call-controller 3 seconds        triggered
10       2    2   manual          toggle           off
```

To display information about contact closure relay 1:

```
G450-001(super)# show contact-closure 10/1:1
MODULE PORT RELAY ADMIN           PULSE DURATION   STATUS
------ ---- ----- --------------- ---------------  ------
10     2    1     mgc             3 secs           off
```

Related Commands - Contact closure

set contact-closure admin, set contact-closure pulse-duration

Related Commands - Policy

cookie, ip-fragments-in, ip-option-in, ip-rule (policy, policy-based routing, packet sniffing), name, owner, show isdn bri link, show list

Counters

clear counters (interface)

Use the **clear counters** command to clear counters for the selected interface or the entire device.

Syntax

clear counters [*interface_type interface_identifier*]

Parameters

Parameter	Description	Possible Values	Default Value
interface_type	The type of interface		
interface_identifier	The interface number. The format varies depending on the value of interface_type: For FastEthernet: **module/port** For Serial: **module/port:channel-group** For Vlan: **Vlan id** For LoopBack: **Loopback number**	For FastEthernet: **10/2 or 10/4** For Serial(USP): **3/1, 4/1, 8/1** For Serial (DS1): module/port: **3/1, 4/1, 8/1** channel-group: E1: **0-30** T1: **0-23** For VLAN: **1-4090** For Loopback: **1-99**	

User Level

read-write

Context

general

Example

To clear counters on interface Vlan 1:

```
G450-001(super)# clear counters Vlan 1
```

clear ip traffic

Use the **clear ip traffic** command to clear the IP counters.

Syntax

clear ip traffic

User Level

read-only

Context

general

Example

To clear the IP counters:

```
G450-001(super)# clear ip traffic
```

show ip traffic

Use the **show ip traffic** command to display IP counters information for a given protocol. If no protocol is specified information for all protocols is displayed.

Syntax

show ip traffic [*protocol_type*]

Parameters

Parameter	Description	Possible Values	Default Value
protocol_type	The type of IP protocol for which to display information	**arp**, **bootp-dhcp**, **icmp**, **ip**, **ospf**	

User Level

read-only

Context

general

Example

To display traffic information for all protocols:

```
G450-001(super)# show ip traffic
IP statistics:
    Received:
5644 total, 4012 local destination
0 bad hop count, 0 packet header errors
0 unknown protocol, 0 address errors
1632 discarded
    Fragments:
```

```
0 reassembled, 0 timeouts
0 couldn't reassemble, 0 fragmented

    Sent:
4014 generated, 0 forwarded
0 no route, 0 discarded

ICMP statistics:
    Received:
0 total, 0 ICMP errors
0 unreachables, 0 time exceeded
0 parameter, 0 quench
0 echo, 0 echo reply
0 timestamps request, 0 timestamp reply
0 mask requests, 0 mask replies
0 redirects

    Sent:
0 total, 0 ICMP errors
0 unreachables, 0 time exceeded
0 parameter, 0 quench
0 echo, 0 echo reply
0 timestamps request, 0 timestamp reply
0 mask requests, 0 mask replies
0 redirects

OSPF statistics:
    Received:
0 total, 0 checksum errors
0 hello, 0 database desc
0 link state req, 0 link state updates
0 link state acks

    Sent:
0 total
ARP statistics:
    Received:
5394 requests, 2 replies
    Sent:
36 requests, 16 replies (0 proxy)
DHCP  statistics:
Requests: 0 , Replies: 0
BOOTP statistics:
Requests: 0 , Replies: 0
```

CSU loopbacks

show csu loopbacks

Use the **show csu loopbacks** command to view the state of the server SAT-controlled CSU loopbacks on a media module.

Syntax

show csu loopbacks *mmID*

Parameters

Parameter	Description	Possible Values	Default Value
mmID	The Media Module ID		

User Level

read-only

Context

general

Example

To view the state of loopbacks on module 2:

```
G450-001(super)#show csu loopbacks v2
CSU LOOPBACK STATUS
-----------------------------------
Towards DTE Port-
    Digital Diagnostics: OFF
Towards Network-
    Payload: OFF
    Line   : OFF
```

Related Commands

show csu status

show csu status

Use the **show csu status** command to view the status of the CSU on a media module.

Syntax

show csu status *mmID*

Parameters

Parameter	Description	Possible Values	Default Value
mmID	The Media Module ID		

User Level

read-only

Context

general

Example

To display the status of the CSU on module 4:

```
G450-001(super)# show csu status v4

TI version of csu status:
CSU NETWORK INTERFACE STATUS
------------------------------------------------------------------
LOS:ON          00F:         OFF
EER:OFF         L00PD:       OFF
AIS:OFF         PDV:         OFF
LOF:OFF         YEL:         ON

E1 version of csu status:
CSU NETWORK INTERFACE STATUS
------------------------------------------------------------------
LOS:ON              00F:OFF
EER:OFF         L00PD:OFF
AIS:OFF         PDV:OFF
LOF:OFF         LMA:OFF
RMA:OFF         LCM:ON
```

Output fields

Name	Description
LOS	Loss of signal
OOF	Out of frame
EER	Excessive error rate
LOOPD	Looped
AIS	Alarm indication signal
PDV	Pulse density violation (same as BPV)
LOF	Loss of frame
LMA	Local multiframe alignment
YEL	Yellow
RMA	Remote multiframe alignment
LCM	Loss of CRC multiframe

Related Commands

show csu loopbacks

Date and time setting

set date

Use the **`set date`** command to set the current date.

Note:

If the gateway is registered to a call controller, the call controller overwrites the date set manually by this command.

Syntax

set date ***`mm/dd/yyyy`***

Parameters

Parameter	Description	Possible Values	Default Value
mm	A two-digit number denoting the month	**01-12**	
dd	A two-digit number denoting the day	**01-31**	
yyyy	A four-digit number denoting the year	**1994-2020**	

User Level

admin

Context

general

Example

To set the current date to January 13, 2007:

```
G450-001(super)# set date 01/13/2007
```

Related Commands

set date, set time, show system

set time

Use the **`set time`** command to set the current time.

Note:

If the gateway is registered to a call controller, the call controller overwrites the time set manually by this command.

Syntax

set time ***HH:MM:SS***

Parameters

Parameter	Description	Possible Values	Default Value
HH	A two-digit number denoting the hour	**00-23**	
MM	A two-digit number denoting the minute	**00-59**	
SS	A two-digit number denoting the second	**00-59**	

User Level

admin

Context

general

Example

To set the current time to 9 hours, 20 minutes, and 12 seconds:

```
G450-001(super)# set time 09:20:12
```

Related Commands

set date, show system

Default gateway

ip default-gateway

Use the **ip default-gateway** command to define a default gateway (router). Use the **no** form of this command to remove the default gateway.

Syntax

ip default-gateway {*ip_address* | {*interface_type interface_number*}}
[*cost*] [*preference*] [permanent | track *track-index*]

no ip default-gateway

Parameters

Parameter	Description	Possible Values	Default Value
ip_address	The IP address of the router		
interface_type	The interface type		
interface_number	The interface number		
cost	The path cost		**1**
preference	The preference	**High**, **Low**	**Low**
permanent	Keyword that specifies not to disable the router if the interface is down		
track	Keyword that specifies to apply tracking to monitor the default gateway. **Note:** Tracking only applies to non-permanent default gateways.		
track-index	The index number of the object tracker	**1-50**	

User Level

read-write

Context

general

Example

To set the default gateway to the IP address 132.55.4.45, having a cost value of 4 with high preference, and applying object tracker 20:

```
G450-001(super)# ip default-gateway 132.55.4.45 4 high track 20
```

To set the default gateway to be the Serial interface:

```
G450-001(super)# ip default-gateway Serial 4/1:1.1 permanent
```

Related Commands

clear ip route, ip route, show ip route, show ip route best-match, show ip route static, show ip route summary, show ip route track-table, traceroute

Default settings

zeroize

Use the **zeroize** command to clear all secret parameters and initialize the NVRAM to its factory defaults.

CAUTION:
This command restores factory defaults and disconnects the current session.

CAUTION:
This command erases all announcement files in the G450 announcement directory.

Syntax

zeroize

User Level

admin

Context

general

Example

To clear all secret parameters and initialize the NVRAM to its factory defaults:

```
G450-001(super)# zeroize
This command will  restore factory defaults, and disconnect your existing
session.
               *** Zeroize *** - do you want to continue (Y/N)? Y
```

Related Commands

show system

Device status

clear utilization cpu

Use the **clear utilization cpu** command to disable CPU utilization measurements.

Syntax

clear utilization cpu *module*

Parameters

Parameter	Description	Possible Values	Default Value
module	The module for which to disable CPU utilization measurements		

User Level

read-write

Context

general

Example

To disable CPU utilization measurements for module 10:

```
G450-001(super)# clear utilization cpu 10
```

set utilization cpu

Use the **set utilization cpu** command to enable CPU utilization measurements.

Syntax

set utilization cpu *module*

Parameters

Parameter	Description	Possible Values	Default Value
module	Number of the module		

User Level

read-write

Context

general

Example

To enable CPU utilization measurements on module 10:

```
G450-001# set utilization cpu 10
CPU utilization is set on module 10
```

Related Commands

set utilization cpu, show faults, show mg list config, show mgc, show mm, show module, show recovery, show restart-log, show download, show system, show temp, show timeout, show utilization, show voltages, test led

show download

Use the **show download** command to display the status of the current file copy process to the device.

Syntax

show download {software [*mmID*] | config} status

Parameters

Parameter	Description	Possible Values	Default Value
software	Keyword specifying that software download or upload information is displayed		
mmId	The Media Module ID number		
config	Keyword specifying that configuration download or upload information is displayed		

User Level

read-only

Context

general

Example

To display the status of software downloads for all media modules:

```
G450-001(super)# show download software status
TFTP STATUS
-------------------------------------------
Module                                    : MGP
Source File                               : mg01_3.com
Destination File: BANK B
Host                                      : 0.0.0.0
Running State                             : idle
Last Failure                              : No Error
Last Warning                              : (null)
Progress                                  : [0/0]  0%
```

Related Commands

set utilization cpu, show faults, show mg list config, show mgc, show mm, show module, show recovery, show restart-log, show system, show temp, show timeout, show utilization, show voltages, test led

show faults

Use the **show faults** command to display the active faults for the media gateway.

Syntax

show faults

User Level

read-only

Context

general

Example

To display the current fault list:

```
G450-001(super)# show faults

CURRENTLY ACTIVE FAULTS
------------------------------------------------------------------------
-- Hardware Faults --
        + Multiple fans outage, 01/01-18:26:35.00
        + PSU fan brief outage, 01/01-18:26:35.00
-- MGP Faults --
        + No controller found, 01/01-00:00:01.00
```

Related Commands

set utilization cpu, show mg list_config, show mgc, show mm, show module, show recovery, show restart-log, show download, show system, show temp, show timeout, show utilization, show voltages, test led

show mg list_config

Use the **show mg list_config** command to show the installed media gateway equipment. It displays the current hardware and firmware configurations of the media gateway.

The **show mg list_config** command is an alias for show module on page 290.

Syntax

show mg list_config

User Level

read-only

Context

general

Example

To display the list of installed equipment:

```
G450-001(super)# show mg list_config

SLOT  TYPE      CODE    SUFFIX  HW VINTAGE  FW VINTAGE
----  ------    ------  ------  ----------  -----------
v1    S8300     ICC     A       0           1
v2    USP       MM342   A       0           N/A
v3    DCP       MM717   A       1           2
v4    Analog    MM714   A       1           61
v5    E1T1      MM340   A       0           N/A
v6    E1T1      MM340   A       0           N/A
v7    E1T1      MM340   A       0           N/A
v8    Analog    MM711   A       1           61
V10   Mainboard G450    A       17          25
```

Related Commands

set utilization cpu, show faults, show mgc, show mm, show module, show recovery, show restart-log, show download, show system, show temp, show timeout, show utilization, show voltages, test led

---

show mgc

Use the **show mgc** command to display the currently active media gateway controller state and setup parameters.

Syntax

show mgc

User Level

read-only

Context

general

Example

To display media gateway controller information:

```
G450-001(super)# show mgc

CALL CONTROLLER STATUS
-----------------------------------------
Registered          : NO
```

```
Active Controller   : 255.255.255.255
H248 Link Status    : DOWN
H248 Link Error Code: 0x0

CONFIGURED MGC HOST
--------------------
-- Not Available --
-- Not Available --
-- Not Available --
-- Not Available --
```

Related Commands - Media Gateway Controller

clear mgc list, session, set icc-monitoring, set mediaserver, set mgc list, set reset-times, show icc-monitoring, show mediaserver, show mgc list

Related Commands - Device status

set utilization cpu, show faults, show mg list config, show mm, show module, show recovery, show restart-log, show download, show system, show temp, show timeout, show utilization, show voltages, test led

---

show mm

Use the **show mm** command to show the media gateway media module information. It displays the types and serial numbers of media modules installed on the media gateway. If no media module ID is specified, information for all media modules is displayed.

Syntax

show mm [*mmID*]

Parameters

Parameter	Description	Possible Values	Default Value
mmID	The Media Module ID number		

User Level

read-only

Context

general

Example

To display information about media module 7:

```
G450-001(super)# show mm 7

MEDIA MODULE DESCRIPTION: v7
------------------------------------------------
Uptime(d,h:m:s): 0, 00:23:19
Type           : Voice (Initializing)
Description    : N/A
Serial Number  : N/A
HW Vintage     : N/A
HW Suffix      : N/A
FW Version     : N/A
No. of ports   : 0
Faults         : No Fault Messages
```

Related Commands

set utilization cpu, show faults, show mg list_config, show mgc, show module, show recovery, show restart-log, show download, show system, show temp, show timeout, show utilization, show voltages, test led

show module

Use the **show module** command to view information about a media module. If no media module is specified, information about all media modules is displayed.

Syntax

show module [*mmID*]

Parameters

Parameter	Description	Possible Values	Default Value
mmID	The Media Module ID		

User Level

read-only

Context

general

Example

To show information about media module 2:

```
G450-001(super)# show module v2
SLOT TYPE        CODE     SUFFIX  HW VINTAGE  FW VINTAGE
---- ---------  ----     ------  ----------  ----------
v2   DS1        MM710    A       4           5
```

To show information about all media modules:

```
G450-001(super)# show module
SLOT TYPE        CODE     SUFFIX  HW VINTAGE  FW VINTAGE
---- ---------  ----     ------  ----------  ----------
v1    S8300        ICC      A       0           1
v2    USP          MM342    A       0           N/A
v3    DCP          MM717    A       1           2
v4    Analog       MM714    A       1           61
v5    E1T1         MM340    A       0           N/A
v6    E1T1         MM340    A       0           N/A
v7    E1T1         MM340    A       0           N/A
v8    Analog       MM711    A       1           61
V10   Mainboard    G450     A       17          25
```

Related Commands

set utilization cpu, show faults, show mg list config, show mgc, show mm, show recovery, show restart-log, show download, show system, show temp, show timeout, show utilization, show voltages, test led

---

show recovery

Use the **show recovery** command to show the media gateway monitoring and recovery setup.

Syntax

show recovery

User Level

read-only

Context

general

Example

To show recovery information:

```
G450-001(super)# show recovery

RECOVERY TIMES
--------------------------------
Primary Search  : 1
Total Search    : 30
Transition Point: 1
```

Related Commands

set utilization cpu, show faults, show mg list_config, show mgc, show mm, show module, show restart-log, show download, show system, show temp, show timeout, show utilization, show voltages, test led

show restart-log

Use the **show restart-log** command to retrieve restart data that is stored in a log in flash memory.

Syntax

show restart-log

User Level

read-only

Context

general

Example

To display restart information:

```
G450-001(super)# show restart-log

RESET ID  MM/DD-hh:mm:ss.hs STR
---------- ------------------ -----------------------------------
0000000000 01/01-02:54:17.00 MgFw#:48.46.48 REBOOT
0000000000 01/01-02:54:12.00 MgFw#:48.46.48 WWD-STYCRINO-XXXXX REBOOT from
RecoveryEngineUti
EOF
```

Related Commands

set utilization cpu, show faults, show mg list_config, show mgc, show mm, show module, show recovery, show download, show system, show temp, show timeout, show utilization, show voltages, test led

show system

Use the **show system** command to display information about the device.

Syntax

show system

User Level

read-only

Context

general

Example

To display device information:

```
G450-001(super)# show system
System Name             : G450
System Location         :
System Contact          :
Uptime (d,h:m:s)        : 0,03:41:57
MV Time                 : 15:02:27 27-SEP-2005
Serial No               : 0PIS81865230
Model No                : G450
HW Ready for FIPS       : No
HW Vintage              : 1
Chassis HW Suffix       :
Mainboard HW Vintage  : 1
Mainboard HW Suffix   : A
Mainboard FW Vintage  : 25.16.50
LAN MAC Address         : 00:04:0d:29:c6:bd
WAN1 MAC address        : 00:04:0d:29:c6:bb
WAN2 MAC address        : 00:04:0d:29:c6:bc
SERVICES MAC address    : 00:04:0d:29:c6:be
Memory #1               : 256MB
Memory  #2              : Not present
PSU #1                  : xxxx400W
PSU #2                  : xxxx400W
Media Socket #1         : VoIP DSP xxxxx8102
Media Socket #2         : VoIP DSP xxxxx7119
Media Socket #3         : Not present
Media Socket #4         : Sync-Over-IP xxxxxZarlink222
FAN Trays               : xxxxxxxxx
```

Related Commands - Device status

set utilization cpu, show faults, show mg list_config, show mgc, show mm, show module, show recovery, show restart-log, show download, show temp, show timeout, show utilization, show voltages, test led

---

show temp

Use the **show temp** command to view the device temperature.

Syntax

show temp

User Level

read-only

Context

general

Example:

To display temperature information:

```
G450-001(super)# show temp

Ambient
-------
Temperature : 40C
High Warning: 45C
Low Warning : -5C
```

Related Commands

set utilization cpu, show faults, show mg list config, show mgc, show mm, show module, show recovery, show restart-log, show download, show system, show timeout, show utilization, show voltages, test led

show timeout

Use the **show timeout** command to display the amount of time in minutes the terminal remains idle before timing out. If the timeout value is 0, there is no timeout limit. The default timeout value is 15 minutes.

Syntax

show timeout

User Level

read-only

Context

general

Example

To display the timeout value:

```
G450-001(super)# show timeout
CLI timeout is 15 minutes
```

Related Commands

set utilization cpu, show faults, show mg list_config, show mgc, show mm, show module, show recovery, show restart-log, show download, show system, show temp, show utilization, show voltages, test led

show upload

Use the **show upload** command to display the status of the current file copy process from the device.

Syntax

show upload {software [*mmID*] | config} status

Parameters

Parameter	Description	Possible Values	Default Value
software	Keyword specifying that software download or upload information is displayed		
mmId	The Media Module ID number		
config	Keyword specifying that configuration download or upload information is displayed		

User Level

read-only

Context

general

Example

To display the status of software downloads for all media modules:

```
G450-001(super)# show upload software status
```

Related Commands

set utilization cpu, show faults, show mg list_config, show mgc, show mm, show module, show recovery, show restart-log, show system, show temp, show timeout, show utilization, show voltages, test led

show utilization

Use the **show utilization** command to display information about CPU usage. If no module is specified, information for all modules is displayed.

Syntax

show utilization [*module*]

Parameters

Parameter	Description	Possible Values	Default Value
module	Module to display		

User Level

read-write

Context

general

Example

To display utilization information for all modules:

```
G450-001(super)# show utilization

Mod    CPU       CPU      RAM       RAM
       5sec      60sec    used(%)   Total(Kb)
---    ------    -----   -------   ----------
10        4%        4%     21%      105313 Kb
```

Related Commands

set utilization cpu, show faults, show mg list_config, show mgc, show mm, show module, show restart-log, show system, show temp, show voltages, test led

show voltages

Use the **show voltages** command to view power supply voltages.

Syntax

show voltages

User Level

read-only

Context

general

Example

To display voltage information:

```
G450-001(super)# show voltages
                PSU#1               PSU#2
Voltages        5v, 48v             5v, 48v
PRESENT         YES                 YES
AC IN           YES                 YES
STATUS          OK                  OK
```

Related Commands

set utilization cpu, show faults, show mg list config, show mgc, show mm, show module, show recovery, show restart-log, show download, show system, show temp, show timeout, show utilization, test led

---

test led

Use the **`test led`** command to run a test of the device's LED operation.

Syntax

`test led`

User Level

read-only

Context

general

Example

To run a test of the device's LED operation:

```
G450-001(super)# test led
```

Related Commands

set utilization cpu, show faults, show mg list_config, show mgc, show mm, show module, show recovery, show restart-log, show download, show system, show temp, show timeout, show utilization, show voltages

DHCP and BOOTP relay

ip bootp-dhcp network

Use the **ip bootp-dhcp network** command to select the network from which the BOOTP/DHCP server should allocate an address. This command is required only when there are multiple IP interfaces over the VLAN. Use the **no** form of this command to remove the specified network.

Note:

More than one network can be configured. For requests to servers, all configured networks are used. The networks are used on a round-robin basis.

Syntax

ip bootp-dhcp network *ip_net*

no ip bootp-dhcp network [*ip_net*]

Parameters

Parameter	Description	Possible Values	Default Value
ip_net	The IP subnet		

User Level

read-write

Context

interface:FastEthernet (L2, L2-L3), VLAN (L2, L2-L3)

Example

To select the network 192.168.169.0 as the network from which an address should be allocated for BOOTP/DHCP requests:

```
G450-001(if:Vlan 1.20)# ip bootp-dhcp network 192.168.169.0
```

Related Commands

ip bootp-dhcp relay, ip bootp-dhcp server

ip bootp-dhcp relay

Use the **ip bootp-dhcp relay** command to enable relaying of BOOTP and DHCP requests to the BOOTP/DHCP server. Use the **no** form of this command to disable relaying of BOOTP and DHCP requests.

Syntax

[no] ip bootp-dhcp relay

User Level

read-write

Context

general

Example

To enable relaying of BOOTP and DHCP requests:

```
G450-001(super)# ip bootp-dhcp relay
```

Related Commands

ip bootp-dhcp network, ip bootp-dhcp server

ip bootp-dhcp server

Use the **ip bootp-dhcp server** command to add a BOOTP/DHCP server to handle BOOTP/DHCP requests received by this interface. A maximum of two servers can be added to a single interface. Use the **no** form of this command to remove a server.

Syntax

[no] ip bootp-dhcp server *ip_address*

Parameters

Parameter	Description	Possible Values	Default Value
ip_address	The IP address of the server		

User Level

read-write

Context

interface:FastEthernet (L2 L2-L3,), VLAN (L2, L2-L3)

Example

To add station 192.168.37.46 as a BOOTP/DHCP server to handle BOOTP/DHCP requests:

```
G450-001(if:Vlan 1.2)# ip bootp-dhcp server 192.168.37.46
```

Related Commands

ip bootp-dhcp network, ip bootp-dhcp relay

DHCP binding file

copy dhcp-binding ftp

Use the **copy dhcp-binding ftp** command to copy the DHCP bindings file to a remote server using FTP.

Syntax

copy dhcp-binding ftp *filename ip*

Parameters

Parameter	Description	Possible Values	Default Value
filename	File name with full path	string	
ip	IP address of the host	IP address	

User Level

read-write

Context

general

Example

To copy the binding file, `dhcp_binding.txt`, to the host with IP address 192.168.49.10:

```
G450-001(super)# copy dhcp-binding ftp dhcp_binding.txt 192.168.49.10
```

Related Commands

copy dhcp-binding scp, copy dhcp-binding tftp, copy announcement-file usb, show upload dhcp-binding-file status

copy dhcp-binding scp

Use the **`copy dhcp-binding scp`** command to copy the DHCP bindings file to a remote server using SCP.

Syntax

`copy dhcp-binding scp` ***`filename ip`***

Parameters

Parameter	Description	Possible Values	Default Value
`filename`	File name with full path	string	
`ip`	IP address of the host	IP address	

User Level

read-write

Context

general

Example

To copy the binding file, `dhcp_binding.txt`, to the host with IP address 192.168.49.10:

```
G450-001(super)# copy dhcp-binding scp dhcp_binding.txt 192.168.49.10
```

Related Commands

copy dhcp-binding ftp, copy dhcp-binding tftp, copy announcement-file usb, show upload dhcp-binding-file status

copy dhcp-binding tftp

Use the **copy dhcp-binding tftp** command to copy the DHCP bindings file to a remote server, using TFTP.

Syntax

copy dhcp-binding tftp *filename ip*

Parameters

Parameter	Description	Possible Values	Default Value
filename	File name with full path	string	
ip	IP address of the host	IP address	

User Level

read-write

Context

general

Example

To copy the binding file with file name `dhcp_binding.txt` to the host with IP address 192.168.49.10:

```
G450-001(super)# copy dhcp-binding tftp dhcp_binding.txt 192.168.49.10
```

Related Commands

copy dhcp-binding ftp, copy dhcp-binding scp, copy announcement-file usb, show upload dhcp-binding-file status

copy dhcp-binding usb

Use the **copy dhcp-binding usb** command to upload the DHCP bindings file from the gateway to the USB mass storage device.

Syntax

copy dhcp-binding usb *source-filename destination-usb-device* [*destination-filename*]

Parameters

Parameter	Description	Possible Values	Default Value
source-filename	The logical name for the source file		
destination usb-device	The destination USB mass storage device	**usb-device0**	
destination-filename	The destination file name and path		

User Level

admin

read-write

Context

general

Examples

To upload `dhcp_binding.txt` from the gateway to usb-device0:

```
G450-001(super)# copy dhcp-binding usb dhcp_binding.txt usb-device0
```

Related Commands

backup config usb, copy usb announcement-file, erase usb, restore usb, safe-removal usb, show backup status, show restore status, show usb

show upload dhcp-binding-file status

Use the **show upload dhcp-binding-file status** command to display the upload status of a DHCP binding file.

Syntax

show upload dhcp-binding-file status

User Level

read-only

Context

general

Example

To display the upload status of a DHCP binding file:

(If no download was done)

```
G450-001(super)# show upload dhcp-binding-file status

Module #10
===========
No dest file for download operation - no download operation was done.
(If download was done)
G450-001(super)# show upload dhcp-binding-file status
Module #10
===========

Module : 10
Source file : dhcp-binding
Destination file : bbbb
Host : 135.64.102.64
Running state : Idle
Failure display : (null)
Last warning : No-warning
```

Related Commands

copy dhcp-binding ftp, copy dhcp-binding scp, copy dhcp-binding tftp, copy announcement-file usb

DHCP client

clear ip dhcp-client statistics

Use the **clear ip dhcp-client statistics** command to clear the DHCP client statistics counters.

Syntax

clear ip dhcp-client statistics

User Level

read-only

Context

general, interface:FastEthernet

Note:

When you use this command in the interface context, the counters of the specified interface are cleared. When you use this command in the general context, all DHCP client counters are cleared.

Example

To clear the DHCP client statistics counters:

```
G450-001(config-if:FastEthernet 10/2)# clear ip dhcp-client statistics
```

ip address dhcp

Use the **ip address dhcp** command to enable IP address negotiation via DHCP. Use the **no** form of this command to disable IP address negotiation via DHCP.

Note:

The **ip address dhcp** command can only be used on FastEthernet 10/2.

Note:

You cannot configure both **ip address dhcp** and **keepalive-track** (object tracking) on the WAN FastEthernet interface.
You cannot configure both **ip address dhcp** and **keepalive-icmp** (extended keepalive) on the WAN FastEthernet interface.
You cannot configure both **ip address dhcp** and **ip address negotiated** (PPP/IPCP address negotiation) on the WAN FastEthernet interface.

Note:

You can run **ip address dhcp** as many times as desired to re-initiate DHCP address negotiation. Whenever you change the value of a DHCP client parameter (such as client-id, client hostname), run **ip address dhcp** again to re-initiate DHCP address negotiation using the new values.

Syntax

[no] ip address dhcp

User Level

read-write

Context

interface:FastEthernet (L2-L3)

Example

To enable IP address negotiation via DHCP:

```
G450-001(config-if:FastEthernet 10/2)#ip address dhcp
```

Related Commands

clear ip dhcp-client statistics, ip dhcp client client-id, ip dhcp client hostname, ip dhcp client lease, ip dhcp client request, ip dhcp client route track, release dhcp, renew dhcp, show ip dhcp-client, show ip dhcp-client statistics

ip dhcp client client-id

Use the **ip dhcp client client-id** command to specify the client-identifier for the DHCP client. Use the **no** form of this command to restore the default value, which is the MAC address of the interface.

Note:

To obtain the MAC address of the interface, use the **show system** command or the **show interfaces fastethernet 10/2** command.

Syntax

[no] ip dhcp client client-id {hex *hex-string*}

Parameters

Parameter	Description	Possible Values	Default Value
hex	Keyword indicating that a hex string specifies the class identifier for the DHCP client		
hex-string	A Hex string specifying the class identifier for the DHCP client	string, 1-80 bytes	**01**: MAC address of the interface

User Level

read-write

Context

interface:FastEthernet

Example

To specify the client-identifier as hexadecimal code 02:34:56:

```
G450-001(config-if:FastEthernet 10/2)#ip dhcp client client-id hex 02:34:56
```

Related Commands

clear ip dhcp-client statistics, ip address dhcp, ip dhcp client hostname, ip dhcp client lease, ip dhcp client request, ip dhcp client route track, release dhcp, renew dhcp, show ip dhcp-client, show ip dhcp-client statistics

ip dhcp client hostname

Use the **ip dhcp client hostname** command to specify the client host name for the DHCP client. Use the **no** form of this command to restore the default value, which is the G450's hostname.

Syntax

[no] ip dhcp client hostname *host-name*

Parameters

Parameter	Description	Possible Values	Default Value
host-name	The host name	string, 1-80 bytes	The device hostname

User Level

read-write

Context

interface:FastEthernet

Example

To specify the client host name as Gateway1:

```
G450-001(config-if:FastEthernet 10/2)#ip dhcp client hostname "Gateway1"
```

Related Commands

clear ip dhcp-client statistics, ip address dhcp, ip dhcp client client-id, ip dhcp client lease, ip dhcp client request, ip dhcp client route track, release dhcp, renew dhcp, show ip dhcp-client, show ip dhcp-client statistics

ip dhcp client lease

Use the **ip dhcp client lease** command to set the lease requested by the DHCP client. Use the **no** form of this command to specify the default behavior, which is that the client does not request a lease from the DHCP server.

Syntax

[no] ip dhcp client lease *days* [*hours* [*minutes*]]

Parameters

Parameter	Description	Possible Values	Default Value
days ***hours*** ***minutes***	The lease time, in D H M format	Minimum value: **0 0 1**	No lease requested from the server

User Level

read-write

Context

interface:FastEthernet

Example

To set the lease as time for 1 day, 4 hours, and 15 minutes:

```
G450-001(config-if:FastEthernet 10/2)#ip dhcp client lease 1 4 15
```

Related Commands

clear ip dhcp-client statistics, ip address dhcp, ip dhcp client client-id, ip dhcp client hostname, ip dhcp client request, ip dhcp client route track, release dhcp, renew dhcp, show ip dhcp-client, show ip dhcp-client statistics

ip dhcp client request

Use the **ip dhcp client request** command to determine which DHCP options the DHCP client requests from the DHCP server. By default, the DHCP client requests all DHCP options. Use the **no** form of this command to disable requesting of a specific option.

Note:

The DHCP client receives the requested options only if they were previously configured for the DHCP pool in the DHCP server.

Syntax

[no] ip dhcp client request {domain-name | dns-nameserver | router }

Parameters

Parameter	Description	Possible Values	Default Value
domain-name	A keyword indicating the DHCP client is requesting the domain name from the DHCP server		Option requested

Parameter	Description	Possible Values	Default Value
dns-nameserver	A keyword indicating the DHCP client is requesting the list of available DNS servers from the DHCP server		Option requested
router	A keyword indicating the DHCP client is requesting the list of default routers from the DHCP server		Option requested

User Level

read-write

Context

interface:FastEthernet

Example

To set that the DHCP client requests the default routers list:

```
G450-001(config-if:FastEthernet 10/2)#ip dhcp client request router
```

Related Commands

clear ip dhcp-client statistics, ip address dhcp, ip dhcp client client-id, ip dhcp client hostname, ip dhcp client lease, ip dhcp client route track, release dhcp, renew dhcp, show ip dhcp-client, show ip dhcp-client statistics

ip dhcp client route track

Use the **ip dhcp client route track** command to apply object tracking in order to monitor the DHCP client's default route. Use the **no** form of this command to restore the default value, which is that no object tracker is specified to check the default route.

Syntax

[no] ip dhcp client route track *track-index*

Parameters

Parameter	Description	Possible Values	Default Value
track-index	The index number of the object tracker	**1-50**	

User Level

read-write

Context

interface:FastEthernet (not running ARPA)

Example

To apply object tracker 3:

```
G450-001(config-if:FastEthernet 10/2)#ip dhcp client route track 3
```

Related Commands

clear ip dhcp-client statistics, ip address dhcp, ip dhcp client client-id, ip dhcp client hostname, ip dhcp client lease, ip dhcp client request, release dhcp, renew dhcp, show ip dhcp-client, show ip dhcp-client statistics

release dhcp

Use the **`release dhcp`** command to release a DHCP lease for an interface. This effectively releases the client IP address on the specified interface.

Note:

If you are releasing a dynamic IP address with DNS information (DNS servers list), the DNS information is removed as well, and the DNS Resolver application will not use it any more.

Syntax

`release dhcp` ***`interface-type interface-identifier`***

Parameters

Parameter	Description	Possible Values	Default Value
interface-type	The type of interface	**FastEthernet**	
interface-identifier	The interface identifier	module number/ port number	

User Level

read-write

Context

general

Example

To release DHCP for interface FastEthernet 10/2:

```
G450-001(super)# release dhcp FastEthernet 10/2
```

Related Commands

clear ip dhcp-client statistics, ip address dhcp, ip dhcp client client-id, ip dhcp client hostname, ip dhcp client lease, ip dhcp client request, ip dhcp client route track, renew dhcp, show ip dhcp-client, show ip dhcp-client statistics

renew dhcp

Use the **`renew dhcp`** command to renew a DHCP lease for an interface. This is effectively a request to renew an existing IP address, or the start of a new process of requesting a new IP address.

Syntax

`renew dhcp` ***`interface-type interface-identifier`***

Parameters

Parameter	Description	Possible Values	Default Value
interface-type	The type of interface	**FastEthernet**	
interface-identifier	The interface identifier	module number/ port number	

User Level

read-write

Context

general

Example

To renew a DHCP lease for interface FastEthernet 10/2:

```
G450-001(super)# renew dhcp FastEthernet 10/2
```

Related Commands

clear ip dhcp-client statistics, ip address dhcp, ip address negotiated, ip dhcp client client-id, ip dhcp client hostname, ip dhcp client lease, ip dhcp client request, ppp ipcp dns request, release dhcp, ip dhcp client route track, show ip dhcp-client, show ip dhcp-client statistics

show ip dhcp-client

Use the **show ip dhcp-client** command to show the configuration of the DHCP client.

Syntax

show ip dhcp-client (in the interface context)

show ip dhcp-client {***interface-type interface-identifier*** | **brief** } (in the general context)

Parameters

Parameter	Description	Possible Values	Default Value
interface-type	The type of interface	**FastEthernet**	
interface-identifier	The interface identifier	module number/port number	
brief	A keyword indicating to display the configuration in brief		

User Level

read-only

Context

interface:FastEthernet 10/2
general

Example

To show the configuration of the DHCP client in the FastEthernet 10/2 context:

```
G450-001(config-if:FastEthernet 10/2)# show ip dhcp-client

DHCP Client Mode:                    Enable
Status:                              Bound.
IP address:                          10.1.1.2
Subnet Mask:                         255.255.255.0
Default Router:                      10.1.1.1 10.1.1.250
DHCP Server:                         10.1.2.20
Domain name:                         avaya.com
DNS Server:                          122.22.22.33 133.33.33.33
Lease Received (D:H:M:S):            2:2:3:4
Lease Remains (D:H:M:S):            1:2:3:4
Lease Rebind (D:H:M:S):              0:0:8:45
Lease Renew (D:H:M:S):               0:0:5:0
Lease Requested (D:H:M:S):           5:0:0:0
Host Name:                           G450-1
Client Identifier:                   01:11:22:33:44:55:66
Requested Options:                   default - router(3)
                                     Dns-servers(6)
                                     Domain-name(15)
Track-id:                            1
```

To show the configuration of the DHCP client in the general context:

```
G450-001(super)# show ip dhcp-client brief

Interface              Status       IP address     Lease-Remain
                                                   (D:H:M:S)
---------              ------       ----------     ------------
Fastethernet 10/2      Bound         1.1.1.2         1:2:3:4
```

Output fields

Name	Description
DHCP Client Mode	Whether DHCP Client is Enabled or Disabled
Status	The status of the DHCP client: • Select. Sending DISCOVER packets. • Request. Requesting IP address after selecting from all the offered packets. • Bound. Receiving ACK packet and there is no conflict detection by sending ARP packets. • Rebind. 0.875 of the lease time has passed, so the renewal phase entered rebind. • Renew. 0.5 of the lease time has passed, so the device is trying to renew the lease until 0.875 of the lease time will have passed. • Release. The client released the lease. • Decline. The client detected an IP conflict by sending an ARP packet. • Idle. The client did not get an IP address and keeps trying after an Idle time (~40 seconds) to reach new IP address.
IP address	The IP address received from the DHCP server
Subnet Mask	The subnet mask received from the DHCP server
Default Router	The list of default routers received from the DHCP server
DHCP Server	The IP address of the DHCP server
Domain name	The DHCP client's domain name received from the DHCP server
DNS Server	The list of available DNS servers received from the DHCP server

1 of 2

Name	Description
Lease Received	The amount of time the DHCP server grants the DHCP client an IP address
Lease Remains	The amount of time remaining until the expiration of the current lease.
Lease Rebind	The amount of time remaining until the rebind phase (0.875 of the lease time)
Lease Renew	The amount of time remaining until the renew phase (0.5 of the lease time)
Lease Requested	The lease requested by the DHCP client (see ip dhcp client lease)
Host Name	The host name of the DHCP client. The default value is the gateway's hostname, unless otherwise specified using the ip dhcp client hostname command.
Client Identifier	The client identifier of the DHCP client. The value is the MAC address of the interface, unless otherwise specified using the **`ip dhcp client client-id`** command.
Requested Options	The options requested by the DHCP client from the DHCP server. These options include: • the default routers • the available DNS servers • the domain name These options can be changed using the **`ip dhcp client request`** command.
Track-id	The index of the object tracker monitoring the route, if applied
	2 of 2

Related Commands

clear ip dhcp-client statistics, ip address dhcp, ip dhcp client client-id, ip dhcp client hostname, ip dhcp client lease, ip dhcp client request, ip dhcp client route track, ip dhcp client route track, release dhcp, renew dhcp, show ip dhcp-client statistics

show ip dhcp-client statistics

Use the **show ip dhcp-client statistics** command to show the DHCP Client statistics counters.

Note:

When you use this command in the interface context, the output displays the counters of the interface. When you use this command in the general context, the output displays the sum of all DHCP client counters, for all interfaces on which it is configured.

Note:

When the ip address dhcp command is used, the DHCP Client statistics counters for the relevant interface are cleared. The global parameters are not cleared.

Syntax

show ip dhcp-client statistics

User Level

read-only

Context

interface:FastEthernet 10/2,
general

Examples

To show the DHCP Client statistics counters in the interface context:

```
G450-001(config-if:FastEthernet 10/2)# show ip dhcp-client statistics
DHCP client interface statistics:

Tx counters:
Discover          : 1
Request           : 1
Decline           : 0
Release           : 0

Rx counters:
Offer             : 1
Ack               : 1
Nak               : 0
```

To show the DHCP Client statistics counters in the general context:

```
G450-001# show ip dhcp-client statistics
DHCP clients total statistics:

Tx counters:
Discover          : 1
Request           : 2
Decline           : 0
Release           : 0

Rx counters:
Offer             : 1
Ack               : 2
Nak               : 0
```

Output fields

Name	Description
Tx counters	The number of transmitted packets of the following types
Discover	A DHCP Client's first packet, to discover a DHCP server and request an IP address allocation
Request	A DHCP Client packet to request/renew a specific IP address offered/allocated by the DHCP server
Decline	A DHCP client packet sent when discovering congestion with the IP address allocated by the DHCP server
Release	A DHCP client release packet sent when releasing the IP address allocated by the DHCP server
Rx counters	The number of received packets of the following types:
Offer	A DHCP server packet sent as a response to a DHCP client Discover packet, containing the offered IP address
Ack	A DHCP server acknowledgement of the DHCP client request packet
Nak	A DHCP server refusal packet to a DHCP client request

Related Commands

clear ip dhcp-client statistics, ip address dhcp, ip dhcp client client-id, ip dhcp client hostname, ip dhcp client lease, ip dhcp client request, ip dhcp client route track, release dhcp, renew dhcp, show ip dhcp-client

DHCP server

clear ip dhcp-server binding

Binding is the allocation of an IP address to a client. Use the **clear ip dhcp-server binding** command to delete IP address binding. You can delete all bindings or the binding of a specific IP address. Clearing the binding of an IP address frees the IP address for reallocation by the DHCP server.

When the DHCP server detects an IP address conflict after attempting to allocate an IP address that is already in use, the server locks the IP address for half an hour by marking the IP address with client-identifier 00:00:00:00:00:00:00. If you have solved the conflict before half an hour, you can use this command to free the IP address for reallocation.

Syntax

clear ip dhcp-server binding {***ip-address***|**all**}

Parameters

Parameter	Description	Possible Values	Default Value
ip-address	Clears any existing allocation of the specified IP address	**1-32**	
all	Clears all IP address allocations.		

User Level

read-write

Context

general

Example

To clear the allocation of IP address 1.1.1.1:

```
G450-001(super)# clear ip dhcp-server binding 1.1.1.1
```

To clear all DHCP server IP address allocations:

```
G450-001(super)# clear ip dhcp-server binding all
```

Related Commands

clear ip dhcp server statistics, ip dhcp activate pool, ip dhcp ping packets, ip dhcp ping timeout, ip dhcp pool, ip dhcp-server, show ip dhcp-pool, show ip dhcp-server bindings, show ip dhcp-server statistics

clear ip dhcp server statistics

Use the **clear ip dhcp server statistics** command to clear the statistics of the DHCP server.

Syntax

clear ip dhcp server statistics

User Level

read-write

Context

general

Example

To clear the statistics of the DHCP server:

```
G450-001(super)# clear ip dhcp server statistics
```

Related Commands

clear ip dhcp-server binding, ip dhcp activate pool, ip dhcp ping packets, ip dhcp ping timeout, ip dhcp pool, ip dhcp-server, show ip dhcp-pool, show ip dhcp-server bindings, show ip dhcp-server statistics

ip dhcp activate pool

When you create a DHCP pool, the pool remains inactive until you activate it. This allows you to modify the pool configuration with no effect on network devices. Use the **ip dhcp activate pool** command to activate the pool. Use the **no** form of this command to deactivate the pool. When you deactivate a pool, the binding information of all IP addresses from the pool that were allocated is erased.

Syntax

[no] ip dhcp activate pool ***pool_id***

Parameters

Parameter	Description	Possible Values	Default Value
pool_id	The pool index	**1-32**	

User Level

read-write

Context

general

Example

To activate DHCP pool 5:

```
G450-001(super)# ip dhcp activate pool 5
```

Related Commands

clear ip dhcp-server binding, clear ip dhcp server statistics, ip dhcp ping packets, ip dhcp ping timeout, ip dhcp pool, ip dhcp-server, show ip dhcp-pool, show ip dhcp-server bindings, show ip dhcp-server statistics

ip dhcp ping packets

Use the **ip dhcp ping packets** command to enable the sending of a ping packet by the DHCP server to check if the IP address it is about to allocate is already in use by another client. The purpose of this feature is to prevent IP address congestion. Use the **no** form of this command to disable the sending of these ping packets.

Note:

Sending a ping packet before each IP address allocation reduces the rate at which DHCP clients can get new IP addresses from the server. Therefore, by default, ping packets are not sent.

Syntax

[no] ip dhcp ping packets

User Level

read-write

Context

general

Example

To configure the DHCP server to send ping packets to an IP address before assigning the IP address to a requesting client:

```
G450-001(DHCP 5)# ip dhcp ping packets
```

Related Commands

clear ip dhcp-server binding, clear ip dhcp server statistics, ip dhcp activate pool, ip dhcp ping timeout, ip dhcp pool, ip dhcp-server, show ip dhcp-pool, show ip dhcp-server bindings, show ip dhcp-server statistics

ip dhcp ping timeout

Use the **ip dhcp ping timeout** command to set the ping timeout. This is the time the DHCP server waits for a reply to a sent ping packet before allocating an IP address to a DHCP client. A lack of reply after the configured timeout indicates that the IP address is not in use and therefore can be allocated.

Syntax

ip dhcp ping timeout ***timeout***

Parameters

Parameter	Description	Possible Values	Default Value
timeout	The amount of time, in milliseconds, that the DHCP server waits for a ping reply before it stops attempting to reach a pool address for client assignment	**25-1000** ms	**500**

User Level

read-write

Context

general

Example

To set the ping timeout to one second:

```
G450-001(DHCP 5)# ip dhcp ping timeout 1000
```

Related Commands

clear ip dhcp-server binding, clear ip dhcp server statistics, ip dhcp activate pool, ip dhcp ping packets, ip dhcp pool, ip dhcp-server, show ip dhcp-pool, show ip dhcp-server bindings, show ip dhcp-server statistics

ip dhcp pool

Use the **ip dhcp pool** to create a DHCP pool or to enter the context of a DHCP pool. Use the **no** form of this command to delete a DHCP pool.

Note:

You cannot delete an active DHCP pool. Use the **no** form of the **dhcp-pool** command to deactivate a pool. When you deactivate the pool, any associated binding information is erased.

Syntax

[no] ip dhcp pool *pool-num*

Parameters

Parameter	Description	Possible Values	Default Value
pool-num	The DHCP pool index	**1-32**	

User Level

read-write

Context

general

Example

To enter the context of pool 5:

```
G450-001(super)# ip dhcp pool 5
G450-001(DHCP 5)#
```

Related Commands

clear ip dhcp-server binding, clear ip dhcp server statistics, ip dhcp activate pool, ip dhcp ping packets, ip dhcp ping timeout, ip dhcp-server, show ip dhcp-pool, show ip dhcp-server bindings, show ip dhcp-server statistics

bootfile

The bootfile provides startup parameters for the DHCP client device. Use the **bootfile** command to specify the file name to be used as boot file. Use the **no** form of this command to clear the boot file name.

Syntax

[no] bootfile *file-name*

Parameters

Parameter	Description	Possible Values	Default Value
file-name	The name of the file to be used as boot file	string, 1-128 bytes	null string

User Level

read-write

Context

dhcp pool

Example

To set `booter` as the bootfile:

```
G450-001(DHCP 5)# bootfile "booter"
```

To clear the bootfile definition:

```
G450-001(DHCP 5)# no bootfile
```

Related Commands

client-identifier, default-router, dns-server, domain-name, end-ip-addr, lease, name, next-server, option, server-name, show ip dhcp-pool, start-ip-addr, subnet-mask, value, vendor-specific-option

client-identifier

Use the **client-identifier** command to configure a reservation/manual pool. A reservation/manual pool reserves one IP address for a specific client. This command specifies a unique identifier for the client. The pool for which you configure a client identifier must contain one IP address only. This means that the start and end IP addresses of the pool must be equal. The DHCP server uses the client identifier to recognize the DHCP client and allocates the reserved IP address to the client. Use the **no** form of this command to clear a specified unique identifier for a DHCP client.

Syntax

[no] client-identifier *unique-identifier*

Parameters

Parameter	Description	Possible Values	Default Value
unique-identifier	A unique identifier for a DHCP client, in the format ***type*:*data***	Hex string, any value. For Ethernet MAC use ***type*:*data*** format, where ***type*** is **01** and ***data*** is the MAC address of the device.	null hex string

User Level

read-write

Context

dhcp pool

Example

To set the MAC address as a client identifier for an Ethernet MAC client with MAC address 00:11:22:33:44:55:

```
G450-001(DHCP 5)# client-identifier 01:00:11:22:33:44:55
```

Related Commands

bootfile, default-router, dns-server, domain-name, end-ip-addr, lease, name, next-server, option, server-name, show ip dhcp-pool, start-ip-addr, subnet-mask, value, vendor-specific-option

default-router

Use the **default-router** command to set up to eight default router IP addresses in order of preference. Use the **no** form of this command to clear the default router IP address(es).

Syntax

[no] default-router *ip-addr-list*

Parameters

Parameter	Description	Possible Values	Default Value
ip-addr-list	A list of up to eight IP addresses for the default router	A list of IP addresses separated by spaces	**0.0.0.0**

User Level

read-write

Context

dhcp pool

Example

To set 164.35.2.4 and 135.64.102.3 as default router IP addresses:

```
G450-001(DHCP 5)# default-router 164.35.2.4 135.64.102.3
```

Related Commands

bootfile, client-identifier, dns-server, domain-name, end-ip-addr, lease, name, next-server, option, server-name, show ip dhcp-pool, start-ip-addr, subnet-mask, value, vendor-specific-option

dns-server

Use the **dns-server** command to set up to eight Domain Name Server (DNS) IP addresses. Use the **no** form of this command to clear the DNS IP addresses.

Syntax

[no] dns-server *ip-addr-list*

Parameters

Parameter	Description	Possible Values	Default Value
ip-addr-list	A list of up to eight IP addresses for the Domain Name Server	A list of IP addresses separated by spaces	**0.0.0.0**

User Level

read-write

Context

dhcp pool

Example

To set 164.35.2.4 as the DNS IP address:

```
G450-001(DHCP 5)# dns-server 164.35.2.4
```

To set 164.35.2.4 and 135.64.102.3 as DNS IP addresses:

```
G450-001(DHCP 5)# dns-server 164.35.2.4 135.64.102.3
```

Related Commands

bootfile, client-identifier, default-router, domain-name, end-ip-addr, lease, name, next-server, option, server-name, show ip dhcp-pool, start-ip-addr, subnet-mask, value, vendor-specific-option

domain-name

Use the **domain-name** command to set a domain name string for the client. Use the **no** form of this command to clear the domain name.

Syntax

[no] domain-name *domain name*

Parameters

Parameter	Description	Possible Values	Default Value
domain name	The domain name	string, 1-255 bytes	null string

User Level

read-write

Context

dhcp pool

Example

To set the domain name to avaya.com:

```
G450-001(DHCP 5)# domain-name avaya.com
```

Related Commands

bootfile, client-identifier, default-router, dns-server, end-ip-addr, lease, name, next-server, option, server-name, show ip dhcp-pool, start-ip-addr, subnet-mask, value, vendor-specific-option

end-ip-addr

Use the **end-ip-addr** command to set the end IP address of a DHCP pool IP address range. For manual/reservation leasing, set the end IP address to be identical to the start IP address.

Syntax

[no] end-ip-addr *ip-addr*

Parameters

Parameter	Description	Possible Values	Default Value
ip-addr	The end IP address of the DHCP pool IP address range	The end IP address must be larger than the start IP address. The number of IP addresses in one pool cannot exceed 256.	**0.0.0.0**

User Level

read-write

Context

dhcp pool

Example

To set the end IP address of a DHCP pool IP address range as 135.64.120.4:

```
G450-001(DHCP 5)# end-ip-addr 135.64.120.4
```

Related Commands

bootfile, client-identifier, default-router, dns-server, domain-name, lease, name, next-server, option, server-name, show ip dhcp-pool, start-ip-addr, subnet-mask, value, vendor-specific-option

lease

Use the **lease** command to set the lease of a DHCP pool.

Syntax

lease {***seconds***|**infinite**}

Parameters

Parameter	Description	Possible Values	Default Value
seconds	The duration of the lease, in seconds	Unsigned integer 32	**691200** (8 days)
infinite	Sets the lease to permanent		

User Level

read-write

Context

dhcp pool

Example

To set a lease of 1 day:

```
G450-001(DHCP 5)# lease 86400
```

Related Commands

interface serial, ppp ipcp dns request, show interfaces,

name

Use the **name** command to assign a name to the specified list or operation. Use the **no** form of the command to return the name to the default value.

Syntax

[no] name *name*

Parameters

Parameter	Description	Possible Values	Default Value
name	The name of the list or operation. **Note:** If you wish to include spaces in the description, you must enclose the string in quotation marks (“”).	String of 1-31 characters	

User Level

read-write

Context

dhcp pool, dhcp pool vendor specific, dhcp pool option, ip qos-list, ip qos-list dscp-table, ip qos-list composite-operation, ip access-control-list, ip next-hop-list, ip capture-list, ip pbr-list, ip crypto-list.

Example

To specify the name of access control list 330 as Admin13:

```
G450-001(ACL 330)# name Admin13
```

Related Commands - DHCP server

bootfile, client-identifier, default-router, dns-server, domain-name, end-ip-addr, lease, next-server, option, server-name, show ip dhcp-pool, start-ip-addr, subnet-mask, value, vendor-specific-option

Related Commands - Packet sniffing

capture buffer-mode, capture buffer-size, capture filter-group, capture interface, capture ipsec, capture max-frame-size, capture start, capture stop, capture-service, clear capture-buffer, ip capture-list, show capture, show capture-buffer hex

Related Commands - Policy-based routing

ip-rule (policy, policy-based routing, packet sniffing), owner, show isdn bri link, show list

Related Commands - Policy

composite-operation, cookie, ip-fragments-in, ip-option-in, ip-rule (policy, policy-based routing, packet sniffing), owner, show composite-operation, show dscp-table, show isdn bri link, show list, cos, dscp (policy)

---

next-server

Use the **next-server** command to specify the IP address of the next server in the boot process of a DHCP client. Use the **no** form of this command to clear the next server IP address.

Syntax

[no] next-server *ip-address*

Parameters

Parameter	Description	Possible Values	Default Value
ip-address	The IP address of the next server in the boot process of a DHCP client	IP address	**0.0.0.0**

User Level

read-write

Context

dhcp pool

Example

To set 1.1.1.1 as the IP address of the next server in the boot process of a DHCP client:

```
G450-001(DHCP 5)# next-server 1.1.1.1
```

Related Commands

bootfile, client-identifier, default-router, dns-server, domain-name, end-ip-addr, lease, name, option, server-name, show ip dhcp-pool, start-ip-addr, subnet-mask, value, vendor-specific-option

option

Use the **option** command to create a DHCP general option or to enter the context of a DHCP general option. Use the **no** form of this command to clear a DHCP general option.

Syntax

[no] option *option-num*

Parameters

Parameter	Description	Possible Values	Default Value
option-num	The index of the DHCP option	**1-255** The exceptions are options configurable with specific commands and options that are part of the DHCP protocol, which are: 0, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 255.	

User Level

read-write

Context

dhcp pool

Example

To enter the context for option 42:

```
G450-001(DHCP 5)# option 42
G450-001(DHCP 5/option 42)#
```

Related Commands

bootfile, client-identifier, default-router, dns-server, domain-name, end-ip-addr, lease, name, next-server, server-name, show ip dhcp-pool, start-ip-addr, subnet-mask, value, vendor-specific-option

name

Use the **name** command to assign a name to the specified list or operation. Use the **no** form of the command to return the name to the default value.

Syntax

[no] name *name*

Parameters

Parameter	Description	Possible Values	Default Value
name	The name of the list or operation. **Note:** If you wish to include spaces in the description, you must enclose the string in quotation marks (“”).	String of 1-31 characters	

User Level

read-write

Context

dhcp pool, dhcp pool vendor specific, dhcp pool option, ip qos-list, ip qos-list dscp-table, ip qos-list composite-operation, ip access-control-list, ip next-hop-list, ip capture-list, ip pbr-list, ip crypto-list.

Example

To specify the name of access control list 330 as Admin13:

```
G450-001(ACL 330)# name Admin13
```

Related Commands - DHCP server

bootfile, client-identifier, default-router, dns-server, domain-name, end-ip-addr, lease, next-server, option, server-name, show ip dhcp-pool, start-ip-addr, subnet-mask, value, vendor-specific-option

Related Commands - Packet sniffing

capture buffer-mode, capture buffer-size, capture filter-group, capture interface, capture max-frame-size, capture start, capture stop, capture-service, clear capture-buffer, ip capture-list, show capture, show capture-buffer hex

Related Commands - Policy-based routing

ip-rule (policy, policy-based routing, packet sniffing), owner, show isdn bri link, show list

Related Commands - Policy

composite-operation, cookie, ip-fragments-in, ip-option-in, ip-rule (policy, policy-based routing, packet sniffing), owner, show composite-operation, show dscp-table, show isdn bri link, show list, cos, dscp (policy)

value

Use the **value** command to set the value of a DHCP option or a vendor-specific option. Use the **no** form of this command to clear the vendor-specific value.

Syntax

[no] value raw *type value*

Parameters

Parameter	Description	Possible Values	Default Value
raw	Non-encapsulated value		
type	Type of sub-option	**ascii** — ASCII **hex string** — hexadecimal **ip-address** — IP address **word** — 16 bit number **integer** — 32 bit number	
value	The sub-option value		

User Level

read-write

Context

dhcp pool vendor specific, dhcp pool option

Example

To specify IP addresses for World Wide Web servers (DHCP option 72):

```
G450-001(dhcp 5/option 72)# value raw ip-address "135.64.102.1, 135.64.102.2"
```

To enable IP forwarding (DHCP option 19 specifies whether the client should configure its IP layer for packet forwarding):

```
G450-001(dhcp 5/option 19)# value raw hex 01
```

To set a non-encapsulated value in ASCII format for vendor-specific option 1:

```
G450-001(DHCP 5/vendor specific 1)# value raw ascii
"MCIPADD=10.10.2.140,MCPORT=1719,TFTPSRVR=10.10.5.188"
```

To set a non-encapsulated value in Hex format for vendor-specific option 1:

```
G450-001(DHCP 5/vendor specific 1)# value raw hex 00:00:11:22:33:44:55:66:77
```

Related Commands

bootfile, class-identifier, client-identifier, default-router, dns-server, domain-name, end-ip-addr, lease, name, next-server, option, server-name, show ip dhcp-pool, start-ip-addr, subnet-mask, vendor-specific-option

server-name

Use the **server-name** command to specify the optional server name in the boot process of a DHCP client. Use the **no** form of this command to clear the optional server name.

Syntax

server-name *server-name*

no server-name

Parameters

Parameter	Description	Possible Values	Default Value
server-name	A name for the optional server, enclosed in quotes	string, 1-64 bytes	null string

User Level

read-write

Context

dhcp pool

Example

To set the optional server name to avaya:

```
G450-001(DHCP 5)# server-name "avaya"
```

Related Commands

bootfile, client-identifier, default-router, dns-server, domain-name, end-ip-addr, lease, name, next-server, option, show ip dhcp-pool, start-ip-addr, subnet-mask, value, vendor-specific-option

show ip dhcp-pool

Use the **show ip dhcp-pool** command to display DHCP pool configurations.

Syntax

show ip dhcp-pool [*pool-index*|all] [detailed]

Parameters

Parameter	Description	Possible Values	Default Value
pool-index	The index of a specific pool	**1-32**	
all	Displays all DHCP pools		
detailed	Displays detailed configuration information		

User Level

read-only

Context

general, dhcp pool

Example

To display the configuration of the current DHCP pool:

```
G450-001(DHCP 5)# show ip dhcp-pool
Index           Name
-------       ------------------
5             DHCP pool #5

Mode:                    Inactive
Start IP Address Range: 1.1.1.1
End IP Address Range:   1.1.1.20
Lease Time:              8 days 0 hours 0 minutes 0 seconds
BootFile:                N/A
Next-Server:             N/A
Client-Identifier:       N/A
```

```
Server-Name:            N/A
DHCP options
Option Num              1               Name     subnet-maskValue
255.255.255.0

Option Num              3               Name     default-router
Value                   1.1.1.1

Vendor Specific Information
Index                   1               Name     ccp.avaya.com
```

To display the configuration of DHCP pool 5:

```
G450-001(super)# show ip dhcp-pool 5
Index           Name
-------       ------------------
5             DHCP pool #5
Mode:                   Inactive
Start IP Address Range: 1.1.1.1
End IP Address Range:   1.1.1.20
Lease Time:             8 days 0 hours 0 minutes 0 seconds
BootFile:               N/A
Next-Server:            N/A
Client-Identifier:      N/A
Server-Name:            N/A

DHCP options
Option Num              1                Name     subnet-mask
Value                   255.255.255.0
Option Num              3                Name     default-router
Value                   1.1.1.1
Option Num              176              Name     SSON
Value                   This is an example

Vendor Specific Information
Index                   1                Name     ccp.avaya.com
Class-Identifier        (null)
Value                   This is an example too
```

To display the names and statuses of all configured DHCP pools:

```
G450-001(super)# show ip dhcp-pool all
Index   Name                        Mode
------  -------------------------  ------------
5       DHCP pool #5                Inactive
6       DHCP pool #6                Inactive
```

To display configuration information for all configured DHCP pools:

```
G450-001(super)# show ip dhcp-pool all detailed
```

```
Index           Name
-------       ------------------
5             DHCP pool #5
Mode:                    Inactive
Start IP Address Range: 1.1.1.1
End IP Address Range:   1.1.1.20
Lease Time:              8 days 0 hours 0 minutes 0 seconds
BootFile:                N/A
Next-Server:             N/A
Client-Identifier:       N/A
Server-Name:             N/A

DHCP options
Option Num                1                 Name     subnet-mask
Value                     255.255.255.0

Option Num                3                 Name     default-router
Value                     1.1.1.1

Option Num                176               Name     SSON
Value                     This is an example

Vendor Specific Information
Index                     1                 Name     ccp.avaya.com
Class-Identifier          (null)
Value                     This is an example too

Index           Name
-------       ------------------
6             DHCP pool #6

Mode:                    Inactive
Start IP Address Range: 2.2.2.2
End IP Address Range:   2.2.2.20
Lease Time:              8 days 0 hours 0 minutes 0 seconds
BootFile:                N/A
Next-Server:             N/A
Client-Identifier:       N/A
Server-Name:             N/A

DHCP options
Option Num                1                 Name     subnet-mask
Value                     255.255.255.248
Option Num                6                 Name     dns-server
Value                     1.1.1.1 2.2.2.2
```

Output fields

Name	Description
Index	The index number of the DHCP pool
Name	The name of the DHCP pool
Mode	Whether the DHCP pool is active or inactive
Start IP Address Range	The lower bound of the DHCP pool
End IP Address Range	The upper bound of the DHCP pool
Lease Time	The length of time for which an IP address allocated from the pool, belongs to a DHCP client
Bootfile	For BOOTP clients – the file to be downloaded by the client after the DHCP transaction ends
Next-Server	The IP address of the Server to be accessed by the DHCP client after the DHCP transaction ends
Client-Identifier	Used for static (manual) pools only, where permanent IP address allocation is done according to the configured client identifier
Server-Name	The optional server host name
DHCP options	The DHCP options configured for the pool. For each option, the following is displayed: Option Num — the DHCP option number Name — the name of the option Value — the value that the DHCP client receives
Vendor Specific Information	The DHCP options unique to an individual vendor class. These options differ according to the different vendors.

Related Commands

bootfile, client-identifier, default-router, dns-server, domain-name, end-ip-addr, lease, name, next-server, option, server-name, start-ip-addr, subnet-mask, value, vendor-specific-option

start-ip-addr

Use the **start-ip-addr** command to set the start IP address of a DHCP pool. For manual/reservation leasing, set the start IP address to be identical to the end IP address. Use the **no** form of this command to clear the start IP address of the pool. Since there is a combined limit of 256 IP addresses for all pools, clear both the start and end IP addresses in a pool using the **no** forms of **start-ip-addr** and **end-ip-addr** before you configure a new range.

Syntax

[no] start-ip-addr *ip-addr*

Parameters

Parameter	Description	Possible Values	Default Value
ip_addr	The start IP address of the DHCP pool	The start IP address must be smaller than the end IP address. The number of IP addresses in one pool cannot exceed 256.	**0.0.0.0**

User Level

read-write

Context

dhcp pool

Example

To set the start IP address of a DHCP pool to IP address 135.64.120.2:

```
G450-001(DHCP 5)# start-ip-addr 135.64.120.2
```

Related Commands

bootfile, client-identifier, default-router, dns-server, domain-name, end-ip-addr, lease, name, next-server, option, server-name, show ip dhcp-pool, subnet-mask, value, vendor-specific-option

subnet-mask

Use the **subnet-mask** command to set the subnet mask of a DHCP pool. Use the **no** form of this command to reset the subnet mask of the pool to default.

Syntax

[no] subnet-mask {*mask*|*prefix-length*}

Parameters

Parameter	Description	Possible Values	Default Value
mask	The subnet mask of the DHCP pool	**255.0.0.0-255.255.255.0**	**255.255.255.0**
prefix-length	The prefix length of subnet mask	**8-32**	**24**

User Level

read-write

Context

dhcp pool

Example

To set the subnet-mask for DHCP pool 5 to 255.255.255.240:

```
G450-001(DHCP 5)# subnet-mask 255.255.255.240
```

To set the subnet-mask for DHCP pool 5 to 255.255.255.240 by stating the subnet mask prefix:

```
G450-001(DHCP 5)# subnet-mask 28
```

Related Commands

bootfile, client-identifier, default-router, dns-server, domain-name, end-ip-addr, lease, name, next-server, option, server-name, show ip dhcp-pool, start-ip-addr, value, vendor-specific-option

vendor-specific-option

A vendor specific option is an option unique to an individual vendor class. Use the **vendor-specific-option** command to set a vendor specific option. Use the **no** form of this command to delete a vendor-specific option.

Syntax

[no] vendor-specific-option *index-num*

Parameters

Parameter	Description	Possible Values	Default Value
index-num	The index number of the vendor-specific option	**1-10**	

User Level

read-write

Context

dhcp pool

Example

To set vendor-specific-option number 1:

```
G450-001(DHCP 5)# vendor-specific-option 1
```

Related Commands

bootfile, client-identifier, default-router, dns-server, domain-name, end-ip-addr, lease, name, next-server, option, server-name, show ip dhcp-pool, start-ip-addr, subnet-mask, value

class-identifier

Use the **class-identifier** command to set a vendor specific identifier string.

Syntax

[no] class-identifier *string*

Parameters

Parameter	Description	Possible Values	Default Value
string	Identifier string for vendor specific option	string, 1-255 bytes	null string

Note:

To define an identifier string that includes spaces, enclose the entire string in quotation marks (for example, “New York”).

User Level

read-write

Context

dhcp pool vendor specific

Example

To set an identifier string for vendor-specific option 1:

```
G450-001(DHCP 5/vendor specific 1)# class-identifier ccp.avaya.com
```

Related Commands

value

---

name

Use the **name** command to assign a name to the specified list or operation. Use the **no** form of the command to return the name to the default value.

Syntax

[no] name *name*

Parameters

Parameter	Description	Possible Values	Default Value
name	The name of the list or operation. **Note:** If you wish to include spaces in the description, you must enclose the string in quotation marks (“”).	String of 1-31 characters	

User Level

read-write

Context

dhcp pool, dhcp pool vendor specific, dhcp pool option, ip qos-list, ip qos-list dscp-table, ip qos-list composite-operation, ip access-control-list, ip next-hop-list, ip capture-list, ip pbr-list, ip crypto-list.

Example

To specify the name of access control list 330 as Admin13:

```
G450-001(ACL 330)# name Admin13
```

Related Commands - DHCP server

bootfile, client-identifier, default-router, dns-server, domain-name, end-ip-addr, lease, next-server, option, server-name, show ip dhcp-pool, start-ip-addr, subnet-mask, value, vendor-specific-option

Related Commands - Packet sniffing

capture buffer-mode, capture buffer-size, capture filter-group, capture interface, capture max-frame-size, capture start, capture stop, capture-service, clear capture-buffer, ip capture-list, show capture, show capture-buffer hex

Related Commands - Policy-based routing

ip-rule (policy, policy-based routing, packet sniffing), owner, show isdn bri link, show list

Related Commands - Policy

composite-operation, cookie, ip-fragments-in, ip-option-in, ip-rule (policy, policy-based routing, packet sniffing), owner, show composite-operation, show dscp-table, show isdn bri link, show list, cos, dscp (policy)

---

value

Use the **value** command to set the value of a DHCP option or a vendor-specific option. Use the **no** form of this command to clear the vendor-specific value.

Syntax

[no] value raw *type value*

Parameters

Parameter	Description	Possible Values	Default Value
raw	Non-encapsulated value		
type	Type of sub-option	**ascii** — ASCII **hex string** — hexadecimal **ip-address** — IP address **word** — 16 bit number **integer** — 32 bit number	
value	The sub-option value		

User Level

read-write

Context

dhcp pool vendor specific, dhcp pool option

Example

To specify IP addresses for World Wide Web servers (DHCP option 72):

```
G450-001(dhcp 5/option 72)# value raw ip-address "135.64.102.1, 135.64.102.2"
```

To enable IP forwarding (DHCP option 19 specifies whether the client should configure its IP layer for packet forwarding):

```
G450-001(dhcp 5/option 19)# value raw hex 01
```

To set a non-encapsulated value in ASCII format for vendor-specific option 1:

```
G450-001(DHCP 5/vendor specific 1)# value raw ascii
"MCIPADD=10.10.2.140,MCPORT=1719,TFTPSRVR=10.10.5.188"
```

To set a non-encapsulated value in Hex format for vendor-specific option 1:

```
G450-001(DHCP 5/vendor specific 1)# value raw hex 00:00:11:22:33:44:55:66:77
```

Related Commands

bootfile, class-identifier, client-identifier, default-router, dns-server, domain-name, end-ip-addr, lease, name, next-server, option, server-name, show ip dhcp-pool, start-ip-addr, subnet-mask, vendor-specific-option

ip dhcp-server

By default, DHCP server is inactive. Use the **dhcp-server** command to activate the DHCP server on the G450. Use the **no** form of this command to deactivate the DHCP server.

Syntax

[no] ip dhcp-server

User Level

read-write

Context

general

Example

To enable DHCP server:

```
G450-001(super)# ip dhcp-server
```

Related Commands

clear ip dhcp-server binding, clear ip dhcp server statistics, ip dhcp activate pool, ip dhcp ping packets, ip dhcp ping timeout, ip dhcp pool, show ip dhcp-pool, show ip dhcp-server bindings, show ip dhcp-server statistics

show ip dhcp-server bindings

A binding is an assignment of an IP address to a client. Use the **show ip dhcp-server bindings** command to display bindings.

Syntax

show ip dhcp-server bindings

Parameters

User Level

read-only

Context

general

Example

To display all IP address allocations to clients:

```
G450-001(super)# show ip dhcp-server bindings

IP Address  Lease Expiration (seconds) Type      Client-Identifier
----------     ------------------    --------    ------------------
3.3.3.2        Infinite              Automatic   01:00:11:22:33:44:55
3.3.3.3        303244                Manual      01:00:11:22:33:44:56
```

Output fields

Name	Description
IP Address	The IP addresses allocated/reserved by the DHCP server
Lease Expiration (seconds)	The length of time that the IP address is kept for a specific client-id/ MAC address
Type	The type of address allocation. Options are: • Automatic — Dynamic IP address allocation • Manual — Static IP address allocation or a specific client-id, according to user configuration
Client-Identifier	The distinct identification of the DHCP client in dotted-hexadecimal notation. **Note:** The client-identifier for Ethernet stations is the MAC address, preceded by `01`.

Related Commands

clear ip dhcp-server binding, clear ip dhcp server statistics, ip dhcp activate pool, ip dhcp ping packets, ip dhcp ping timeout, ip dhcp pool, ip dhcp-server, show ip dhcp-pool, show ip dhcp-server statistics

show ip dhcp-server statistics

Use the **`show ip dhcp-server statistics`** command to display DHCP server statistics.

Syntax

`show ip dhcp-server statistics`

User Level

read-only

Context

general

Example

To display DHCP server statistics:

```
G450-001(super)# show ip dhcp-server statistics

Counter                Value
-----------           -------
BOOTP Requests           1
DHCP Discovers           2
DHCP Requests            3
DHCP Declines            4
DHCP Releases            5
DHCP Informs             6
BOOTP Replies            7
DHCP Offers              8
DHCP Acks                9
```

Output fields

Name	Description
BOOTP Requests	The number of BOOTP Request packets received by the DHCP server
DHCP Discovers	The number of DHCP Discover packets that arrived from DHCP clients, requesting allocation of a new IP address
DHCP Requests	The number of DHCP Request packets that arrived from DHCP clients, to request/renew new/allocated IP addresses
DHCP Declines	The number of DHCP Decline packets that arrived from DHCP clients, due to IP address congestion detected by the DHCP clients
DHCP Releases	The number of DHCP Release packets that arrived from DHCP clients for releasing allocated IP addresses
DHCP Informs	The number of DHCP Inform packets that arrived from DHCP clients, requesting configuration only
BOOTP Replies	The number of BOOTP Reply packets sent by the DHCP server

1 of 2

Name	Description
DHCP Offers	The number of DHCP Offer packets sent by the DHCP server, offering a new IP address to a DHCP client
DHCP Acks	The number of DHCP Acknowledge packets sent by the DHCP server, acknowledging requests of DHCP clients

2 of 2

Related Commands

clear ip dhcp-server binding, clear ip dhcp server statistics, ip dhcp activate pool, ip dhcp ping packets, ip dhcp ping timeout, ip dhcp pool, ip dhcp-server, show ip dhcp-pool, show ip dhcp-server bindings

Dialer interface

interface dialer

Use the **`interface dialer`** command to enter the interface dialer context and create or configure the Dialer interface. Use the **`no`** form of this command to delete the Dialer interface.

Syntax

`[no] interface dialer` ***`dialer-id`***

Parameters

Parameter	Description	Possible Values	Default Value
`dialer-id`	Identification number for the Dialer interface	**1**	**1**

User Level

read-write

Context

general

Example

To enter the context for interface dialer 1:

```
G450-001(super)# interface dialer 1
G450-001(if:dialer 1)#
```

Related Commands

dialer modem-interface, dialer order, dialer persistent, dialer persistent delay, dialer persistent initial delay, dialer persistent max-attempts, dialer persistent re-enable, dialer string, dialer wait-for-ipcp

dialer modem-interface

Use the **dialer modem-interface** command to associate a dialer to a modem interface. Use the **no** form of the command to remove the association.

Syntax

[no] dialer modem-interface *modem-interface-name*

Parameters

Parameter	Description	Possible Values	Default Value
modem-interface-name	Name of interface to which the modem is connected	**console** **usb-modem**	**N/A**

User Level

read-write

Context

interface:Dialer (L2, L2-L3)

Example

To associate a dialer to the Console:

```
G450-001(if:Dialer 1)# dialer modem-interface console
```

Related Commands

interface dialer, dialer order, dialer persistent, dialer persistent delay, dialer persistent initial delay, dialer persistent max-attempts, dialer persistent re-enable, dialer string, dialer wait-for-ipcp

dialer order

Use the **dialer order** command to set which dial strings are used upon a new dial trigger event. Use the **no** form of the command to clear the order. The default value is **sequential**.

Syntax

[no] dialer order {sequential | round-robin | last-successful}

Parameters

Parameter	Description	Possible Values	Default Value
sequential	Restart from beginning of dial list. This is the default.		
round-robin	Restarts dialing using the dial string following the most recently used dial string		
last-successful	Restarts dialing using the most recently successful string and continues to the next dial string in a list if a call fails		

User Level

read-write

Context

interface:Dialer (L2, L2-L3)

Example

To set that the last successful dial string is used upon a new dial trigger event:

```
G450-001(if:Dialer 1)# dialer order last-successful
```

Related Commands

interface dialer, dialer modem-interface, dialer persistent, dialer persistent delay, dialer persistent initial delay, dialer persistent max-attempts, dialer persistent re-enable, dialer string, dialer wait-for-ipcp

dialer persistent

Use the **dialer persistent** command to force the dialer to attempt to reconnect every second. Use the **no** form of the command to disable forcing of reconnect attempts.

Syntax

[no] dialer persistent

User Level

read-write

Context

interface:Dialer (L2, L2-L3)

Example

To force the dialer to attempt to reconnect every second:

```
G450-001(if:Dialer 1)# dialer persistent
```

Related Commands

interface dialer, dialer modem-interface, dialer order, dialer persistent delay, dialer persistent initial delay, dialer persistent max-attempts, dialer persistent re-enable, dialer string, dialer wait-for-ipcp

dialer persistent delay

Use the **dialer persistent delay** command to set the redial interval. Use the **no** form of the command to set the redial interval to 1.

Syntax

[no] dialer persistent delay *sec*

Parameters

Parameter	Description	Possible Values	Default Value
sec	Redial interval	**1-1000**	**20**

User Level

read-write

Context

interface:Dialer (L2, L2-L3)

Example

To set the redial interval to 20 seconds:

```
G450-001(if:Dialer 1)# dialer persistent delay 20
```

Related Commands

interface dialer, dialer modem-interface, dialer order, dialer persistent, dialer persistent initial delay, dialer persistent max-attempts, dialer persistent re-enable, dialer string, dialer wait-for-ipcp

dialer persistent initial delay

Use the **dialer persistent initial delay** command to set the minimum delay from boot to persistent dialing. Use the **no** form of the command to return the delay to the default value.

Note:

Use this command to prevent the Dialer interface from dialing out after the G450 is reset. This is needed because the primary interface does not become active immediately after the reset.

Syntax

[no] dialer persistent initial delay *sec*

Parameters

Parameter	Description	Possible Values	Default Value
sec	Initial delay	**1-1000**	**1**

User Level

read-write

Context

interface:Dialer (L2, L2-L3)

Example

To set the minimum delay from boot to persistent dialing to 20 seconds:

```
G450-001(if:Dialer 1)# dialer persistent initial delay 20
```

Related Commands

interface dialer, dialer modem-interface, dialer order, dialer persistent, dialer persistent delay, dialer persistent max-attempts, dialer persistent re-enable, dialer string, dialer wait-for-ipcp

dialer persistent max-attempts

Use the **dialer persistent max-attempts** command to set the number of consecutive dial attempts for the dial list. Use the **no** form of the command to set unlimited dial attempts.

Syntax

[no] dialer persistent max-attempts *max-att*

Parameters

Parameter	Description	Possible Values	Default Value
max-att	Maximum number of attempts	**1-1000**	**unlimited**

User Level

read-write

Context

interface:Dialer (L2, L2-L3)

Example

To set the number of consecutive dial attempts for the dial list to 50:

```
G450-001(if:Dialer 1)# dialer persistent max-attempts 50
```

Related Commands

interface dialer, dialer modem-interface, dialer order, dialer persistent, dialer persistent delay, dialer persistent initial delay, dialer persistent re-enable, dialer string, dialer wait-for-ipcp

dialer persistent re-enable

Use the **dialer persistent re-enable** command to set the persistent re-enable timer after the maximum number of dial attempts has been reached. Use the **no** form of the command to disable the persistent re-enable timer.

Syntax

[no] dialer persistent re-enable

User Level

read-write

Context

interface:Dialer (L2, L2-L3)

Example

To set the persistent re-enable timer after the maximum number of dial attempts has been reached:

```
G450-001(if:Dialer 1)# dialer persistent re-enable
```

Related Commands

interface dialer, dialer modem-interface, dialer order, dialer persistent, dialer persistent delay, dialer persistent initial delay, dialer persistent max-attempts, dialer string, dialer wait-for-ipcp

dialer string

Use the **dialer string** command to add a phone number to the dial list. Use the **no** form of the command to delete a number from the dial list.

Syntax

[no] dialer string *id dial-string*

Parameters

Parameter	Description	Possible Values	Default Value
id	The location of the phone number in the list	**1-5**	
dial-string	The modem string. The modem dial string may include non-numeric characters. Refer to the modem "AT Command" documentation at www.multitech.com.		

User Level

read-write

Context

interface:Dialer (L2, L2-L3)

Example

To add the phone number 6458458 to the dial list:

```
G450-001(if:Dialer 1)# dialer string 1 6458458
```

Related Commands

interface dialer, dialer modem-interface, dialer order, dialer persistent, dialer persistent delay, dialer persistent initial delay, dialer persistent max-attempts, dialer persistent re-enable, dialer wait-for-ipcp

dialer wait-for-ipcp

Use the **`dialer wait-for-ipcp`** command to set the maximum time the dialer waits between dialing a number to successfully establishing PPP/IPCP.

Syntax

`[no] dialer wait-for-ipcp sec`

Parameters

Parameter	Description	Possible Values	Default Value
`sec`	Time to wait	**1-300**	**45**

User Level

read-write

Context

interface:Dialer (L2, L2-L3)

Example

To set the maximum time the dialer waits between dialing a number to successfully establishing PPP/IPCP to 10 seconds:

```
G450-001(if:Dialer 1)# dialer wait-for-ipcp 10
```

Related Commands

interface dialer, dialer modem-interface, dialer order, dialer persistent, dialer persistent delay, dialer persistent initial delay, dialer persistent max-attempts, dialer persistent re-enable, dialer string

ip address negotiated

Use the **ip address negotiated** command to enable obtaining an IP address via PPP/IPCP negotiation. Use the **no** form of this command to disable IP address negotiation.

Note:

The **ip address negotiated** command is intended primarily for PPPoE and dialer modem.

Note:

When you release a negotiated IP address using **no ip address negotiated**, any DNS information is removed as well.

Note:

You cannot configure both DHCP address negotiation and PPP/ICMP address negotiation on the FastEthernet interface.

Syntax

[no] ip address negotiated

User Level

read-write

Context

interface:FastEthernet (PPP L2-L3), Dialer (L2-L3)

Example

To enable obtaining an IP address via PPP/IPCP negotiation:

```
G450-001(config-if:FastEthernet 10/2)# ip address negotiated
```

Related Commands

ppp ipcp dns request

Display

banner login

Use the **banner login** command to enter the login banner configuration mode. Use the **no** form of this command to set the login banner to its default value. The login banner appears before the user is prompted for the login name. To enter text for the login banner, refer to the command line on page 362.

Note:

Before creating a new banner, delete the current banner using the **no banner login** command.

Syntax

[no] banner login

User Level

admin

Context

general

Example

To enter login banner configuration mode:

```
G450-001(super)# banner login
G450-001(super-login)#
```

Related Commands

banner post-login, clear screen, hostname, line, show banner login, show banner post-login, terminal length, terminal width

banner post-login

Use the **banner post-login** command to enter the post-login banner configuration mode. The post-login banner appears after the user has logged in successfully. Use the **no** form of this command to set the post-login banner to its default value. To enter text for the post-login banner, refer to the command line on page 362.

Note:

Before creating a new banner, delete the current banner using the **no banner post-login** command.

Syntax

[no] banner post-login

User Level

admin

Context

general

Example

To enter the post-login banner configuration mode:

```
G450-001(super)# banner post-login
G450-001(super-post-login)#
```

Related Commands

banner login, clear screen, hostname, line, show banner login, show banner post-login, terminal length, terminal width

clear screen

Use the **clear screen** command to clear the current terminal display.

Syntax

clear screen

User Level

read-only

Context

general

Related Commands

banner login, banner post-login, hostname, line, show banner login, show banner post-login, terminal length, terminal width

hostname

Use the **hostname** command to change the Command Line Interface (CLI) prompt. The prompt is written as **hostname-registration**, where the ***hostname*** is the value entered with the **hostname** command, and ***registration*** is the media gateway registration information. If the device is registered, the current media gateway number appears. If the device is not registered, question marks are displayed.

Use the **hostname** command with no parameters to display the current prompt value. Use the **no** form of this command to return the CLI prompt to the default.

Syntax

hostname [*hostname_string*]

no hostname

Parameters

Parameter	Description	Possible Values	Default Value
hostname_string	The hostname	A string of up to 20 characters	**G450**

User Level

read-write

Context

general

Example

To set the CLI prompt to “GTW-HQ”:

```
G450-001(super)# hostname GTW-HQ
GTW-HQ-001(super)# hostname
Session hostname is 'GTW-HQ'
```

To reset the CLI prompt to the default:

```
GTW-HQ-001(super)# no hostname
G450-001(super)#
```

Related Commands

banner login, banner post-login, clear screen, line, show banner login, show banner post-login, terminal length, terminal width

line

Use the **line** command to add a line to the current banner message.

Syntax

line *number* [*string*]

Parameters

Parameter	Description	Possible Values	Default Value
number	The line number to add the specified text	**1-24**	
string	The text to display on the specified line		

Note:

To define a string that includes spaces, enclose the entire string in quotation marks (for example, “New York”).

User Level

admin

Context

banner login, banner post-login

Example

To specify text for the third line of the banner displayed after a successful login:

```
G450-001(super-banner-post-login)# line 3 “Welcome to the G450 Media Gateway
CLI Interface”
```

Related Commands

banner login, banner post-login, clear screen, hostname, show banner login, show banner post-login, terminal length, terminal width

show banner login

Use the **show banner login** command to display the banner that appears before the login prompt.

Syntax

show banner login

User Level

admin

Context

general

Example

To display the banner that appears before the login prompt:

```
G450-001(super)# show banner login
Welcome to G450 Media Gateway
FW version 0.11.0
```

Related Commands

banner login, banner post-login, clear screen, hostname, line, show banner post-login, terminal length, terminal width

show banner post-login

Use the **show banner post-login** command to display the banner that appears after a user logs in successfully.

Syntax

show banner post-login

User Level

admin

Context

general

Example

To display the banner that appears after a successful login:

```
G450-001(super)# show banner post-login
*** Welcome to the G450 Media Gateway CLI Interface ***
For questions, please refer to the CLI Reference Guide
```

Related Commands

banner login, banner post-login, clear screen, hostname, line, show banner login, terminal length, terminal width

terminal length

Use the **terminal length** command to set the length of the terminal display in characters.

Syntax

terminal length [*lines*]

Parameters

Parameter	Description	Possible Values	Default Value
lines	The number of lines in the terminal display	**none** - Displays the current length. **3-200** - Sets the new screen length to the value.	

User Level

read-only

Context

general

Example

To set the screen to display 24 lines:

```
G450-001(super)# terminal length 24
```

Related Commands

banner login, banner post-login, clear screen, hostname, line, show banner login, show banner post-login, terminal width

terminal width

Use the **terminal width** command to set the width of the terminal display in characters.

Syntax

terminal width [*characters*]

Parameters

Parameter	Description	Possible Values	Default Value
characters	The number of characters in the width of the terminal display	**none** - Displays the current width. **10-200** - Sets the new screen width to the value.	

User Level

read-only

Context

general

Example

To limit the display to a width of 60 characters:

```
G450-001(super)# terminal width 60
```

Related Commands

banner login, banner post-login, clear screen, hostname, line, show banner login, show banner post-login, terminal length

DNS resolver

clear ip domain statistics

Use the **clear ip domain statistics** command to clear the DNS Resolver's statistics counters.

Syntax

clear ip domain statistics

User Level

read-write

Context

general

Example

To clear the DNS Resolver's statistics counters:

```
G450-001(super)# clear ip domain statistics
```

Related Commands

ip domain list, ip domain lookup, ip domain name-server-list, ip domain retry, ip domain timeout, nslookup, show ip domain, show ip domain statistics

ip domain list

Use the **ip domain list** command to specify static domain names (suffixes) to complete non-FQDN names (host names that do not end with a dot). This aids the DNS Resolver in resolving the remote peer host name to an IP address. Use the **no** form of this command to delete a domain suffix.

Syntax

ip domain list *index domain-name*

no ip domain list *domain-name*

Parameters

Parameter	Description	Possible Values	Default Value
index	The index number of the suffix in the list of suffixes	**1-6**	
domain-name	The domain-name		

User Level

read-write

Context

general

Example

To specify the name support.avaya.com for suffix number 2:

```
G450-001(super)# ip domain list 2 support.avaya.com
```

Related Commands

clear ip domain statistics, ip domain lookup, ip domain name-server-list, ip domain retry, ip domain timeout, nslookup, show ip domain, show ip domain statistics

ip domain lookup

Use the **ip domain lookup** command to enable the DNS Resolver. Use the **no** form of this command to disable the DNS Resolver.

Note:

The DNS Resolver is enabled by default.

Syntax

[no] ip domain lookup

User Level

read-write

Context

general

Example

To enable the DNS Resolver:

```
G450-001(super)# ip domain lookup
```

Related Commands

clear ip domain statistics, ip domain list, ip domain name-server-list, ip domain retry, ip domain timeout, nslookup, show ip domain, show ip domain statistics

ip domain name-server-list

Use the **ip domain name-server-list** command to set up the list of DNS servers, or enter the list's context. Once you are in the context of the list, use the **name-server** command to add or delete DNS servers in the list.

Syntax

ip domain name-server-list *index*

Parameters

Parameter	Description	Possible Values	Default Value
index	The index number of the list	**1**	

User Level

read-write

Context

general

Example

To create DNS server list 1 and enter its context:

```
G450-001(super)# ip domain name-server-list 1
G450-001(name-server-list:1)#
```

Related Commands

clear ip domain statistics, description (DNS resolver), ip domain list, ip domain lookup, ip domain retry, ip domain timeout, name-server, nslookup, show ip domain, show ip domain statistics

description (DNS resolver)

Use the **description** command to specify a name for the DNS servers list. Use the **no** form of this command to restore the description of the list to the default value, which is **DNS list #1**.

Syntax

[no] description *description*

Parameters

Parameter	Description	Possible Values	Default Value
description	The name of the DNS servers list	string, 1-64 bytes	**DNS list #1**

User Level

read-write

Context

ip domain name-server-list

Example

To specify the DNS servers list name as All DNS servers:

```
G450-001(name-server-list:1)# description "All DNS servers"
```

Related Commands

clear ip domain statistics, ip domain list, ip domain lookup, ip domain name-server-list, ip domain retry, ip domain timeout, name-server, nslookup, show ip domain, show ip domain statistics,

name-server

Use the **name-server** command to add a DNS server to the list of up to six DNS servers. Use the **no** form of this command to delete the server from the list of DNS servers.

Syntax

name-server *index ip-addr*

no name-server { *ip-addr* | all | dynamic | static }

Parameters

Parameter	Description	Possible Values	Default Value
index	The index number of the DNS server, indicating its priority in the list	**1-6**	
ip-addr	The IP address of the DNS server		
all	Keyword indicating to delete all DNS servers from the list		
dynamic	Keyword indicating to delete all dynamic DNS servers from the list		
static	Keyword indicating to delete all static DNS servers from the list		

User Level

read-write

Context

ip domain name-server-list

Example

To add the DNS server with IP address 1.1.1.1 as the second server in list 1:

```
G450-001(name-server-list:1)# name-server 2 1.1.1.1
```

To delete all static DNS servers from list 1:

```
G450-001(name-server-list:1)# no name-server static
```

Related Commands

clear ip domain statistics, description (DNS resolver), ip domain list, ip domain lookup, ip domain name-server-list, ip domain retry, ip domain timeout, nslookup, show ip domain, show ip domain statistics

ip domain retry

Use the **ip domain retry** command to set the number of retries for a DNS query. Use the **no** form of this command to restore the retries value to the default value of 2.

Syntax

[no] ip domain retry *retries*

Parameters

Parameter	Description	Possible Values	Default Value
retries	The number of retries	**0-100**	**2**

User Level

read-write

Context

general

Example

To set the number of retries to 4:

```
G450-001(super)# ip domain retry 4
```

Related Commands

clear ip domain statistics, ip domain list, ip domain lookup, ip domain name-server-list, ip domain timeout, nslookup, show ip domain, show ip domain statistics

ip domain timeout

Use the **ip domain timeout** command to set the timeout for a DNS query. Use the **no** form of this command to restore the timeout value to the default value of 3 seconds.

Syntax

[no] ip domain timeout *timeout*

Parameters

Parameter	Description	Possible Values	Default Value
timeout	The timeout in seconds	**1-3600**	**3**

User Level

read-write

Context

general

Example

To set the timeout for a DNS query to 4 seconds:

```
G450-001(super)# ip domain timeout 4
```

Related Commands

clear ip domain statistics, ip domain list, ip domain lookup, ip domain name-server-list, ip domain retry, nslookup, show ip domain, show ip domain statistics

nslookup

Use the **nslookup** command to resolve a host name to an IP address.

Note:

The **nslookup** command has a timeout of 30 seconds.

Syntax

nslookup *hostname*

Parameters

Parameter	Description	Possible Values	Default Value
hostname	The host name		

User Level

read-only

Context

general

Example

To resolve the host name www.avaya.com to an IP address:

```
G450-001(super)# nslookup www.avaya.com
DNS server : 135.64.19.81
Host name  : pcmsnj.avaya.com
IP address : 216.74.135.14
Host alias : www.avaya.com
             pcms.avaya.com
```

Related Commands

clear ip domain statistics, ip domain list, ip domain lookup, ip domain name-server-list, ip domain retry, ip domain timeout, show ip domain, show ip domain statistics

ppp ipcp dns request

Use the **ppp ipcp dns request** command to enable requesting DNS information from the remote peer during the PPP/IPCP session. Use the **no** form of this command to restore the default value, which is not to request DNS information during the PPP/IPCP session.

Note:
The DNS Resolver uses the DNS servers discovered using this command.

Syntax

ppp ipcp dns request

no ppp ipcp dns

User Level

read-write

Context

Interface: Console, FastEthernet (PPP L2, PPP L2-L3), Serial (DS1 PPP L2, DS1 PPP L2-L3, USP PPP L2, USP PPP L2-L3) Dialer (L2, L2-L3), USB-modem

Example

To enable DNS information requests from the remote peer during the PPP/IPCP session:

```
G450-001(config-if:FastEthernet 10/2)# ppp ipcp dns request
```

Related Commands

ip address negotiated

show ip domain

Use the **show ip domain** command to display the DNS Resolver's configuration. The output shows the DNS servers that were statically configured and those which were gathered using DHCP or PPP protocols, as well as the list of domain suffixes.

Syntax

show ip domain

User Level

read-only

Context

general

Example

To display the DNS Resolver's configuration:

```
G450-001(super)# show ip domain
DNS resolver is enabled
Retries:                  2
Timeout (seconds):        3
Description: List #1
Index     IP Address    Type        Interface
-----     ----------    ----        ---------
1         1.1.1.1       Static      N/A
5         2.2.2.2       Static      N/A
100       3.3.3.3       PPP         FastEthernet 10/2

Index     Domain name
-----     ----------
1         emea.avaya.com
2         global.avaya.com
3         avaya.com
```

Output fields

Field	Description
Retries	The configured number of retries for a DNS query
Timeout (seconds)	The configured timeout for a DNS query
Description	The description of the DNS servers list
Index	The Index number of the DNS server. This number determines the order in which the DNS servers are accessed when the device tries to resolve a remote peer host name.
IP Address	The IP address of the DNS server
Type	How the DNS server was added to the list: • Static — added manually • PPP — gathered using PPP protocol • DHCP — gathered using DHCP protocol

1 of 2

Field	Description
Interface	The interface running the PPP or DHCP protocol that discovered the DNS server (where applicable)
Following is the list of configured static domain names (suffixes) used to complete non-FQDN names (host names that do not end with a dot). They aid the DNS Resolver in resolving a remote peer host name to an IP address.	
Index	The index number of the domain suffix. This number determines the order in which the domain suffixes are applied when trying to resolve a remote peer host name.
Domain name	The domain suffix
	2 of 2

Related Commands

clear ip domain statistics, ip domain list, ip domain lookup, ip domain name-server-list, ip domain retry, ip domain timeout, nslookup, show ip domain statistics

show ip domain statistics

Use the **show ip domain statistics** command to display the DNS Resolver's statistics counters.

Syntax

show ip domain statistics

User Level

read-only

Context

general

Example

To display the DNS Resolver's statistics counters:

```
G450-001(super)# show ip domain statistics
Transaction Type   Total Transactions  Success    Failures
---------------    ------------------  -------    --------
Standard query       1                   1           0
```

```
Query Type          Total Queries  Total Responses  Timeouts
--------------      ------------   ---------------  --------
Standard query        3              3                0

Return Code                         Responses
----------                          --------
No Error                              1
Format Error                          0
Server failure                        0
Name Error                            2
Note Implemented                      0
Refused                               0
Empty response                        0
Non requested DNS server response     0
Non recursive Server response         0
Too long UDP packet (>512B)           0
General errors                        0
```

Output fields

Field	Description
Total transactions	The total number of DNS resolution requests
Success	The number of successful transactions
Failures	The number of failed transactions
Total queries	The total number of DNS query packets sent by the DNS Resolver
Total responses	The total number of valid responses received from the DNS server
Timeouts	The total number of DNS query packets that timed out

Related Commands

clear ip domain statistics, ip domain list, ip domain lookup, ip domain name-server-list, ip domain retry, ip domain timeout, nslookup, show ip domain

show protocol

Use the **show protocol** command to display the status of a specific management protocol, or all protocols.

Syntax

show protocol
[ssh|telnet-client|ssh-client|https|snmp|telnet|telnet-services|http|scp|icmp|recovery-password|ftp-client|tftp|dhcp|dns-client]

Parameters

Parameter	Description	Possible Values	Default Value
ssh	Keyword indicating to display the status of the ssh protocol		
telnet-client	Keyword indicating to display the status of the telnet-client protocol		
ssh-client	Keyword indicating to display the status of the ssh-client protocol		
https	Keyword indicating to display the status of the https protocol		
snmp	Keyword indicating to display the status of the SNMP protocol		
telnet	Keyword indicating to display the status of the telnet protocol		
telnet-services	Keyword indicating to display the status of the telnet protocol on the Services interface		
http	Keyword indicating to display the status of the HTTP protocol		
scp	Keyword indicating to display the status of the SCP protocol		
icmp	Keyword indicating to display the status of the ICMP protocol		
recovery-password	Keyword indicating to display the status of the recovery-password protocol		
ftp-client	Keyword indicating to display the status of the FTP-client protocol		
tftp	Keyword indicating to display the status of the TFTP protocol		

Parameter	Description	Possible Values	Default Value
dhcp	Keyword indicating to display the status of the DHCP protocol		
dns-client	Keyword indicating to display the status of the DNS-client protocol		

User Level

admin

Context

general

Example

To display information about all protocols:

```
G450-001(super)# show protocol
Protocols                       Status
------------                    --------
SSH-CLIENT                        ON
TELNET-CLIENT                     OFF
SNMPv1                            ON
SNMPv3                            ON
TELNET                            ON
TELNET-SERVICES                   ON
HTTP                              ON
RECOVERY-PASSWORD                 ON
FTP-CLIENT                        ON
TFTP                              OFF
DHCP                              ON
DNS-CLIENT                        ON
```

Dynamic CAC

dynamic-cac

Use the **dynamic-cac** command to set the dynamic CAC bearer bandwidth limit for the current interface. You can also specify an activation priority for the interface. In case more than one interface with a BBL value is up, the G450 reports the BBL of the interface with the highest activation priority.

Syntax

[no] dynamic-cac *bbl* [*activation_priority*]

Parameters

Parameter	Description	Possible Values	Default Value
bbl	The bearer bandwidth for the current interface	**0-100,000,000** Kbits/sec	**-1**
activation_priority	The priority value of this interface	**1-255**	**50**

User Level

read-write

Context

interface:Serial (DS1 PPP L2, DS1 PPP L2-L3, DS1 FR-SUB L2, DS1 FR-SUB L2-L3, USP PPP L2 USP PPP L2-L3,), FastEthernet (L2, L2-L3, PPP L2, PPP L2-L3), Tunnel (L2, L2-L3), Dialer (L2, L2-L3), Loopback (L2, L2-L3), VLAN (L2, L2-L3)

Example

To set dynamic CAC on FastEthernet interface 10/2, with a bearer bandwidth limit of 128 and an activation priority of 100:

```
G450-001(super-if:FastEthernet 10/2)# dynamic-cac 128 100
```

Related Commands

show dynamic-cac

show dynamic-cac

Use the **show dynamic-cac** command to display information about the most recent dynamic CAC event.

Syntax

show dynamic-cac

User Level

read-only

Context

general

Example

To display information about the most recent dynamic CAC event:

```
G450-001(super)# show dynamic-cac
Current RBBL : 256 kbps
event : 0 Days, 1:21:00
Last event BBL : 256 kbps
```

Related Commands

dynamic-cac

Dynamic trap manager

clear dynamic-trap-manager

Use the **clear dynamic-trap-manager** command to remove administration of the dynamic trap manager.

Syntax

clear dynamic-trap-manager

User Level

read-write

Context

snmp-server dynamic-trap-manager

Example

To remove administration of the dynamic trap manager:

```
G450-001(super-survivable-call-engine)# clear dynamic-trap-manager
```

Related Commands

snmp-server dynamic-trap-manager

snmp-server dynamic-trap-manager

Use the **snmp-server dynamic-trap-manager** command to modify the SNMP settings of the dynamic trap manager. Use the **no** form of the command to restore the dynamic trap manager to its default settings, and remove all notification type filters.

Syntax

snmp-server dynamic-trap-manager {**traps**|**informs**} {**v1**|**v2c**} ***community-name*** [**udp-port** ***port***] [***notification-list***]

no snmp-server dynamic-trap-manager ***notification-list***

Parameters

Parameter	Description	Possible Values	Default Value
traps	Keyword indicating that the dynamic trap manager send messages without requesting acknowledgement. This is the default.		
informs	Keyword indicating that the dynamic trap manager send messages requiring acknowledgement		
v1	Keyword indicating that the dynamic trap manager use SNMP v1 functionality. This is the default.		
v2c	Keyword indicating that the dynamic trap manager use SNMP v2c functionality		

Parameter	Description	Possible Values	Default Value
community -name	The community string for accessing SNMP services		
port	The udp port of the SNMP host		
notification -list	The specific types of messages that the dynamic trap manager sends. Use this list to filter the messages controlled by the dynamic trap manager.	**all** — all traps **generic** — generic traps **hardware** — hardware faults **rmon** — RMON rising/falling alarm **dhcp server** — DHCP server error **dhcp-clients** — DHCP client error **rtp-stat-faults** — RTP statistics: QoS fault/clear traps **rtp-stat-qos** — RTP statistics: end-of-call QoS traps **wan** — WAN router traps **media-gateway** — media gateway traps **security** — security traps **config** — configuration change notifications **eth-port-faults** — notifications of Ethernet port faults **sw-redundancy** — software redundancy notifications **temperature** — temperature warning notifications **cam-change** — notifications about changes in CAM **l3-events** — notifications about L3 faults (duplicate IP, VLAN violations) **lag-event** — notifications about link aggregation faults and configuration changes **policy** — notifications about changes in policy (for L3 devices) **link-faults** — link-down notifications **supply** — power supply notifications	**all**

User Level

admin

Context

general

Example

To modify the SNMP settings of the dynamic trap manager:

```
G450-001(super)# snmp-server dynamic-trap-manager traps v2c public all
```

Related Commands - SNMP access configuration

ip snmp, set snmp community, set snmp retries, set snmp timeout, show snmp, show snmp engineID, show snmp group, show snmp retries, show snmp timeout, show snmp user, show snmp usertogroup, show snmp view, snmp-server community, snmp-server engineID, snmp-server group, snmp-server remote-user, snmp-server user, snmp-server view

Related Commands - SNMP trap configuration

set port trap, set snmp trap enable | disable auth, set snmp trap enable | disable frame-relay, show port trap, show snmp, snmp trap link-status, snmp-server enable notifications, snmp-server host, snmp-server informs

Related Commands - Dynamic trap manager

clear dynamic-trap-manager

E1/T1 interfaces

clear controller counters

Use the **clear controller counters** command to reset the controller counters.

Syntax

clear controller counters ***controller_number***

Parameters

Parameter	Description	Possible Values	Default Value
controller_number	The controller module number and port number		

User Level

read-only

Context

general

Example

To clear counters for controller 3/1:

```
G450-001(super)# clear controller counters 3/1
```

Related Commands

controller, cablelength long, cablelength short, channel-group, clock source, ds-mode, fdl, framing, interface serial, ip address, linecode (E1), linecode (T1), loopback, remote, show controllers, show controllers remote, show ds-mode

controller

Use the **controller** command to enter configuration mode for a specific controller.

Syntax

controller {e1 | t1} ***module_number/port_number***

Parameters

Parameter	Description	Possible Values	Default Value
module_number	The module number to configure	**3**, **4**, **8**	
port_number	The port to configure	**1**	

User Level

read-write

Context

general

Example

To enter configuration mode for a T1 controller on port 5/1:

```
G450-001(super)# controller t1 5/1
```

Related Commands

clear controller counters, cablelength long, cablelength short, channel-group, clock source, ds-mode, fdl, framing, interface serial, ip address, linecode (E1), linecode (T1), loopback, remote, show controllers, show controllers remote, show ds-mode

cablelength long

Use the **cablelength long** command to configure, transmit, and receive levels for a cable longer than 655 feet. Use the **no** form of the command to restore the transmit and receive levels to their default values.

Syntax

cablelength long *rx_level tx_level*

no cablelength long

Parameters

Parameter	Description	Possible Values	Default Value
rx_level	The receive sensitivity	**gain26**, **gain36**	**gain26**
tx_level	The transmit attenuation	**-15db, -22.5db, -7.5db, 0db**	**0db**

User Level

read-write

Context

interface:Controller (T1)

Example

To set the receive and transmit values for the cable to gain36 and -7.5db:

```
G450-001(super-controller:5/1)# cablelength long gain36 -7.5db
```

Related Commands

clear controller counters, controller, cablelength short, channel-group, clock source, ds-mode, fdl, framing, interface serial, ip address, linecode (E1), linecode (T1), loopback, remote, show controllers, show controllers remote, show ds-mode

cablelength short

Use the **cablelength short** command to configure transmit levels for a cable of length 655 feet or shorter. Use the **no** form of the command to restore the transmit level to its default value.

Note:

The transmit attenuation is configured using the loop length.

Syntax

cablelength short *tx_value*

Parameters

Parameter	Description	Possible Values	Default Value
tx_value	The transmit level	**133ft**, **266ft**, **399ft**, **533ft**, **655ft**	**133ft**

User Level

read-write

Context

interface:Controller (T1)

Example

To set the transmit value for the cable to 399ft:

```
G450-001(super-controller:5/1)# cablelength short 399ft
```

Related Commands

clear controller counters, controller, cablelength long, channel-group, clock source, ds-mode, fdl, framing, interface serial, ip address, linecode (E1), linecode (T1), loopback, remote, show controllers, show controllers remote, show ds-mode

channel-group

Use the **channel-group** command to create a channel group logical interface for a PPP or Frame Relay session. Use the **no** form of the command to delete a channel group.

Note:

If you issue this command with an existing channel number, the timeslots you specify will replace any that already exist.

Syntax

channel-group *channel_number* timeslots *ts_list* speed *speed_value*

no channel-group *channel_number*

Parameters

Parameter	Description	Possible Values	Default Value
channel_number	The ID number to identify the channel group	For T1: **0-23** For E1: **0-30**	
ts_list	The time slots to include in this channel group. Values can be separated either by a "–" for a range, or by commas for a list.	For T1: **1-24** For E1: **1-31**	
speed_value	The acceptable speed values	**56**, **64**	**56**

User Level

read-write

Context

interface:Controller

Example

To create a new channel group number 2, with time slots 5, 6, and 8 and speed of 56:

```
G450-001(super-controller:5/1)# channel-group 2 timeslots 5-6,8 speed 56
```

Related Commands

clear controller counters, controller, cablelength long, cablelength short, clock source, ds-mode, fdl, framing, interface serial, ip address, linecode (E1), linecode (T1), loopback, remote, show controllers, show controllers remote, show ds-mode

clock source

Use the **clock source** command to configure the clock source for an E1/T1 controller. Use the **no** form of the command to return the clock source to the default value of **line**.

Syntax

clock source {line | internal}

no clock source

Parameters

Parameter	Description	Possible Values	Default Value
line	Keyword that specifies to use an external clock		
internal	Keyword that specifies to synchronize to the internal clock		

User Level

read-write

Context

interface:Controller

Example

To specify that controller number 5 uses an external clock:

```
G450-001(super-controller:5/1)# clock source line
```

Related Commands

clear controller counters, controller, cablelength long, cablelength short, channel-group, ds-mode, fdl, framing, interface serial, ip address, linecode (E1), linecode (T1), loopback, remote, show controllers, show controllers remote, show ds-mode

fdl

Use the **fdl** command to define the type of Facility Data Link loopback that the remote line is requested to enter. Use the **no** form of the command to disable FDL.

Note:

This command can only be used when ESF framing is defined.

Syntax

fdl *fdl_mode*

no fdl

Parameters

Parameter	Description	Possible Values	Default Value
fdl_mode	The FDL type	**ansi**, **att**, **both**	**both**

User Level

read-write

Context

interface:Controller (T1)

Example

To set the FDL type to ansi:

```
G450-001(super-controller:5/1)# fdl ansi
```

Related Commands

clear controller counters, controller, cablelength long, cablelength short, channel-group, clock source, ds-mode, framing, interface serial, ip address, linecode (E1), linecode (T1), loopback, remote, show controllers, show controllers remote, show ds-mode

framing

Use the **framing** command to specify the frame type for an E1 or T1 data line. Use the **no** form of the command to restore the controller to the default frame type.

Syntax

framing ***frame_type***

no framing

Parameters

Parameter	Description	Possible Values	Default Value
frame_type	The framing method to use	**sf**, **esf**, **crc4**, **no-crc4**, **unframed**	For T1: **sf** For E1: **crc4**

User Level

read-write

Context

interface:Controller

Example

To set the frame type to extended super frame:

```
G450-001(super-controller:5/1)# framing esf
```

Related Commands

clear controller counters, controller, cablelength long, cablelength short, channel-group, clock source, ds-mode, fdl, interface serial, ip address, linecode (E1), linecode (T1), loopback, remote, show controllers, show controllers remote, show ds-mode

linecode (E1)

Use the **linecode** command to specify the type of line-code transmission for the an E1 line. Use the **no** form of the command to restore the default line-code value of **hbd3**.

Note:

Normally the E1 service provider determines which type of line-code is required for your E1 circuit.

Syntax

linecode {ami|hdb3}

Parameters

Parameter	Description	Possible Values	Default Value
ami	Keyword that specifies the Alternate Mode Inversion line-code type		
hbd3	Keyword that specifies the High-Density Bipolar 3 line-code type		

User Level

read-write

Context

interface:Controller (E1)

Example

To set the line-code type to ami:

```
G450-001(super-controller:5/1)# linecode ami
```

Related Commands

clear controller counters, controller, cablelength long, cablelength short, channel-group, clock source, ds-mode, fdl, framing, interface serial, ip address, linecode (T1), loopback, remote, show controllers, show controllers remote, show ds-mode

linecode (T1)

Use the **linecode** command to specify the type of line-code transmission for the a T1 line. Use the **no** form of the command to restore the default line-code value of **b8zs**.

Note:

Normally the T1 service provider determines which type of line-code is required for your T1 circuit.

Syntax

linecode {ami|b8zs}

Parameters

Parameter	Description	Possible Values	Default Value
ami	Keyword that specifies the Alternate Mode Inversion line-code type		
b8zs	Keyword that specifies the B8ZS line-code type		

User Level

read-write

Context

interface:Controller (T1)

Example

To set the line-code type to ami:

```
G450-001(super-controller:5/1)# linecode ami
```

Related Commands

clear controller counters, controller, cablelength long, cablelength short, channel-group, clock source, ds-mode, fdl, framing, interface serial, ip address, linecode (E1), loopback, remote, show controllers, show controllers remote, show ds-mode

loopback

Use the **loopback** command to put a T1 or E1 line into loopback mode. Use the **no** form of the command to disable loopback mode.

Syntax

For an E1 line:

loopback {[local {line | payload}] | diag}

no loopback

For a T1 line:

loopback {[local {line | payload}] | diag | [remote {line | payload}]}

no loopback

Parameters

Parameter	Description	Possible Values	Default Value
local	Keyword indicating that the controller loop the internal transmit signal back to the internal receive signal		
line	Keyword indicating that the controller loop the external line signal back toward the network without reframing the DS1 signal		
payload	Keyword indicating that the controller loop the external line signal back toward the network and reframes the DS1 signal		
diag	Keyword indicating that a loopback to the device is in place		
remote	Keyword indicating to create either a remote payload or a remote line loopback. Only in esf framing.		

User Level

read-write

Context

interface:Controller

Example

The following example establishes a local line loopback on the controller interface:

```
G450-001(super-controller:5/1)# loopback local line
```

Related Commands

clear controller counters, controller, cablelength long, cablelength short, channel-group, clock source, ds-mode, fdl, framing, interface serial, ip address, linecode (E1), linecode (T1), remote, show controllers, show controllers remote, show ds-mode

remote

Use the **remote** command to reset the far end counters on a T1 line.

Syntax

remote ***fdl_request_type***

Parameters

Parameter	Description	Possible Values	Default Value
fdl_request_type	The type of counters to reset	**reset-performance-monitoring-counters**, **reset-errored-esf-data**	

User Level

read-write

Context

interface:Controller (T1)

Example

To reset performance monitoring counters:

```
G450-001(super-controller:5/1)# remote reset-performance-monitoring-counters
```

Related Commands

clear controller counters, controller, cablelength long, cablelength short, channel-group, clock source, ds-mode, fdl, framing, interface serial, ip address, linecode (E1), linecode (T1), loopback, show controllers, show controllers remote, show ds-mode

ds-mode

Use the **ds-mode** command to specify the mode of the controller.

Note:

When you change the ds-mode, you must copy the running configuration to the startup configuration and reset the device.

Syntax

ds-mode {e1|t1}

Parameters

Parameter	Description	Possible Values	Default Value
e1	Keyword specifying to set the mode to E1		
t1	Keyword specifying to set the mode to T1		

User Level

admin

Context

general

Example

To set the controller to operate in T1 mode:

```
G450-001(super)# ds-mode t1
```

To change ds-mode, copy the running configuration to the start-up configuration file, and reset the device.

Related Commands

clear controller counters, controller, cablelength long, cablelength short, channel-group, clock source, fdl, framing, interface serial, ip address, linecode (E1), linecode (T1), loopback, remote, show controllers, show controllers remote, show ds-mode

interface serial

Use the **interface serial** command to enter Serial interface or sub interface configuration mode. If the specified interface or sub interface does not exist, the system creates it and enters its configuration mode.

Use the **no** form of the command to delete the interface. The **no** form can only be used to delete sub L3 and sub frame relay interfaces. The command fails for USP interfaces and when higher or lower layers are defined for that interface.

Syntax

[no] interface Serial *module/if_number* [*if_link_type*]

For USP interfaces ***if_number*** has the syntax:

port[.***ip_interface*** | {.***sub_interface***[.***ip_interface***]}]

For DS1 interfaces ***if_number*** has the syntax:

port:***channel_group***[.***ip_interface*** | {.***sub_interface***[.***ip_interface***]}]

Parameters

Parameter	Description	Possible Values	Default Value
module	The interface module number		
port	The port number of the interface		
channel_group		For E1: **0-30** For T1: **0-23**	
sub_interface		**1-127**	
ip_interface		**0-1024**	
if_link_type		**point-to-point**	

User Level

read-write

Context

general, interface:Serial (FR SUB)

Example

To create point to point sub-interface number 17 over channel group 2 over E1/T1 controller number 1:

```
G450-001(super)# interface Serial 3/1:2.17 point-to-point
```

Related Commands

clear controller counters, controller, cablelength long, cablelength short, channel-group, clock source, ds-mode, fdl, framing, ip address, linecode (E1), linecode (T1), loopback, remote, show controllers, show controllers remote, show ds-mode

ip address

Use the **ip address** command to assign an IP address and mask to an interface. Use the **no** form of this command to delete an IP interface.

Syntax

ip address {***ip_address mask*** [***admin_state***]}|**negotiated**

no ip address

Parameters

Parameter	Description	Possible Values	Default Value
ip_address	The IP address assigned to the interface		
mask	Mask for the associated IP subnet		
admin_state	The administration status. This parameter is not used with the Console interface.	**up**, **down**	**up**
negotiated	Keyword specifying that the interface receive address and mask from a remote device		

User Level

read-write

Context

Interface: Console, Serial (DS1 PPP L2-L3, DS1 PPP L3, DS1 FR-SUB L2-L3, DS1 FR-SUB L3, USP PPP L2-L3, USP PPP L3), FastEthernet (L2-L3, L3, PPP L2-L3, PPP L3), VLAN (L2-L3, L3), USB-modem, Loopback (L2-L3, L3), Tunnel (L2-L3, L3), Dialer (L2-L3, L3)

Example

To assign the IP address 192.168.22.33 with mask 255.255.255.0 to the FastEthernet interface:

```
G450-001(if:FastEthernet 10/2)# ip address 192.168.22.33 255.255.255.0
```

Related Commands

clear controller counters, controller, cablelength long, cablelength short, channel-group, clock source, ds-mode, fdl, framing, interface serial, linecode (E1), linecode (T1), loopback, remote, show controllers, show controllers remote, show ds-mode

show controllers

Use the **show controllers** command to display status information about a controller interface.

Syntax

show controllers [*module/port*]

Parameters

Parameter	Description	Possible Values	Default Value
module	The module number		
port	The port number		

User Level

read-write

Context

general

Example

To display controller status information:

```
G450-001(super)# show controllers

T1 5/1 is down.
Cablelength is long gain26 0db.
Transmitter is sending remote alarm.
Receiver has loss of signal.
Framing is SF, Line Code is AMI, Clock Source is Line.
```

```
Data in current interval (802 seconds elapsed):
0 Line Code Violations, 0 Path Code Violations
0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 802 Unavail Secs
Total Data (last 4 15 minute intervals):
10 Line Code Violations, 0 Path Code Violations
0 Slip Secs, 0 Fr Loss Secs, 1 Line Err Secs, 0 Degraded Mins
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 3600 Unavail Secs
```

Related Commands - E1/T1 interfaces

clear controller counters, controller, cablelength long, cablelength short, channel-group, clock source, ds-mode, fdl, framing, interface serial, ip address, linecode (E1), linecode (T1), loopback, remote, show controllers remote, show ds-mode

Related Commands - Verifying WAN configuration

show frame-relay fragment, show frame-relay lmi, show frame-relay pvc, show frame-relay traffic, show interfaces, show ip interface, show map-class frame-relay

show controllers remote

Use the **show controllers remote** command to display controller statistics from a peer station. If the Facility Data Link (FDL) for this controller is set to **att**, the system displays the status (up or down) of the line. Otherwise, the system displays statistics for the controller. To set the Facility Data Link, refer to fdl on page 389.

Syntax

show controllers remote *module/port fdl_data_type*

Parameters

Parameter	Description	Possible Values	Default Value
module	The module number		
port	The port number		
fdl_data_type	The type of statistics to display	**1h-data, errored-esf-data, enhanced-1h, enhanced-c1-configuration**	

User Level

read-write

Context

general

Example

To display 1h-data statistics for the T1 controller on port 1 of module 4:

```
G450-001(super)# show controllers remote 5/1 1h-data
```

Related Commands

clear controller counters, controller, cablelength long, cablelength short, channel-group, clock source, ds-mode, fdl, framing, interface serial, ip address, linecode (E1), linecode (T1), loopback, remote, show controllers, show ds-mode

---

show ds-mode

Use the **show ds-mode** command to display the current mode of the controller.

Syntax

show ds-mode

User Level

read-only

Context

general

Example

To display the current mode of the controller:

```
G450-001(super)# show ds-mode

Current ds-mode:    T1
Configured ds-mode: T1
```

Related Commands

clear controller counters, controller, cablelength long, cablelength short, channel-group, clock source, ds-mode, fdl, framing, interface serial, ip address, linecode (E1), linecode (T1), loopback, remote, show controllers, show controllers remote

Echo cancellation

set echo-cancellation analog

Use the **set echo-cancellation analog** command to control echo cancellation on analog lines and trunks.

Note:

The recommended setting for all analog trunks and lines is the default `auto` mode.

Syntax

set echo-cancellation analog *slot* [*port*] {on|off|auto}

Parameters

Parameter	Description	Possible Values	Default Value
slot	Number of the slot, represented as a number preceded by the letter **v**. For example, slot 1 is represented as **v1**.		
port	Number of the port on the module, represented as two digits. For example, port 2 is represented as **02**. If you do not specify a port, the command applies to all ports in this slot.		
on	Keyword specifying that echo cancellation be always on for the analog line or trunk		
off	Keyword specifying that echo cancellation be always off for the analog line or trunk		
auto	• For analog lines: keyword specifying that echo cancellation be always on. • For analog trunks: keyword specifying that the gateway controller function chooses when to employ the analog echo canceller on a call-by-call basis automatically for best echo coverage. This is the default value.		

User Level

read-write

Context

general

Example

To place port 7 in slot 3 under control of the gateway in auto mode:

```
G450-001(super)# set echo-cancellation analog v307 auto
```

Related Commands

set echo-cancellation config analog, set echo-cancellation config voip, set echo-cancellation voip, show echo-cancellation

set echo-cancellation config analog

Use the **set echo-cancellation config analog** command to configure echo cancellation on analog lines or trunks.

Note:

The recommended setting for all analog trunks and lines is the default configuration `31`.

Syntax

set echo-cancellation config analog ***slot*** [***port***] ***config1 config2***

Parameters

Parameter	Description	Possible Values	Default Value
slot	Number of the slot, represented as a number preceded by the letter **v**. For example, slot 1 is represented as **v1**.		
port	Number of the port on the module, represented as two digits. For example, port 2 is represented as **02**. If you do not specify a port, the command applies to all ports in this slot.		
config1	A number representing an echo cancellation configuration, as shown in Table 111. **Note**: The recommended setting is the default configuration. Do not change this setting unless instructed to do so for diagnostic purposes only.	**0-255**	**31**
config2	Reserved for future use	**0-255**	**0**

Table 111: Analog Trunk/Line Echo Cancellation Settings

Setting	Mode	Description	Comfort Noise Insertion	Call Start-up
0	NLP option 1	Basic NLP Operation	ON	Full reset
1	NLP option 2	More aggressive echo control but less open	ON	Full reset
2	NLP option 3	More full-duplex but less echo control	ON	Full reset
3-7	Reserved	WARNING!: UNEXPECTED RESULTS		
8	NLP option 1	Basic NLP Operation	OFF	Full reset
9	NLP option 2	More aggressive echo control but less open	OFF	Full reset
10	NLP option 3	More full-duplex but less echo control	OFF	Full reset
11-14	Reserved	WARNING!: UNEXPECTED RESULTS		

Table 111: Analog Trunk/Line Echo Cancellation Settings (continued)

Setting	Mode	Description	Comfort Noise Insertion	Call Start-up
15	NLP off	NLP disabled	OFF	Full reset
16	NLP option 1	Basic NLP Operation	ON	No reset
17	NLP option 2	More aggressive echo control but less open	ON	No reset
18	NLP option 3	More full-duplex but less echo control	ON	No reset
19-23	Reserved	WARNING!: UNEXPECTED RESULTS		
24	NLP option 1	Basic NLP Operation	OFF	No reset
25	NLP option 2	More aggressive echo control but less open	OFF	No reset
26	NLP option 3	More full-duplex but less echo control	OFF	No reset
27-30	Reserved	WARNING!: UNEXPECTED RESULTS		
31	NLP off	NLP disabled	OFF	Partial reset
32	NLP option 1	Basic NLP Operation	ON	Partial reset
33	NLP option 2	More aggressive echo control but less open	ON	Partial reset
34	NLP option 3	More full-duplex but less echo control	ON	Partial reset
35 - 39	Reserved	WARNING!: UNEXPECTED RESULTS		
40	NLP option 1	Basic NLP Operation	OFF	Partial reset
41	NLP option 2	More aggressive echo control but less open	OFF	Partial reset
42	NLP option 3	More full-duplex but less echo control	OFF	Partial reset
43 - 46	Reserved	WARNING!: UNEXPECTED RESULTS		

Table 111: Analog Trunk/Line Echo Cancellation Settings (continued)

Setting	Mode	Description	Comfort Noise Insertion	Call Start-up
47	NLP off	NLP disabled	OFF	Partial reset
48-255	Reserved	WARNING!: UNEXPECTED RESULTS		

User Level

read-write

Context

general

Examples

To configure line or trunk echo cancellation in port 1 of slot 4 to configuration 31:

```
G450-001(super)# set echo-cancellation config analog v401 31
```

Related Commands

set echo-cancellation analog, set echo-cancellation config voip, set echo-cancellation voip, show echo-cancellation

set echo-cancellation config voip

Use the **`set echo-cancellation config voip`** command to configure echo cancellation on the VoIP engine.

Note:

The recommended setting is the default configuration `0`.

Note:

This command takes effect immediately. It also affects currently active calls.

Syntax

`set echo-cancellation config voip` ***`config1 config2`***

Parameters

Parameter	Description	Possible Values	Default Value
config	A number representing an echo cancellation configuration, as shown in Table 112. **Note**: The recommended setting is the default configuration. Do not change this setting unless instructed to do so for diagnostic purposes only.	**0-255**	**0**
config2	Reserved for future use	**0-255**	**0**

Table 112: VoIP engine echo cancellation settings

Setting	Mode	Description	Comfort Noise Generation
0	NLP option 1	Default Non-linear Processing (NLP) Operation	ON
1	NLP option 2	More aggressive echo control but less open	ON
2	NLP option 3	More full-duplex but less echo control.	ON
3-7	Reserved	WARNING!: UNEXPECTED RESULTS	
8	NLP option 1	Default NLP Operation	OFF
9	NLP option 2	More aggressive echo control but less open	OFF
10	NLP option 3	More full-duplex but less echo control.	OFF
11-14	Reserved	WARNING!: UNEXPECTED RESULTS	
15	NLP off	NLP disabled. (For diagnostic purposes only, do not use. It will result in audible echo.)	OFF
16-255	Reserved	WARNING!: UNEXPECTED RESULTS	

User Level

read-write

Context

general

Examples

To configure echo cancellation on the VoIP engine to configuration 0:

```
G450-001(super)# set echo-cancellation config voip 0
```

Related Commands

set echo-cancellation analog, set echo-cancellation config analog, set echo-cancellation voip, show echo-cancellation

set echo-cancellation voip

Use the **set echo-cancellation voip** command to control echo cancellation on the VoIP engine.

Note:

The recommended setting is the default `auto` mode.

Syntax

set echo-cancellation voip {on|off|auto}

Parameters

Parameter	Description	Possible Values	Default Value
on	Keyword specifying that echo cancellation be always on		
off	Keyword specifying that echo cancellation be always off		
auto	keyword specifying that the gateway controller function chooses when to employ the VoIP echo canceller on a call-by-call basis automatically for best echo coverage. This is the default value.		

User Level

read-write

Context

general

Examples

To set echo cancellation for the VoIP engine to auto mode:

```
G450-001(super)# set echo-cancellation voip auto
```

Related Commands

set echo-cancellation analog, set echo-cancellation config analog, set echo-cancellation config voip, show echo-cancellation

show echo-cancellation

Use the **show echo-cancellation** command to display echo cancellation settings and configuration information.

Syntax

show echo-cancellation [{voip |*slot* [*port*]}]

Parameters

Parameter	Description	Possible Values	Default Value
voip	A keyword specifying to display VoIP engine echo cancellation mode and configuration information.		
slot	Number of the slot, represented as a number preceded by the letter **v**. For example, slot 1 is represented as **v1**.		
port	Number of the port on the module, represented as two digits. For example, port 2 is represented as **02**. If you do not specify a port, the command applies to all ports in this slot.		

User Level

read-write

Context

general

Examples

- To display echo cancellation settings for the entire gateway:

```
G450-001(super)# show echo-cancellation
VoIP setting:               echo cancellers are set to auto
VoIP configuration:         3
VoIP echo tail length:      32ms
v2 analog:
  Port  Setting  Config
  ----  -------  ------
     0     auto       8
     1      off       7
     2       on       8
   ...
v2 analog echo tail length: 8ms
```

- To display echo cancellation settings for the VoIP engine:

```
G450-001(super)# show echo-cancellation voip
VoIP setting:               echo cancellers are set to auto
VoIP configuration:         3
VoIP echo tail length:      32ms
```

- To display echo cancellation settings for slot 2:

```
G450-001(super)# show echo-cancellation v2
v2 analog:
  Port  Setting  Config
  ----  -------  ------
     0     auto       8
     1      off       7
     2       on       8
   ...
v2 analog echo tail length: 8ms
```

Related Commands

set echo-cancellation analog, set echo-cancellation config analog, set echo-cancellation config voip, set echo-cancellation voip

Ethernet port configuration

set port auto-negotiation-flowcontrol-advertisement

Use the **set port auto-negotiation-flowcontrol-advertisement** command to set the flowcontrol advertisement for the specified port when performing auto-negotiation.

Syntax

set port auto-negotiation-flowcontrol-advertisement ***module/port*** {**no-flowcontrol**|**asym-tx-only**|**sym-only**|**sym-and-asym-rx**}

Parameters

Parameter	Description	Possible Values	Default Value
module	Number of the module		
port	Number of the port on the module. You can also specify a range of ports separated by a dash, for example, 10/5-6 for both ETH LAN ports 5-6 on the front panel.		
no-flowcontrol	Keyword specifying that the port will advertise no pause capabilities		
asym-tx-only	Keyword specifying that the port will advertise asymmetric Tx pause capabilities only		
sym-only	Keyword specifying that the port will advertise symmetric pause capabilities only		
sym-and-asym-rx	Keyword specifying that the port will advertise both symmetric and asymmetric Rx pause capabilities		

User Level

read-write

Context

general

Example

To specify that port 6/5 will advertise asymmetric Tx pause capabilities only:

```
G450-001(super)# set port auto-negotiation-flowcontrol-advertisement 6/5
asym-tx-only
Port 6/5 pause capabilities was set
```

Related Commands

set port duplex, set port edge admin state, set port enable | disable, set port flowcontrol, set port level, set port name, set port negotiation, set port point-to-point admin status, set port speed, show port auto-negotiation-flowcontrol-advertisement, show port edge state, show port flowcontrol

set port duplex

Use the **set port duplex** command to configure the duplex type of an Ethernet or Fast Ethernet port or range of ports. You can configure Ethernet and FastEthernet interfaces to either full duplex or half duplex.

The duplex status of a port in auto-negotiation mode is determined by auto-negotiation. An error message is generated if you try to set the transmission type of auto-negotiation Fast Ethernet ports to half-duplex or full-duplex mode.

Syntax

set port duplex *module/port* {full|half}

Parameters

Parameter	Description	Possible Values	Default Value
module	Number of the module		
port	Number of the port on the module. You can also specify a range of ports separated by a dash, for example, 10/5-6 for both ETH LAN ports 5-6 on the front panel.		
full	Keyword specifying to set full-duplex transmission		
half	Keyword specifying to set half-duplex transmission		

User Level

read-write

Context

general

Example

To set port 6/5 to full duplex:

```
G450-001(super)# set port duplex 6/5 full
Port 6/5 set to full-duplex.
```

Related Commands

set port auto-negotiation-flowcontrol-advertisement, set port edge admin state, set port enable | disable, set port flowcontrol, set port level, set port name, set port negotiation, set port point-to-point admin status, set port speed, show port auto-negotiation-flowcontrol-advertisement, show port edge state, show port flowcontrol

set port edge admin state

Use the **set port edge admin state** command to assign or de-assign RSTP edge-port admin state to a port for Rapid Spanning Tree Protocol (RSTP) treatment.

Syntax

set port edge admin state *module/port admin_state*

Parameters

Parameter	Description	Possible Values	Default Value
module	Number of the module		
port	Number of the port on the module. You can also specify a range of ports separated by a dash, for example, 10/5-6 for both ETH LAN ports 5-6 on the front panel.		
admin_state	The type of the specified port	**edge-port**, **non-edge-port**	

User Level

read-write

Context

general

Example

To specify that port 6/5 is an edge port:

```
G450-001(super)# set port edge admin state 6/5 edge-port
```

Related Commands

set port auto-negotiation-flowcontrol-advertisement, set port duplex, set port enable | disable, set port flowcontrol, set port level, set port name, set port negotiation, set port point-to-point admin status, set port speed, show port auto-negotiation-flowcontrol-advertisement, show port edge state, show port flowcontrol

set port enable | disable

Use the **set port enable** | **disable** command to enable or disable a port or a range of ports.

Syntax

set port {**enable** | **disable**} ***module/port***

Parameters

Parameter	Description	Possible Values	Default Value
enable	Enable a port		
disable	Disable a port		
module	Number of the module		
port	Number of the port on the module. You can also specify a range of ports separated by a dash, for example, 10/5-6 for both ETH LAN ports 5-6 on the front panel.		

User Level

read-write

Context

general

Example

To enable port 6/5:

```
G450-001# set port enable 6/5
Port 6/5 enabled.
```

Related Commands

set port auto-negotiation-flowcontrol-advertisement, set port enable | disable, set port duplex, set port edge admin state, set port flowcontrol, set port level, set port name, set port negotiation, set port point-to-point admin status, set port speed, show port auto-negotiation-flowcontrol-advertisement, show port edge state, show port flowcontrol

set port flowcontrol

Use the **set port flowcontrol** command to set the send/receive mode for flow-control frames (IEEE 802.3x or proprietary) for a full duplex port. Each direction (send or receive) can be configured separately.

Syntax

set port flowcontrol {receive | send | all} ***module/port*** **{off | on | proprietary}**

Parameters

Parameter	Description	Possible Values	Default Value
receive	Keyword specifying whether the port can receive its administrative status from a remote device. This option is only available for Gigabit Ethernet modules with negotiation set to off.		
send	Keyword specifying whether the local port can send its administrative status to a remote device. This option is only available for Gigabit Ethernet modules with negotiation set to off.		
all	Keyword specifying whether the port can send and receive (symmetric flow control). Used with **on** indicates that the local port acts upon and sends flow control frames. Used with **off** indicates that the local port discards and does not send flow control frames.		
module	Number of the module		

Parameter	Description	Possible Values	Default Value
port	Number of the port on the module		
off	Used with **receive** to turn off an attached device's ability to send flow-control packets to a local port. Used with **send** to turn off the local port's ability to send administrative status to a remote device.		
on	Used with **receive** to specify that a local port receives administrative status from a remote device. Used with **send** to specify that a local port sends administrative status to a remote device.		
proprietary	Used with **all** to indicate that the local port acts on and sends Avaya proprietary flow control frames		

User Level

read-write

Context

general

Example

To specify that port 6/5 receives administrative status from a remote device:

```
G450-001# set port flowcontrol receive 6/5 on
Port 6/5 flow control receive administration status set to on
(port will require far end to send flowcontrol)
```

To specify that port 6/5 cannot send administrative status to a remote device:

```
G450-001# set port flowcontrol send 6/5 off
Port 6/5 flow control send administration status set to off
(port will send flowcontrol to far end)
```

Related Commands

set port auto-negotiation-flowcontrol-advertisement, set port enable | disable, set port duplex, set port edge admin state, set port enable | disable, set port level, set port name, set port negotiation, set port point-to-point admin status, set port speed, show port auto-negotiation-flowcontrol-advertisement, show port edge state, show port flowcontrol

set port level

Use the **set port level** command to set the priority level of a port or range of ports on the switching bus. Packets traveling through a port set at normal priority are served only after packets traveling through a port set at high priority are served.

Syntax

set port level *module/port* [*value*]

Parameters

Parameter	Description	Possible Values	Default Value
module	Number of the module		
port	Number of the port on the module. You can also specify a range of ports separated by a dash, for example, 10/5-6 for both ETH LAN ports 5-6 on the front panel.		
value	Priority level	**0-7**	

User Level

read-write

Context

general

Example

To set the priority level of port 6/5 to 5:

```
G450-001# set port level 6/5 5
Port 6/5 level set to 5
```

Related Commands

set port auto-negotiation-flowcontrol-advertisement, set port enable | disable, set port duplex, set port edge admin state, set port enable | disable, set port flowcontrol, set port name, set port negotiation, set port point-to-point admin status, set port speed, show port auto-negotiation-flowcontrol-advertisement, show port edge state, show port flowcontrol

set port name

Use the **set port name** command to configure a name for a port. If you do not specify a name, the port name displays as **NO NAME**.

Syntax

set port name *module/port* [*name*]

Parameter

Parameter	Description	Possible Values	Default Value
module	Number of the module		
port	Number of the port on the module. You can also specify a range of ports separated by a dash, for example, 10/5-6 for both ETH LAN ports 5-6 on the front panel.		
name	The port name	maximum 16-character string	

User Level

read-write

Context

general

Example

To set the name of port 6/5 to “arthur”:

```
G450-001# set port name 6/5 arthur
Port 6/5 name set.
```

Note:

If you wish to define a name which includes spaces, you must enclose the entire name in quotation marks, for example “new york”.

Related Commands

set port auto-negotiation-flowcontrol-advertisement, set port enable | disable, set port duplex, set port edge admin state, set port enable | disable, set port flowcontrol, set port level, set port negotiation, set port point-to-point admin status, set port speed, show port auto-negotiation-flowcontrol-advertisement, show port edge state, show port flowcontrol

set port negotiation

Use the **`set port negotiation`** command to enable or disable auto-negotiation on the specified port. Auto-negotiation uses a link negotiation protocol to determine the highest connection parameters available to connected ports, and configures the port speed and duplex setting of both ports. This command applies to Fast Ethernet or Gigabit Ethernet ports.

If negotiation is disabled, the user can set the speed and duplex of the Fast Ethernet ports.

Syntax

`set port negotiation` ***`module/port`*** **`{enable|disable}`**

Parameters

Parameter	Description	Possible Values	Default Value
`module`	Number of the module		
`port`	Number of the port on the module. You can also specify a range of ports separated by a dash, for example, 10/5-6 for both ETH LAN ports 5-6 on the front panel.		
`enable`	Keyword specifying to enable port negotiation protocol		
`disable`	Keyword specifying to disable port negotiation protocol		

User Level

read-write

Context

general

Example

To disable auto-negotiation on port 6/5:

```
G450-001# set port negotiation 6/5 disable
Link negotiation protocol disabled on port 6/5.
```

Related Commands

set port auto-negotiation-flowcontrol-advertisement, set port enable | disable, set port duplex, set port edge admin state, set port enable | disable, set port flowcontrol, set port level, set port name, set port point-to-point admin status, set port speed, show port auto-negotiation-flowcontrol-advertisement, show port edge state, show port flowcontrol

set port point-to-point admin status

Use the **set port point-to-point admin status** command to manage the connection type of the port.

Syntax

set port point-to-point admin status *module/port admin_status*

Parameters

Parameter	Description	Possible Values	Default Value
module	Number of the module		
port	Number of the port on the module. You can also specify a range of ports separated by a dash, for example, 10/5-6 for both ETH LAN ports 5-6 on the front panel.		
admin_status	The connection type of the port	**force-true** — specify that the port is connected point-to-point **force-false** — specify that this port is shared media **auto** — try to automatically detect the connection type of the port	

User Level

read-write

Context

general

Example

To specify that the connection type of port 6/5 is automatically detected:

```
G450-001(super)# set port point-to-point admin status 6/5 auto
```

Related Commands

set port auto-negotiation-flowcontrol-advertisement, set port enable | disable, set port duplex, set port edge admin state, set port enable | disable, set port flowcontrol, set port level, set port name, set port negotiation, set port speed, show port auto-negotiation-flowcontrol-advertisement, show port edge state, show port flowcontrol

set port speed

Use the **`set port speed`** command to configure the speed of a port or range of ports.

In auto-negotiation mode, the port's speed is determined by auto-negotiation. An error message is generated if you try to set the speed when auto-negotiation is enabled

Syntax

`set port speed` ***`module/port`*** **`10MB|100MB|1GB`**

Parameters

Parameter	Description	Possible Values	Default Value
`module`	Number of the module		
`port`	Number of the port on the module. You can also specify a range of ports separated by a dash, for example, 10/5-6 for both ETH LAN ports 5-6 on the front panel.		
`10MB`	Keyword that sets the specified port to a speed of 10 Mbps		

Parameter	Description	Possible Values	Default Value
100MB	Keyword that sets the specified port to a speed of 100 Mbps		
1GB	Keyword that sets the specified port to a speed of 1 Gbps		

User Level

read-write

Context

general

Example

To configure port 6/5 to 100 Mbps

```
G450-001(super)# set port speed 6/5 100MB
Port 6/5 speed set to 100 Mbps.
```

Related Commands

set port auto-negotiation-flowcontrol-advertisement, set port enable | disable, set port duplex, set port edge admin state, set port enable | disable, set port flowcontrol, set port level, set port name, set port negotiation, set port point-to-point admin status, show port auto-negotiation-flowcontrol-advertisement, show port edge state, show port flowcontrol

show port auto-negotiation-flowcontrol-advertisement

Use the **show port auto-negotiation-flowcontrol-advertisement** command to display the flowcontrol advertisement for a Gigabit port used to perform auto-negotiation. If no port is specified, information for all ports is displayed.

Syntax

show port auto-negotiation-flowcontrol-advertisement [*module/port*]

Parameters

Parameter	Description	Possible Values	Default Value
module	The module number		
port	The port number		

User Level

read-only

Context

general

Example

To display the flowcontrol advertisement for all ports:

```
G450-001(super)# show port auto-negotiation-flowcontrol-advertisement
asym-tx-only 4/49
Port 4/49 pause capabilities was set
```

Related Commands

set port auto-negotiation-flowcontrol-advertisement, set port enable | disable, set port duplex, set port edge admin state, set port enable | disable, set port flowcontrol, set port level, set port name, set port negotiation, set port point-to-point admin status, set port speed, show port edge state, show port flowcontrol

show port edge state

Use the **show port edge state** command to display the edge state of the specified port. If no port is specified, information for all ports is displayed.

Syntax

show port edge state [module/[port]]

Parameters

Parameter	Description	Possible Values	Default Value
module	Number of the module		
port	Number of the port on the module. You can also specify a range of ports separated by a dash, for example, 10/5-6 for both ETH LAN ports 5-6 on the front panel.		

User Level

read-only

Context

general

Example

To show edge state for all ports:

```
G450-001(super)# show port edge state
```

Related Commands

set port auto-negotiation-flowcontrol-advertisement, set port enable | disable, set port duplex, set port edge admin state, set port enable | disable, set port flowcontrol, set port level, set port name, set port negotiation, set port point-to-point admin status, set port speed, show port auto-negotiation-flowcontrol-advertisement, show port flowcontrol

show port flowcontrol

Use the **show port flowcontrol** command to display port flow control information. If no port is specified, information for all ports is displayed.

Syntax

show port flowcontrol [*module*[/*port*]]

Parameters

Parameter	Description	Possible Values	Default Value
module	Number of the module		
port	Number of the port on the module		

User Level

read-only

Context

general

Example

To display flowcontrol information for port 4 of module 3 on the G450:

```
G450-001(super)# show port flowcontrol 3/4

Port   Send-Flowcontrol Receive-Flowcontrol
       Admin Oper       Admin Oper
------ ----- ----      ----- ----
3/4    off   off        off   off
```

Related Commands

set port auto-negotiation-flowcontrol-advertisement, set port enable | disable, set port duplex, set port edge admin state, set port enable | disable, set port flowcontrol, set port level, set port name, set port negotiation, set port point-to-point admin status, set port speed, show port auto-negotiation-flowcontrol-advertisement, show port edge state

Output fields

Field	Description
Port	Module and port number
Send-Flowcontrol-Admin	Send flow-control administration. Possible settings: On — indicates that the local port is allowed to send flow control frames to the far end. Off — indicates that the local port is *not* allowed to send flow control frames to the far end.

1 of 2

Field	Description
Send-Flowcontrol-Oper	Send flow-control operation mode. Possible modes: On — indicates that the local port will send flow control frames to the far end. Off — indicates that the local port will *not* send flow control frames to the far end.
Receive-Flowcontrol-Admin	Receive flow-control administration. Possible settings: On — indicates that the local port will act upon flow control indications if received from the far end. Off — indicates that the local port will discard flow control frames if received from the far end.
Receive-Flowcontrol-Oper	Receive flow-control operation mode. Possible modes: On — indicates that the local port will act upon flow control indications received from the far end. Off — indicates that the local port will discard flow control frames received from the far end.

2 of 2

ETR

set etr

Use the **`set etr`** command to enable or disable Emergency Transfer Relay (ETR) mode, or to allow the gateway to control ETR mode automatically.

Note:

If a call is in progress when the communications problem ends, the gateway does not turn off ETR mode automatically. If you specify **manual-off**, the call terminates.

Syntax

`set etr` ***`module`*** **`{auto | manual-on }`**

Parameters

Parameter	Description	Possible Values	Default Value
module	Module number	**10**	
auto	Allow the gateway to control ETR mode automatically		
manual-on	Keyword specifying to set ETR mode to on		

User Level

read-write

Context

general

Example

To specify that the gateway will control ETR mode automatically on module 10:

```
G450-001(super)# set etr 10 auto
```

Related Commands

show etr

---

show etr

Use the **show etr** command to view the status of Emergency Transfer Relay (ETR) mode.

Syntax

show etr

User Level

read-only

Context

general

Example

To display the ETR status:

```
G450-001(super)# show etr
Module: 7
```

```
Admin State: auto
Module status: in service
Trunk line  line status
----- ----  -----------
1     2     off hook
```

Related Commands

set etr

Fans

show platform fans

Use the **show platform fans** command to display information about the fan tray unit.

Syntax

show platform fans

User Level

admin

Context

general

Example

To display information on the fan tray unit:

```
G450-001(super)# show platform fans
FAN TRAY UNIT #1:
-------------------------------------------------
Type            : G450 FAN TRAY
Description     : G450 FAN TRAY UNIT
Serial Number   : xxxxxxxxxxxx
HW Vintage      : 1
HW Suffix       : A
Faults          : No Fault Messages
```

Related Commands

show platform power, show platform mainboard

```
System Name             : G450
System Location         :
System Contact          :
Uptime (d,h:m:s)        : 0,03:41:57
MV Time                 : 15:02:27 27-SEP-2005
Serial No               : 0PIS81865230
Model No                : G450
HW Ready for FIPS       : No
HW Vintage              : 1
Chassis HW Suffix       :
Mainboard HW Vintage  : 1
Mainboard HW Suffix   : A
Mainboard FW Vintage  : 25.16.50
LAN MAC Address         : 00:04:0d:29:c6:bd
WAN1 MAC address        : 00:04:0d:29:c6:bb
WAN2 MAC address        : 00:04:0d:29:c6:bc
SERVICES MAC address    : 00:04:0d:29:c6:be
Memory #1               : 256MB
Memory  #2              : Not present
PSU #1                  : xxxx400W
PSU #2                  : xxxx400W
Media Socket #1         : VoIP DSP xxxxx8102
Media Socket #2         : VoIP DSP xxxxx7119
Media Socket #3         : Not present
Media Socket #4         : Sync-Over-IP xxxxxZarlink222
FAN Trays               : xxxxxxxxx
```

Firmware management

copy ftp EW_archive

Use the **copy ftp EW_archive** command to download Avaya G450 Manager software from an FTP server. The FTP command prompts for the username and password after the command is entered.

Syntax

copy ftp EW_archive *filename ip*

Parameters

Parameter	Description	Possible Values	Default Value
filename	The file name on the FTP server		
ip	The IP address of the FTP server		

User Level

read-write

Context

general

Example

To download `g450.img` from the FTP server at IP address 135.64.10.33, using login dan:

```
G450-001(super)# copy ftp EW_archive g450.img 135.64.10.33
Username: dan
Password:
```

Related Commands

copy ftp module, copy ftp SW_imageA, copy ftp SW_imageB, copy tftp EW_archive, copy tftp module, copy tftp SW_imageA, copy tftp SW_imageB, copy usb announcement-file, dir, set boot bank, show boot bank, show download software status, show image version

copy ftp module

Use the **`copy ftp module`** command to download firmware from an FTP server into a media module. The FTP command prompts for the username and password after the command is entered.

Syntax

`copy ftp module` ***`module_number filename ip`***

Parameters

Parameter	Description	Possible Values	Default Value
module_number	The Media Module number		
filename	The file name on the FTP server		
ip	The IP address of the FTP server		

User Level

read-write

Context

general

Example

To download the firmware file, `mm.img`, into media module 3 from the FTP server at IP address 135.64.10.33 using login dan:

```
G450-001(super)# copy ftp module 3 mm.img 135.64.10.33
Username: dan
Password:
```

Related Commands

copy ftp EW_archive, copy ftp SW_imageA, copy ftp SW_imageB, copy tftp EW_archive, copy tftp module, copy tftp SW_imageA, copy tftp SW_imageB, copy usb announcement-file, dir, set boot bank, show boot bank, show download software status, show image version

copy ftp SW_imageA

Use the **`copy ftp SW_imageA`** command to download a software image from an FTP server into Bank A. The command prompts for the username and password.

Syntax

`copy ftp SW_imageA` ***`filename ip`***

Parameters

Parameter	Description	Possible Values	Default Value
filename	File name on the FTP server		
ip	IP address of the FTP server		

User Level

read-write

Context

general

Example

To download the software image file, `G450.img`, from the FTP site at IP address 135.64.10.33 using login dan:

```
G450-001(super)# copy ftp SW_imageA G450.img 135.64.10.33
Username: dan
Password:
```

Related Commands

copy ftp EW_archive, copy ftp module, copy ftp SW_imageB, copy tftp EW_archive, copy tftp module, copy tftp SW_imageA, copy tftp SW_imageB, copy usb announcement-file, dir, set boot bank, show boot bank, show download software status, show image version

copy ftp SW_imageB

Use the **`copy ftp SW_imageB`** command to download a software image from an FTP server into Bank B. The command prompts for the username and password.

Syntax

`copy ftp SW_imageB` ***`filename ip`***

Parameters

Parameter	Description	Possible Values	Default Value
filename	File name on the FTP server		
ip	IP address of the FTP server		

User Level

read-write

Context

general

Example

To download the software image file `G450.img` from the FTP site at IP address 135.64.10.33 using login dan:

```
G450-001(super)# copy ftp SW_imageB G450.img 135.64.10.33
Username: dan
Password:
```

Related Commands

copy ftp EW_archive, copy ftp module, copy ftp SW_imageA, copy tftp EW_archive, copy tftp module, copy tftp SW_imageA, copy tftp SW_imageB, copy usb announcement-file, dir, set boot bank, show boot bank, show download software status, show image version

copy tftp EW_archive

Use the **`copy tftp EW_archive`** command to download the media gateway manager application into the media gateway via TFTP.

To use this command, you need to have an active TFTP server, and to create a file into which to download the data. If Avaya Network Manager is running, you do not need an additional TFTP server.

Syntax

`copy tftp EW_archive` ***`filename ip`***

Parameters

Parameter	Description	Possible Values	Default Value
filename	The manager image file name (full path)		
ip	The IP address of the host		

User Level

read-write

Context

general

Example

To download the media gateway manager software with filename `mgr.cfg` from the TFTP server located at IP address 192.168.49.10:

```
G450-001(super)# copy tftp EW_archive c:\G450\mgr.cfg 192.168.49.10
```

Related Commands

copy ftp EW_archive, copy ftp module, copy ftp SW_imageA, copy ftp SW_imageB, copy tftp module, copy tftp SW_imageA, copy tftp SW_imageB, copy usb announcement-file, dir, set boot bank, show boot bank, show download software status, show image version

copy tftp module

Use the **`copy tftp module`** command to download a new version of module software into a particular media module from a saved file, via TFTP.

To use this command, you need to have an active TFTP server, and to create a file into which to download the software. If Avaya Network Manager is running, you do not need an additional TFTP server.

Note:

Perform the **`nvram initialize`** command prior to the **`copy tftp module`** command.

Syntax

`copy tftp module` ***`module_number filename ip`***

Parameters

Parameter	Description	Possible Values	Default Value
module_number	The module number		
filename	The file name, including the full path		
ip	The IP address of the TFTP server		

User Level

read-write

Context

general

Example

To download the software file, `mm1.cfg`, for media module 5 from the TFTP server 192.168.49.10:

```
G450-001(super)# copy tftp module 5 c:\config\mm1.cfg 192.168.49.10
```

Related Commands

copy ftp EW_archive, copy ftp module, copy ftp SW_imageA, copy ftp SW_imageB, copy tftp EW_archive, copy tftp SW_imageA, copy tftp SW_imageB, copy usb announcement-file, dir, set boot bank, show boot bank, show download software status, show image version

copy tftp SW_imageA

Use the **`copy tftp SW_imageA`** command to update the software image in Bank A of the media gateway.

To use this command, you need to have an active TFTP server, and to create a file into which to download the data. If Avaya Network Manager is running, you do not need an additional TFTP server.

Syntax

`copy tftp SW_imageA` ***`filename ip`***

Parameters

Parameter	Description	Possible Values	Default Value
filename	The file name, including the full path		
ip	IP address of the host		

User Level

read-write

Context

general

Example

To download the software file, `imgA.bin`, from the TFTP server 149.49.36.200 into boot bank A:

```
G450-001(super)# copy tftp SW_imageA c:\imgA.bin 149.49.36.200

Beginning download operation ...
This operation may take a few minutes...
Please refrain from any other operation during this time.
```

Related Commands

copy ftp EW_archive, copy ftp module, copy ftp SW_imageA, copy ftp SW_imageB, copy tftp EW_archive, copy tftp module, copy tftp SW_imageB, copy usb announcement-file, copy usb announcement-file, dir, set boot bank, show boot bank, show download software status, show image version

copy tftp SW_imageB

Use the **`copy tftp SW_imageB`** command to update the software image in Bank B of the media gateway.

To use this command, you need to have an active TFTP server, and to create a file into which to download the data. If Avaya Network Manager is running, you do not need an additional TFTP server.

Syntax

`copy tftp SW_imageB` ***`filename ip`***

Parameters

Parameter	Description	Possible Values	Default Value
filename	The file name, including the full path		
ip	IP address of the host		

User Level

read-write

Context

general

Example

To download the software file, `imgB.bin`, from the TFTP server 149.49.36.200 into boot bank B:

```
G450-001(super)# copy tftp SW_imageB c:\imgB.bin 149.49.36.200

Beginning download operation ...
This operation may take a few minutes...
Please refrain from any other operation during this time.
```

Related Commands

copy ftp EW_archive, copy ftp module, copy ftp SW_imageA, copy ftp SW_imageB, copy tftp EW_archive, copy tftp module, copy tftp SW_imageA, copy usb announcement-file, dir, set boot bank, show boot bank, show download software status, show image version

copy usb EW_archive

Use the **`copy usb EW_archive`** command to download Avaya G450 Manager software from the external USB mass storage device to the gateway.

Syntax

copy usb EW_archive ***source-usb-device source-filename***

Parameters

Parameter	Description	Possible Values	Default Value
source usb-device	The source USB mass storage device	**usb-device0**	
source-filename	The full name and path of the file to be downloaded		

User Level

Admin

Context

general

Example

To download `g450_emweb_4_0.bin` from usb-device0 to the gateway:

```
G450-001(super)# copy usb announcement-file usb-device0 \temp\
g450_emweb_4_0.bin
```

Related Commands

backup config usb, copy announcement-file usb, erase usb, restore usb, safe-removal usb, show backup status, show restore status, show usb

copy usb module

Use the **`copy usb module`** command to download firmware from the external USB mass storage device to the gateway.

Syntax

copy usb module ***source-usb-device source-filename module-number***

Parameters

Parameter	Description	Possible Values	Default Value
source usb-device	The source USB mass storage device	**usb-device0**	

Parameter	Description	Possible Values	Default Value
source-filename	The full name and path of the file to be downloaded		
module-number	The slot number of the media module being upgraded		

User Level

Admin

Context

general

Example

To download the firmware file, `mm714v67.fdl`, from usb-device0 to the media module in slot 3 of the gateway:

```
G450-001(super)# copy usb module usb-device0 \temp\mm714v67.fdl 3
```

Related Commands

backup config usb, copy announcement-file usb, erase usb, restore usb, safe-removal usb, show backup status, show restore status, show usb

copy usb SW_image

Use the **`copy usb SW_image`** command to download a software from the external USB mass storage device into Bank A or Bank B.

Syntax

copy usb {SW_imageA | SW_imageB} ***source-usb-device source-filename***

Parameters

Parameter	Description	Possible Values	Default Value
source usb-device	The source USB mass storage device	**usb-device0**	
source-filename	The full name and path of the file to be downloaded		

User Level

Admin

Context

general

Example

To download `G450.img` from usb-device0 to Bank B:

```
G450-001(super)# copy usb SW_imageB usb-device0 \temp\G450.img
```

Related Commands

backup config usb, copy announcement-file usb, erase usb, restore usb, safe-removal usb, show backup status, show restore status, show usb

dir

Use the **dir** command to show either:

- The files that have been downloaded to the media gateway using the G450-001 Download interface and the SNMP MIB.
- The files in the USB mass storage device.

Syntax

dir {*module_number* | *file-system* [*directory*]}

Parameters

Parameter	Description	Possible Values	Default Value
module_number	Displays downloaded files for the specified module only		
file-system	Displays files on the USB mass storage device	**usbdevice0**	
directory	Displays files for the specified directory on the USB mass storage device		

User Level

read-write

Context

general

Example

To display a list of downloaded files:

```
G450-001(super)# dir
M# file              ver num   file type    file location  file description
-- ----              --------  ----------   -------------  ----------------
1  MM712             5         SW RT Image  Nv-Ram         MM712 - image
3  MM711             17        SW RT Image  Nv-Ram         MM711 - image
4  MM722             2         SW RT Image  Nv-Ram         MM722 - image
9  hi.wav            N/A       Annc files   Nv-Ram         Announcement files
9  hi1.wav           N/A       Annc files   Nv-Ram         Announcement files
9  hi2.wav           N/A       Annc files   Nv-Ram         Announcement files
10 startup-config    N/A       Startup Conf Nv-Ram         Startup Config
10 running-config    N/A       Running Conf Ram            Running Config
10 G450-A           24.6.0    SW RT Image  Flash Bank A   Software Image Bank A
10 G450-B           24.8.0    SW Component Flash Bank B   Software Image Bank B
10 G450              2.2.4     SW Web Image Nv-Ram          EmWeb application
10 G450-Booter       21.12.0   SW BootImage Nv-Ram          Booter Image
10 sniffer           N/A       Other        Ram             Sniffer Capture
10 phone-ScriptA     N/A       Phone Script Nv-Ram          N/A
10 phone-ScriptB     N/A       Phone Script Nv-Ram          46xxupgrade.scr
10 phone-ScriptC     N/A       Phone Script Nv-Ram          N/A
10 phone-ScriptD     N/A       Phone Script Nv-Ram          N/A
10 phone-ImageA      N/A       Phone Image  Ram             N/A
10 phone-ImageB      N/A       Phone Image  Ram             N/A
10 phone-ImageC      N/A       Phone Image  Ram             4601dbte1_82.bin
10 phone-ImageD      N/A       Phone Image  Ram             4602dbte1_82.bin
10 phone-ImageE      N/A       Phone Image  Ram             4602dape1_82.bin
10 phone-ImageF      N/A       Phone Image  Ram             4601dape1_82.bin
10 dhcp-binding      N/A       DHCP Binding Nv-Ram          Ip Address Binding
```

To display a list of the files in the USB mass storage device:

```
G450-001(super)# dir usbdevice0 1
  Date                 Type        Size(Bytes)       Filename
  -------              --------     ----------        --------
2006-11-13,14:56:58    <DIR>             1024        IPPHONE
2006-11-13,14:57:22    <DIR>             1024        GWANNC
2006-11-13,14:56:58    <DIR>             1024        MM
2006-11-13,14:56:58    file              3146        startup_config.cfg
2006-11-13,14:56:58    file               953        vpn_license.cfg
2006-11-13,14:57:22    file               718        readme.txt
```

Related Commands

copy ftp EW_archive, copy ftp module, copy ftp SW_imageA, copy ftp SW_imageB, copy tftp EW_archive, copy tftp module, copy tftp SW_imageA, copy tftp SW_imageB, copy usb announcement-file, set boot bank, show boot bank, show download software status, show image version

set boot bank

Use the **set boot bank** command to set the system boot bank for the active Supervisor Module.

Syntax

set boot bank ***value***

Parameters

Parameter	Description	Possible Values	Default Value
value	Boot bank name	**bank-a** - set the boot bank to A **bank-b** - set the boot bank to B	

User Level

read-write

Context

general

Example

To specify that the media gateway boots from boot bank A:

```
G450-001(super)# set boot bank bank-A
boot bank set to bank-A
```

Related Commands

copy ftp EW_archive, copy ftp module, copy ftp SW_imageA, copy ftp SW_imageB, copy tftp EW_archive, copy tftp module, copy tftp SW_imageA, copy tftp SW_imageB, copy usb announcement-file, dir, show boot bank, show download software status, show image version

show boot bank

Use the **show boot bank** command to display the software bank from which the device boots at the next boot process.

Syntax

show boot bank

User Level

read-only

Context

general

Example

To display the bank from which booting currently takes place:

```
G450-001(super)# show boot bank
Boot bank set to bank-a
```

Related Commands

copy ftp EW_archive, copy ftp module, copy ftp SW_imageA, copy ftp SW_imageB, copy tftp EW_archive, copy tftp module, copy tftp SW_imageA, copy tftp SW_imageB, copy usb announcement-file, dir, set boot bank, show download software status, show image version

show download software status

Use the **show download software status** command to display the status of the current firmware download process as the software is being loaded into the module.

Syntax

show download software status [*module_number*]

Parameters

Parameter	Description	Possible Values	Default Value
module_number	The number of the module for which to display information	**0-10**	

User Level

read-only

Context

general

Example

To display the status of a device software download into module 1:

```
G450-001(super)# show download software status 1

Module #1
===========
Module           : 1
Source file      : d:\p340sw\gt-ml\3.5.18\p340.web
Destination file : EW_Archive
Host             : 149.49.70.61
Running state    : Writing ...
Failure display  : (null)
Last warning     : No-warning
```

Related Commands

copy ftp EW_archive, copy ftp module, copy ftp SW_imageA, copy ftp SW_imageB, copy tftp EW_archive, copy tftp module, copy tftp SW_imageA, copy tftp SW_imageB, copy usb announcement-file, dir, set boot bank, show boot bank, show image version

---

show image version

Use the **show image version** command to display the software version of the image on both memory banks of the device.

Syntax

show image version

User Level

read-only

Context

general

Example

To display the current image software versions:

```
G450-001(super)# show image version

Bank          Version
-----------   -------
A (current)   26.23.0
B             26.22.0
```

Related Commands

copy ftp EW_archive, copy ftp module, copy ftp SW_imageA, copy ftp SW_imageB, copy tftp EW_archive, copy tftp module, copy tftp SW_imageA, copy tftp SW_imageB, copy usb announcement-file, dir, set boot bank, show boot bank, show download software status

Fragmentation

clear fragment

Use the **clear fragment** command to clear the fragment database and restore its default values.

Note:
No IP reassembly is performed on packets in transit through the router.

Syntax

clear fragment

User Level

read-write

Context

general

Related Commands

fragment chain, fragment size, fragment timeout, show fragment

fragment chain

Use the **fragment chain** command to set the maximum number of fragments that can comprise a single IP packet destined to the router. Use the **no** form of this command to set the fragment chain to its default value.

Note:

No IP reassembly is performed on packets in transit through the router.

Syntax

fragment chain *chain_limit*

no fragment chain

Parameters

Parameter	Description	Possible Values	Default Value
chain_limit	The maximum number of fragments that can comprise a single IP packet	**2-2048**	**64**

User Level

read-write

Context

general

Example

To set the maximum number of fragments for a single IP packet to 30:

```
G450-001(super)# fragment chain 30
```

Related Commands

clear fragment, fragment size, fragment timeout, show fragment

fragment size

Use the **fragment size** command to set the maximum number of fragmented IP packets to reassemble at any given time. Use the **no** form of this command to set the fragment size to its default value.

Note:

No IP reassembly is performed on packets in transit through the router.

Syntax

fragment size *database_limit*

no fragment size

Parameters

Parameter	Description	Possible Values	Default Value
database_limit	The maximum number of packets allowed to undergo re-assembly at any given time	**0-200**	**100**

User Level

read-write

Context

general

Example

To set the maximum number of packets to reassemble to 150:

```
G450-001(super)# fragment size 150
```

Related Commands

clear fragment, fragment chain, fragment timeout, show fragment

fragment timeout

Use the **fragment timeout** command to set the maximum number of seconds to reassemble a fragmented IP packet destined to the router. Use the **no** form of this command to set the fragment timeout to its default value.

Note:

No IP reassembly of packets in transit through the router is performed.

Syntax

fragment timeout *timeout*

no fragment timeout

Parameters

Parameter	Description	Possible Values	Default Value
timeout	The maximum number of seconds to reassemble an IP packet	**5-120**	**10**

User Level

read-write

Context

general

Example

To set the maximum time to reassemble packets to be 30 seconds:

```
G450-001(super)# fragment timeout 30
```

Related Commands

clear fragment, fragment chain, fragment size, show fragment

show fragment

Use the **show fragment** command to display information about IP packets that are passing from or to the router.

Note:

No IP reassembly is performed on packets in transit through the router.

Syntax

show fragment

User Level

read-only

Context

general

Example

To display fragmented IP packets information:

```
G450-001(super)# show fragment

Max number of concurrently reassembled packets is 100
Max number of fragments per packet is 64
Fragment timeout is 10 sec
Number of packets waiting to be reassembled is 0
Number of successfully reassembled packets is 11954
Number of packets which failed to be reassembled is 0
Number of packets which overflowed the database is 0
```

Related Commands

clear fragment, fragment chain, fragment size, fragment timeout

Frame relay encapsulation

clear frame-relay counters

Use the **clear frame-relay counters** command to clear the Frame Relay counters.

Syntax

clear frame-relay counters [interface *interface_name*]

Parameters

Parameter	Description	Possible Values	Default Value
interface	Keyword specifying that the counters should be cleared on the specified interface		
interface_name	The name of the interface		

User Level

read-only

Context

general

Example

To clear the Frame Relay counters:

```
G450-001(super)# clear frame-relay counters
```

To clear a specific Frame Relay interface's counters:

```
G450-001(super)# clear frame-relay counters interface "Serial 4/1.100"
```

Related Commands

interface serial, encapsulation, frame-relay class-dlci, frame-relay interface-dlci, frame-relay lmi-n391dte, frame-relay lmi-n392dte, frame-relay lmi-n393dte, frame-relay lmi-type, frame-relay priority-dlci-group, frame-relay traffic-shaping, ip address, map-class frame-relay, bc out, be out, cir out, fragment, show frame-relay map, show frame-relay pvc brief, show interfaces, show traffic-shape, GRE tunneling, show traffic-shape-statistics

interface serial

Use the **interface serial** command to enter Serial interface or sub interface configuration mode. If the specified interface or sub interface does not exist, the system creates it and enters its configuration mode.

Use the **no** form of the command to delete the interface. The **no** form can only be used to delete sub L3 and sub frame relay interfaces. The command fails for USP interfaces and when higher or lower layers are defined for that interface.

Syntax

[no] interface Serial *module/if_number* [*if_link_type*]

For USP interfaces ***if_number*** has the syntax:

port[.***ip_interface*** | {.***sub_interface***[.***ip_interface***]}]

For DS1 interfaces ***if_number*** has the syntax:

port:***channel_group***[.***ip_interface*** | {.***sub_interface***[.***ip_interface***]}]

Parameters

Parameter	Description	Possible Values	Default Value
module	The interface module number		
port	The port number of the interface		
channel_group		For E1: **0-30** For T1: **0-23**	
sub_interface		**1-127**	
ip_interface		**0-1024**	
if_link_type		**point-to-point**	

User Level

read-write

Context

general, interface:Serial (FR SUB)

Example

To create point to point sub-interface number 17 over channel group 2 over E1/T1 controller number 1:

```
G450-001(super)# interface Serial 3/1:2.17 point-to-point
```

Related Commands - Frame relay encapsulation

clear frame-relay counters, encapsulation, frame-relay class-dlci, frame-relay interface-dlci, frame-relay lmi-n391dte, frame-relay lmi-n392dte, frame-relay lmi-n393dte, frame-relay lmi-type, frame-relay priority-dlci-group, frame-relay traffic-shaping, ip address, map-class frame-relay, bc out, be out, cir out, fragment, show frame-relay map, show frame-relay pvc brief, show interfaces, show traffic-shape, GRE tunneling, show traffic-shape-statistics

Related Commands - IP interface configuration

description (interface), interface console, interface fastethernet, interface loopback, interface tunnel, interface USB-modem, interface vlan, ip address, ip admin-state, ip broadcast-address, ip crypto-group, load-interval, show ip interface brief

encapsulation

Use the **encapsulation** command to set the encapsulation mode for a Serial interface. By default, the Serial interface has PPP encapsulation. Use the **no** form of this command, which has no parameters, to return to the default.

Use the **encapsulation frame-relay** option to create a frame-relay interface of the IETF (RFC1490/RFC2427) type or non-IETF type. This command deletes the PPP interface associated with the current Serial interface. The PPP interface cannot be deleted if at least one IP interface is defined on it. Instead, the following message appears, “You cannot update this L2 interface since L3 interfaces are defined on it.”

By default, the Frame Relay encapsulation type for the main interface is IETF.

Note:

Non-IETF encapsulation is compatible with other vendors.

Syntax

encapsulation {ppp | frame-relay [*type*]}

no encapsulation

Parameters

Parameter	Description	Possible Values	Default Value
ppp	Keyword indicating that the encapsulation be set to PPP		
frame-relay	Keyword indicating that the encapsulation be set to Frame Relay		
type	The value for the type of Frame Relay encapsulation	**IETF** (RFC1490/RFC2427), **non-IETF**	**IETF**

User Level

read-write

Context

interface:Serial (DS1 PPP L2, DS1 PPP L2-L3, DS1 FR L2, USP PPP L2, USP PPP L2-L3, USP FR L2)

Example

To create a Frame-Relay interface with IETF encapsulation:

```
G450-001(if:Serial 3/1:1)# encapsulation frame-relay ietf
```

Related Commands - Frame relay encapsulation

clear frame-relay counters, interface serial, frame-relay class-dlci, frame-relay interface-dlci, frame-relay lmi-n391dte, frame-relay lmi-n392dte, frame-relay lmi-n393dte, frame-relay lmi-type, frame-relay priority-dlci-group, frame-relay traffic-shaping, ip address, map-class frame-relay, bc out, be out, cir out, fragment, show frame-relay map, show frame-relay pvc brief, show interfaces, show traffic-shape, GRE tunneling, show traffic-shape-statistics

Related Commands - PPP encapsulation

ip address, keepalive (PPP), ppp timeout ncp, ppp timeout retry, show interfaces

frame-relay class-dlci

Use the **`frame-relay class-dlci`** command to associate a Virtual Channel with a named QoS or Traffic shaping template (map-class). Traffic shaping only works if it is enabled on the frame relay interface.

Use the **`no`** form of this command to return to the default map class.

Note:

The VC must exist and be associated with the sub-interface.

Syntax

`[no] frame-relay class-dlci` ***`DLCI_number map_class_name`***

Parameters

Parameter	Description	Possible Values	Default Value
`DLCI_number`	The VC Data Link Channel Identifier	**16-1007**	
`map_class_name`	The name of a user defined map class. Default - the default map class		

User Level

read-write

Context

interface:Serial (DS1 FR-SUB L2, DS1 FR-SUB L2-L3)

Example

To associate Virtual Channel number 17 with the map-class frame-relay named myVoIpClass:

```
G450-001(super-if:Serial 3/1:1)#frame-relay class-dlci 17 myVoIpClass
```

Related Commands

clear frame-relay counters, interface serial, encapsulation, frame-relay interface-dlci, frame-relay lmi-n391dte, frame-relay lmi-n392dte, frame-relay lmi-n393dte, frame-relay lmi-type, frame-relay priority-dlci-group, frame-relay traffic-shaping, ip address, map-class frame-relay, bc out, be out, cir out, fragment, show frame-relay map, show frame-relay pvc brief, show interfaces, show traffic-shape, GRE tunneling, show traffic-shape-statistics

frame-relay interface-dlci

Use the **frame-relay interface-dlci** command to associate a frame relay Virtual Channel with the current interface. This VC will be in the primary role (that is, will determine the operational status of the interface).

Use the **no** form of this command to delete the association of the VC and the sub-interface. To replace the currently configured interface-DLCI, use the **no** form of the command.

Use the optional **type** parameter to set the encapsulation type. By default, the Frame Relay sub-interface inherits its encapsulation type from the Frame Relay interface encapsulation type.

Syntax

[no] frame-relay interface-dlci *DLCI_number* [*type*]

Parameters

Parameter	Description	Possible Values	Default Value
DLCI_number	The Virtual Channel DLCI	**16-1007**	
type	The encapsulation type	**IETF** (RFC1490/RFC2427), **non-IETF**	**IETF**

Note:

Non-IETF encapsulation is compatible with other vendors.

User Level

read-write

Context

interface:Serial (DS1 FR-SUB L2, DS1 FR-SUB L2-L3)

Example

The following example creates and associates DLCI number 17 with the current sub-interface. This VC will carry all traffic (if no priority dlci-group is defined for this interface), and will be in the primary role.

```
G450-001(super-if:Serial 3/1:1)# frame-relay interface-dlci 17
```

Related Commands

clear frame-relay counters, interface serial, encapsulation, frame-relay class-dlci, frame-relay lmi-n391dte, frame-relay lmi-n392dte, frame-relay lmi-n393dte, frame-relay lmi-type, frame-relay priority-dlci-group, frame-relay traffic-shaping, ip address, map-class frame-relay, bc out, be out, cir out, fragment, show frame-relay map, show frame-relay pvc brief, show interfaces, show traffic-shape, GRE tunneling, show traffic-shape-statistics

frame-relay lmi-n391dte

Use the **frame-relay lmi-n391dte** command to set the number of status enquiry intervals that pass before issuing a full status enquiry message.

Use the **no** form of this command to set the number of status enquiry intervals to its default.

Syntax

[no] frame-relay lmi-n391dte *polling_counter*

Parameters

Parameter	Description	Possible Values	Default Value
polling_counter	Number of status enquiry intervals	**1-255**	**6**

User Level

read-write

Context

interface:Serial (DS1 FR L2, USP FR L2)

Example

To set the full status polling counter to 17:

```
G450-001(if:Serial 3/1:1)# frame-relay lmi-n391dte 17
```

Related Commands

clear frame-relay counters, interface serial, encapsulation, frame-relay class-dlci, frame-relay interface-dlci, frame-relay lmi-n392dte, frame-relay lmi-n393dte, frame-relay lmi-type, frame-relay priority-dlci-group, frame-relay traffic-shaping, ip address, map-class frame-relay, bc out, be out, cir out, fragment, show frame-relay map, show frame-relay pvc brief, show interfaces, show traffic-shape, GRE tunneling, show traffic-shape-statistics

frame-relay lmi-n392dte

Use the **frame-relay lmi-n392dte** command to set the maximum number of unanswered status enquiries the equipment accepts before declaring the interface down.

Use the **no** form of this command to revert to the default value.

Syntax

[no] frame-relay lmi-n392dte *threshold*

Parameters

Parameter	Description	Possible Values	Default Value
threshold	Error threshold value	**1-10**	**3**

User Level

read-write

Context

interface:Serial (DS1 FR L2, USP FR L2)

Example

To set the maximum number of unanswered status enquiries allowed to 5:

```
G450-001(if:Serial 3/1:1)# frame-relay lmi-n392dte 5
```

Related Commands

clear frame-relay counters, interface serial, encapsulation, frame-relay class-dlci, frame-relay interface-dlci, frame-relay lmi-n391dte, frame-relay lmi-n393dte, frame-relay lmi-type, frame-relay priority-dlci-group, frame-relay traffic-shaping, ip address, map-class frame-relay, bc out, be out, cir out, fragment, show frame-relay map, show frame-relay pvc brief, show interfaces, show traffic-shape, GRE tunneling, show traffic-shape-statistics

frame-relay lmi-n393dte

Use the **frame-relay lmi-n393dte** command to set the number of status polling intervals over which the error threshold is counted (the monitored event count). To set the error threshold, refer to frame-relay lmi-n392dte on page 455. In other words, if within ***events*** number of events the station receives ***error_threshold*** number of errors, the interface is marked as down.

Use the **no** form of this command to revert to the default value.

Syntax

[no] frame-relay lmi-n393dte *events*

Parameters

Parameter	Description	Possible Values	Default Value
events	The number of events	**1-10**	**4**

User Level

read-write

Context

interface:Serial (DS1 FR L2, USP FR L2)

Example

To set the number of events over which the error threshold is calculated to 5:

```
G450-001(if:Serial 3/1:1)# frame-relay lmi-n393dte 5
```

Related Commands

clear frame-relay counters, interface serial, encapsulation, frame-relay class-dlci, frame-relay interface-dlci, frame-relay lmi-n391dte, frame-relay lmi-n392dte, frame-relay lmi-type, frame-relay priority-dlci-group, frame-relay traffic-shaping, ip address, map-class frame-relay, bc out, be out, cir out, fragment, show frame-relay map, show frame-relay pvc brief, show interfaces, show traffic-shape, GRE tunneling, show traffic-shape-statistics

frame-relay lmi-type

Use the **`frame-relay lmi-type`** command to manually define the type of the Local Management Interface (LMI) to use.

Use the **`no`** form of this command to specify automatic detection of the LMI type (auto-sensing). If auto-sense fails, ANSI is used as the default.

Syntax

`[no] frame-relay lmi-type` ***`lmi_type`***

Parameters

Parameter	Description	Possible Values	Default Value
`lmi_type`	The type of local management interface	**ansi** - LMI according to ANSI T1.617 [9] **q933a** - LMI according to ITU-T Q.933 [7] **autosense** **lmi-rev1** **disable**	

User Level

read-write

Context

interface:Serial (DS1 FR L2, USP FR L2)

Example

To select the q933a LMI type:

```
G450-001(if:Serial 3/1:1)# frame-relay lmi-type q933a
```

Related Commands

clear frame-relay counters, interface serial, encapsulation, frame-relay class-dlci, frame-relay interface-dlci, frame-relay lmi-n391dte, frame-relay lmi-n392dte, frame-relay lmi-n393dte, frame-relay priority-dlci-group, frame-relay traffic-shaping, ip address, map-class frame-relay, bc out, be out, cir out, fragment, show frame-relay map, show frame-relay pvc brief, show interfaces, show traffic-shape, GRE tunneling, show traffic-shape-statistics

frame-relay priority-dlci-group

Use the **frame-relay priority-dlci-group** command to assign Virtual Channels to priority classifications, for supporting traffic separation. The first DLCI is assigned to the high priority traffic. Other DLCIs are assigned to Medium (L2:4-5), Normal (L2:2-3), and Low (L2:0-1) priorities. When fewer than 4 DLCIs are specified, the last DLCI on the command line is assigned to all the remaining unassigned priority classes.

Use the **no** form of this command to clear the current priority DLCI group.

Syntax

[no] frame-relay priority-dlci-group *DLCI1* [*DLCI2* [*DLCI3* [*DLCI4*]]]

Parameters

Parameter	Description	Possible Values	Default Value
DLCI1	The DLCI assigned to the High priority traffic	**16-1007**	
DLCI2	The DLCI assigned to the Medium priority traffic	**16-1007**	
DLCI3	The DLCI assigned to the Normal priority traffic	**16-1007**	
DLCI4	The DLCI assigned to the Low priority traffic	**16-1007**	

User Level

read-write

Context

interface:Serial (DS1 FR-SUB L2, DS1 FR-SUB L2-L3)

Example

To assign VC number 17 to the High Priority traffic, VC number 18 to the Medium Priority traffic, and VC number 19 to the Normal to Low priority traffic:

```
G450-001(if:Serial 3/1:1.1)# frame-relay priority-dlci-group 17 18 19
```

Related Commands

clear frame-relay counters, interface serial, encapsulation, frame-relay class-dlci, frame-relay interface-dlci, frame-relay lmi-n391dte, frame-relay lmi-n392dte, frame-relay lmi-n393dte, frame-relay lmi-type, frame-relay traffic-shaping, ip address, map-class frame-relay, bc out, be out, cir out, fragment, show frame-relay map, show frame-relay pvc brief, show interfaces, show traffic-shape, GRE tunneling, show traffic-shape-statistics

frame-relay traffic-shaping

Use the **frame-relay traffic-shaping** command to turn on/off traffic shaping and Frame-Relay fragmentation. Virtual Channels that are not explicitly assigned to a map-class frame-relay, are assigned to the default map-class frame-relay.

Use the **no** form of this command to turn off traffic shaping.

Syntax

[no] frame-relay traffic-shaping

User Level

read-write

Context

interface:Serial (DS1 FR L2, USP FR L2)

Example

To enable traffic shaping on the interface:

```
G450-001(if:Serial 3/1:1)# frame-relay traffic-shaping
```

Related Commands - Traffic shaping

map-class frame-relay, bc out, be out, cir out, fragment, show map-class frame-relay, show traffic-shape, show traffic-shape-queue, show traffic-shape-statistics, traffic-shape rate

Related Commands - Frame relay encapsulation

clear frame-relay counters, interface serial, encapsulation, frame-relay class-dlci, frame-relay interface-dlci, frame-relay lmi-n391dte, frame-relay lmi-n392dte, frame-relay lmi-n393dte, frame-relay lmi-type, frame-relay priority-dlci-group, ip address, map-class frame-relay, bc out, be out, cir out, fragment, show frame-relay map, show frame-relay pvc brief, show interfaces, show traffic-shape, GRE tunneling, show traffic-shape-statistics

ip address

Use the **ip address** command to assign an IP address and mask to an interface. Use the **no** form of this command to delete an IP interface.

Syntax

ip address {*ip_address mask* [*admin_state*]}|negotiated

no ip address

Parameters

Parameter	Description	Possible Values	Default Value
ip_address	The IP address assigned to the interface		
mask	Mask for the associated IP subnet		
admin_state	The administration status. This parameter is not used with the Console interface	**up**, **down**	**up**
negotiated	Interface receives address and mask from a remote device		

User Level

read-write

Context

Interface: Console, Serial (DS1 PPP L2-L3, DS1 PPP L3, DS1 FR-SUB L2-L3, DS1 FR-SUB L3, USP PPP L2-L3, USP PPP L3), FastEthernet (L2-L3, L3, PPP L2-L3, PPP L3), VLAN (L2-L3, L3), USB-modem, Loopback (L2-L3, L3), Tunnel (L2-L3, L3), Dialer (L2-L3, L3)

Example

To assign the IP address 192.168.22.33 with mask 255.255.255.0 to the FastEthernet interface:

```
G450-001(if:FastEthernet 10/2)# ip address 192.168.22.33 255.255.255.0
```

Related Commands - Frame relay encapsulation

clear frame-relay counters, interface serial, encapsulation, frame-relay class-dlci, frame-relay interface-dlci, frame-relay lmi-n391dte, frame-relay lmi-n392dte, frame-relay lmi-n393dte, frame-relay lmi-type, frame-relay priority-dlci-group, frame-relay traffic-shaping, map-class frame-relay, bc out, be out, cir out, fragment, show frame-relay map, show frame-relay pvc brief, show interfaces, show traffic-shape, GRE tunneling, show traffic-shape-statistics

Related Commands - IP interface configuration

description (interface), interface console, interface fastethernet, interface loopback, interface serial, interface tunnel, interface USB-modem, interface vlan, ip admin-state, ip broadcast-address, load-interval, show ip interface brief

map-class frame-relay

Use the **map-class frame-relay** command to create a QoS template named ***map_class_name***, which can later be assigned to DLCIs.

Use the **no** form of this command to delete a map class.

Note:

This command fails if the map class is currently associated with a DLCI.

Syntax

[no] map-class frame-relay *map_class_name*

Parameters

Parameter	Description	Possible Values	Default Value
map_class_name	The name of a map class configured by the user		

User Level

read-write

Context

general

Example

To create a map class named mySVoip1:

```
G450-001(super)# map-class frame-relay mySVoip1
```

```
G450-001(super-map-class)#
```

Related Commands - Traffic shaping

frame-relay traffic-shaping, bc out, be out, cir out, fragment, show map-class frame-relay, show traffic-shape, show traffic-shape-queue, show traffic-shape-statistics, traffic-shape rate

Related Commands

clear frame-relay counters, interface serial, encapsulation, frame-relay class-dlci, frame-relay interface-dlci, frame-relay lmi-n391dte, frame-relay lmi-n392dte, frame-relay lmi-n393dte, frame-relay lmi-type, frame-relay priority-dlci-group, frame-relay traffic-shaping, ip address, bc out, be out, cir out, fragment, show frame-relay map, show frame-relay pvc brief, show interfaces, show traffic-shape, GRE tunneling, show traffic-shape-statistics

---

bc out

Use the **bc out** command to configure the committed burst size in bits, for the outbound direction. Use the **no** form of this command to return the committed burst size to its default value.

Syntax

bc out *bits*

no bc out

Parameters

Parameter	Description	Possible Values	Default Value
bits	The committed burst size in bits	**300-39999999**	**7000**

User Level

read-write

Context

map-class frame-relay

Example

To configure outbound BC to be 64 Kbit:

```
G450-001(map-class)# bc out 64000
```

Related Commands - Traffic shaping

frame-relay traffic-shaping, map-class frame-relay, be out, cir out, fragment, show map-class frame-relay, show traffic-shape, show traffic-shape-queue, show traffic-shape-statistics, traffic-shape rate

Related Commands

clear frame-relay counters, interface serial, encapsulation, frame-relay class-dlci, frame-relay interface-dlci, frame-relay lmi-n391dte, frame-relay lmi-n392dte, frame-relay lmi-n393dte, frame-relay lmi-type, frame-relay priority-dlci-group, frame-relay traffic-shaping, ip address, map-class frame-relay, be out, cir out, fragment, show frame-relay map, show frame-relay pvc brief, show interfaces, show traffic-shape, GRE tunneling, show traffic-shape-statistics

be out

Use the **be out** command to configure the excess burst size in bits, for the outbound direction. Use the **no** form of this command to return the excess burst size to its default value.

Note:

The Excess Information Rate (EIR) is equal to: (BC+BE)/Tc/1000, where Tc is the Frame Relay meter time interval in mSec, BC is the committed burst rate and BE is the excess burst size.

Syntax

be out ***bits***

no be out

Parameters

Parameter	Description	Possible Values	Default Value
bits	The excess burst size in bits	**0-39999999**	**7000**

User Level

read-write

Context

map-class frame-relay

Example

To configure outbound BE to be 64 Kbit:

```
G450-001(map-class)# be out 64000
```

Related Commands - Traffic shaping

frame-relay traffic-shaping, map-class frame-relay, bc out, cir out, fragment, show map-class frame-relay, show traffic-shape, show traffic-shape-queue, show traffic-shape-statistics, traffic-shape rate

Related Commands - Frame relay encapsulation

clear frame-relay counters, interface serial, encapsulation, frame-relay class-dlci, frame-relay interface-dlci, frame-relay lmi-n391dte, frame-relay lmi-n392dte, frame-relay lmi-n393dte, frame-relay lmi-type, frame-relay priority-dlci-group, frame-relay traffic-shaping, ip address, map-class frame-relay, bc out, cir out, fragment, show frame-relay map, show frame-relay pvc brief, show interfaces, show traffic-shape, GRE tunneling, show traffic-shape-statistics

cir out

Use the **cir out** command to configure the Committed Information Rate (CIR) in bits per second, for the outbound direction. Use the **no** form of this command to return the CIR to its default value.

Note:
This command fails if the map class is currently associated with a DLCI.

Syntax

cir out ***cir***

no cir out

Parameters

Parameter	Description	Possible Values	Default Value
cir	The CIR in bits per second	**1000-39999999**	**56000**

User Level

read-only

Context

map-class frame-relay

Example

To configure outbound CIR to be 64 Kbps:

```
G450-001(map-class)# cir out 64000
```

Related Commands - Traffic shaping

frame-relay traffic-shaping, map-class frame-relay, bc out, be out, fragment, show map-class frame-relay, show traffic-shape, show traffic-shape-queue, show traffic-shape-statistics, traffic-shape rate

Related Commands - Frame relay encapsulation

clear frame-relay counters, interface serial, encapsulation, frame-relay class-dlci, frame-relay interface-dlci, frame-relay lmi-n391dte, frame-relay lmi-n392dte, frame-relay lmi-n393dte, frame-relay lmi-type, frame-relay priority-dlci-group, frame-relay traffic-shaping, ip address, map-class frame-relay, bc out, be out, fragment, show frame-relay map, show frame-relay pvc brief, show interfaces, show traffic-shape, GRE tunneling, show traffic-shape-statistics

fragment

Use the **fragment** command to enable FRF.12 fragmentation and configure the fragment size. Use the **no** form of this command to disable FRF.12 fragmentation. By default, FRF.12 fragmentation is disabled.

Syntax

[no] fragment *size*

Parameters

Parameter	Description	Possible Values	Default Value
size	The size of the fragment in octets, including the Frame Relay Header (2 octets) and Fragmentation header (4 octets)	**16-1600**	**88**

User Level

read-write

Context

map-class frame-relay

Example

To enable FRF.12 fragmentation and set the fragment size to 63:

```
G450-001(super-map-class)# fragment 63
```

Related Commands - Traffic shaping

frame-relay traffic-shaping, map-class frame-relay, bc out, be out, cir out, show map-class frame-relay, show traffic-shape, show traffic-shape-queue, show traffic-shape-statistics, traffic-shape rate

Related Commands - Frame relay encapsulation

clear frame-relay counters, interface serial, encapsulation, frame-relay class-dlci, frame-relay interface-dlci, frame-relay lmi-n391dte, frame-relay lmi-n392dte, frame-relay lmi-n393dte, frame-relay lmi-type, frame-relay priority-dlci-group, frame-relay traffic-shaping, ip address, map-class frame-relay, bc out, be out, cir out, show frame-relay map, show frame-relay pvc brief, show interfaces, show traffic-shape, GRE tunneling, show traffic-shape-statistics

show frame-relay map

Use the **show frame-relay map** command to display a summary table of Frame Relay sub-interfaces, and DLCIs associated with the sub-interfaces.

Syntax

show frame-relay map

User Level

read-only

Context

general

Example

To display information about the Frame Relay sub-interfaces:

```
G450-001(super)# show frame-relay map

Showing 2 frame-relay map entries
Interface   State  Interface Type DLCI DLCI Type DLCI State
----------- ------ -------------- ---- --------- ------
Serial 1.1  down   point-to-point   17 broadcast deleted
Serial 1.1  down   point-to-point   18 broadcast deleted
```

Related Commands

clear frame-relay counters, interface serial, encapsulation, frame-relay class-dlci, frame-relay interface-dlci, frame-relay lmi-n391dte, frame-relay lmi-n392dte, frame-relay lmi-n393dte, frame-relay lmi-type, frame-relay priority-dlci-group, frame-relay traffic-shaping, ip address, map-class frame-relay, bc out, be out, cir out, fragment, show frame-relay pvc brief, show interfaces, show traffic-shape, GRE tunneling, show traffic-shape-statistics

show frame-relay pvc brief

Use the **show frame-relay pvc brief** command to display information on all PVCs known to the device, in a table form.

Syntax

show frame-relay pvc brief

User Level

read-only

Context

general

Example

To show a table of all PVCs known to the device:

```
G450-001(super)# show frame-relay pvc brief
```

Related Commands

clear frame-relay counters, interface serial, encapsulation, frame-relay class-dlci, frame-relay interface-dlci, frame-relay lmi-n391dte, frame-relay lmi-n392dte, frame-relay lmi-n393dte, frame-relay lmi-type, frame-relay priority-dlci-group, frame-relay traffic-shaping, ip address, map-class frame-relay, bc out, be out, cir out, fragment, show frame-relay map, show interfaces, show traffic-shape, GRE tunneling, show traffic-shape-statistics

show interfaces

Use the **show interfaces** command to display interface configuration and statistics for a particular interface or all interfaces. The Frame Relay sub-interface only includes the following counters:

- packets & bytes in

- packets & bytes out
- input errors
- output drops

Syntax

show interfaces [*interface_type interface_identifier*]

Parameters

Parameter	Description	Possible Values	Default Value
interface_type	The type of interface	**Dialer, FastEthernet, Serial, Vlan, Loopback, Console, Tunnel, USB**	
interface_identifier	The interface number. The format varies depending on the value of interface_type: For FastEthernet: **module/port** For Serial: **module/port:channel-group** For Vlan: **Vlan id** For LoopBack: **Loopback number** For Tunnel: **Tunnel number**	For FastEthernet: **10/2 or 10/4** For Serial(USP): **3/1, 4/1, 8/1** For Serial (DS1): module/port: **3/1, 4/1, 8/1** channel-group: E1: **0-30** T1: **0-23** For VLAN: **1-4090** For Loopback: **1-99** For Tunnel: **1-50** For Dialer: **1**	

User Level

read-write

Context

general

Example

To show information about all the interfaces:

```
G450-001(super)# show interfaces
Vlan 1 is up, line protocol is up
Physical address is 00.04.0d.29.c5.11.
Internet address is 172.16.1.139, mask is 255.255.255.240
```

```
Primary management interface
MTU 1500 bytes. Bandwidth 100000 kbit.
Reliability 255/255 txLoad 1/255 rxLoad 1/255
Encapsulation ARPA, ICC-VLAN
Link status trap disabled
Full-duplex, 100Mb/s
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:30, Last output 00:00:30
Last clearing of 'show interface' counters never.
5 minute input rate 144 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 input drops, 0 output drops, 0 unknown protocols
3425 packets input, 323518 bytes
3425 broadcasts received, 0 giants
0 input errors, 0 CRC
32 packets output, 896 bytes
0 output errors, 0 collisions

FastEthernet 10/2 is up, line protocol is down
Physical address is 00.04.0d.29.c5.10.
MTU 1500 bytes. Bandwidth 10000 kbit.
Reliability 1/255 txLoad 255/255 rxLoad 255/255
Encapsulation ARPA
Link status trap disabled
Half-duplex, 10Mb/s, 10BaseTX
ARP type: ARPA, ARP Timeout 04:00:00
Dynamic CAC BBL: 1500 kbps
Dynamic CAC activation priority: 50
Dynamic CAC interface status: active
Last input never, Last output never
Last clearing of 'show interface' counters never.
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 input drops, 0 output drops, 0 unknown protocols
0 packets input, 0 bytes
0 broadcasts received, 0 giants
0 input errors, 0 CRC
0 packets output, 0 bytes
0 output errors, 0 collisions

Tunnel 1 is up, line protocol is up
Internet address is 177.0.0.17, mask is 255.0.0.0
MTU 468 bytes. Bandwidth 9 kbit
Reliability 255/255 txLoad 1/255 rxLoad 1/255
Encapsulation GRE
Link status trap enabled
Keepalive set (10 sec), retries 3
Tunnel source 17.0.0.17, destination 12.0.0.3
Tunnel protocol/transport GRE/IP, key 777
Checksumming of packets enabled
Tunnel DSCP 63, Tunnel TTL 255
```

```
Path MTU Discovery, ager 10 mins, MTU 976, expires 00:09:33
Last input never, Last output never
Last clearing of 'show interface' counters never.
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 input drops, 0 output drops, 0 unknown protocols
0 packets input, 0 bytes
0 broadcasts received, 0 giants
0 input errors, 0 CRC
0 packets output, 0 bytes
0 output errors, 0 collisions

Console asynchronous mode is terminal
Terminal baud rate is 9600
```

Related Commands - Frame relay encapsulation

clear frame-relay counters, interface serial, encapsulation, frame-relay class-dlci, frame-relay interface-dlci, frame-relay lmi-n391dte, frame-relay lmi-n392dte, frame-relay lmi-n393dte, frame-relay lmi-type, frame-relay priority-dlci-group, frame-relay traffic-shaping, ip address, map-class frame-relay, bc out, be out, cir out, fragment, show frame-relay map, show frame-relay pvc brief, show traffic-shape, GRE tunneling, show traffic-shape-statistics

Related Commands - PPP encapsulation

interface dialer, interface fastethernet, interface serial

Related Commands - Verifying WAN configuration

show controllers, show frame-relay fragment, show frame-relay lmi, show frame-relay pvc, show frame-relay traffic, show interfaces, show ip interface, show map-class frame-relay

show map-class frame-relay

Use the **`show map-class frame-relay`** command to display the map-class Frame Relay table.

Syntax

`show map-class frame-relay`

User Level

read-only

Context

general

Example

To display the map class Frame Relay table:

```
G450-001(super)# show map-class frame-relay
Showing 3 frame-relay map-class entries
       Map Class Name           CIR       BC        BE      Fragment
---------------------------- --------- --------- --------- --------
default                          56000      7000         0       OFF
orna1                            56000      7000         0       OFF
stam                             56000      7000         0       OFF
```

Related Commands - Frame relay encapsulation

clear frame-relay counters, interface serial, encapsulation, frame-relay class-dlci, frame-relay interface-dlci, frame-relay lmi-n391dte, frame-relay lmi-n392dte, frame-relay lmi-n393dte, frame-relay lmi-type, frame-relay priority-dlci-group, frame-relay traffic-shaping, ip address, map-class frame-relay, bc out, be out, cir out, fragment, show frame-relay map, show frame-relay pvc brief, show interfaces, show traffic-shape, GRE tunneling, show traffic-shape-statistics

Related Commands - Traffic shaping

frame-relay traffic-shaping, map-class frame-relay, bc out, be out, cir out, fragment, show traffic-shape, show traffic-shape-queue, show traffic-shape-statistics, traffic-shape rate

Related Commands - Verifying WAN configuration

show frame-relay fragment, show frame-relay lmi, show frame-relay map, show frame-relay pvc, show frame-relay traffic, show interfaces

show traffic-shape

Use the **show traffic-shape** command to display traffic shaping and Frame Relay Traffic Shaping configuration information.

Syntax

show traffic-shape [*interface-name-number*]

Parameters

Parameter	Description	Possible Values	Default Value
interface-name-number	Interface or sub-interface type and number		

User Level

read-only

Context

general

Example

To display traffic shaping and Frame Relay Traffic Shaping information for the G450:

```
G450-001(super)# show traffic-shape
                     Target    Byte   Sustain   Excess    Interval Increment
Interface         VC Rate      Limit  bits/int  bits/int  (ms)     (bytes)
----------------- --- --------- ------ --------- --------- -------- ---------
Serial 5/0:11.11  16      24000  12375     24000     96000      125       375
Serial 5/0:11.11  20      24000  12375     24000     96000      125       375
Serial 3/1:1.2    30      24000  12375     24000     96000      125       375
FastEthernet 10/2        128000   1518    128000         0        1        16
```

To display traffic shaping and Frame Relay Traffic Shaping information for the Serial 5/0 interface:

```
G450-001(super)# show traffic-shape interface Serial 5/0:11.11
                     Target    Byte   Sustain   Excess    Interval Increment
Interface         VC Rate      Limit  bits/int  bits/int  (ms)     (bytes)
----------------- --- --------- ------ --------- --------- -------- ---------
Serial 5/0:11.11  16      24000  12375     24000     96000      125       375
Serial 5/0:11.11  20      24000  12375     24000     96000      125       375
```

Output fields:

Field	Description
Interface	Interface or sub-interface type and number
VC	Virtual circuit, which is the DLCI number

1 of 2

Field	Description
Target Rate	Rate that traffic is shaped to, in bits per second. This is the CIR.
Byte Limit	Maximum number of bytes sent per internal interval. This is the high-watermark, which is equivalent to (inBc + Be)/8.
Sustain bits/int	Configured sustained bits per interval. This is the Bc.
Excess bits/int	Configured excess bits in the first interval. This is the Be.
Interval (ms)	The internal interval being used, in milliseconds. This is the inTc.
Increment (bytes)	Number of bytes that will be sustained per internal interval. This is the inBc/8.
	2 of 2

Related Commands - Traffic shaping

frame-relay traffic-shaping, map-class frame-relay, bc out, be out, cir out, fragment, show map-class frame-relay, show traffic-shape-queue, show traffic-shape-statistics, traffic-shape rate

Related Commands - Frame relay encapsulation

clear frame-relay counters, interface serial, encapsulation, frame-relay class-dlci, frame-relay interface-dlci, frame-relay lmi-n391dte, frame-relay lmi-n392dte, frame-relay lmi-n393dte, frame-relay lmi-type, frame-relay priority-dlci-group, frame-relay traffic-shaping, ip address, map-class frame-relay, bc out, be out, cir out, fragment, show frame-relay map, show frame-relay pvc brief, show interfaces, GRE tunneling, show traffic-shape-statistics

show traffic-shape-queue

Use the **`show traffic-shape-queue`** command to display information about the real-time status of traffic-shaping and Frame Relay Traffic Shaping queues.

Syntax

`show traffic-shape-queue [`*`interface-name-number`*`]`

Parameters

Parameter	Description	Possible Values	Default Value
interface-name-number	Interface or sub-interface type and number		

User Level

read-only

Context

general

Example

To display traffic shaping and Frame Relay Traffic Shaping queueing data for the G450:

```
G450-001(super)# show traffic-shape-queue
  Traffic queued in shaping queue on 4/1:11.11 dlci 16
  Queueing strategy: weighted fair voip
   Voip queue: 0/0/20/0/0 (size/max size/threshold-ms/drops/tx)
   Weighted fair queue: 1/2/64/0/127 (size/max size/threshold/drops/tx)
        Conversations 1/1/256 (active/max active/max total)
   Available Bandwidth 64 kilobits/sec

Voip queue:
 Voip queue is empty

Weighted fair queue:
 Idx Source ip       Destination ip  Prot Sport Dport Cnt Total drop Total tx
 --- --------------- --------------- ---- ----- ----- --- ---------- --------
 228 149.49.70.155   135.64.102.240  tcp     23  2515   1          0         127
```

Related Commands - Traffic shaping

frame-relay traffic-shaping, map-class frame-relay, bc out, be out, cir out, fragment, show map-class frame-relay, show traffic-shape, show traffic-shape-statistics, traffic-shape rate

Related Commands - Frame relay encapsulation

clear frame-relay counters, interface serial, encapsulation, frame-relay class-dlci, frame-relay interface-dlci, frame-relay lmi-n391dte, frame-relay lmi-n392dte, frame-relay lmi-n393dte, frame-relay lmi-type, frame-relay priority-dlci-group, frame-relay traffic-shaping, ip address, map-class frame-relay, bc out, be out, cir out, fragment, show frame-relay map, show frame-relay pvc brief, show interfaces, show traffic-shape, show traffic-shape-statistics

show traffic-shape-statistics

Use the **show traffic-shape-statistics** command to display traffic shaping and Frame Relay Traffic Shaping statistics.

Syntax

show traffic-shape-statistics [*interface-name-number*]

Parameters

Parameter	Description	Possible Values	Default Value
interface-name-number	Interface or sub-interface type and number		

User Level

read-only

Context

general

Example

To display traffic shaping and Frame Relay Traffic Shaping statistics for the G450:

```
G450-001(super)# show traffic-shape-statistics

Queue Packets   Bytes     Packets   Bytes     Shaping
Interface         VC   Depth                    Delayed   Delayed   Active
----------------- ---- ----- -------- ---------- --------- -------- ---------
Serial 4/1:11.11    16     0      455     220218       375    182250    No
Serial 3/1:1.2      30    50      455     220218       375    182250    yes
FastEthernet 10/2            0     1031    1938990       534    938270    No
```

To display traffic shaping and Frame Relay Traffic Shaping statistics for the Serial 4/1 interface:

```
G450-001(super)# show traffic-shape statistics Serial 4/1:11.11

Queue Packets   Bytes     Packets   Bytes     Shaping
Interface         VC   Depth                    Delayed   Delayed   Active
----------------- ---- ----- -------- ---------- --------- -------- ---------
Serial 4/1:11.11    16     0      455     220218       375    182250    No
```

Output fields:

Field	Description
Interface	Interface or sub-interface type and number
VC	Virtual circuit, which is the DLCI number
Queue Depth	Number of frames currently in the VC (Virtual Circuit) queue
Packets	Number of packets sent through the VC
Bytes	Number of bytes sent through the VC
Packets Delayed	Number of packets sent through the VC that were delayed in the traffic-shaping queue
Bytes Delayed	Number of bytes sent through the VC that were delayed in the traffic-shaping queue
Shaping Active	Whether traffic shaping is active. Possible values: • **Yes** – traffic shaping is occurring, i.e. VC-Q is not empty • **No** – traffic shaping is not occurring, i.e. VC-Q is empty

Related Commands - Traffic shaping

frame-relay traffic-shaping, map-class frame-relay, bc out, be out, cir out, fragment, show map-class frame-relay, show traffic-shape, show traffic-shape-queue, traffic-shape rate

Related Commands - Frame relay encapsulation

clear frame-relay counters, interface serial, encapsulation, frame-relay class-dlci, frame-relay interface-dlci, frame-relay lmi-n391dte, frame-relay lmi-n392dte, frame-relay lmi-n393dte, frame-relay lmi-type, frame-relay priority-dlci-group, frame-relay traffic-shaping, ip address, map-class frame-relay, bc out, be out, cir out, fragment, show frame-relay map, show frame-relay pvc brief, show interfaces, show traffic-shape, GRE tunneling

GRE tunneling

interface tunnel

Use the **interface tunnel** command to enter Interface Tunnel configuration mode. Use the **no** form of this command to delete an interface tunnel.

If the specified interface does not exist, the system creates it and enters its configuration mode.

Syntax

[no] interface tunnel *tunnel_number*

Parameters

Parameter	Description	Possible Values	Default Value
tunnel_number	The number of the interface	**1-99**	

User Level

read-write

Context

general

Example

To create interface tunnel 1 and enter its configuration mode:

```
G450-001(super)# interface tunnel 1
```

Related Commands - IP interface configuration

description (interface), interface console, interface fastethernet, interface loopback, interface serial, interface USB-modem, interface vlan, ip address, ip admin-state, ip broadcast-address, load-interval, show ip interface brief

Related Commands - GRE tunneling

interface fastethernet, tunnel dscp, tunnel mode

keepalive (GRE tunnel)

Use the **keepalive** command in the context of a GRE tunnel to specify that the tunnel sends keepalive packets to determine if the tunnel endpoint is up. Packets are sent according to the interval specified in the seconds parameters, and resent according to the number of the retries parameter.

Use the **no** form of the command to disable keepalive packets.

If the tunnel's destination interface fails to respond to a consecutive number of keepalive packets equal to the ***<retries>*** parameter, the tunnel informs the hosts, which send packets to the tunnel that the tunnel is down. It does so, even though the source interface continues to send keepalive packets.

Syntax

keepalive [*seconds* [*retries*]]

no keepalive

Parameters

Parameter	Description	Possible Values	Default Value
seconds	The rate at which keepalive packets are sent	**0-32767**	10
retries	The number of times that a device continues to send keepalive packets without a response before the interface becomes inactive	**0-255**	3

User Level

read-write

Context

Interface: Tunnel (L2, L2-L3)

Example

To enable GRE tunnel keepalives, setting the rate to 10 seconds and retries to 3:

```
G450-001(super if:Tunnel 1)# keepalive 10 3
```

Related Commands

tunnel checksum, tunnel destination, tunnel key, tunnel path-mtu-discovery, tunnel source, tunnel ttl

tunnel checksum

Use the **tunnel checksum** command to specify that the router adds a checksum bit to the outgoing GRE packet, for data verification. Use the **no** form of the command to specify that no checksum bit should be added.

Syntax

[no] tunnel checksum

User Level

read-write

Context

Interface: Tunnel (L2, L2-L3)

Example

To specify that the router adds a checksum bit to the outgoing GRE packet:

```
G450-001(super)# tunnel checksum
```

Related Commands

keepalive (GRE tunnel), tunnel destination, tunnel key, tunnel path-mtu-discovery, tunnel source, tunnel ttl

tunnel destination

Use the **tunnel destination** command to specify the destination IP address for the GRE tunnel. The destination is the IP address of the tunnel's endpoint.

Note:

The CLI does not verify that the specified IP address actually exists.

Syntax

tunnel destination *ip-address*

Parameters

Parameter	Description	Possible Values	Default Value
ip-address	The destination IP address for the GRE tunnel		

User Level

read-write

Context

Interface: Tunnel (L2, L2-L3)

Example

To specify that the GRE tunnel destination IP address is 168.30.10.2:

```
G450-001(super)# tunnel destination 168.30.10.2
```

Related Commands

keepalive (GRE tunnel), tunnel checksum, tunnel key, tunnel path-mtu-discovery, tunnel source, tunnel ttl

tunnel dscp

By default, the GRE header copies the DSCP value from the header of the original packet. Use the **tunnel dscp** command to override the original packet's DSCP with the specified DSCP value. Use the **no** form of the command to use the DSCP value of the original packet.

Syntax

tunnel dscp *dscp*

no tunnel dscp

Parameters

Parameter	Description	Possible Values	Default Value
dscp	The DSCP value to be used instead of the DSCP from the header of the original packet	**0-63**	

User Level

read-write

Context

Interface: Tunnel (L2, L2-L3)

Example

To override the original packet DSCP with DSCP value 0:

```
G450-001(super)# tunnel dscp 0
```

Related Commands

interface fastethernet, interface tunnel, tunnel mode

tunnel key

Use the **tunnel key** command to instruct the router to send GRE packets with a security key number. The tunnel endpoint must also be configured to use a security key, and the key numbers must be identical. If a security key is not configured on the tunnel endpoint, or a different key number is used, the packets are discarded. Use the **no** form of the command to specify that no security key should be sent.

Syntax

tunnel key *key_id*

no tunnel key

Parameters

Parameter	Description	Possible Values	Default Value
key_id	The ID number of the security key to be sent with GRE packets	**0-2147483647**	

User Level

read-write

Context

Interface: Tunnel (L2, L2-L3)

Example

To instruct the router to send GRE packets with security key number 7:

```
G450-001(super)# tunnel key 7
```

Related Commands

keepalive (GRE tunnel), tunnel checksum, tunnel destination, tunnel path-mtu-discovery, tunnel source, tunnel ttl

tunnel mode

Use the **tunnel mode** command to specify the encapsulation method of the tunnel. This command is only included for future development, and for conformity with other systems. Currently, the tunnel can only perform GRE encapsulation.

Syntax

tunnel mode ***encapsulation***

no tunnel mode

Parameters

Parameter	Description	Possible Values	Default Value
encapsulation	The encapsulation method of the tunnel	**gre**	

User Level

read-write

Context

Interface: Tunnel (L2, L2-L3)

Example

To specify GRE tunnel encapsulation:

```
G450-001(super)# tunnel mode gre
```

Related Commands

interface fastethernet, interface tunnel, tunnel dscp

tunnel path-mtu-discovery

Use the **tunnel path-mtu-discovery** command to specify that the tunnel maintain information on the maximum allowable packet size (smallest MTU) for the entire routing path of the tunnel. Packets entering the tunnel that are larger than the tunnel's MTU are either fragmented, or sent back with a request for fragmentation (depending on the DF bit of the packet).

Use the age-timer parameter to force the tunnel to update the MTU after a specified number of minutes. Specify infinite to make the MTU value permanent (no updating).

Use the **no** form of the command to disable MTU discovery.

Note:

When MTU discovery is disabled, the tunnel's source interface marks all packets *may be fragmented*, even if the packet's original setting is *do not fragment*. It is highly recommended to enable the MTU-discovery feature on a tunnel.

Syntax

tunnel path-mtu-discovery [age-timer {*minutes* | *infinite*}]

no tunnel path-mtu-discovery

Parameters

Parameter	Description	Possible Values	Default Value
age-timer	Keyword for specifying how often the tunnel must update the MTU		
minutes	Number of minutes after which the tunnel is updated	**10-30**	**10**
infinite	The tunnel does not update the MTU and its value remains permanent		

User Level

read-write

Context

Interface: Tunnel (L2, L2-L3)

Example

To specify that the tunnel maintain information on the minimum MTU for the entire routing path of the tunnel, updating the MPU every 20 minutes:

```
G450-001(super)# tunnel path-mtu-discovery age-timer 20
```

Related Commands

keepalive (GRE tunnel), tunnel checksum, tunnel destination, tunnel key, tunnel source, tunnel ttl

tunnel source

Use the **tunnel source** command to specify the IP address of the source interface for the GRE tunnel. The source interface is the interface used to direct all traffic into the tunnel.

Note:

The CLI does not verify that the specified IP address actually exists.

Syntax

tunnel source *ip-address*

Parameters

Parameter	Description	Possible Values	Default Value
ip-address	The IP address of the source interface for the GRE tunnel		

User Level

read-write

Context

Interface: Tunnel (L2, L2-L3)

Example

To specify the GRE tunnel source interface IP address as 90.0.0.10:

```
G450-001(super)# tunnel source 90.0.0.10
```

Related Commands

keepalive (GRE tunnel), tunnel checksum, tunnel destination, tunnel key, tunnel path-mtu-discovery, tunnel ttl

tunnel ttl

By default, GRE packets are given a ttl value of 255, since there is an unknown number of hops to reach the tunnel endpoint. Use the **`tunnel ttl`** command to override this default. Use the **`no`** form of the command to use the default ttl value.

Syntax

`tunnel ttl` ***`ttl`***

`no tunnel ttl`

Parameters

Parameter	Description	Possible Values	Default Value
`ttl`	The ttl value to be used instead of the default ttl value of 255	**1-255**	

User Level

read-write

Context

Interface: Tunnel (L2, L2-L3)

Example

To set the ttl value to 16:

```
G450-001(super)# tunnel ttl 16
```

Related Commands

keepalive (GRE tunnel), tunnel checksum, tunnel destination, tunnel key, tunnel path-mtu-discovery, tunnel source

show interfaces

Use the **show interfaces** command to display interface configuration and statistics for a particular interface or all interfaces. The Frame Relay sub-interface only includes the following counters:

- packets & bytes in
- packets & bytes out
- input errors
- output drops

Syntax

show interfaces [*interface_type interface_identifier*]

Parameters

Parameter	Description	Possible Values	Default Value
interface_type	The type of interface	**Dialer, FastEthernet, Serial, Vlan, Loopback, Console, Tunnel, USB**	
interface_identifier	The interface number. The format varies depending on the value of interface_type: For FastEthernet: **module/port** For Serial: **module/ port:channel-group** For Vlan: **Vlan id** For LoopBack: **Loopback number** For Tunnel: **Tunnel number**	For FastEthernet: **10/2 or 10/4** For Serial(USP): **3/1, 4/1, 8/1** For Serial (DS1): module/port: **3/1, 4/1, 8/1** channel-group: E1: **0-30** T1: **0-23** For VLAN: **1-4090** For Loopback: **1-99** For Tunnel: **1-50** For Dialer: **1**	

User Level

read-write

Context

general

Example

To show information about all the interfaces:

```
G450-001(super)# show interfaces
Vlan 1 is up, line protocol is up
Physical address is 00.04.0d.29.c5.11.
Internet address is 172.16.1.139, mask is 255.255.255.240
Primary management interface
MTU 1500 bytes. Bandwidth 100000 kbit.
Reliability 255/255 txLoad 1/255 rxLoad 1/255
Encapsulation ARPA, ICC-VLAN
Link status trap disabled
Full-duplex, 100Mb/s
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:30, Last output 00:00:30
Last clearing of 'show interface' counters never.
5 minute input rate 144 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 input drops, 0 output drops, 0 unknown protocols
3425 packets input, 323518 bytes
3425 broadcasts received, 0 giants
0 input errors, 0 CRC
32 packets output, 896 bytes
0 output errors, 0 collisions

FastEthernet 10/2 is up, line protocol is down
Physical address is 00.04.0d.29.c5.10.
MTU 1500 bytes. Bandwidth 10000 kbit.
Reliability 1/255 txLoad 255/255 rxLoad 255/255
Encapsulation ARPA
Link status trap disabled
Half-duplex, 10Mb/s, 10BaseTX
ARP type: ARPA, ARP Timeout 04:00:00
Dynamic CAC BBL: 1500 kbps
Dynamic CAC activation priority: 50
Dynamic CAC interface status: active
Last input never, Last output never
Last clearing of 'show interface' counters never.
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 input drops, 0 output drops, 0 unknown protocols
0 packets input, 0 bytes
0 broadcasts received, 0 giants
0 input errors, 0 CRC
0 packets output, 0 bytes
0 output errors, 0 collisions

Tunnel 1 is up, line protocol is up
Internet address is 177.0.0.17, mask is 255.0.0.0
MTU 468 bytes. Bandwidth 9 kbit
Reliability 255/255 txLoad 1/255 rxLoad 1/255
```

```
Encapsulation GRE
Link status trap enabled
Keepalive set (10 sec), retries 3
Tunnel source 17.0.0.17, destination 12.0.0.3
Tunnel protocol/transport GRE/IP, key 777
Checksumming of packets enabled
Tunnel DSCP 63, Tunnel TTL 255
Path MTU Discovery, ager 10 mins, MTU 976, expires 00:09:33
Last input never, Last output never
Last clearing of 'show interface' counters never.
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 input drops, 0 output drops, 0 unknown protocols
0 packets input, 0 bytes
0 broadcasts received, 0 giants
0 input errors, 0 CRC
0 packets output, 0 bytes
0 output errors, 0 collisions

Console asynchronous mode is terminal
Terminal baud rate is 9600
```

Related Commands - Frame relay encapsulation

clear frame-relay counters, frame-relay class-dlci, interface serial, map-class frame-relay, fragment, show frame-relay pvc brief

Related Commands - PPP encapsulation

interface dialer, interface fastethernet, interface serial

Related Commands - Verifying WAN configuration

show controllers, show frame-relay fragment, show frame-relay lmi, show frame-relay pvc, show frame-relay traffic, show interfaces, show ip interface, show map-class frame-relay

HTTP server

ip http

Use the **ip http** command to enable the HTTP server. Use the **no** form of the command to disable the HTTP server.

Syntax

ip http [port *port_number*]

[no] ip http

Parameters

Parameter	Description	Possible Values	Default Value
port	Keyword that changes the default port of the HTTP server		
port_number	The number of the new port for the HTTP server	**1-65535**	**80**

User Level

admin

Context

general

ICC configuration

icc-vlan

Use the **icc-vlan** command to set the current VLAN as the ICC-VLAN.

Syntax

icc-vlan

User Level

read-write

Context

interface: VLAN (L2, L2-L3)

Example

To set VLAN 2 as the ICC VLAN:

```
G450-001(super)# interface vlan 2
G450-001(if:Vlan 2)# icc-vlan
```

Related Commands - ICC configuration

show icc-vlan

Related Commands - VLAN configuration

clear port static-vlan, clear vlan, interface vlan, set port static-vlan, set port vlan, set port vlan-binding-mode, set trunk, set vlan, show cam vlan, show port vlan-binding-mode, show trunk, show vlan

show icc-vlan

Use the **show icc-vlan** command to view the ICC-VLAN.

Syntax

show icc-vlan

User Level

read-only

Context

general

Example

To display the ICC VLAN:

```
G450-001(super)# show icc-vlan
VLAN 1
```

Related Commands

icc-vlan

ICMP errors

ip icmp-errors

Use the **ip icmp-errors** command to set ICMP error messages to On. Use the **no** form of this command to set ICMP error messages to Off.

Syntax

[no] ip icmp-errors

User Level

read-write

Context

general

Related Commands

description (interface), interface console, interface fastethernet, interface loopback, interface serial, interface tunnel, interface USB-modem, interface vlan, ip address, ip admin-state, ip broadcast-address, load-interval

show ip icmp

Use the **show ip icmp** command to display the status of ICMP error messages.

Syntax

show ip icmp

User Level

read-only

Context

general

Example

To display ICMP error message status:

```
G450-001(super)# show ip icmp
ICMP error messages status is ENABLE
```

Related Commands

ip icmp-errors

ICMP keepalive

keepalive-icmp

Use the **keepalive-icmp** command to enable the ICMP keepalive mechanism on an interface. ICMP keepalive is a mechanism that reports on the status of an IP address *and its next hop*. The destination interface is only declared to be alive if the next hop is also reachable. This feature is critical for mechanisms such as policy-based routing that must guarantee service on a particular path.

Use the **no** form of the command to disable extended keepalive on the interface.

Note:

You cannot configure both **keepalive-icmp** and **ip address dhcp** (DHCP Client) on the WAN FastEthernet interface.

Syntax

[no] keepalive-icmp *dest_ip_address next_hop_mac_address*

Parameters

Parameter	Description	Possible Values	Default Value
dest_ip_address	The destination address whose status is being monitored		
next_hop_ mac_address	The next hop address for the keepalive packets. This parameter is only relevant for the WAN FastEthernet port.		

User Level

read-write

Context

interface:FastEthernet

Example

To enable ICMP keepalive on the FastEthernet 10/2 interface for destination IP address 135.64.2.12 using MAC 11.22.33.44.55.66:

```
G450-001(if:FastEthernet 10/2)# keepalive-icmp 135.64.2.12 11.22.33.44.55.66
```

Related Commands

keepalive-icmp failure-retries, keepalive-icmp interval, keepalive-icmp source-address, keepalive-icmp success-retries, keepalive-icmp timeout, show keepalive-icmp

keepalive-icmp failure-retries

Use the **keepalive-icmp failure-retries** command to set the number of consecutive failed keepalive packets necessary to set the interface's keepalive status as down. Using this command without a parameter resets the failure-retry value to the default value.

Syntax

keepalive-icmp failure-retries *failure-retries-number*

Parameters

Parameter	Description	Possible Values	Default Value
failure-retries-number	The number of failed keepalive packets required	**1-32**	**4**

User Level

read-write

Context

interface:FastEthernet

Example

To set the number of consecutive failed keepalive packets necessary to set the interface's keepalive status as down to 3:

```
G450-001(if:FastEthernet 10/2)# keepalive-icmp failure-retries 3
```

Related Commands

keepalive-icmp, keepalive-icmp interval, keepalive-icmp source-address, keepalive-icmp success-retries, keepalive-icmp timeout, show keepalive-icmp

keepalive-icmp interval

Use the **keepalive-icmp interval** command to set the interval (in seconds) between keepalive packets. Using this command without a parameter resets the interval value to the default value.

Syntax

keepalive-icmp interval ***seconds***

Parameters

Parameter	Description	Possible Values	Default Value
seconds	The interval time (in seconds)	**1-36**	**5**

User Level

read-write

Context

interface:FastEthernet

Example

To set the interval between keepalive packets to 5 seconds:

```
G450-001(if:FastEthernet 10/2)# keepalive-icmp interval 5
```

Related Commands

keepalive-icmp, keepalive-icmp failure-retries, keepalive-icmp source-address, keepalive-icmp success-retries, keepalive-icmp timeout, show keepalive-icmp

keepalive-icmp source-address

Use the **keepalive-icmp source-address** command to set the source IP address of the keepalive packets. Using this command without a parameter sets the source IP address to the default value, which is the interface's primary IP address.

Syntax

keepalive-icmp source-address *source_ip_address*

Parameters

Parameter	Description	Possible Values	Default Value
source_ip_address	The source IP address of the keepalive packets		The interface's primary IP address

User Level

read-write

Context

interface:FastEthernet

Example

To set the source IP address of the keepalive packets to 149.49.78.96:

```
G450-001(if:FastEthernet 10/2)# keepalive-icmp source-address 149.49.78.96
```

Related Commands

keepalive-icmp, keepalive-icmp failure-retries, keepalive-icmp interval, keepalive-icmp success-retries, keepalive-icmp timeout, show keepalive-icmp

keepalive-icmp success-retries

Use the **keepalive-icmp success-retries** command to set the number of consecutive successful keepalive packets necessary to set the interface's keepalive status as Up. Using this command without a parameter resets the success-retry value to the default value.

Syntax

keepalive-icmp success-retries *success-retries-number*

Parameters

Parameter	Description	Possible Values	Default Value
success-retries-number	The number of successful keepalive packets required	**1-32**	**1**

User Level

read-write

Context

interface:FastEthernet

Example

To set the number of consecutive successful keepalive packets necessary to set the interface's keepalive status as up to 2:

```
G450-001(if:FastEthernet 10/2)# keepalive-icmp success-retries 2
```

Related Commands

keepalive-icmp, keepalive-icmp failure-retries, keepalive-icmp interval, keepalive-icmp timeout, keepalive-icmp source-address, show keepalive-icmp

keepalive-icmp timeout

Use the **keepalive-icmp timeout** command to set the timeout (in seconds) for receiving the keepalive response. Using this command without a parameter resets the timeout value to the default value.

Syntax

keepalive-icmp timeout *timeout*

Parameters

Parameter	Description	Possible Values	Default Value
timeout	The number of seconds to wait for a response	**1-10**	**1**

User Level

read-write

Context

interface:FastEthernet

Example

To set the timeout for receiving the keepalive response to 1 second:

```
G450-001(if:FastEthernet 10/2)# keepalive-icmp timeout 1
```

Related Commands

keepalive-icmp, keepalive-icmp failure-retries, keepalive-icmp interval, keepalive-icmp source-address, keepalive-icmp success-retries, show keepalive-icmp

show keepalive-icmp

Use the **show keepalive-icmp** command to display information about the extended keepalive settings.

Syntax

show keepalive-icmp

User Level

read-only

Context

interface:FastEthernet

Example

To display information about the extended keepalive settings:

```
G450-001(if:FastEthernet 10/2)# show keepalive-icmp

Mode:                       Disable
Status:                     Disable
Destination IP:             135.64.103.27
Next-Hop MAC:               0x11-22-33-44-55-66
Source IP:                  135.63.33.44
Timeout:                    1 Sec
Interval:                   20 Sec
Success Retries:            1
Failure Retries:            4
Success Retries Counter:    4
Failure Retries Counter:    0
```

Related Commands

keepalive-icmp, keepalive-icmp failure-retries, keepalive-icmp interval, keepalive-icmp source-address, keepalive-icmp success-retries, keepalive-icmp timeout

IP interface configuration

interface console

Use the **interface console** command to enter the Console interface configuration mode. The interface is created if it does not exist. Use the **no** form of this command to set the Console parameters to their default values.

Syntax

[no] interface console

User Level

read-write

Context

general

Example

To enter the Console interface context:

```
G450-001(super)# interface console
G450-001(if:Console)#
```

Related Commands - Modem configuration

async modem-init-string, interface USB-modem, ppp chap-secret

Related Commands - IP interface configuration

description (interface), interface fastethernet, interface loopback, interface serial, interface tunnel, interface USB-modem, interface vlan, ip address, ip admin-state, ip broadcast-address, load-interval, show ip interface brief

interface dialer

Use the **interface dialer** command to enter the Dialer interface context and create or configure the Dialer interface. Use the **no** form of this command to delete the Dialer interface.

Syntax

[no] interface dialer *dialer-id*

Parameters

Parameter	Description	Possible Values	Default Value
dialer-id	Identification number for the Dialer interface	**1**	**1**

User Level

read-write

Context

general

Example

To enter the context for interface dialer 1:

```
G450-001(super)# interface dialer 1
G450-001(if:dialer 1)#
```

Related Commands

dialer modem-interface, dialer order, dialer persistent, dialer persistent delay, dialer persistent initial delay, dialer persistent max-attempts, dialer persistent re-enable, dialer string, dialer wait-for-ipcp

interface fastethernet

Use the **interface fastethernet** command to enter the FastEthernet interface configuration mode. Use the **no** form of this command to delete an IP interface.

If the specified interface does not exist, the system creates it and enters its configuration mode.

Syntax

[no] interface fastethernet [*module*/*port*[.*ip_interface*]]

Parameters

Parameter	Description	Possible Values	Default Value
module	The module number of the interface	**10**	
port	The port number of the interface	**3**	
ip_interface	The IP sub-interface number within this interface. A number of IP interfaces may be bound to a Layer 3 interface.	**0-1024**	

User Level

read-write

Context

general

Example

To create a FastEthernet interface and enter its context:

```
G450-001(super)# interface fastethernet 10/2
```

To create a Level 3 sub-interface on the FastEthernet interface:

```
G450-001(super)# interface fastethernet 10/2.1
```

Related Commands

description (interface), interface console, interface loopback, interface serial, interface tunnel, interface USB-modem, interface vlan, ip address, ip admin-state, ip broadcast-address, ip crypto-group, load-interval, show ip interface brief

interface loopback

Use the **interface Loopback** command to enter Loopback interface configuration mode. Use the **no** form of this command to delete a Loopback interface or sub-interface.

If the specified interface does not exist, the system creates it and enters its configuration mode.

Syntax

[no] interface loopback [*interface_number*[.*ip_interface*]]

Parameters

Parameter	Description	Possible Values	Default Value
interface_number	The number of the interface	**1-99**	
ip_interface	The IP sub-interface number within this interface. A number of IP interfaces may be bound to a Layer 3 interface.	**0-1024**	

User Level

read-write

Context

general

Example

To create Loopback interface 1 and enter its configuration mode:

```
G450-001(super)# interface loopback 1
```

To create a Layer 3 sub-interface:

```
G450-001(super)# interface loopback 1.1
```

Related Commands

description (interface), interface console, interface fastethernet, interface serial, interface tunnel, interface USB-modem, interface vlan, ip address, ip admin-state, ip broadcast-address, load-interval, show ip interface brief

interface serial

Use the **interface serial** command to enter Serial interface or sub interface configuration mode. If the specified interface or sub interface does not exist, the system creates it and enters its configuration mode.

Use the **no** form of the command to delete the interface. The **no** form can only be used to delete sub L3 and sub frame relay interfaces. The command fails for USP interfaces and when higher or lower layers are defined for that interface.

Syntax

[no] interface serial *module/if_number* [*if_link_type*]

For USP interfaces ***if_number*** has the syntax:

port[.***ip_interface*** | {.***sub_interface***[.***ip_interface***]}]

For DS1 interfaces ***if_number*** has the syntax:

port:***channel_group***[.***ip_interface*** | {.***sub_interface***[.***ip_interface***]}]

Parameters

Parameter	Description	Possible Values	Default Value
module	The interface module number		
port	The port number of the interface		
channel_group		For E1: **0-30** For T1: **0-23**	
sub_interface		**1-127**	
ip_interface		**0-1024**	
if_link_type		**point-to-point**	

User Level

read-write

Context

general, interface:serial (FR SUB)

Example

To create point to point sub-interface number 17 over channel group 2 over E1/T1 controller number 1:

```
G450-001(super)# interface serial 3/1:2.17 point-to-point
```

Related Commands

description (interface), interface console, interface fastethernet, interface loopback, interface tunnel, interface USB-modem, interface vlan, ip address, ip admin-state, ip broadcast-address, ip crypto-group, load-interval, show ip interface brief

interface tunnel

Use the **interface tunnel** command to enter Tunnel interface configuration mode. Use the **no** form of this command to delete a Tunnel interface.

If the specified interface does not exist, the system creates it and enters its configuration mode.

Syntax

[no] interface tunnel *tunnel_number*

Parameters

Parameter	Description	Possible Values	Default Value
tunnel_number	The number of the interface	**1-99**	

User Level

read-write

Context

general

Example

To create interface tunnel 1 and enter its configuration mode:

```
G450-001(super)# interface tunnel 1
```

Related Commands - IP interface configuration

description (interface), interface console, interface fastethernet, interface loopback, interface serial, interface USB-modem, interface vlan, ip address, ip admin-state, ip broadcast-address, load-interval, show ip interface brief

Related Commands - GRE tunneling

interface fastethernet, tunnel dscp, tunnel mode

interface USB-modem

Use the **interface usb-modem** command to enter the configuration context for the USB interface. Use the **no** form of the command to reset the USB interface settings to their factory defaults.

The USB interface always exists, but is disabled by default. Use the **no shutdown** command to enable the interface.

The default settings for the USB-modem interface are:

Interface status	DOWN
IP address	10.3.0.3
Netmask	255.255.255.0
timeout	no timeout
PPP speed	38400 bps
Async modem-init-string	"AT S7=45 S0=2 L1 V1 X4 &c1 E0 Q0"

Syntax

[no] interface usb-modem

User Level

read-write

Context

general

Example

To enter the USB-modem interface context:

```
G450-001(super)# interface usb-modem
G450-001(super-if:USB-modem)#
```

Related Commands - IP interface configuration

description (interface), interface console, interface fastethernet, interface loopback, interface serial, interface tunnel, interface vlan, ip address, ip admin-state, ip broadcast-address, load-interval, show ip interface brief

Related Commands - Modem configuration

async modem-init-string, interface console, ppp chap-secret

interface vlan

Use the **interface vlan** command to enter VLAN interface configuration mode. Use the **no** form of this command to delete the interface.

If the specified interface does not exist, the system creates it and enters its configuration mode.

Syntax

[no] interface vlan *vlan_id*[.*ip_interface*]

Parameters

Parameter	Description	Possible Values	Default Value
vlan_id	The VLAN ID number of this interface	**1-4090**	
ip_interface	The IP sub-interface number within this interface. A number of IP interfaces may be bound to a Layer 3 interface.	**0-1024**	

User Level

read-write

Context

general

Example

To create VLAN 2 and enter its configuration context:

```
G450-001(super)# interface vlan 2
```

To create a sub interface 1 on VLAN 2:

```
G450-001(if:Vlan 2)# interface vlan 2.1
```

Related Commands - IP interface configuration

description (interface), interface console, interface fastethernet, interface loopback, interface serial, interface tunnel, interface USB-modem, ip address, ip admin-state, ip broadcast-address, load-interval, show ip interface brief

Related Commands - VLAN configuration

clear port static-vlan, clear vlan, icc-vlan, set port static-vlan, set port vlan, set port vlan-binding-mode, set trunk, set vlan, show cam vlan, show port vlan-binding-mode, show trunk, show vlan

description (interface)

Use the **description** command to configure a description for the current interface. Use the **no** form of this command to clear the description of the current interface.

Syntax

description ***string***

no description

Parameters

Parameter	Description	Possible Values	Default Value
string	The description of the interface		

User Level

read-write

Context

Interface: Console, Serial (DS1 PPP L2, DS1 PPP L2-L3, DS1 FR L2, DS1 FR-SUB L2, DS1 FR-SUB L2-L3, USP PPP L2, USP PPP L2-L3, USP FR L2), FastEthernet (L2, L2-L3, PPP L2, PPP L2-L3), VLAN (L2, L2-L3), Loopback (L2, L2-L3), Tunnel (L2, L2-L3), Dialer (L2, L2-L3), USB-modem

Example

To specify the VLAN 3 interface description as Marketing VLAN:

```
G450-001(if:Vlan 3)# description "Marketing VLAN"
```

Related Commands

interface console, interface fastethernet, interface loopback, interface serial, interface tunnel, interface USB-modem, interface vlan, ip address, ip admin-state, ip broadcast-address, load-interval, show ip interface brief

ip address

Use the **ip address** command to assign an IP address and mask to an interface. Use the **no** form of this command to delete an IP interface.

Syntax

ip address {*ip_address mask* [*admin_state*]}|negotiated

no ip address

Parameters

Parameter	Description	Possible Values	Default Value
ip_address	The IP address assigned to the interface		
mask	Mask for the associated IP subnet		
admin_state	The administration status. This parameter is not used with the Console interface.	**up**, **down**	**up**
negotiated	Interface receives address and mask from a remote device		

User Level

read-write

Context

Interface: Console, Serial (DS1 PPP L2-L3, DS1 PPP L3, DS1 FR-SUB L2-L3, DS1 FR-SUB L3, USP PPP L2-L3, USP PPP L3), FastEthernet (L2-L3, L3, PPP L2-L3, PPP L3), VLAN (L2-L3, L3), USB-modem, Loopback (L2-L3, L3), Tunnel (L2-L3, L3), Dialer (L2-L3, L3)

Example

To assign the IP address 192.168.22.33 with mask 255.255.255.0 to the FastEthernet interface:

```
G450-001(if:FastEthernet 10/2)# ip address 192.168.22.33 255.255.255.0
```

Related Commands

description (interface), interface console, interface fastethernet, interface loopback, interface serial, interface tunnel, interface USB-modem, interface vlan, ip admin-state, ip broadcast-address, load-interval, show ip interface brief

ip admin-state

Use the **ip admin-state** command to set the administrative state of an IP interface. The default state is **up**.

Syntax

ip admin-state up|down

Parameters

Parameter	Description	Possible Values	Default Value
up	Keyword specifying the administrative state of the IP interface is set to up (active)		
down	Keyword specifying the administrative state of the IP interface is set to down (inactive)		

User Level

read-write

Context

interface:Serial (DS1 PPP L2-L3, DS1 PPP L3, DS1 FR-SUB L2-L3, DS1 FR-SUB L3, USP PPP L2-L3, USP PPP L3), FastEthernet (L2-L3, L3), VLAN (L2-L3, L3), Loopback (L2-L3, L3), Tunnel (L2-L3, L3), Dialer (L2-L3, L3, PPP L2-L3, PPP L3)

Example

To set the administrative state of an IP interface to up:

```
G450-001(super-if:FastEthernet 10/2)# ip admin-state up
```

Related Commands

description (interface), interface console, interface fastethernet, interface loopback, interface serial, interface tunnel, interface USB-modem, interface vlan, ip address, ip broadcast-address, load-interval, show ip interface brief

ip broadcast-address

Use the **ip broadcast-address** command to update the interface broadcast address.

Syntax

ip broadcast-address ***bc_addr***

Parameters

Parameter	Description	Possible Values	Default Value
bc_addr	The broadcast IP address		

User Level

read-write

Context

interface:Serial (DS1 PPP L2-L3, DS1 PPP L3, DS1 FR-SUB L2-L3, DS1 FR-SUB L3, USP PPP L2-L3, USP PPP L3), FastEthernet (L2-L3, L3, PPP L2, PPP L2-L3, PPP L3), Tunnel (L2-L3, L3), VLAN (L2-L3, L3), Dialer (L2, L2-L3, L3)

Example

To set the broadcast address for the VLAN 1 interface to 192.168.255.255:

```
G450-001(if:Vlan 1)# ip broadcast-address 192.168.255.255
```

Related Commands

description (interface), interface console, interface fastethernet, interface loopback, interface serial, interface tunnel, interface USB-modem, interface vlan, ip address, ip admin-state, load-interval, show ip interface brief

load-interval

Use the **load-interval** command to set the load calculation interval for an interface. Use the **no** form of the command to restore the load calculation to its default value.

Note:

The load interval must be in increments of 30 seconds.

Syntax

load-interval *seconds*

no load-interval

Parameters

Parameter	Description	Possible Values	Default Value
seconds	The load calculation interval, in seconds. This parameter must be divisible by 30.	**30-600**	**300**

User Level

read-write

Context

Interface: Console, Serial (DS1 PPP L2, DS1 PPP L2-L3, DS1 FR L2, USP PPP L2, USP PPP L2-L3, USP FR L2), FastEthernet (L2, L2-L3, PPP L2, PPP L2-L3), VLAN (L2, L2-L3), Loopback (L2, L2-L3), Tunnel (L2, L2-L3), Dialer (L2, L2-L3), USB-modem

Example

To set the load calculation interval to 60 seconds:

```
G450-001(if:Serial 3/1:1)# load-interval 60
```

Related Commands

description (interface), interface console, interface fastethernet, interface loopback, interface serial, interface tunnel, interface USB-modem, interface vlan, ip address, ip admin-state, ip broadcast-address, show ip interface brief

show ip interface

Use the **show ip interface** command to display information about an interface that has an IP address or about all interfaces that have IP addresses.

Syntax

show ip interface [*interface_name*|*ip_interface*|*ip_address*]

Parameters

Parameter	Description	Possible Values	Default Value
interface_name	The name of the interface whose information you want to display		
ip_interface	The name of the IP interface whose information you want to display	string (1-32 chars)	
ip_address	The IP address of the interface whose information you want to display		

Note:

When specifying an interface name that includes spaces, enclose the entire name in quotation marks (for example, “FastEthernet 10/2”).

User Level

read-only

Context

general

Example

To display information for the FastEthernet interface:

```
G450-001(super)# show ip interface "FastEthernet 10/2"
```

To display information for the sub-interface 0 of the FastEthernet interface:

```
G450-001(super)# show ip interface "FastEthernet 10/2.0"
```

To display all IP interfaces:

```
G450-001(super)# show ip interface
Showing 2 Interfaces
Serial 1:1 is down
Internet address is 2.2.2.2, subnet mask is 255.255.255.0
Advertised IPCP address
Broadcast address is 2.2.2.255
Directed broadcast forwarding is disabled
Proxy ARP is disabled
Primary management IP interface

FastEthernet 10/2 is up
Internet address is 149.49.75.71, subnet mask is 255.255.255.0
Broadcast address is 149.49.75.255
Directed broadcast forwarding is disabled
Proxy ARP is disabled
```

Note:

If address negotiation is configured on the PPP connection, the following appears:
`Internet address will be negotiated using IPCP`, or
`Address determined by IPCP`.

If DHCP client was configured on the interface, the following appears: `Internet address will be negotiated using DHCP`, or
`Address determined by DHCP`.

Header Compression Output Fields

If header compression was enabled on the interface, one of the following header compression status messages appears:

Status message	Meaning
RTP/IP header compression is enabled and not compressing	RTP header compression was enabled on this interface, but is not actively compressing. This can be caused by failure to negotiate.
RTP /IP header compression is enabled and compressing	RTP header compression was enabled on this interface, and is functioning properly
RTP /IP header compression is disabled	RTP header compression is disabled (default)
TCP/IP header compression is enabled and not compressing	VJ header compression was enabled on this interface, but is not actively compressing. This can be caused by failure to negotiate.
TCP/IP header compression is enabled and compressing	Header compression was enabled on this interface, and is functioning properly
TCP/IP header compression is disabled	VJ header compression is disabled (default)

Related Commands

show controllers, show frame-relay fragment, show frame-relay lmi, show frame-relay pvc, show frame-relay traffic, show interfaces, show map-class frame-relay

show ip interface brief

Use the **show ip interface brief** command to display a summary of the information for a specific interface or for all of the interfaces.

Syntax

show ip interface brief [*interface_name*|*ip_interface*|*ip_address*]

Parameters

Parameter	Description	Possible Values	Default Value
interface_name	The name of the interface whose information you want to display		
ip_interface	The name of the IP interface whose information you want to display	string (1-32 chars)	
ip_address	The IP address of the interface whose information you want to display		

Note:

When specifying an interface name that includes spaces, enclose the entire name in quotation marks (for example, “FastEthernet 10/2”).

User Level

read-only

Context

general

Example

To show a summary of information for all interfaces (in this example, PPP is activated on the FastEthernet interface and no IP address has been gathered):

```
G450-001(super)# show ip interface brief
Showing 6 Interfaces
Interface             Address            Mask Method    Status
------------------  ------------------  ---- ------    ------------
FastEth  10/2         unassigned          32   IPCP      down
Vlan     10           10.0.0.1             8   manual    up
Vlan     20           20.0.0.1             8   manual    up
Serial   3/1:1        51.0.0.1             8   manual    up
Console               10.3.0.1            24   manual    down
Usb                   10.3.0.3            24   manual    down
```

(In this example, PPP is activated on the FastEthernet interface and an IP address has been gathered)

```
G450-001(super)# show ip interface brief
Showing 1 Interface
        Interface             Address     Mask Method        Status
------------------------ --------------- ---- ------ --------------------
FastEth  10/2              10.0.0.50         32 IPCP        up
```

(In this example, no IP address has been gathered for the interface configured with DHCP client.)

```
G450-001(super)# show ip interface brief
Showing 1 Interface
        Interface             Address     Mask Method        Status
------------------------ --------------- ---- ------ --------------------
FastEth  10/2              unassigned        32 DHCP        down
```

(In this example, an IP address has been gathered for the interface configured with DHCP client.)

```
G450-001(super)# show ip interface brief
Showing 1 Interface
        Interface             Address     Mask Method        Status
------------------------ --------------- ---- ------ --------------------
FastEth  10/2              10.0.0.40         24  DHCP        up
```

Related Commands

description (interface), interface console, interface fastethernet, interface loopback, interface serial, interface tunnel, interface USB-modem, interface vlan, ip address, ip admin-state, ip broadcast-address, load-interval

shutdown (interface)

Use the **shutdown** command to set the administrative status of the current interface to down. Use the **no** form of this command to restore the administrative status for the interface to up.

Syntax

[no] shutdown

User Level

read-write

Context

interface:Serial (DS1 PPP L2, DS1 PPP L2-L3, DS1 FR L2, DS1 FR-SUB L2, DS1 FR-SUB L2-L3, USP PPP L2, USP PPP L2-L3, USP FR L2), FastEthernet (L2, L2-L3, PPP L2, PPP L2-L3), VLAN (L2, L2-L3), Console, Loopback (L2, L2-L3), Controller, Tunnel (L2, L2-L3), Dialer (L2, L2-L3)

Example

To shutdown the VLAN 2 interface:

```
G450-001(if:Vlan 2)# shutdown
Interface Vlan 2, changed state to administratively down
Line protocol on Interface Vlan 2, changed state to down
```

Related Commands - WAN Ethernet port configuration

autoneg, duplex, speed (interface), traffic-shape rate

Related Commands - Modem configuration

async mode interactive, async mode terminal, async reset-modem (Console port), ip address, ppp authentication, speed (PPP), timeout absolute

IP phone upgrades

clear ip tftp-server statistics

Use the **clear ip tftp-server statistics** command to clear TFTP server statistics.

Syntax

clear ip tftp-server statistics

User Level

read-write

Context

general

Example

To clear TFTP server statistics:

```
G450-001# clear ip tftp-server statistics
```

Related Commands

copy ftp phone-image, copy ftp phone-script, copy running-config startup-config, copy scp phone-script, copy tftp phone-image, copy tftp phone-script, erase phone-image, ip tftp-server file-system size, show application-memory, show download phone-script-file status, show ip tftp-server files, show ip tftp-server statistics, show upload phone-script-file status

copy ftp phone-image

Use the **copy ftp phone-image** command to download a file from a remote FTP server to phone image bank A, B, C, or D in the local gateway TFTP directory. The G450 prompts you for a username and password when you enter a command to transfer a file using FTP.

Syntax

copy ftp phone-imageA|phone-imageB|phone-imageC|phone-imageD *filename ip*

Context

general

Parameters

Parameter	Description	Possible Values	Default Value
filename	The name of the image file, including the full path		
ip	The IP address of the host		

User Level

read-write

Example

To download `4602sape1_8.bin` from a remote FTP server at IP address 192.168.49.10 to phone image bank A using login anonymous:

```
G450-001# copy ftp phone-imageA c:\IpphoneRelease\4602sape1_8.bin
192.168.49.10
Confirmation - do you want to continue (Y/N)? y
```

```
Username: anonymous
Password:
Beginning download operation ...
This operation may take up to 20 seconds.
Please refrain from any other operation during this time.
```

Related Commands

copy ftp phone-script, copy scp phone-script, copy tftp phone-image, copy tftp phone-script, copy usb announcement-file, erase phone-image, ip tftp-server file-system size, show application-memory, show ip tftp-server files, show download phone-script-file status, show upload phone-script-file status

copy ftp phone-script

Use the **copy ftp phone-script** command to download a file from a remote FTP server to phone script bank A or B on the local G450 TFTP directory. The G450 prompts you for a username and password when you enter a command to transfer a file using FTP.

Syntax

copy ftp phone-scriptA|phone-scriptB *filename ip*

Parameters

Parameter	Description	Possible Values	Default Value
filename	The name of the configuration file, including the full path		
ip	The IP address of the host		

User Level

read-write

Context

general

Example

To download `46xxupgrade.txt` from a remote FTP server at IP address 192.168.49.10 to phone script bank A using login anonymous:

```
G450-001# copy ftp phone-scriptA 46xxupgrade.txt 192.168.49.10
Confirmation - do you want to continue (Y/N)? y
```

```
Username: anonymous
Password:
Beginning download operation ...
This operation may take up to 20 seconds.
Please refrain from any other operation during this time.
```

Related Commands

copy announcement-file usb, copy ftp phone-image, copy scp phone-script, copy tftp phone-image, copy tftp phone-script, copy usb announcement-file, erase phone-image, ip tftp-server file-system size, show application-memory, show ip tftp-server files, show download phone-script-file status, show upload phone-script-file status

copy phone-script ftp

Use the **copy phone-script ftp** command to upload a phone script file from the local G450 TFTP directory to a remote server, using FTP.

Syntax

copy phone-scriptA|phone-scriptB|phone-scriptC|phone-scriptD ftp *filename ip*

Parameters

Parameter	Description	Possible Values	Default Value
filename	The name of the configuration file, including the full path		
ip	The IP address of the host		

User Level

read-write

Context

general

Example

To upload `46xxupgrade.txt` to the host at IP address 192.168.49.10 using login anonymous:

```
G450-001# copy phone-scriptA ftp 46xxupgrade.txt 192.168.49.10
Confirmation - do you want to continue (Y/N)? y
Username: anonymous
```

```
Password:
Beginning upload operation ...
This operation may take up to 20 seconds.
Please refrain from any other operation during this time.
```

Related Commands

copy announcement-file usb, copy ftp phone-script, copy scp phone-script, copy tftp phone-image, copy phone-script ftp, copy phone-script scp, copy phone-script tftp, copy scp phone-script, copy tftp phone-image, copy usb announcement-file

copy phone-script scp

Use the **copy phone-script scp** command to upload a phone script file from the local G450 TFTP directory to a remote server, using SCP.

Syntax

copy phone-scriptA|phone-scriptB|phone-scriptC|phone-scriptD scp *filename ip*

Parameters

Parameter	Description	Possible Values	Default Value
filename	The name of the configuration file, including the full path		
ip	The IP address of the host		

User Level

read-write

Context

general

Example

To copy `46xxupgrade.txt` to the host at IP address 192.168.49.10 using login anonymous:

```
G450-001# copy phone-scriptA scp 46xxupgrade.txt 192.168.49.10
Confirmation - do you want to continue (Y/N)? y
Username: anonymous
Password:
Beginning upload operation ...
```

```
This operation may take up to 20 seconds.
Please refrain from any other operation during this time.
```

Related Commands

copy announcement-file usb, copy ftp phone-script, copy scp phone-script, copy tftp phone-image, copy phone-script ftp, copy phone-script tftp, copy scp phone-script, copy tftp phone-image, copy usb announcement-file

copy phone-script tftp

Use the **copy phone-script tftp** command to upload a phone script file from the local G450 TFTP directory to a remote server, using TFTP.

Syntax

copy phone-scriptA|phone-scriptB|phone-scriptC|phone-scriptD tftp *filename ip*

Parameters

Parameter	Description	Possible Values	Default Value
filename	The name of the configuration file, including the full path		
ip	The IP address of the host		

User Level

read-write

Context

general

Example

To upload `46xxupgrade.txt` to the host at IP address 192.168.49.10:

```
G450-001(super)# copy phone-scriptA tftp 46xxupgrade.txt 192.168.49.10
```

Related Commands

copy announcement-file usb, copy ftp phone-script, copy scp phone-script, copy tftp phone-image, copy phone-script ftp, copy phone-script scp, copy scp phone-script, copy tftp phone-image, copy usb announcement-file

copy phone-script usb

Use the **copy phone-script usb** command to upload a phone script file from the gateway to the USB mass storage device.

Syntax

copy {phone-scriptA | phone-scriptB} usb *source-filename* *destination-usb-device* [*destination-filename*]

Parameters

Parameter	Description	Possible Values	Default Value
source-filename	The logical name for the source file		
destination usb-device	The destination USB mass storage device	**usb-device0**	
destination-filename	The destination file name and path		

User Level

read-write

Context

general

Example

To upload `46xxupgrade.scr` from the gateway to usb-device0:

```
G450-001(super)# copy phone-scriptA usb 46xxupgrade.scr usb-device0
```

Related Commands

backup config usb, copy usb announcement-file, erase usb, restore usb, safe-removal usb, show backup status, show restore status, show usb

copy scp phone-script

Use the **copy scp phone-script** command to download a file from a remote SCP server to phone script bank A or B in the local G450 TFTP directory.

Syntax

copy scp phone-scriptA|phone-scriptB *filename ip*

Parameters

Parameter	Description	Possible Values	Default Value
filename	The name of the configuration file, including the full path		
ip	The IP address of the host		

User Level

read-write

Context

general

Example

To download `46xxupgrade.txt` from the host at IP address 192.168.49.10 using login anonymous:

```
G450-001# copy scp phone-scriptA 46xxupgrade.txt 192.168.49.10
Confirmation - do you want to continue (Y/N)? y
Username: anonymous
Password:
Beginning download operation ...
This operation may take up to 20 seconds.
Please refrain from any other operation during this time.
```

Related Commands

copy announcement-file usb, copy ftp phone-image, copy ftp phone-script, copy tftp phone-image, copy tftp phone-script, copy usb announcement-file, erase phone-image, ip tftp-server file-system size, show application-memory, show ip tftp-server files, show download phone-script-file status, show upload phone-script-file status

copy tftp phone-image

Use the **copy tftp phone-image** command to download a file from a remote TFTP server to phone image bank A, B, C, or D in the local G450 TFTP directory.

Syntax

copy tftp phone-imageA|**phone-imageB**|**phone-imageC**|**phone-imageD** ***filename ip***

Parameters

Parameter	Description	Possible Values	Default Value
filename	The name of the configuration file, including the full path		
ip	The IP address of the host		

User Level

read-write

Context

general

Example

To download `4602sape1_8.bin` from the host at IP address 192.168.49.10:

```
G450-001(super)# copy tftp phone-imageA c:\IpphoneRelease\4602sape1_8.bin
192.168.49.10
```

Related Commands

copy ftp phone-image, copy ftp phone-script, copy scp phone-script, copy tftp phone-script, copy usb announcement-file, erase phone-image, ip tftp-server file-system size, show application-memory, show ip tftp-server files, show download phone-script-file status, show upload phone-script-file status

copy tftp phone-script

Use the **copy tftp phone-script** command to download a file from a remote TFTP server to phone script bank A or B in the local G450 TFTP directory.

Syntax

copy tftp phone-scriptA|phone-scriptB *filename ip*

Parameters

Parameter	Description	Possible Values	Default Value
filename	The name of the configuration file, including the full path		
ip	The IP address of the host		

User Level

read-write

Context

general

Example

To download `file1.txt` from the host at IP address 135.64.100.205:

```
G450-001(super)# copy tftp phone-scriptA file1.txt 135.64.100.205
Confirmation - do you want to continue (Y/N)? y
```

Related Commands

copy announcement-file usb, copy ftp phone-image, copy ftp phone-script, copy scp phone-script, copy tftp phone-image, copy usb announcement-file, erase phone-image, ip tftp-server file-system size, show application-memory, show ip tftp-server files, show download phone-script-file status, show upload phone-script-file status

copy usb phone-image

Use the **copy usb** command to download a file from the external USB mass storage device to phone image bank A, B, C, or D in the local gateway TFTP directory.

Syntax

copy usb {phone-imageA | phone-imageB | phone-imageC | phone-imageD} ***source-usb-device source-filename***

Parameters

Parameter	Description	Possible Values	Default Value
source usb-device	The source USB mass storage device	**usb-device0**	
source-filename	The full name and path of the file to be downloaded		

User Level

read-write

Context

general

Example

To download `4601dape1_82.bin` from usb-device0 to phone image bank A in the local gateway TFTP directory:

```
G450-001(super)# copy usb phone-imageA usb-device0 \temp\4601dape1_82.bin
```

Related Commands

backup config usb, copy announcement-file usb, erase usb, restore usb, safe-removal usb, show backup status, show restore status, show usb

copy usb phone-script

Use the **copy usb phone-script** command to download a phone script file from the external USB mass storage device to phone script bank A or B on the local gateway's TFTP directory.

Syntax

copy usb {phone-scriptA | phone-scriptB} ***source-usb-device source-filename***

Parameters

Parameter	Description	Possible Values	Default Value
source usb-device	The source USB mass storage device	**usb-device0**	
source-filename	The full name and path of the file to be downloaded		

User Level

read-write

Context

general

Example

To download `46xxupgrade.scr` from usb-device0 to phone script bank A on the local gateway's TFTP directory:

```
G450-001(super)# copy usb phone-scriptA usb-device0 \temp\46xxupgrade.scr
```

Related Commands

backup config usb, copy announcement-file usb, erase usb, restore usb, safe-removal usb, show backup status, show restore status, show usb

erase phone-image

Use the **erase phone-image** command to delete phone-image A, B, C, D, E, or F.

Syntax

erase phone-imageA|phone-imageB|phone-imageC|phone-imageD|phone-imageE|phone-imageF

User Level

read-write

Context

general

Example

To delete phone-image A:

```
G450-001# erase phone-imageA
Beginning erase operation .... Done!
```

Related Commands

copy ftp phone-script, copy scp phone-script, copy ftp phone-image, copy tftp phone-image, copy tftp phone-script, copy usb announcement-file, ip tftp-server file-system size, show application-memory, show ip tftp-server files, show download phone-script-file status, show upload phone-script-file status

erase phone-script

Use the **erase phone-script** command to delete phone-script A, B, C, or D.

Syntax

erase phone-scriptA|phone-scriptB|phone-scriptC|phone-scriptD

User Level

read-write

Context

general

Example

To delete phone-script A:

```
G450-001(super)# erase phone-scriptA
Beginning erase operation .... Done!
```

Related Commands

copy announcement-file usb, copy scp phone-script, copy tftp phone-script, copy usb announcement-file, show download phone-script-file status, show upload phone-script-file status

ip tftp-server file-system size

Use the **ip tftp-server file-system-size** command to set the TFTP file system size. Use the **no ip tftp-server file-system-size** command to reset the TFTP file system size to its default size.

Note:

It is possible to increase the memory allocation for the Sniffer cache application at the expense of the TFTP file system size. The Sniffer cache application may have been configured to use up to 1000 Kb of the default TFTP allocation of 18560 Kb, which would cause a conflict when setting the TFTP allocation to a high value.

Syntax

[no] ip tftp-server file-system-size *size*

Parameters

Parameter	Description	Possible Values	Default Value
size	The TFTP server total file size in KB	**256-19456**	**18560**

User Level

read-write

Context

general

Example

To set the TFTP file system size to 18128 KB:

```
G450-001# ip tftp-server file-system-size 18128
To change ip tftp-server file system size, copy the running configuration to
the start-up configuration file, and reset the device
```

Related Commands

copy ftp phone-image, copy ftp phone-script, copy running-config startup-config, copy scp phone-script, copy tftp phone-image, copy tftp phone-script, erase phone-image, show application-memory, show ip tftp-server files, show upload phone-script-file status, ip tftp-server

show application-memory

Use the **show application-memory** CLI command to show the configured and allocated application memory.

Syntax

show application-memory

User Level

read-only

Context

general

Example

To show the configured and allocated application memory:

```
G450-001(super)# show application-memory

Application                                        Memory(KB)
                                              Allocated  Configured
----------------------------------------  ---------------------
Sniffer (capture buffer-size)                      1024        1024
TFTP (ip tftp-server file-system-size)            18560       18560
----------------------------------------  ---------------------
Total used memory                                 19584       19584
Total free memory                                   896         896
Total memory (fixed)                              20480
```

Related Commands

copy ftp phone-image, copy ftp phone-script, copy running-config startup-config, copy scp phone-script, copy tftp phone-image, copy tftp phone-script, erase phone-image, ip tftp-server file-system size, show ip tftp-server files, show upload phone-script-file status

show download phone-image-file status

Use the **show download phone-image-file status** command to display the status of the download of a phone-image file.

Syntax

show download phone-image-file status

Context

general

User Level

read-only

Example

To display the status of the download of a phone-image file:

```
G450-001(super)# show download phone-image-file status
Module #10
===========
Module           : 10
Source file      : start
Destination file : phone-ImageA
Host             : 135.64.102.64
Running state    : Idle
Failure display  : (null)
Last warning     : No-warning
Bytes Downloaded : 7825
```

Related Commands

copy ftp phone-image, copy ftp phone-script, copy running-config startup-config, copy scp phone-script, copy tftp phone-image, copy tftp phone-script, copy usb announcement-file, erase phone-image, ip tftp-server file-system size, show application-memory, show download phone-script-file status, show upload phone-script-file status, show ip tftp-server files

show download phone-script-file status

Use the **show download phone-script-file status** command to show the status of a download of a phone-script file.

Syntax

show download phone-script-file status

User Level

read-only

Context

general

Example

To show the status of a download of a phone-script file:

If no download has been performed:

```
G450-001# show download phone-script-file status
Module #10
===========
No dest file for download operation - no download operation was done.
```

If a download has been performed:

```
G450-001# show download phone-script-file status
Module #10
===========
Module           : 10
Source file      : /home/p46xx-script
Destination file : phone-ScriptA
Host             : 135.64.103.116
Running state    : Idle
Failure display  : (null)
Last warning     : No-warning
Bytes Downloaded : 27
```

Related Commands

copy announcement-file usb, copy ftp phone-image, copy ftp phone-script, copy running-config startup-config, copy scp phone-script, copy tftp phone-image, copy tftp phone-script, copy usb announcement-file, erase phone-image, ip tftp-server file-system size, show application-memory, show upload phone-script-file status, show ip tftp-server files

show ip tftp-server files

Use the **show ip tftp-server files** command to display the phone image and script files.

Syntax

show ip tftp-server files

User Level

read-write

Example

To display the phone image and script files:

```
G450-001(super)# show ip tftp-server files
File               Bank           Location  Size (bytes)
----------------   ------------   --------  -------------
46xxupgrade.txt    phone-scriptA  Nv-Ram    4096
46xxsettings.txt   phone-scriptB  Nv-Ram    16384
4602dbte1_8.bin    phone-imageA   Ram       1048576
4602dape1_8.bin    phone-imageD   Ram       2097152

Nv-Ram:
Total bytes used:              20480
Total bytes free:              110592
Total bytes capacity (fixed): 131072

Ram:
Total bytes used:                   3166208
Total bytes free:                   2076672
Total bytes capacity (Allocated)    3166208
Total bytes capacity (Configured)   5242880
```

Related Commands

copy ftp phone-image, copy ftp phone-script, copy running-config startup-config, copy scp phone-script, copy tftp phone-image, copy tftp phone-script, erase phone-image, ip tftp-server file-system size, show application-memory, show download phone-script-file status, show upload phone-script-file status

show ip tftp-server statistics

Use the **show ip tftp-server statistics** command to display TFTP server error counters. The error counters count several types of errors in download and upload operations.

Note:

Upload operations by TFTP clients, such as IP phones, are not supported. Therefore, any attempts to upload files to the G450 TFTP server are counted as access violation errors.

Syntax

show ip tftp-server statistics

User Level

read-only

Context

general

Example

To display TFTP server error counters:

```
G450-001(super)# show ip tftp-server statistics

Counter                                        Value
-----------------------------------------     --------
File downloads (OK)                               0
File download Timeouts                            0
Total TFTP server errors                          0
Non defined TFTP errors                           0
File not found errors                             0
Access violation errors                           0
Illegal TFTP operation errors                     0
```

Output fields

Name	Description
File downloads (OK)	The number of successful downloads
File download Timeouts	The number of timeouts that occurred during download operations

1 of 2

Name	Description
Total TFTP server errors	The total number of download/upload errors
Non defined TFTP errors	The number of undefined errors
File not found errors	The number of file not found errors
Access violation errors	The number of access violation errors caused by requesting invalid filenames or file paths, or by attempts to upload files to the TFTP server directory
Illegal TFTP operation errors	The number of illegal TFTP operation errors

2 of 2

Related Commands

copy ftp phone-image, copy ftp phone-script, copy running-config startup-config, copy scp phone-script, copy tftp phone-image, copy tftp phone-script, erase phone-image, ip tftp-server file-system size, show application-memory, show download phone-script-file status, show ip tftp-server files, show upload phone-script-file status

show upload phone-script-file status

Use the **`show upload phone-script-file status`** command to display the upload phone-script file.

Syntax

`show upload phone-script-file status`

User Level

read-only

Context

general

Example

To display the upload phone-script file:

(If no upload has been performed)

```
G450-001# show upload phone-script-file status
Module #10
===========
```

```
No source file for upload operation - no upload operation was done.
============================
```

(If an upload has been performed)

```
G450-001(super)# show upload phone-script-file status
Module #10
===========
Module           : 10
Source file      : phone-ScriptB
Destination file : 444
Host             : 135.64.102.114
Running state    : Idle
Failure display  : (null)
Last warning     : No-warning
```

Related Commands

copy announcement-file usb, copy ftp phone-image, copy ftp phone-script, copy running-config startup-config, copy scp phone-script, copy tftp phone-image, copy tftp phone-script, copy usb announcement-file, erase phone-image, ip tftp-server file-system size, show application-memory, show download phone-script-file status, show ip tftp-server files

IP unnumbered

ip unnumbered

Use the **ip unnumbered** command to specify an interface from which to borrow an IP address. Use the **no** form of the command to delete an unnumbered IP configuration on the interface.

Syntax

[no] ip unnumbered *index interface-type identifier*

Parameters

Parameter	Description	Possible Values	Default Value
index	An arbitrary index for the unnumbered interface configuration	**1-255**	
interface-type	The interface type of the interface from which to borrow an IP address	**FastEthernet** **Serial** **Vlan** **Loopback** **Tunnel** **Dialer**	
identifier	The identifier depends on the interface type: For FastEthernet: **module/port** For Serial: **module/port:channel-group [.sub-interface]** For Vlan: **vlan-id** For loopback: **loopback number** For Tunnel: **tunnel number** For Dialer: **dialer number**	For FastEthernet: **10/2 or 10/4** For Serial: **3/1, 4/1, 8/1** channel-group: E1: **0-30** T1: **0-23** For VLAN: **1-4090** For Loopback: **1-99** For Tunnel: **1-50** For Dialer: **1**	

Context

interface:Serial (DS1 PPP L2-L3, DS1 FR-SUB L2-L3, USP PPP L2-L3), FastEthernet (PPP L2-L3), Tunnel (L2-L3), Dialer (L2-L3)

User Level

read-write

Example

To borrow an IP address from Loopback 1:

```
G450-001(super-if:Dialer 1)# ip unnumbered 1 loopback 1
```

IPHC header compression

clear ip rtp header-compression

Use the **clear ip rtp header-compression** command to clear IP RTP header compression statistics either for all enabled interfaces or for a specific interface. To clear IP RTP compression statistics for all enabled interfaces, do not enter an interface type and number.

Note:

There is no renegotiation of parameters.

Syntax

clear ip rtp header-compression [*interface_type interface_number*]

Parameters

Parameter	Description	Possible Values	Default Value
interface_type	The type of interface		
interface_number	The interface number		

User Level

read-only

Context

general

Example

To clear header compression statistics for all interfaces:

```
G450-001(super)# clear ip rtp header-compression
```

Related Commands

clear ip tcp header-compression, ip rtp compression-connections, ip rtp header-compression, ip rtp max-period, ip rtp max-time, ip rtp non-tcp-mode, ip rtp port-range, ip tcp compression-connections, show ip rtp header-compression, show ip rtp header-compression brief, show ip tcp header-compression

clear ip tcp header-compression

Use the **clear ip tcp header-compression** command to clear TCP compression statistics either for all enabled interfaces or for a specific interface. To clear TCP compression statistics for all enabled interfaces, do not enter an interface type and number.

Note:

There is no renegotiation of parameters.

Syntax

clear ip tcp header-compression [*interface_type interface_number*]

Parameters

Parameter	Description	Possible Values	Default Value
interface_type	The type of interface		
interface_number	The interface number		

User Level

read-only

Context

general

Example

To clear TCP compression statistics for all enabled interfaces:

```
G450-001(super)# clear ip tcp header-compression
```

Related Commands

clear ip rtp header-compression, ip rtp compression-connections, ip rtp header-compression, ip rtp max-period, ip rtp max-time, ip rtp non-tcp-mode, ip rtp port-range, ip tcp compression-connections, ip tcp header-compression, show ip rtp header-compression, show ip rtp header-compression brief, show ip tcp header-compression

ip rtp compression-connections

Use the **ip rtp compression-connections** command to control the number of Real-Time Transport Protocol (RTP) connections supported on the current interface. Use the **no** form of this command to restore the default. This command also sets the number of connections in the non-TCP space, not just RTP.

Note:

This command automatically enables TCP header compression on the current interface.

Syntax

[no] ip rtp compression-connections *number*

Parameters

Parameter	Description	Possible Values	Default Value
number	The total number of connections in the non-TCP space to support on the current interface	**3-1000**	**16**

User Level

read-write

Context

interface:Serial (DS1 PPP L2, DS1 PPP L2-L3, DS1 FR-SUB L2, DS1 FR-SUB L2-L3, USP PPP L2, USP PPP L2-L3), Dialer (L2, L2-L3, L3)

Example

To allow 48 RTP connections on the Serial interface:

```
G450-001(if:Serial 3/1:1.1) ip rtp compression-connections 48
```

Related Commands

clear ip rtp header-compression, clear ip tcp header-compression, ip rtp header-compression, ip rtp max-period, ip rtp max-time, ip rtp non-tcp-mode, ip rtp port-range, ip tcp compression-connections, show ip rtp header-compression, show ip rtp header-compression brief, show ip tcp header-compression

ip rtp header-compression

Use the **ip rtp header-compression** command to enable both RTP and TCP header compression on the current interface. Use the **no** form of this command to disable both RTP and TCP compression on the current interface.

Note:

The **ip rtp header-compression** command always overrides the **ip tcp header-compression** command. Both commands enable TCP header compression, but they differ in the methods employed.

Note:

If TCP compression was enabled on the current interface using the **ip tcp header-compression** command and not the **ip rtp header-compression** command, then **no ip rtp header-compression** does not disable TCP compression on the interface.

Syntax

[no] ip rtp header-compression [iphc-format]

Parameters

Parameter	Description	Possible Values	Default Value
iphc-format	Keyword specifying the header compression format. This command activates IPHC compression whether or not you specify the **iphc-format** parameter. The only exception is the Frame Relay non-IETF interface. For this interface, the **iphc-format** parameter is invalid and the **ip rtp header-compression** command enables compression for RTP headers only, in non-IETF mode.		

Note:

Non-IETF encapsulation is compatible with other vendors.

User Level

read-write

Context

interface:Serial (DS1 PPP L2, DS1 PPP L2-L3, DS1 FR-SUB L2, DS1 FR-SUB L2-L3, USP PPP L2, USP PPP L2-L3), Dialer (L2, L2-L3, L3)

Example

To enable RTP and TCP header compression on a Serial interface:

```
G450-001(config-if:Serial 3/1:1.1) ip rtp header-compression
```

Related Commands

clear ip rtp header-compression, clear ip tcp header-compression, ip rtp compression-connections, ip rtp max-period, ip rtp max-time, ip rtp non-tcp-mode, ip rtp port-range, ip tcp compression-connections, ip tcp header-compression, show ip rtp header-compression, show ip rtp header-compression brief, show ip tcp header-compression

ip rtp max-period

Use the **ip rtp max-period** command to set the maximum number of compressed headers that can be sent between full headers.

Syntax

[no] ip rtp max-period *number*

Parameters

Parameter	Description	Possible Values	Default Value
number	The maximum number of compressed headers that can be sent until a full header is sent	**32-65535**	**256**

User Level

read-write

Context

interface:Serial (DS1 PPP L2, DS1 PPP L2-L3, DS1 FR-SUB L2, DS1 FR-SUB L2-L3, USP PPP L2, USP PPP L2-L3), Dialer (L2, L2-L3, L3)

Example

To allow a maximum of 512 compressed headers to be sent before a full header must be sent:

```
G450-001(config-if:Serial 3/1:1.1)# ip rtp max-period 512
```

Related Commands

clear ip rtp header-compression, clear ip tcp header-compression, ip rtp compression-connections, ip rtp header-compression, ip rtp max-time, ip rtp non-tcp-mode, ip rtp port-range, ip tcp compression-connections, show ip rtp header-compression, show ip rtp header-compression brief, show ip tcp header-compression

ip rtp max-time

Use the **ip rtp max-time** command to set the maximum number of seconds between full headers.

Syntax

[no] ip rtp max-time *number*

Parameters

Parameter	Description	Possible Values	Default Value
number	The maximum number of seconds between full headers	**1-255**	**5**

User Level

read-write

Context

interface:Serial (DS1 PPP L2-, DS1 PPP L2L3, DS1 FR-SUB L2, DS1 FR-SUB L2-L3, USP PPP L2, USP PPP L2-L3), Dialer (L2, L2-L3, L3)

Example

To allow no more than 15 seconds to pass between the sending of full headers:

```
G450-001(if:Serial 3/1:1.1)# ip rtp max-time 15
```

Related Commands

clear ip rtp header-compression, clear ip tcp header-compression, ip rtp compression-connections, ip rtp header-compression, ip rtp max-period, ip rtp non-tcp-mode, ip rtp port-range, ip tcp compression-connections, show ip rtp header-compression, show ip rtp header-compression brief, show ip tcp header-compression

ip rtp non-tcp-mode

Use the **ip rtp non-tcp-mode** command to set the type of IP header compression to perform. When set to **ietf**, the command performs IP header compression according to IPHC RFCs. When set to **non-ietf**, the command performs IP header compression compatible with other vendors, which do not strictly follow the RFCs.

Note:

IETF mode is incompatible with non-IETF mode.The default of the **ip rtp non-tcp-mode** command is **non-ietf**.

Note:

Non-IETF encapsulation is compatible with other vendors.

Syntax

[no] ip rtp non-tcp-mode {ietf | non-ietf}

Parameters

Parameter	Description	Possible Values	Default Value
ietf	Keyword specifying ietf mode		
non-ietf	Keyword specifying non-ietf mode		

User Level

read-write

Context

interface:Serial (DS1 PPP L2, DS1 PPP L2-L3, DS1 FR-SUB L2, DS1 FR-SUB L2-L3, USP PPP L2, USP PPP L2-L3), Dialer (L2, L2-L3, L3)

Example

To set the Serial interface to perform IPHC RFC header compression:

```
G450-001(if:Serial 3/1:1.1)# ip rtp non-tcp-mode ietf
```

Related Commands

clear ip rtp header-compression, clear ip tcp header-compression, ip rtp compression-connections, ip rtp header-compression, ip rtp max-period, ip rtp max-time, ip rtp port-range, ip tcp compression-connections, show ip rtp header-compression, show ip rtp header-compression brief, show ip tcp header-compression

ip rtp port-range

Use the **ip rtp port-range** command to set the range of UDP ports considered as RTP on the current interface. Set the range to be identical to the peer's configuration.

Some vendors use port range 49,152 through 65,535. For interoperability, the same port range should be used.

Syntax

[no] ip rtp port-range *min max*

Parameters

Parameter	Description	Possible Values	Default Value
min	The starting port range to be considered RTP	**1025-65535**	**2048**
max	The ending port range to be considered RTP	**1025-65535**	**65535**

User Level

read-write

Context

interface:Serial (DS1 PPP L2, DS1 PPP L2-L3, DS1 FR-SUB L2, DS1 FR-SUB L2-L3, USP PPP L2, USP PPP L2-L3), Dialer (L2, L2-L3, L3)

Example

To specify that ports in the range 49,152 through 65535 are RTP ports:

```
G450-001(if:Serial 3/1:1.1)# ip rtp port-range 49152 65535
```

Related Commands

clear ip rtp header-compression, clear ip tcp header-compression, ip rtp compression-connections, ip rtp header-compression, ip rtp max-period, ip rtp max-time, ip rtp non-tcp-mode, ip tcp compression-connections, show ip rtp header-compression, show ip rtp header-compression brief, show ip tcp header-compression

ip tcp compression-connections

Use the **ip tcp compression-connections** command to specify the total number of TCP header compression connections supported on the current interface. Use the **no** form of this command to restore the default value of 16 connections.

Syntax

[no] ip tcp compression-connections *number*

Parameters

Parameter	Description	Possible Values	Default Value
number	The number of TCP compression connections	**3-256**	**16**

User Level

read-write

Context

interface:Serial (DS1 PPP L2, DS1 PPP L2-L3, DS1 FR-SUB L2, DS1 FR-SUB L2-L3, USP PPP L2, USP PPP L2-L3), Dialer (L2, L2-L3, L3)

Example

To specify that 20 TCP header compression connections are to be supported in the current interface:

```
G450-001(super-if:Dialer 1)# ip tcp compression-connections 20
```

Related Commands

clear ip rtp header-compression, clear ip tcp header-compression, ip rtp compression-connections, ip rtp header-compression, ip rtp max-period, ip rtp max-time, ip rtp non-tcp-mode, ip rtp port-range, ip tcp header-compression, show ip rtp header-compression, show ip rtp header-compression brief, show ip tcp header-compression

show ip rtp header-compression

Use the **show ip rtp header-compression** command to display the RTP header compression statistics for a specific interface. If no interface is specified, statistics for all interfaces are displayed.

Syntax

show ip rtp header-compression [*interface_name*]

Parameters

Parameter	Description	Possible Values	Default Value
interface_name	The name of the interface		

User Level

read-only

Context

general

Example

To display RTP compression statistics for all interfaces:

```
G450-001(super)# show ip rtp header-compression

IP RTP header compression statistics:
Interface Serial 3/1:1.1:
  Rcvd:    0 Full Headers, 0 Compressed, 0 Errors
  Sent:    9 Full Headers, 394 Compressed,
           8274 Bytes Saved, 14202 Bytes Sent,
           1.58 Efficiency Improvement Factor
  Connect: Active, 100 Rx Slots, 100 Tx Slots,
           Max Time 5, Max Period 256
```

Output fields

Name	Description
Rcvd	Information on received RTP packets, as follows: • Full Headers — the number of RTP packets with full headers received • Compressed — the number of RTP packets with compressed headers received • Errors — the number of packets discarded during de-compression due to errors
Sent	Information on sent RTP packets, as follows: • Full Headers — the number of RTP packets with full headers sent • Compressed — the number of RTP packets with compressed headers sent • Bytes Saved — the total saving in bytes due to compression • Bytes Sent — the total number of bytes sent after compression • Efficiency Improvement Factor — the improvement factor, calculated as *(bytes saved + bytes sent)/ bytes sent* (rounded to two decimal places)
Connect	Connection information, as follows: • Active/Inactive — whether RTP header compression is negotiated and working on this interface • Rx Slots — the number of RTP sessions to decompress • Tx Slots — the number of RTP sessions to compress • Max Time — the maximum number of seconds between two full header packets • Max Period — the maximum number of compressed packets sent between two full header packets

Related Commands

clear ip rtp header-compression, clear ip tcp header-compression, ip rtp compression-connections, ip rtp header-compression, ip rtp max-period, ip rtp max-time, ip rtp non-tcp-mode, ip rtp port-range, ip tcp compression-connections, show ip rtp header-compression brief, show ip tcp header-compression

show ip rtp header-compression brief

Use the **show ip rtp header-compression brief** command to display a subset of header compression statistics in the form of a table.

Syntax

show ip rtp header-compression brief [*interfaceName*]

Parameters

Parameter	Description	Possible Values	Default Value
interfaceName	The name of the interface		

User Level

read-only

Context

general

Example

To display concise RTP header compression statistics for all interfaces:

```
G450-001(super)# show ip rtp header-compression brief

Interface  Active  Slots Max   Max   Packets    Bytes    Improvement
                         Time Period Sent       Saved       Factor
---------  -------- -----  ----  ------  --------- ---------  ---------
Serial 1:0   NO      16    5   256      0         0          1.00
```

Output fields

Name	Description
Interface	The interface on which RTP header compressions is being applied
Active	Indicates whether RTP header compression is negotiated and working on this interface (YES) or not (NO)
Slots	The number of Rx and Tx slots, that is, the total number of RTP header compression connections supported on the current interface

1 of 2

Name	Description
Max Time	The maximum number of seconds between two full header packets
Max Period	The maximum number of compressed packets sent between two full header packets
Packets Sent	The number of compressed packets sent + the number of full headers sent
Bytes Saved	The total saving in bytes due to compression
Improvement Factor	The efficiency of the compression, calculated as *(bytes saved + bytes sent)/ bytes sent* (rounded to two decimal places)

2 of 2

Related Commands

clear ip rtp header-compression, clear ip tcp header-compression, ip rtp compression-connections, ip rtp header-compression, ip rtp max-period, ip rtp max-time, ip rtp non-tcp-mode, ip rtp port-range, ip tcp compression-connections, show ip rtp header-compression, show ip tcp header-compression, show ip tcp header-compression brief

show ip tcp header-compression

Use the **`show ip tcp header-compression`** command to display TCP header compression statistics for a specific interface. If no interface is specified, it shows TCP header compression statistics for all interfaces.

Syntax

`show ip tcp header-compression [`*`interface_name`*`]`

Parameters

Parameter	Description	Possible Values	Default Value
`interface_name`	The name of the interface		

User Level

read-only

Context

general

Example

To display TCP header compression statistics for all interfaces:

```
G450-001(super)# show ip tcp header-compression

IP TCP header compression statistics:
Interface Serial 3/1:1.1:
  Rcvd:    0 Full Headers, 0 Compressed, 0 Errors
  Sent:    85 Full Headers, 34 Compressed,
           1139 Bytes Saved, 4335 Bytes Sent,
           1.26 Efficiency Improvement Factor
  Connect: Active, 3 Rx Slots, 3 Tx Slots
```

Output fields

Name	Description
Rcvd	Information on received TCP packets, as follows: • **Full Headers** — the number of TCP packets with full headers received • **Compressed** — the number of TCP packets with compressed headers received • **Errors** — the number of packets discarded during de-compression due to errors
Sent	Information on sent TCP packets, as follows: • **Full Headers** — the number of TCP packets with full headers sent • **Compressed** — the number of TCP packets with compressed headers sent • **Bytes Saved** — the total saving in bytes due to compression • **Bytes Sent** — the total number of bytes sent after compression • **Efficiency Improvement Factor** — the improvement factor, calculated as *(bytes saved + bytes sent)/ bytes sent* (rounded to two decimal places)
Connect	Connection information, as follows: • **Active/Inactive** — whether TCP header compression is negotiated and working on this interface • **Rx Slots** — the number of TCP sessions to decompress • **Tx Slots** — the number of TCP sessions to compress

Related Commands

clear ip rtp header-compression, clear ip tcp header-compression, ip rtp compression-connections, ip rtp header-compression, ip rtp max-period, ip rtp max-time, ip rtp non-tcp-mode, ip rtp port-range, ip tcp compression-connections, ip tcp header-compression, show ip rtp header-compression, show ip rtp header-compression brief

show ip tcp header-compression brief

Use the **show ip tcp header-compression brief** command to display a subset of TCP header compression statistics for a specific interface. If no interface is specified, it shows TCP header compression statistics for all interfaces.

Syntax

show ip tcp header-compression brief [*interface_name*]

Parameters

Parameter	Description	Possible Values	Default Value
interface_name	The name of the interface		

User Level

read-only

Context

general

Example

To display concise TCP header compression statistics for all interfaces:

```
G450-001(super)# show ip tcp header-compression brief

Interface   Active   Slots  Packets   Bytes     Improvement
                            Sent      Saved       Factor
---------- -------- ------  --------  --------- -----------
Serial 1:0   NO      16      0          0          1.00
```

Output fields

Name	Description
Interface	The interface on which TCP header compressions is being applied
Active	Whether TCP header compression is active and working on this interface
Slots	The number of Rx and Tx slots. That is, the total number of TCP header compression connections supported on this interface.
Packets Sent	The number of compressed packets sent + the number of full headers sent
Bytes Saved	The total saving in bytes due to compression
Improvement Factor	The efficiency of the compression, calculated as *(bytes saved + bytes sent)/ bytes sent* (rounded to two decimal places)

Related Commands

clear ip rtp header-compression, clear ip tcp header-compression, ip rtp compression-connections, ip rtp header-compression, ip rtp max-period, ip rtp max-time, ip rtp non-tcp-mode, ip rtp port-range, ip tcp compression-connections, show ip rtp header-compression, show ip rtp header-compression brief, show ip tcp header-compression

License file of CM

ip license-server

Use the **`ip license-server`** command to enable the media gateway to supply a hardware serial number on behalf of an S8500 local survivable processor (LSP). The serial number is required when an S8500 LSP registers with its primary controller (S8400 or S8500 Server) using the Processor Ethernet interface.

The serial number might also be required if the S8500 is a primary controller, but is using Processor Ethernet exclusively with H.248 media gateways. In this case, the S8500 does not have an IPSI-controlled gateway to use for its hardware license verification.

Note:

There must be at least one H.248 media gateway (G700, G250, G350, G450, or IG550) for each LSP in the main server's network. Only one LSP or primary controller can use the serial number of a media gateway for license verification.

Syntax

ip license-server

User Level

read-only

Context

general

Example

To enable the serial number assignment to an LSP:

```
G450-001(super)# ip license-server
```

Related Commands

show ip icmp

License file of gateway

copy ftp license-file

Use the **copy ftp license-file** command to download a VPN license from an FTP server.

Syntax

copy ftp license-file *filename ip*

Parameters

Parameter	Description	Possible Values	Default Value
filename	The filename of the VPN license, including the full path, on the FTP server		
ip	The IP address of the FTP server		

User Level

admin

Context

general

Example

To download the VPN license g450.lic from the FTP site at IP address 198.87.134.153:

```
G450-001(super)# copy ftp license-file g450.lic 198.87.134.153
```

Related Commands

copy license-file ftp, copy license-file scp, copy license-file tftp, copy scp license-file, copy tftp license-file, show download license-file status, show license status, show upload license-file status

copy license-file ftp

Use the **`copy license-file ftp`** command to copy the license file to a remote server using FTP.

Syntax

`copy license-file ftp` ***`filename ip`***

Parameters

Parameter	Description	Possible Values	Default Value
`filename`	File name with full path	string	
`ip`	IP address of the host	IP address	

User Level

admin

Context

general

Example

To copy the license file `vpn-license` to the host with IP address 192.168.49.10:

```
G450-001(super)# copy license-file ftp vpn-license 192.168.49.10
```

Related Commands

copy ftp license-file, copy license-file scp, copy license-file tftp, copy scp license-file, copy tftp license-file, show download license-file status, show license status, show upload license-file status

copy license-file scp

Use the **copy license-file scp** command to copy the license file to a remote server using SCP.

Syntax

copy license-file scp *filename ip*

Parameters

Parameter	Description	Possible Values	Default Value
filename	File name with full path	string	
ip	IP address of the host	IP address	

User Level

admin

Context

general

Example

To copy the license file `vpn-license` to the host with IP address 192.168.49.10:

```
G450-001(super)# copy license-file scp vpn-license 192.168.49.10
```

Related Commands

copy ftp license-file, copy license-file ftp, copy license-file tftp, copy scp license-file, copy tftp license-file, show download license-file status, show license status, show upload license-file status

copy license-file tftp

Use the **copy license-file tftp** command to copy the license file to a remote server using TFTP.

Syntax

copy license-file tftp *filename ip*

Parameters

Parameter	Description	Possible Values	Default Value
filename	File name with full path	string	
ip	IP address of the host	IP address	

User Level

admin

Context

general

Example

To copy the license file `vpn-license` to the host with IP address 192.168.49.10:

```
G450-001(super)# copy license-file tftp vpn-license 192.168.49.10
```

Related Commands

copy ftp license-file, copy license-file ftp, copy license-file scp, copy scp license-file, copy tftp license-file, show download license-file status, show license status, show upload license-file status

copy license-file usb

Use the **copy license-file usb** command to upload the license file from the gateway to the USB mass storage device.

Syntax

copy license-file usb *source-filename destination-usb-device* [*destination-filename*]

Parameters

Parameter	Description	Possible Values	Default Value
source-filename	The logical name for the source file		
destination usb-device	The destination USB mass storage device	**usb-device0**	
destination-filename	The destination file name and path		

User Level

admin

Context

general

Example

To upload `vpn_license.cfg` from the gateway to usb-device0:

```
G450-001(super)# copy license-file usb vpn_license.cfg usb-device0
```

Related Commands

backup config usb, copy usb announcement-file, erase usb, restore usb, safe-removal usb, show backup status, show restore status, show usb

copy scp license-file

Use the **`copy scp license-file`** command to download a VPN license from an SCP server.

Syntax

`copy scp license-file` ***`filename ip`***

Parameters

Parameter	Description	Possible Values	Default Value
filename	The filename of the VPN license, including the full path, on the SCP server		
ip	The IP address of the SCP server		

User Level

admin

Context

general

Example

To download the VPN license `g450.lic` from the SCP site at IP address 198.87.134.153:

```
G450-001(super)# copy scp license-file g450.lic 198.87.134.153
```

Related Commands

copy ftp license-file, copy license-file ftp, copy license-file scp, copy license-file tftp, copy tftp license-file, show download license-file status, show license status, show upload license-file status

copy tftp license-file

Use the **`copy tftp license-file`** command to download a VPN license from a TFTP server.

Syntax

`copy tftp license-file` ***`filename ip`***

Parameters

Parameter	Description	Possible Values	Default Value
filename	The filename of the VPN license, including the full path, on the TFTP server		
ip	The IP address of the TFTP server		

User Level

admin

Context

general

Example

To download the VPN license `g450.lic` from the TFTP site at IP address 198.87.134.153:

```
G450-001(super)# copy tftp license-file g450.lic 198.87.134.153
```

Related Commands

copy ftp license-file, copy license-file ftp, copy license-file scp, copy license-file tftp, copy scp license-file, show download license-file status, show license status, show upload license-file status

copy usb license-file

se the **`copy usb license-file`** command to download a VPN license file from the external USB mass storage device to the gateway.

Syntax

copy usb license-file ***source-usb-device source-filename***

Parameters

Parameter	Description	Possible Values	Default Value
source usb-device	The source USB mass storage device	**usb-device0**	
source-filename	The full name and path of the file to be downloaded		

User Level

Admin

Context

general

Example

To download `vpn_license.cfg` from usb-device0 to the gateway:

```
G450-001(super)# copy usb license-file usb-device0 \temp\vpn_license.cfg
```

Related Commands

backup config usb, copy announcement-file usb, erase usb, restore usb, safe-removal usb, show backup status, show restore status, show usb

show download license-file status

Use the **`show download license-file status`** command to display the status of the download process of the VPN license to the device.

Syntax

```
show download license-file status
```

User Level

read-only

Context

general

Example

To display the status of the download process of the VPN license to the device:

```
G450-001(super)# show download license-file status
Module #10
===========
Module           : 10
Source file      : /home/llevinsk/EI2/03IS70594996.xml
Destination file : license-file
Host             : 135.64.103.112
Running state    : Idle
Failure display  : (null)
Last warning     : (null)
Bytes Downloaded : 0
```

Related Commands

copy ftp license-file, copy license-file ftp, copy license-file scp, copy license-file tftp, copy scp license-file, copy tftp license-file, show license status, show upload license-file status

show license status

Use the **show license status** command to display the status of the VPN license.

Syntax

show license status

User Level

read-only

Context

general

Example

To display the status of the VPN license:

```
G450-001(super)# show license status
```

License was installed.

Related Commands

copy ftp license-file, copy license-file ftp, copy license-file scp, copy license-file tftp, copy scp license-file, copy tftp license-file, show download license-file status, show upload license-file status

show upload license-file status

Use the **show upload license-file status** command to view the status of the upload operation of a license file.

Syntax

show upload license-file status

User Level

read-only

Context

general

Example

To view the status of the upload operation of a license file:

- In the following example, an upload command has been issued and the upload succeeds:

```
G450-001(super)# Show upload license-file status
Module #10
===========
Module           : 10
Source file      : license file
Destination file : 444
Host             : 135.64.102.114
Running state    : Idle
Failure display  : (null)
Last warning     : No-warning
```

- In the following example, an upload command has been issued, but the upload fails:

```
G450-001(super)# Show upload license-file status
Module #10
===========
Module           : 10
Source file      : license file.
Destination file : d:\zion\run.cfg
Host             : 135.64.102.39
Running state    : Idle
Failure display  : SCP - Permission denied
Last warning     : No-warning
```

- In this example, no upload command has been issued:

```
G450-001(super)# show upload license-file status
Module #10
===========
No source file for upload operation - no upload operation was done.
```

Related Commands

copy ftp license-file, copy license-file ftp, copy license-file scp, copy license-file tftp, copy scp license-file, copy tftp license-file, show download license-file status, show license status, show upload license-file status

Link status

show isdn bri link

Use the **show isdn bri link** command to view the status of all BRI links on a media module.

Syntax

show isdn bri link *mmID*

Parameters

Parameter	Description	Possible Values	Default Value
mmID	The Media Module ID		

User Level

read-only

Context

general

Example

To display the status of all BRI links on media module 1:

```
G450-001(super)# show isdn bri link 1

LOCATION  TYPE    LINK ID    DLCI       SIDE  STATE
--------- ------- ---------- ---------- ----- ------------
v1        NO LINK N/A        N/A        N/A   N/A
```

Related Commands

show isdn link summary, show isdn pri link

---

show isdn link summary

Use the **show isdn link summary** command to view a summary of all ISDN links.

Syntax

show isdn link summary

User Level

read-only

Context

general

Example

To display information about all ISDN links:

```
G450-001(super)# show isdn link summary

LOCATION      TYPE         NO. OF LINKS UP
---------     --------     ---------------
MG            NO LINK      N/A
```

Related Commands

show isdn bri link, show isdn pri link

show isdn pri link

Use the **show isdn pri link** command to view the status of all PRI links on a media module.

Syntax

show isdn pri link *mmID*

Parameters

Parameter	Description	Possible Values	Default Value
mmID	The Media Module ID		

User Level

read-only

Context

general

Example

To display PRI link information for media module 1:

```
G450-001(super)# show isdn pri link 1

LOCATION  TYPE    LINK ID    DLCI       SIDE  STATE
--------- ------- ---------- ---------- ----- ------------
v1        NO LINK N/A        N/A        N/A   N/A
```

Related Commands

show isdn bri link, show isdn link summary

LLDP

set lldp re-init-delay

Use the **`lldp re-init-delay`** command to set the delay from when a port is set to LLDP disable until re-initialization is attempted.

Syntax

`set lldp re-init-delay` ***`value`***

Parameters

Parameter	Description	Possible Values	Default Value
`value`	The delay in seconds from when a port is set to LLDP disable until re-initialization will be attempted	**1-10**	**2**

User Level

read-write

Context

general

Example

To set the re-initialization delay to 5 seconds:

```
G450-001(super)# set lldp re-init-delay 5
```

Related Commands

set lldp system-control, set lldp tx-delay, set lldp tx-hold-multiplier, set lldp tx-interval, set port lldp, set port lldp tlv, show lldp, show lldp config, show port lldp config, show port lldp vlan-name config

set lldp system-control

Use the **set lldp system-control** command to enable or disable the LLDP application globally (per device or stack).

Syntax

set lldp system-control {enable | disable}

Parameters

Parameter	Description	Possible Values	Default Value
enable	Keyword specifying to enable the LLDP application		
disable	Keyword specifying to disable the LLDP application		

User Level

read-write

Context

general

Example

To enable the LLDP application globally:

```
G450-001(super)# set lldp system-control enable
```

Related Commands

set lldp re-init-delay, set lldp tx-delay, set lldp tx-hold-multiplier, set lldp tx-interval, set port lldp, set port lldp tlv, show lldp, show lldp config, show port lldp config, show port lldp vlan-name config

set lldp tx-delay

Use the **set lldp tx-delay** command to set the minimal delay in seconds between successive LLDP frame transmissions, on each port.

The tx delay should be in the range 1 <= TxDelay <= (0.25 * TxInterval)

This transmission rate limiting applies only to situations caused by asynchronous transmission or shutdown when the LLDP application is stopped on a port or system in an Avaya device.

Syntax

`set lldp tx-delay` *`value`*

Parameters

Parameter	Description	Possible Values	Default Value
`value`	Minimum delay in seconds between successive LLDP frame transmissions	**1-8,192**	**30**

User Level

read-write

Context

general

Example

To set the TxDelay to 5 seconds:

```
G450-001(super)# set lldp tx-delay 5
```

Related Commands

set lldp re-init-delay, set lldp system-control, set lldp tx-hold-multiplier, set lldp tx-interval, set port lldp, set port lldp tlv, show lldp, show lldp config, show port lldp config, show port lldp vlan-name config

set lldp tx-hold-multiplier

Use the **`set lldp tx-hold-multiplier`** command to set the multiplier on the interval that determines the actual TTL value sent in an LLDP frame. The time-to-live value transmitted in TTL TLV by the device is expressed by the following formula:

TTL = min(65535, TxInterval * TxHoldMultiplier)

Syntax:

`set lldp tx-hold-multiplier` *`number`*

Parameters

Parameter	Description	Possible Values	Default Value
number	The multiplier	**2-10**	**30**

User Level

read-write

Context

general

Example

To set the TxHoldMultiplier to 4:

```
G450-001(super)# set lldp tx-hold-multiplier 4
```

Related Commands

set lldp re-init-delay, set lldp system-control, set lldp tx-delay, set lldp tx-interval, set port lldp, set port lldp tlv, show lldp, show lldp config, show port lldp config, show port lldp vlan-name config

set lldp tx-interval

Use the **`set lldp tx-interval`** command to configure the interval at which the device transmits LLDP frames.

Syntax

`set lldp tx-interval` ***`seconds`***

Parameters

Parameter	Description	Possible Values	Default Value
seconds	The interval at which the device transmits LLDP frames in seconds	**5-32768**	**30**

User Level

read-write

Context

general

Example

To configure the interval at which the device transmits LLDP frames to 5000 seconds:

```
G450-001(super)# set lldp tx-interval 5000
```

Related Commands

set lldp re-init-delay, set lldp system-control, set lldp tx-delay, set lldp tx-hold-multiplier, set port lldp, set port lldp tlv, show lldp, show lldp config, show port lldp config, show port lldp vlan-name config

set port lldp

Use the **set port lldp** command to change the administrative lldp port status.

Syntax:

set port lldp ***module/port*** **disable|rx-only|tx-only|rx-and-tx**

Parameters

Parameter	Description	Possible Values	Default Value
module	Number of module	**1-10**	
port	Number of port(s)		
disable	Keyword specifying that the LLDP agent will not transmit nor receive LLDP frames on this port		
tx-only	Keyword specifying that the LLDP agent will transmit LLDP frames on this port but it will not store any information about the remote systems connected		
rx-only	Keyword specifying that the LLDP agent will receive, but it will not transmit, LLDP frames on this port		
rx-and-tx	Keyword specifying that the LLDP agent will transmit and receive LLDP frames on this port (default)		

User Level

read-write

Context

general

Example

To set the LLDP status of port 10/3 to transmit and receive LLDP frames:

```
G450-001(super)# set port lldp 10/3 rx-and-tx
```

Related Commands

set lldp re-init-delay, set lldp system-control, set lldp tx-delay, set lldp tx-hold-multiplier, set lldp tx-interval, set port lldp tlv, show lldp, show lldp config, show port lldp config, show port lldp vlan-name config

set port lldp tlv

Use the **set port lldp tlv** command to enable or disable the transmission of the optional TLVs on a per port basis.

The optional TLVs are:

- Port description
- System name
- System description
- System capabilities
- Management address
- Port-vlan-id
- Vlan-name

Syntax:

set port lldp tlv ***module/port*** { **enable** | **disable** } { ***tlv-name*** | **vlan-name** ***vlan-id*** }

Parameters

Parameter	Description	Possible Values	Default Value
module	Number of module	**1-10**	
port	Number of port(s)		

Parameter	Description	Possible Values	Default Value
enable	Keyword specifying to enable transmission of TLV parameter		
disable	Keyword specifying to disable transmission of TLV parameter		
tlv_name	Name of the optional TLV: **port-description** — 802 LAN station's port description **system-name** — an alphanumeric string that indicates the system's administratively assigned name **system-description** — an alphanumeric string that is the textual description of the system **system-capabilities** — identifies the primary function(s) of the system and whether or not these primary functions are enabled **management-address** — identifies an address associated with the local LLDP agent that may be used to reach higher layer management entities **port-vlan-id** — LAN port VLAN (PVID) that will be associated with untagged or priority tagged frames it receives **all** — send all optional TLVs for each port	**port-description** **system-name** **system-description** **system-capabilities** **management-address** **port-vlan-id** **all**	
vlan-id	VLAN number. VLAN identifier of statically bound VLANs on the port. The vlan-id must exist and be bound to that port.	**1-4090**	

Tip:

Executing this command applies only one TLV at a time. To affect all optional TLVs, you should execute the command for different tlv_names, or once with tlv_name=*all*. When using the *"all"* option, the VLAN-Name TLVs are sent indicating all VLANs bound to each port.

User Level

read-write

Context

general

Examples

To enable the transmission of optional TLV management-address for port 10/3:

```
G450-001(super)# set port lldp tlv 10/3 enable management-address
G450-001(super)# set port lldp tlv 10/3 enable vlan-name 2
```

Related Commands

set lldp re-init-delay, set lldp system-control, set lldp tx-delay, set lldp tx-hold-multiplier, set lldp tx-interval, set port lldp, show lldp, show lldp config, show port lldp config, show port lldp vlan-name config

show lldp

Use the **show lldp** command to display the LLDP information received on each port.

Syntax:

show lldp [*module/port*]

Parameters

Parameter	Description	Possible Values	Default Value
module	Number of module	**1-10**	
port	Number of port(s)		

User Level

read-only

Context

general

Example:

To display the LLDP information received on each port:

```
G450-001(super)# show lldp

Gathering and displaying the information might take a while.

Port number 6/1
-------------------
Remote index = 2
Chassis ID: subtype=4 value 00040d29c576
Port ID: subtype=7 value 048313233343536
Port description: Avaya Inc., G450 Media Gateway, 10/100BaseTx-Pwr
System name = System number 1
System description = Avaya Inc., G450 Converged Media Gateway, SW Version
23.8.51


SysCaps :other repeater bridge accessPoint router phone DOCSIS stationOnly
-------  ----- -------- ------ ----------- ------ ----- ------ ---------
Supported:                          +         +
Enabled :                           +         +

Management address: subtype = 1 (ip) value 135.64.103.155
                    subtype = 6 (mac)  value 23a54237bce8

PVID: 50
Static VLANs: 1 name V1
              3 name voice-vlan
              5 name data-e44

Port number 6/2
-------------------
...
```

Output fields

Name	Description
Port number	The port receiving the information about the remote LLDP agent
Remote index	The index assigned to the remote LLDP agent seen on the port. **Note:** All TLVs mentioned below refer to that remote LLDP agent.
Chassis ID	The value of Chassis ID TLV received on the port
Port ID	The value of Port ID TLV received on the port
Port description	The value of Port Description TLV received on the port

1 of 2

Name	Description
System name	The value of System Name TLV received on the port
System description	The value of System Description TLV received on the port
SysCaps	Displays which capabilities the remote LLDP agent supports, and which are enabled. This information is based on the values in the System Capabilities TLV received on the port.
Management Address	The Management Address of the remote agent connected to that port, according to the Management Address TLV received on the port
PVID	The PVID value of the remote agent connected to that port, according to the Port-VLAN-ID TLV received on that port
Static VLANs	A list of VLANs that the remote LLDP agent advertises as VLANs that are statically bound to its port. This information is based on the values in the VLAN Name TLV received on that port.
	2 of 2

Related Commands

`set lldp re-init-delay`, `set lldp system-control`, `set lldp tx-delay`, `set lldp tx-hold-multiplier`, `set lldp tx-interval`, `set port lldp`, `set port lldp tlv`, `show lldp config`, `show port lldp config`, `show port lldp vlan-name config`

show lldp config

Use the **`show lldp config`** command to display the global LLDP configuration.

Syntax

`show lldp config`

User Level

read-only

Context

general

Example

To display the global LLDP configuration:

```
G450-001(super)# show lldp config

Lldp Configuration
------------------
Application status: enable
Tx interval: 30 seconds
Tx hold multiplier: 4
Tx delay: 2 seconds
Reinit delay: 2 seconds
```

Output fields

Name	Description
Application status	Whether the LLDP application is enabled or disabled
Tx interval	The interval at which the device transmits LLDP frames
Tx hold multiplier	The value of the multiplier on the TxInterval that determines the actual TTL value sent in an LLDP frame
Tx delay	The minimum delay between successive LLDP frame transmissions
Reinit delay	The delay in seconds from when a port is set to LLDP "disable", until re-initialization is attempted

Related Commands

set lldp re-init-delay, set lldp system-control, set lldp tx-delay, set lldp tx-hold-multiplier, set lldp tx-interval, set port lldp, set port lldp tlv, show lldp, show port lldp config, show port lldp vlan-name config

show port lldp config

Use the **`show port lldp config`** command to display port-level LLDP configuration.

Syntax:

`show port lldp config [`*`module/port`*`]`

Parameters

Parameter	Description	Possible Values	Default Value
module	Number of module	**1-10**	
port	Number of port(s)		

User Level

read-only

Context

general

Example

To display port-level LLDP configuration:

```
G450-001(super)# show port lldp config

Port    Port      Port         System   System       System     Management
Number  Status    Description  Name     Description  Capability Address     PVID
------  --------  -----------  -------  -----------  ---------- ----------- ------
 10/3   txAndRx   disable      disable   disable      disable    disable     disable
 10/6   txAndRx   disable      disable   disable      disable    disable     disable
```

Output fields

Field	Description
Port Number	The ports on which LLDP is configured
Port Status	The LLDP status of the port. Possible values: • **disable** – The LLDP agent neither transmits nor receives LLDP frames on this port • **tx-only** – The LLDP agent transmits LLDP frames on this port but does not store any information about the remote systems connected • **rx-only** – The LLDP agent receives, but does not transmit, LLDP frames on this port • **rx-and-tx** – The LLDP agent both transmits and receives LLDP frames on this port (default)
Port Description	Whether the Port Description TLV is transmitted (enable) or not transmitted (disable) from the port

1 of 2

Field	Description
System Name	Whether the System Name TLV is transmitted (enable) or not transmitted (disable) from the port
System Description	Whether the System Description TLV is transmitted (enable) or not transmitted (disable) from the port
System Capability	Whether the System Capability TLV is transmitted (enable) or not transmitted (disable) from the port
Management Address	Whether the Management Address TLV is transmitted (enable) or not transmitted (disable) from the port
PVID	Whether the Port-VLAN-ID (PVID) TLV is transmitted (enable) or not transmitted (disable) from the port
	2 of 2

Related Commands

set lldp re-init-delay, set lldp system-control, set lldp tx-delay, set lldp tx-hold-multiplier, set lldp tx-interval, set port lldp, set port lldp tlv, show lldp, show lldp config, show port lldp vlan-name config

show port lldp vlan-name config

Use the **`show port lldp vlan-name config`** command to show the VLANs that are being transmitted on a specific port.

Syntax:

`show port lldp vlan-name config [`*`module/port`*`]`

Parameters

Parameter	Description	Possible Values	Default Value
`module`	Number of module	**1-10**	
`port`	Number of port(s)		

User Level

read-only

Context

general

Example

To show the VLANs that are being transmitted per port:

```
G450-001(super)# show port lldp vlan-name config
Port  Transmitted VLAN-IDs
----  --------------------
10/3  1, 3 , 50 ,300
10/4  3, 50
…
```

Output fields

Name	Description
Port	Module and port numbers
Transmitted VLAN-IDs	Which statically bound VLANs the port will transmit in the VLAN Name TLV

Related Commands

set lldp re-init-delay, set lldp system-control, set lldp tx-delay, set lldp tx-hold-multiplier, set lldp tx-interval, set port lldp, set port lldp tlv, show lldp, show lldp config, show port lldp config

Logging

clear logging file

Use the **`clear logging file`** command to delete the message log file being stored in non-volatile memory (NVRAM), including the history log, and open a new, empty log file.

Syntax

`clear logging file`

User Level

read-write

Context

general

Example

To delete the message log:

```
G450-001(super)# clear logging file
```

Related Commands

clear logging server, set logging file, set logging server, set logging server access-level, set logging server condition, set logging server enable | disable, set logging server facility, set logging session, show logging file content, show logging server condition, show logging session condition

clear logging server

Use the **clear logging server** command to delete the specified Syslog message server from the Syslog server table.

Syntax

clear logging server {***ip_address*** | ***hostname***}

Parameters

Parameter	Description	Possible Values	Default Value
ip_address	The IP address of the Syslog server		
hostname	The name of the Syslog server host		

User Level

read-write

Context

general

Example:

To delete the Syslog message server with IP address 176.15.4.25:

```
G450-001(super)# clear logging server 176.15.4.25
```

Related Commands

clear logging file, set logging file, set logging server, set logging server access-level, set logging server condition, set logging server enable | disable, set logging server facility, set logging session, show logging file content, show logging server condition, show logging session condition

set logging file

Use the **set logging file** command to manage the logging of system messages to non-volatile memory (NVRAM).

Syntax

set logging file {enable|disable}

set logging file condition {all|*MsgFacility*} {none|*severity*}

Parameters

Parameter	Description	Possible Values	Default Value
enable	Keyword specifying to enable logging to the file sink		
disable	Keyword specifying to disable logging to the file sink		
condition	Keyword specifying to define a filter rule for logging		
all	Keyword specifying to apply the filter condition to all MsgFacilities		

Parameter	Description	Possible Values	Default Value
MsgFacility	Apply the filter condition to a specific MsgFacility	**arp, boot, cdr, cli, cna-tp, config, console, dhcp-relay, dhcpc, dhcps, dialer, dnsc, fan, filesys, ids, iphc, ipsec, isakmp, ospf, policy, ppp, pppoe, proxy-arp, qos, router, rtp-stat, saa, security, snmp, stp, supply, switchfabric, system, tftp, threshold, tracker, usb, usb-modem, vj-comp, vlan, voice, wan**	
none	Keyword specifying not to log messages to the file sink		
severity	Severity level is equal to or more severe than the specified level. 0 is the highest severity and 7 the lowest severity.	Use the text value or its numeric equivalent: **emergency (0)** **alert (1)** **critical (2)** **error (3)** **warning (4)** **notification (5)** **informational (6)** **debugging (7)**	

User Level

read-write

Context

general

Example

To filter VLAN messages sending only those having a severity of critical or greater:

```
G450-001(super)# set logging file condition vlan critical
```

Related Commands

clear logging file, clear logging server, set logging server, set logging server access-level, set logging server condition, set logging server enable | disable, set logging server facility, set logging session, show logging file content, show logging server condition, show logging session condition

set logging server

Use the **set logging server** command to define a new Syslog output server for remote logging of system messages. A maximum of three Syslog servers can be configured. A new Syslog server is created in disabled mode.

Syntax

set logging server *ip_address*

Parameters

Parameter	Description	Possible Values	Default Value
ip_address	The IP address of the Syslog server		

User Level

read-write

Context

general

Example

To define a Syslog server at IP address 147.2.3.66:

```
G450-001(super)# set logging server 147.2.3.66
```

Related Commands

clear logging file, clear logging server, set logging file, set logging server access-level, set logging server condition, set logging server enable | disable, set logging server facility, set logging session, show logging file content, show logging server condition, show logging session condition

set logging server access-level

Use the **set logging server access-level** command to define the access level associated with a Syslog server sink. You cannot specify an admission level higher than the assigned level.

Syntax

set logging server access-level ***admission_level*** {***ip_address*** | ***hostname***}

Parameters

Parameter	Description	Possible Values	Default Value
admission_ level		**read-only**, **read-write**, **admin**	
ip_address	The IP address of the Syslog server		
hostname	The name of the Syslog server host		

User Level

read-write

Context

general

Example

To specify a read-write access level for the Syslog server at IP address 172.5.16.33:

```
G450-001(super)# set logging server access-level read-write 172.5.16.33
```

Related Commands

clear logging file, clear logging server, set logging file, set logging server, set logging server condition, set logging server enable | disable, set logging server facility, set logging session, show logging file content, show logging server condition, show logging session condition

set logging server condition

Use the **set logging server condition** command to specify a filter for messages sent to the specified Syslog server. Messages can be filtered by source system, severity, or both.

Syntax

set logging server condition {**all** | ***Msgfacility***} {**none** | ***severity***} ***ip_address***

Parameters

Parameter	Description	Possible Values	Default Value
all	Keyword specifying to apply this filter to all message facility systems		
MsgFacility	Apply this filter to messages produced by a specific system	**arp, boot, cdr, cli, cna-tp, config, console, dhcp-relay, dhcpc, dhcps, dialer, dnsc, fan, filesys, ids, iphc, ipsec, isakmp, ospf, policy, ppp, pppoe, proxy-arp, qos, router, rtp-stat, saa, security, snmp, stp, supply, switchfabric, system, tftp, threshold, tracker, usb, usb-modem, vj-comp, vlan, voice, wan**	
none	Keyword specifying not to log any messages		
severity	Only log messages whose severity level is equal to or more severe than the specified level. 0 is the highest severity and 7 the lowest severity.	Use the text value or its numeric equivalent: **emergency (0)**, **alert (1)**, **critical (2)**, **error (3)**, **warning (4)**, **notification (5)**, **informational (6)**, **debugging (7)**	
ip_address	The IP address of the Syslog server		

User Level

read-write

Context

general

Example

To filter fan messages for the Syslog server at IP address 168.23.1.15, so that only fan messages of warning-level severity or greater are sent:

```
G450-001(super)# set logging server condition fan warning 168.23.1.15
```

Related Commands

clear logging file, clear logging server, set logging file, set logging server, set logging server access-level, set logging server enable | disable, set logging server facility, set logging session, show logging file content, show logging server condition, show logging session condition

set logging server enable | disable

Use the **set logging server enable** or **set logging server disable** command to enable or disable a specific Syslog server.

Syntax

set logging server {enable | disable} ***ip_address***

Parameters

Parameter	Description	Possible Values	Default Value
enable	Keyword specifying to enable logging for the Syslog server		
disable	Keyword specifying to disable logging for the Syslog server		
ip_address	The IP address of the Syslog server		

User Level

read-write

Context

general

Example

To enable logging for the Syslog server at IP address 168.12.1.13:

```
G450-001(super)# set logging server enable 168.12.1.13
```

Related Commands

clear logging file, clear logging server, set logging file, set logging server, set logging server access-level, set logging server condition, set logging server facility, set logging session, show logging file content, show logging server condition, show logging session condition

set logging server facility

Use the **set logging server facility** command to define an output facility for the specified Syslog server.

Syntax

set logging server facility *facility ip_address*

Parameters

Parameter	Description	Possible Values	Default Value
facility	The facility used in Syslog reports	**auth** (Authorization), **daemon** (Background System Process), **clkd** (Clock Daemon), **clkd2** (Clock Daemon), **mail** (Electronic Mail), **local0** — **local7** (For Local Use) **ftpd** (FTP Daemon), **kern** (Kernel), **alert** (Log Alert), **audi** (Log Audit), **ntp** (NTP Subsystem), **lpr** (Printing), **sec** (Security), **syslog** (System Logging), **uucp** (Unix-to-Unix Copy Program), **news** (Usenet news), **user** (User Process)	
ip_address	The IP address of the Syslog server		

User Level

read-write

Context

general

Example

To specify that messages for the Syslog server at IP address 168.12.1.15 be sent to the mail output facility:

```
G450-001(super)# set logging server facility mail 168.12.1.15
```

Related Commands

clear logging file, clear logging server, set logging file, set logging server, set logging server access-level, set logging server condition, set logging server enable | disable, set logging session, show logging file content, show logging server condition, show logging session condition

set logging session

Use the **set logging session** command to manage message logging for the current console session.

Syntax

set logging session {**enable** | **disable** | **condition** {**all** | ***MsgFacility***} {**none** | ***severity***}}

Parameters

Parameter	Description	Possible Values	Default Value
enable	Keyword specifying to enable logging to the console session		
disable	Keyword specifying to disable logging to the console session		
condition	Keyword specifying to define a filter rule for logging		

Parameter	Description	Possible Values	Default Value
all	Keyword specifying to apply the filter condition to all MsgFacilities		
MsgFacility	Apply the filter condition to a specific MsgFacility	**arp, boot, cdr, cli, cna-tp, config, console, dhcp-relay, dhcpc, dhcps, dialer, dnsc, fan, filesys, ids, iphc, ipsec, isakmp, ospf, policy, ppp, pppoe, proxy-arp, qos, router, rtp-stat, saa, security, snmp, stp, supply, switchfabric, system, tftp, threshold, tracker, usb, usb-modem, vj-comp, vlan, voice, wan**	
none	Keyword specifying not to log messages to the console session		
severity	Only log messages whose severity level is equal to or more severe than the specified level. 0 is the highest severity and 7 the lowest severity.	Use the text value or its numeric equivalent: **emergency (0), alert (1), critical (2), error (3), warning (4), notification (5), informational (6), debugging (7)**	**6**

User Level

read-write

Context

general

Example

To filter config messages for the session, sending only those config messages of alert severity or greater:

```
G450-001(super)# set logging session condition config alert
```

Related Commands

clear logging file, clear logging server, set logging file, set logging server, set logging server access-level, set logging server condition, set logging server enable | disable, set logging server facility, show logging file content, show logging server condition, show logging session condition

show dev log file

Use the **show dev log file** command to display the encrypted device's log file.

Syntax

show dev log file

User Level

read-write

Context

general

show logging file condition

Use the **show logging file condition** command to display all conditions that have been defined for the file output sink.

Syntax

show logging file condition

User Level

read-only

Context

general

Example

To show information about conditions that are defined for the file output:

```
G450-001(super)# show logging file condition
*****************************************************
*** Message logging configuration of FILE     sink ***
Sink Is Enabled
```

```
Sink default severity: Informational
Application          ! Severity Override
-----------------------------------------
FAN                  ! Error
VLAN                 ! Critical
```

Related Commands

copy ftp startup-config, copy running-config ftp, copy running-config scp, copy running-config startup-config, copy running-config tftp, copy startup-config ftp, copy startup-config scp, copy startup-config tftp, copy tftp startup-config, erase startup-config, nvram initialize, show copy status, show download status, show erase status, show running-config, show startup-config

show logging file content

Use the **show logging file content** command to output the messages in the log file to the CLI console. The output is arranged with the most recent event first. The content of the file is output according to the current filter settings and user access. If no parameters are specified, information for all message facilities and severities is displayed.

Syntax

show logging file content [*severity*] [all|*Msgfacility*] [*number*]

Parameters

Parameter	Description	Possible Values	Default Value
severity	Minimal severity of messages to be displayed		
all	Keyword specifying to display messages from all facilities		
Msgfacility	Display messages from this facility only		
number	Maximum number of messages to display		

User Level

read-only

Context

general

Example

To display contents of the message file for all message facilities and severities:

```
G450-001(super)# show logging file content

CLI-Notification: root: exit
CLI-Notification: root: exit
CLI-Notification: root:      ip
SECURITY-Warning: Unauthorized Access from IP address = 0.0.0.0, User = super,
Protocol = 23
CLI-Notification: root: exit
```

Related Commands

clear logging file, clear logging server, set logging file, set logging server, set logging server access-level, set logging server condition, set logging server enable | disable, set logging server facility, set logging session, show logging server condition, show logging session condition

show logging server condition

Use the **show logging server condition** command to display the filter conditions that have been defined for the Syslog output sink. If an IP address or hostname is not specified, the configuration of all of the Syslog servers is displayed.

Syntax

show logging server condition [***ip_address*** | ***hostname***]

Parameters

Parameter	Description	Possible Values	Default Value
ip_address	The IP address of the Syslog server		
hostname	The name of the Syslog server host		

User Level

read-only

Context

general

Example

To display filter conditions defined for the Syslog server at IP address 172.16.1.139:

```
G450-001(super)# show logging server condition 172.16.1.139

Logging: enabled
Logging severity: warning
Facility            Severity Override
-------------       ----------------------
System              Critical
Syslog server 222.222.222.222
Logging: enabled
Logging severity: Debug
Facility            Severity Override
-------------       ----------------------
Kernel              Critical
```

Related Commands

clear logging file, clear logging server, set logging file, set logging server, set logging server access-level, set logging server condition, set logging server enable | disable, set logging server facility, set logging session, show logging file content, show logging session condition

show logging session condition

Use the **show logging session condition** command to display the filter conditions defined for message logging to the current console session.

Syntax

show logging session condition

User Level

read-only

Context

general

Example

To display filter conditions defined for console messaging:

```
G450-001(super)# show logging session condition

Logging console: enabled
Logging session severity: warning
Facility            Severity Override
-------------       ----------------------
System              Critical
```

Related Commands

clear logging file, clear logging server, set logging file, set logging server, set logging server access-level, set logging server condition, set logging server enable | disable, set logging server facility, set logging session, show logging file content, show logging server condition

Master key configuration

key config-key password-encryption

Use the **key config-key password-encryption** command to change the default Master Key of the gateway, used to encrypt gateway secrets in the gateway configuration file.

Note:

For security reasons, it is recommended to define a new Master Key upon gateway installation. Otherwise, the default Master Key, common to all gateways, is used to encrypt gateway secrets.

Note:

Record the phrase you entered in the **key config-key password-encryption** command and keep it in a safe place. If you wish to copy one gateway's configuration file to another gateway, you must first configure in the other gateway an identical Master Key (by using the same phrase), otherwise the copy operation will fail.

Note:

When you define a Master Key, you are prompted to save it by copying the running configuration to the start-up configuration using the copy running-config startup-config command. The Master Key will now be in effect.

Note:

The nvram initialize command deletes the user-defined Master Key, and returns it to its default value.

Syntax

key config-key password-encryption *master-key-passphrase*

Parameters

Parameter	Description	Possible Values	Default Value
master-key-phrase	The phrase used to generate the gateway's Master Key, used for encrypting gateway secrets	A string of 13-64 printable ASCII characters	

User Level

admin

Context

general

Example

To change the default Master Key of the gateway to o;3qfhSE&Ydf1\:

```
G450(super)# key config-key password-encryption o;3qfhSE&Ydfl\
```

Related Commands

copy running-config startup-config

MGC (Media Gateway Controller) configuration

clear mgc list

Use the **clear mgc list** command to remove entries from the Media Gateway Controller list. Multiple entries can be removed together, by specifying a list of IP addresses separated by commas. If no arguments are provided, all entries are removed.

Syntax

clear mgc list [*ipaddress1*,…]

Parameters

Parameter	Description	Possible Values	Default Value
ipaddress1	The IP address of a call controller		

User Level

read-only

Context

general

Example

To remove two media gateway controllers from the list, with IP addresses of 132.236.73.2 and 177.13.2.45:

```
G450-001(super)# clear mgc list 132.236.73.2, 177.13.2.45
```

Related Commands

session, set icc-monitoring, set mediaserver, set mgc list, set reset-times, show icc-monitoring, show mediaserver, show mgc, show mgc list

session

Use the **session** command to provide the means to establish a session with the active Media Gateway Controller, SAT, or the device.

This is an alias to Telnet. The **mgc** option Telnets to the active Media Gateway Controller.

Note:

For **session mgc sat**, and **session icc sat** to access the server SAT terminal, the SAT port must be configured to 5023 on the server. For **session mgc** and **session icc**, the server should allow access to the Telnet port (23).

Syntax

session {{mgc [sat]} | icc [sat]}

Parameters

Parameter	Description	Possible Values	Default Value
mgc	Keyword for accessing the LINUX shell login		
icc	Keyword for accessing the S8300		
sat	Keyword for accessing the SAT login		

User Level

read-only

Context

general

Example

To establish a session with the active media gateway controller:

```
G450-001(super)# session mgc
```

Related Commands

clear mgc list, set icc-monitoring, set mediaserver, set mgc list, set reset-times, show icc-monitoring, show mediaserver, show mgc, show mgc list

set icc-monitoring

Use the **set icc-monitoring** command to control heartbeat monitoring of an Inter Carrier Cable (ICC) or Local Survivable Processor (LSP).

Syntax

set icc-monitoring {enable | disable}

Parameters

Parameter	Description	Possible Values	Default Value
enable	Keyword specifying to enable heartbeat monitoring		
disable	Keyword specifying to disable heartbeat monitoring		

User Level

read-write

Context

general

Related Commands

clear mgc list, session, set mediaserver, set mgc list, set reset-times, show icc-monitoring, show mediaserver, show mgc, show mgc list

set mediaserver

Use the **set mediaserver** command to set server management ports.

Syntax

set mediaserver *ip_address1 ip_address2 port name*

Parameters

Parameter	Description	Possible Values	Default Value
ip_address1	Controller IP address used for registration		
ip_address2	Management interface IP address		
port	Service port number		
name	Service type	**telnet**, **sat**	

User Level

read-write

Context

general

Example

To set the server management sat port 3023 to have a controller IP address of 135.6.8.99 and a management IP address of 135.34.54.2:

```
G450-001# set mediaserver 135.6.8.99 135.34.54.2 3023 sat
```

Related Commands

clear mgc list, session, set icc-monitoring, set mgc list, set reset-times, show icc-monitoring, show mediaserver, show mgc, show mgc list

set mgc list

Use the **set mgc list** command to permit the creation of a list of valid Media Gateway Controller(s). The user can configure up to four IP addresses separated by commas.

Note:

The **set mgc list** command appends the new controllers to the existing list of controllers, if any.

Syntax

set mgc list {***ipaddress1,…***}

Parameters

Parameter	Description	Possible Values	Default Value
ipaddress1	The IP address of the call controller		

User Level

read-write

Context

general

Example

To specify two media gateway controllers at IP addresses 132.236.73.2 and 119.52.3.27:

```
G450-001(super)# set mgc list 132.236.73.2, 119.52.3.27
```

Related Commands

clear mgc list, session, set icc-monitoring, set mediaserver, set reset-times, show icc-monitoring, show mediaserver, show mgc, show mgc list

set reset-times

Use the **set reset-times** command to set reset times.

Syntax

set reset-times { {**total-search** | **primary-search**} ***minutes*** | **transition-point** ***value*** }

Parameters

Parameter	Description	Possible Values	Default Value
total-search	Keyword specifying to set the total search timer		
primary-search	Keyword specifying to set the primary search timer		

Parameter	Description	Possible Values	Default Value
minutes	Number of minutes	**1-60**	total-search: **30** primary-search: **1**
transition-point	Keyword specifying to set the entry point		
value		**1-4**	**1**

User Level

read-write

Context

general

Example

To set the primary search timer reset time to 20 minutes:

```
G450-001(super)# set reset-times primary-search 20
```

Related Commands

clear mgc list, session, set icc-monitoring, set mediaserver, set mgc list, show icc-monitoring, show mediaserver, show mgc, show mgc list

show icc-monitoring

Use the **show icc-monitoring** command to display the state of the icc-monitoring process.

Syntax

show icc-monitoring

User Level

read-only

Context

general

Example

To display ICC monitoring status:

```
G450-001(super)# show icc-monitoring
```

Related Commands

clear mgc list, session, set icc-monitoring, set mediaserver, set mgc list, set reset-times, show mediaserver, show mgc, show mgc list

show mediaserver

Use the **show mediaserver** command to show server configuration information.

Syntax

show mediaserver

User Level

read-only

Context

general

Example

To display server configuration information:

```
G450-001(super)# show mediaserver

MGC IP ADDRESS   SAT IP ADDRESS   SAT PORT  SERVER IP ADDRESS  SERVER PORT
--------------   --------------   --------  -----------------  -----------
135.8.65.107        135.8.65.107       5023        135.8.65.107          23
```

Related Commands

clear mgc list, session, set icc-monitoring, set mediaserver, set mgc list, set reset-times, show icc-monitoring, show mgc, show mgc list

show mgc

Use the **show mgc** command to display the currently active media gateway controller state and setup parameters.

Syntax

show mgc

User Level

read-only

Context

general

Example

To display media gateway controller information:

```
G450-001(super)# show mgc
CALL CONTROLLER STATUS
------------------------------------------
Registered          : NO
Active Controller   : 255.255.255.255
H248 Link Status    : DOWN
H248 Link Error Code: 0x0

CONFIGURED MGC HOST
---------------------
-- Not Available --
-- Not Available --
-- Not Available --
-- Not Available --
```

Related Commands - Media Gateway Controller

clear mgc list, session, set icc-monitoring, set mediaserver, set mgc list, set reset-times, show icc-monitoring, show mediaserver, show mgc list

Related Commands - Device status

set utilization cpu, show faults, show mg list_config, show mm, show module, show recovery, show restart-log, show download, show system, show temp, show timeout, show utilization, show voltages, test led

show mgc list

Use the **show mgc list** command to display the list of available Media Gateway Controllers and their IP addresses.

The **show mgc list** command also shows whether SLS survivability is enabled or disabled. If SLS is enabled, the following message appears at the end of the MGC list:

```
SLS
```

If SLS is disabled, the following message appears at the end of the MGC list:

```
SLS    disabled
```

Syntax

show mgc list

User Level

read-only

Context

general

Example

To display the list of media gateway controllers:

```
G450-001(super)# show mgc list

CONFIGURED MGC HOST
---------------------
135.8.48.220
135.34.54.2
149.49.70.230
-- Not Available --
SLS
```

Output fields

Field	Description
CONFIGURED MGC HOST	Lists five administered elements: • The first three are the IP addresses of the next-available call controller in the administered list • The fourth element is (--`Not Available`--) • The fifth element is either: - `SLS` — SLS is enabled - `SLS disabled` — SLS is disabled

Related Commands

clear mgc list, session, set icc-monitoring, set mediaserver, set mgc list, set reset-times, show icc-monitoring, show mediaserver, show mgc

show recovery

Use the **`show recovery`** command to show the media gateway monitoring and recovery setup.

Syntax

`show recovery`

User Level

read-only

Context

general

Example

To show recovery information:

```
G450-001(super)# show recovery

RECOVERY TIMES
--------------------------------
Primary Search  : 1
Total Search    : 30
Transition Point: 1
```

Related Commands

set utilization cpu, show faults, show mg list_config, show mgc, show mm, show module, show restart-log, show download, show system, show temp, show timeout, show utilization, show voltages, test led

Modem configuration – Console port

interface console

Use the **interface console** command to enter the Console interface configuration mode. The interface is created if it does not exist. Use the **no** form of this command to set the Console parameters to their default values.

Syntax

[no] interface console

User Level

read-write

Context

general

Example

To enter the Console interface context:

```
G450-001(super)# interface console
G450-001(if:Console)#
```

Related Commands - Modem configuration

async modem-init-string, interface USB-modem, ppp chap-secret

Related Commands - IP interface configuration

description (interface), interface fastethernet, interface loopback, interface serial, interface tunnel, interface USB-modem, interface vlan, ip address, ip admin-state, ip broadcast-address, load-interval, show ip interface brief

async mode interactive

Use the **async mode interactive** command to enter modem mode every time the proprietary modem cable is plugged into the Console port.

Syntax

async mode interactive

User Level

read-write

Context

Interface: Console

Example

To enter modem mode:

```
G450-001(super-if:Console)# async mode interactive
```

Related Commands

async mode terminal, ip address, ppp authentication, shutdown (interface), speed (PPP), timeout absolute

async mode terminal

Use the **async mode terminal** command to disable interactive mode on the Console.

Syntax

async mode terminal

User Level

read-write

Context

Interface: Console

Example

To disable interactive mode on the Console:

```
G450-001(super-if:Console)# async mode terminal
```

Related Commands

async mode interactive, ip address, ppp authentication, shutdown (interface), speed (PPP), timeout absolute

async modem-init-string

Use the **async modem-init-string** command to change the default modem initialization string. Use the **no** form of the command to return the modem initialization string to its default value.

Syntax

async modem-init-string *modem_string*

no async modem-init-string

Parameters

Parameter	Description	Possible Values	Default Value
modem_string	The modem initialization string		

User Level

admin

Context

Interface: Console, USB-modem

Example

To set the modem initialization string to AT&FE0Q0V0X0&D2N0S37=6:

```
G450-001(super-if:Console)# async modem-init-string AT&FE0Q0V0X0&D2N0S37=6
```

Related Commands

async mode interactive, async mode terminal, async reset-modem (Console port), async reset-modem (USB port), interface console, interface USB-modem, ip peer address, ppp authentication, shutdown (interface), shutdown (USB modem), speed (PPP), timeout absolute

async reset-modem (Console port)

Use the **async reset-modem** command to reset the connected modem.

Syntax

async reset-modem

User Level

read-write

Context

Interface: Console

Related Commands

async mode interactive, async mode terminal, ip address, ppp authentication, shutdown (interface), speed (PPP), timeout absolute

ip peer address

Use the **ip peer address** command to change the IP address offered by the Console or USB interface to a requesting calling host during PPP/IPCP connection establishment. By default, the interface offers its own IP address plus one.

Syntax

ip peer address ***ip-address***

Parameters

Parameter	Description	Possible Values	Default Value
ip-address	The IP address offered	IP address	The interface IP address plus one

User Level

read-write

Context

Interface: Console, USB-modem

Example

To configure the USB interface to offer requesting calling hosts the IP address 192.168.49.2:

```
G450-001(super-if:USB-modem)# ip peer address 192.168.49.2
```

Related Commands

async mode interactive, async mode terminal, ip address, ppp authentication, shutdown (interface), speed (PPP), timeout absolute

ppp authentication

Use the **ppp authentication** command to select the authentication method used when closing a PPP server or client session.

Note:

The value set for **ppp authentication** affects both the USB interface and the Console interface, simultaneously.

Syntax

ppp authentication {pap|chap|none|ras}

Parameters

Parameter	Description	Possible Values	Default Value
pap	Keyword indicating the Password Authentication Protocol. An unencrypted password is sent for authentication. This is the default.		
chap	Keyword indicating the Challenge Handshake Authentication Protocol. An encrypted password is sent for authentication		
ras	Keyword indicating Remote Access Service mode is being used for authentication		
none	Keyword indicating that no password is sent		

User Level

read-write

Context

Interface: Console, USB-modem

Example

To select the CHAP authentication protocol:

```
G450-001(if:CON)# ppp authentication chap
```

Related Commands - Modem configuration - Console port

interface console, async mode interactive, async mode terminal, async modem-init-string, async reset-modem (Console port), ip peer address, ppp chap-secret, ppp timeout authentication, shutdown (interface), speed (PPP), timeout absolute

Related Commands - Modem configuration - USB modem port

interface usb-modem, async modem-init-string, async reset-modem (USB port), ip peer address, ppp chap-secret, ppp timeout authentication, shutdown (USB modem), timeout absolute

Related Commands - ASG authentication

copy auth-file ftp, copy auth-file scp, copy auth-file tftp, copy auth-file usb, copy ftp auth-file, copy scp auth-file, copy tftp auth-file, copy usb auth-file, erase auth-file, login authentication lockout, login authentication local-craft-password, login authentication response-time, login authentication services-login, show auth-file info, show download auth-file status, show login authentication, show upload auth-file status

---

ppp chap-secret

Use the **ppp chap-secret** command to configure the shared secret used in PPP sessions with CHAP authentication. Use the **no** form to disable the default CHAP password.

Note:

The value set for **ppp chap-secret** affects both the USB interface and the Console interface, simultaneously.

Syntax

[no] ppp chap-secret *chap_secret*

Parameters

Parameter	Description	Possible Values	Default Value
chap_secret	The shared secret string	a string of 4-32 characters	

User Level

admin

Context

Interface: Console, USB-modem

Example

To set the shared secret to mypwd3:

```
G450-001(super-if:CON)# ppp chap-secret mypwd3
PPP shared secret for CHAP authentication is set
```

Related Commands

async modem-init-string, interface console, interface USB-modem

ppp timeout authentication

Use the **ppp timeout authentication** command to set the maximum time to wait for an authentication response.

Syntax

[no] ppp timeout authentication *seconds*

Parameters

Parameter	Description	Possible Values	Default Value
seconds	The authentication timeout in seconds	**1-255**	

User Level

admin

Context

Interface: Console, USB-modem

Example

To specify a maximum wait of 20 seconds for an authentication response:

```
G450-001(super-if:CON)# ppp timeout authentication 20
```

Related Commands - Modem configuration - Console port

interface console, async mode interactive, async mode terminal, async modem-init-string, async reset-modem (Console port), ip peer address, ppp authentication, ppp chap-secret, shutdown (interface), speed (PPP), timeout absolute

Related Commands - Modem configuration - USB modem port

interface usb-modem, async modem-init-string, async reset-modem (USB port), ip peer address, ppp authentication, ppp chap-secret, shutdown (USB modem), timeout absolute

show ppp authentication

Use the **show ppp authentication** command to show the PPP authentication status.

Syntax

show ppp authentication

User Level

read-only

Context

Interface: Console, USB-modem

Example

To show the PPP authentication status:

```
G450-001(super-if:CON)# show ppp authentication
PAP sent-username: configured
CHAP refuseCHAP hostname: G450
CHAP password: not configured
```

Related Commands - Modem configuration - Console port

interface console, async mode interactive, async mode terminal, async modem-init-string, async reset-modem (Console port), ip peer address, ppp authentication, ppp chap-secret, ppp timeout authentication, shutdown (interface), speed (PPP), timeout absolute

Related Commands - Modem configuration - USB modem port

interface usb-modem, async modem-init-string, async reset-modem (USB port), ip peer address, ppp authentication, ppp chap-secret, ppp timeout authentication, shutdown (USB modem), timeout absolute

shutdown (interface)

Use the **shutdown** command to set the administrative status of the current interface to down. Use the **no** form of this command to restore the administrative status for the interface to up.

Syntax

[no] shutdown

User Level

read-write

Context

interface:Serial (DS1 PPP L2, DS1 PPP L2-L3, DS1 FR L2, DS1 FR-SUB L2, DS1 FR-SUB L2-L3, USP PPP L2, USP PPP L2-L3, USP FR L2), FastEthernet (L2, L2-L3, PPP L2, PPP L2-L3), VLAN (L2, L2-L3), Console, Loopback (L2, L2-L3), Controller, Tunnel (L2, L2-L3), Dialer (L2, L2-L3)

Example

To shutdown the VLAN 2 interface:

```
G450-001(if:Vlan 2)# shutdown
Interface Vlan 2, changed state to administratively down
Line protocol on Interface Vlan 2, changed state to down
```

Related Commands - WAN Ethernet port configuration

autoneg, duplex, speed (interface), traffic-shape rate

Related Commands - Modem configuration

async mode interactive, async mode terminal, async reset-modem (Console port), ip address, ppp authentication, speed (PPP), timeout absolute

speed (PPP)

Use the **speed** command to set the PPP baud rate to be used by asynchronous PPP ports.

Note:
The peer baud rate must be set to the same value.

Syntax

speed *speed_rate*

Parameters

Parameter	Description	Possible Values	Default Value
speed_rate	The PPP baud rate	**9600**, **19200**, **38400**	**38400**

User Level

read-write

Context

Interface: Console

Example

To set the PPP baud rate to 9600:

```
G450-001(if:CON)# speed 9600
```

Related Commands

async mode interactive, async mode terminal, ip address, ppp authentication, shutdown (interface), shutdown (USB modem), timeout absolute

timeout absolute

Use the **timeout absolute** command to set the number of minutes until the system automatically disconnects an idle PPP incoming session.

Syntax

timeout absolute *time*

Parameters

Parameter	Description	Possible Values	Default Value
time	Interval, in minutes, after which the system automatically disconnects the PPP session. An interval of 0 minutes indicates that no timeout should occur.	**0-999**	**0**

User Level

read-write

Context

Interface: Console, USB-modem

Example

To set the PPP timeout to 30 minutes:

```
G450-001(if:Console)# timeout absolute 30
PPP incoming session will automatically disconnect after 30 minutes of idle
time.
```

Related Commands

async mode interactive, async mode terminal, async reset-modem (USB port), ip address, ppp authentication, shutdown (interface), shutdown (USB modem), speed (PPP)

Modem configuration – USB modem port

interface usb-modem

Use the **interface usb-modem** command to enter configuration context for the USB interface. Use the **no** form of the command to reset the USB interface settings to their factory defaults.

The USB interface always exists, but is disabled by default. Use the **no shutdown** command to enable the interface.

The default settings for the USB interface are:

Interface status	DOWN
IP address	10.3.0.3
Netmask	255.255.255.0
timeout	no timeout
PPP speed	38400 bps
Async modem-init-string	"AT S7=45 S0=2 L1 V1 X4 &c1 E0 Q0"

Syntax

[no] interface usb-modem

User Level

read-write

Context

general

Example

To enter the USB-modem interface context:

```
G450-001(super)# interface usb-modem
G450-001(super-if:USB-modem)#
```

Related Commands - IP interface configuration

description (interface), interface console, interface fastethernet, interface loopback, interface serial, interface tunnel, interface vlan, ip address, ip admin-state, ip broadcast-address, load-interval, show ip interface brief

Related Commands - Modem configuration

async modem-init-string, interface console, ppp chap-secret

async modem-init-string

Use the **async modem-init-string** command to change the default modem initialization string. Use the **no** form of the command to return the modem initialization string to its default value.

Syntax

async modem-init-string *modem_string*

no async modem-init-string

Parameters

Parameter	Description	Possible Values	Default Value
modem_string	The modem initialization string		

User Level

admin

Context

Interface: Console, USB-modem

Example

To set the modem initialization string to AT&FE0Q0V0X0&D2N0S37=6:

```
G450-001(super-if:Console)# async modem-init-string AT&FE0Q0V0X0&D2N0S37=6
```

Related Commands

async mode interactive, async mode terminal, async reset-modem (Console port), async reset-modem (USB port), interface console, interface USB-modem, ip peer address, ppp authentication, shutdown (interface), shutdown (USB modem), timeout absolute

async reset-modem (USB port)

Use the **async reset-modem** command to reset the USB modem. This command resets the PPP stack, deactivates the DTR signal, issues an ATZ (reset) command to the USB modem, and reissues the Init string sequence.

You can perform this command from within an active PPP session to close the session and allow the USB modem to accept a new call.

Syntax

async reset-modem

User Level

read-write

Context

interface:USB-modem

Related Commands

ip address, ppp authentication, shutdown (USB modem), timeout absolute

ip peer address

Use the **ip peer address** command to change the IP address offered by the Console or USB interface to a requesting calling host during PPP/IPCP connection establishment. By default, the interface offers its own IP address plus one.

Syntax

ip peer address *ip-address*

Parameters

Parameter	Description	Possible Values	Default Value
ip-address	The IP address offered	IP address	The interface IP address plus one

User Level

read-write

Context

Interface: Console, USB-modem

Example

To configure the USB interface to offer requesting calling hosts the IP address 192.168.49.2:

```
G450-001(super-if:USB-modem)# ip peer address 192.168.49.2
```

Related Commands

async mode interactive, async mode terminal, ip address, ppp authentication, shutdown (interface), timeout absolute

ppp authentication

Use the **ppp authentication** command to select the authentication method used when closing a PPP server or client session.

Note:

The value set for **ppp authentication**, affects both the USB interface and the Console interface, simultaneously.

Syntax

ppp authentication {pap|chap|none|ras}

Parameters

Parameter	Description	Possible Values	Default Value
pap	Keyword indicating the Password Authentication Protocol. An unencrypted password is sent for authentication. This is the default.		
chap	Keyword indicating the Challenge Handshake Authentication Protocol. An encrypted password is sent for authentication.		
ras	Keyword indicating Remote Access Service mode is being used for authentication		
none	Keyword indicating that no password is sent		

User Level

read-write

Context

Interface: Console, USB-modem

Example

To select the CHAP authentication protocol:

```
G450-001(if:CON)# ppp authentication chap
```

Related Commands - Modem configuration - USB modem port

interface usb-modem, async modem-init-string, async reset-modem (USB port), ip peer address, ppp chap-secret, ppp timeout authentication, shutdown (USB modem), timeout absolute

Related Commands - Modem configuration - Console port

interface console, async mode interactive, async mode terminal, async modem-init-string, async reset-modem (Console port), ip peer address, ppp chap-secret, ppp timeout authentication, shutdown (interface), speed (PPP), timeout absolute

Related Commands - ASG authentication

copy auth-file ftp, copy auth-file scp, copy auth-file tftp, copy auth-file usb, copy ftp auth-file, copy scp auth-file, copy tftp auth-file, copy usb auth-file, erase auth-file, login authentication lockout, login authentication local-craft-password, login authentication response-time, login authentication services-login, show auth-file info, show download auth-file status, show login authentication, show upload auth-file status

ppp chap-secret

Use the **ppp chap-secret** command to configure the shared secret used in PPP sessions with CHAP authentication. Use the **no** form to disable the default CHAP password.

Note:

The value set for **ppp chap-secret** affects both the USB interface and the Console interface, simultaneously.

Syntax

[no] ppp chap-secret *chap_secret*

Parameters

Parameter	Description	Possible Values	Default Value
chap_secret	The shared secret string	a string of 4-32 characters	

User Level

admin

Context

Interface: Console, USB-modem

Example

To set the shared secret to mypwd3:

```
G450-001(super-if:CON)# ppp chap-secret mypwd3
PPP shared secret for CHAP authentication is set
```

Related Commands

async modem-init-string, interface console, interface USB-modem

ppp timeout authentication

Use the **ppp timeout authentication** command to set the maximum time to wait for an authentication response.

Syntax

[no] ppp timeout authentication *seconds*

Parameters

Parameter	Description	Possible Values	Default Value
seconds	The authentication timeout in seconds	**1-255**	

User Level

admin

Context

Interface: Console, USB-modem

Example

To specify a maximum wait of 20 seconds for an authentication response:

```
G450-001(super-if:CON)# ppp timeout authentication 20
```

Related Commands - Modem configuration - Console port

interface console, async mode interactive, async mode terminal, async modem-init-string, async reset-modem (Console port), ip peer address, ppp authentication, ppp chap-secret, ppp timeout authentication, shutdown (interface), speed (PPP), timeout absolute

Related Commands - Modem configuration - USB modem port

interface usb-modem, async modem-init-string, async reset-modem (USB port), ip peer address, ppp authentication, ppp chap-secret, ppp timeout authentication, shutdown (USB modem), timeout absolute

show ppp authentication

Use the **show ppp authentication** command to show the PPP authentication status.

Syntax

show ppp authentication

User Level

read-only

Context

Interface: Console, USB-modem

Example

To show the PPP authentication status:

```
G450-001(super-if:USB-modem)# show ppp authentication
PAP sent-username: configured
CHAP refuseCHAP hostname: G450
CHAP password: not configured
```

Related Commands - Modem configuration - Console port

interface console, async mode interactive, async mode terminal, async modem-init-string, async reset-modem (Console port), ip peer address, ppp authentication, ppp chap-secret, ppp timeout authentication, shutdown (interface), speed (PPP), timeout absolute

Related Commands - Modem configuration - USB modem port

interface usb-modem, async modem-init-string, async reset-modem (USB port), ip peer address, ppp authentication, ppp chap-secret, ppp timeout authentication, shutdown (USB modem), timeout absolute

shutdown (USB modem)

Use the **shutdown** command to disable the USB interface. When the interface is disabled, calls to the modem are immediately hung up. No PPP initialization is performed, and there is no access to the device.

Use the **no** form of this command to enable the USB interface. For security reasons, the USB interface is disabled by default. The USB modem can only be connected after the interface is manually brought up using this command.

Syntax

[no] shutdown

User Level

For **shutdown**: read-write

For **no shutdown**: admin

Context

interface:USB-modem

Example

To disable the USB interface:

```
G450-001(super-if:USB-modem)# shutdown
```

Related Commands

async reset-modem (USB port), ip address, ppp authentication, shutdown (USB modem), timeout absolute

timeout absolute

Use the **timeout absolute** command to set the number of minutes until the system automatically disconnects an idle PPP incoming session.

Syntax

timeout absolute *time*

Parameters

Parameter	Description	Possible Values	Default Value
time	Interval, in minutes, after which the system automatically disconnects the PPP session. An interval of 0 minutes indicates that no timeout should occur.	**0-999**	**0**

User Level

read-write

Context

Interface: Console, USB-modem

Example

To set the PPP timeout to 30 minutes:

```
G450-001(if:Console)# timeout absolute 30
PPP incoming session will automatically disconnect after 30 minutes of idle
time.
```

Related Commands

async mode interactive, async mode terminal, async reset-modem (USB port), ip address, ppp authentication, shutdown (interface), shutdown (USB modem),

MSS notifications

DoS-classification

Use the **DoS-classification** command to label a user-defined DoS attack classification to be reported in MSS notifications.

Syntax

DoS-classification
[na|fraggle|smurf|ip-spoofing|other-attack-100|other-attack-101|other-attack-102|other-attack-103|other-attack-104|other-attack-105]

Parameters

Parameter	Description	Possible Values	Default Value
na	Keyword indicating the default DoS classification for an ACL rule		
fraggle	Keyword indicating the user-defined DoS classification label usually used to report reception of Fraggle packets		
smurf	Keyword indicating the user-defined DoS classification label usually used to report reception of Smurf packets		
ip-spoofing	Keyword indicating the user-defined DoS classification label usually used to report reception of IP-spoofing packets		
other-attack-100	Keyword indicating the user-defined DoS classification label for any packet criteria		
other-attack-101	Keyword indicating the user-defined DoS classification label for any packet criteria		
other-attack-102	Keyword indicating the user-defined DoS classification label for any packet criteria		
other-attack-103	Keyword indicating the user-defined DoS classification label for any packet criteria		
other-attack-104	Keyword indicating the user-defined DoS classification label for any packet criteria		
other-attack-105	Keyword indicating the user-defined DoS classification label for any packet criteria		

User Level

read-write

Context

ip access-control-list/ip-rule

Example

To label a user-defined DoS attack classification for any packet criteria to be reported in MSS notifications:

```
G450-001(config)# DoS-classification other-attack-101
```

Related Commands

set security-association lifetime, show rtp-stat config

icmp in-echo-limit

Use the **icmp in-echo-limit** command to set the maximum number of echo requests that can be received in one second. Use the **no** form of the command to return the limit to its default value.

Syntax

[no]icmp in-echo-limit *size*

Parameters

Parameter	Description	Possible Values	Default Value
size	The number of echo requests	**1-10000**	

User Level

read-write

Context

general

Example

To set the echo request limit at 500 packets per second:

```
G450-001(super)# icmp in-echo-limit 500
```

set mss-notification rate

Use the **set mss-notification rate** command to configure the rate at which the G450 sends Managed Security Services (MSS) notifications. MSS notifications report suspected DoS attacks.

Syntax

set mss-notification rate *seconds*

Parameters

Parameter	Description	Possible Values	Default Value
seconds	The interval, in seconds, between MSS notifications	**10**-**28,800** (up to 8 hours)	**300**

User Level

read-write

Context

general

Example

To set the interval of MMS notifications to 120 seconds:

```
G450-001(super)# set mss-notification rate 120
```

Related Commands

DoS-classification, show rtp-stat config

show mss-notification rate

Use the **show mss-notification rate** command to show the interval time, in seconds, between MSS notifications.

Syntax

show mss-notification rate

User Level

read-write

Context

general

Example

To show the interval time between MSS notifications:

```
G450-001(super)# show mss-notification rate
```

Related Commands

DoS-classification, set security-association lifetime

Object tracking

rtr

Use the **rtr** command to enter RTR configuration mode and specify an identification number for an RTR operation. Use the **no** form of this command to delete the RTR.

Note:

You cannot enter configuration mode for a specific RTR if this RTR is currently probing an object. You must first deactivate the RTR using the **no rtr-schedule** command.

Note:

You cannot delete an RTR being monitored by an object tracker. You must first remove the link between them, using the **no track *track-id*** command.

Syntax

rtr *rtr-id*

Parameters

Parameter	Description	Possible Values	Default Value
rtr-id	The RTR ID	**1-30**	

User Level

read-write

Context

general

Example

To enter RTR configuration mode for RTR operation 1:

```
G450-001(config)# rtr 1
```

Related Commands

rtr-schedule, show rtr configuration, show rtr operational-state, type

---

type

Use the **type** command to specify which type of operation an RTR operation should employ in its probes, and to specify the address of the remote device to be probed.

Note:

The **type** command is available only for newly-created RTRs. You cannot use it for existing RTRs.

Syntax

type echo protocol ipIcmpEcho *ip-address*

type tcpConnect dest-ipaddr *ip-address* dest-port *port*

Parameters

Parameter	Description	Possible Values	Default Value
echo protocol ipIcmpEcho	Keyword indicating to use the ICMP Echo operation for RTR probes		
tcpConnect	Keyword indicating to use the TCP Connection operation for RTR probes		
ip-address	The IP address of the remote device to be probed		
port	The port number of the destination port to be probed		

User Level

read-write

Context

rtr

Example

To specify ICMP Echo operation for RTR probes of the remote device at IP address 137.42.11.1:

```
G450-001(config-rtr 1)# type echo protocol ipIcmpEcho 137.42.11.1
G450-001(config-rtr icmp 1)#
```

To specify TCP Connection operation for RTR probes at port 80 of the remote device at IP address 147.42.11.1:

```
G450-001(config-rtr 2)# type tcpConnect dest-ipaddr 147.42.11.1 dest-port 80
G450-001(config-rtr tcp 2)#
```

Related Commands

dscp-table, fail-retries, frequency, next-hop (object tracking), rtr, source-address, success-retries, wait-interval

dscp (object tracking)

Use the **dscp** command to set the DSCP value in the IP header of an RTR operation's probe packets. Use the **no** form of this command to restore the value to the default value of 48.

Note:

You must run the **type** command to define the RTR operation's probing method and the IP address of the remote device before you can use the **dscp** command.

Syntax

[no] dscp *dscp*

Parameters

Parameter	Description	Possible Values	Default Value
dscp	The dscp value	**0-63**	**48**

User Level

read-write

Context

rtr, rtr type

Example

To set the DSCP value for RTR 1:

```
G450-001(config-rtr icmp 1)# dscp 42
```

Related Commands

fail-retries, frequency, next-hop (object tracking), rtr, source-address, success-retries, type, wait-interval

fail-retries

Use the **fail-retries** command to specify how many consecutive unanswered probes change the status of an RTR operation from up to down. Use the **no** form of this command to restore the value to the default.

Note:

You must run the **type** command to define the RTR operation's probing method and the IP address of the remote device before you can use the **fail-retries** command.

Syntax

[no] fail-retries *retries*

Parameters

Parameter	Description	Possible Values	Default Value
retries	The number of retries	**1-100**	**5**

User Level

read-write

Context

rtr, rtr type

Example

To set the fail-retries value for RTR 1 to 4:

```
G450-001(config-rtr icmp 1)# fail-retries 4
```

Related Commands

dscp (object tracking), frequency, next-hop (object tracking), rtr, source-address, success-retries, type, wait-interval

frequency

Use the **frequency** command to specify how often an RTR operation should send probes. Use the **no** form of this command to restore the frequency value to the default.

Note:

You must run the **type** command to define the RTR operation's probing method and the IP address of the remote device before you can use the **frequency** command.

Syntax

[no] frequency *frequency-value* [seconds | milliseconds]

Parameters

Parameter	Description	Possible Values	Default Value
frequency-value	A number indicating the frequency of RTR probes	**1-60** seconds or **1000-60,000** milliseconds	**5** seconds or **5000** milliseconds
seconds	Keyword specifying to set the frequency of RTR probes in units of seconds		
milliseconds	Keyword specifying to set the frequency of RTR probes in units of milliseconds		

User Level

read-write

Context

rtr, rtr type

Example

To set the frequency value for RTR 1 to 20 seconds:

```
G450-001(config-rtr icmp 1)# frequency 20 seconds
```

Related Commands

dscp (object tracking), fail-retries, next-hop (object tracking), rtr, source-address, success-retries, type, wait-interval

interface-keepalive bypass-logic

The **interface-keepalive bypass-logic** command provides support for an alternative internal path for RTR probes, in cases where next-hop is configured for the RTR probes.

Note:

This command is automatically appended to the configuration if you specify next-hop interface for the RTR probes using the next-hop (object tracking) command.
This command is automatically removed from the configuration when specifying **no next-hop**.

Syntax

interface-keepalive bypass-logic

User Level

read-write

Context

rtr, rtr type

Related Commands

dscp (object tracking), fail-retries, frequency, next-hop (object tracking), rtr, source-address, success-retries, type, wait-interval

next-hop (object tracking)

Use the **next-hop** command to specify the next hop for the RTR probes, bypassing normal routing. Use the **no** form of this command to disable setting of the next hop.

Note:

You must run the **type** command to define the RTR operation's probing method and the IP address of the remote device before you can use the **next-hop** command.

Note:

The **next-hop** command is disabled by default.

Note:

The interface-keepalive bypass-logic command is automatically appended to the RTR configuration if you specify the next hop for the RTR probes, and automatically removed from the configuration if you specify **no next-hop**.

Note:

When applying tracking to a static route, a PBR next hop, or the DHCP client default route, you must specify the same next hop for the object tracker's RTR.

Syntax

[no] next-hop interface {*interface-name* [mac-address *mac-address*] | ip *ip-address*}

Parameters

Parameter	Description	Possible Values	Default Value
interface-name	The next hop interface		
mac-address	The MAC address of the interface. Applies to Ethernet interfaces only: • FastEthernet not running PPPoE • VLAN		
ip-address	The next hop IP address		

User Level

read-write

Context

rtr, rtr type

Examples

To specify the next hop for interface FastEthernet 10/2 is MAC address 00:04:d0:af:12:04:

```
G450-001(config-rtr icmp 1)# next-hop FastEthernet 10/2 interface-name
00:04:d0:af:12:04 mac-address
```

Related Commands

dscp (object tracking), fail-retries, frequency, interface-keepalive bypass-logic, rtr, source-address, success-retries, type, wait-interval

source-address

Use the **source-address** command to set the source IP address for an RTR operation. Use the **no** form of this command to restore the default setting, which is to use the output interface's IP address.

Note:

You must run the **type** command to define the RTR operation's probing method and the IP address of the remote device before you can use the **source-address** command.

Note:

By default, the **source-address** command is disabled, and RTR operations use the output interface's address.

Syntax

[no] source-address *ip-address*

Parameters

Parameter	Description	Possible Values	Default Value
ip-address	The IP address to serve as the source IP address for all RTR operations		

User Level

read-write

Context

rtr, rtr type

Examples

To set the source IP address for RTR operations as IP address 135.64.102.5:

```
G450-001(config-rtr icmp 1)# source-address 135.64.102.5
```

Related Commands

dscp (object tracking), fail-retries, frequency, next-hop (object tracking), rtr, success-retries, type, wait-interval

success-retries

Use the **success-retries** command to specify how many consecutive answered probes change the status of an RTR operation from down to up. Use the **no** form of this command to restore the value to the default.

Note:

You must run the **type** command to define the RTR operation's probing method and the IP address of the remote device before you can use the **success-retries** command.

Syntax

[no] sucess-retries *retries*

Parameters

Parameter	Description	Possible Values	Default Value
retries	The number of retries	**1-100**	**5**

User Level

read-write

Context

rtr, rtr type

Example

To specify that 3 consecutive answered probes changes the status of an RTR operation device from down to up:

```
G450-001(config-rtr icmp 1)# success-retries 3
```

Related Commands

dscp (object tracking), fail-retries, frequency, next-hop (object tracking), rtr, source-address, type, wait-interval

wait-interval

Use the **wait-interval** command to specify how long an RTR operation should wait for a device to answer an RTR probe. When the wait-interval is exceeded, the probe is considered an unanswered probe.
Use the **no** form of this command to restore the value to the default.

Note:

You must run the **type** command to define the RTR operation's probing method and the IP address of the remote device before you can use the **wait-interval** command.

Note:

The value of **wait-interval** cannot be greater than the value of **frequency**.

Syntax

[no] wait-interval *wait-value* [seconds | milliseconds]

Parameters

Parameter	Description	Possible Values	Default Value
wait-value	A number indicating how long to wait for a response to the probe before considering it an unanswered probe	**1-60** seconds or **200-60,000** milliseconds	Same as default value of **frequency**
seconds	Keyword indicating to set the wait interval in units of seconds		
milliseconds	Keyword indicating to set the wait interval in units of milliseconds		

User Level

read-write

Context

rtr, rtr type

Example

To specify a wait of 3 seconds for a device to answer an RTR probe:

```
G450-001(config-rtr icmp 1)# wait-interval 3 seconds
```

Related Commands

dscp (object tracking), fail-retries, frequency, next-hop (object tracking), rtr, source-address, success-retries, type

rtr-schedule

Use the **rtr schedule** command to activate an RTR operation. Use the **no** form of this command to stop an RTR operation. Once you activate an RTR operation, it starts probing immediately and continues running unless stopped by the **no rtr schedule** command.

Syntax

rtr-schedule *rtr-id* start-time now life forever

[no] rtr-schedule *rtr-id*

Parameters

Parameter	Description	Possible Values	Default Value
rtr-id	The RTR ID	**1-30**	

User Level

read-write

Context

general

Example

To activate RTR operation 1:

```
G450-001(config)# rtr-schedule 1 start-time now life forever
```

Related Commands

rtr, show rtr configuration, show rtr operational-state

show rtr configuration

Use the **show rtr configuration** command to display RTR configuration values, including all defaults for a specific RTR operation. If no RTR ID is specified, values for all RTR operations are displayed.

Syntax

show rtr configuration [*rtr-id*]

Parameters

Parameter	Description	Possible Values	Default Value
rtr-id	RTR ID	**1-30**	

User Level

read-only

Context

general

Examples

To display all RTR configuration values:

```
G450-001(super)# show rtr configuration

RTR#  1
-------
Type: ipIcmpEcho
Target Address: 2.2.2.1
Frequency (Milliseconds): 5000
Wait Interval (Milliseconds): 5000
Success Retries: 1
Failure Retries: 5
DSCP: 48
Source Address: 149.49.70.119
Next-Hop interface:FastEthernet 10/2
Next-Hop Mac Address: 00:04:0d:17:28:4b

RTR#  2
-------
Type: tcpConnect
Target Address: 2.2.2.1
Target Port: 21
Frequency (Milliseconds): 5000
```

```
Wait Interval (Milliseconds): 5000
Success Retries: 1
Failure Retries: 5
DSCP: 48
```

Output fields:

Field	Description
Type	The configured RTR type. The supported types are: • IP/ICMP Echo • TCP Connection
Target Address	The destination IP address of the probe packet. That is, the address being monitored
Frequency	The time in milliseconds between successive RTRs
Wait Interval	The amount of time in milliseconds to wait for a response to a probe before considering it an unanswered probe
Success Retries	The number of successive answered probes that will change the status of the RTR operation from down to up
Failure Retries	The number of successive unanswered probes that will change the status of the RTR operation from up to down
DSCP	The DSCP value of the probe packet
Source Address	The source IP address of the probe packet (displayed only if configured)
Next-Hop Interface	The interface through which to route the probe packet, bypassing the normal route (displayed only if configured)
Next-Hop Mac Address	The next hop mac-address for Ethernet interfaces

Related Commands

rtr, rtr-schedule, show rtr operational-state

show rtr operational-state

Use the **show rtr operational-state** command to display the global operational status of the RTR feature for a specific RTR operation. If no RTR ID is specified, information for all RTR operations is displayed.

Syntax

show rtr operational state [*rtr-id*]

Parameters

Parameter	Description	Possible Values	Default Value
rtr-id	RTR ID	**1-30**	

User Level

read-only

Context

general

Example

To display the global operational status of all RTR operations:

```
G450-001(super)# show rtr operational-state
                                                    Wait            Last Change
ID    Type      Dest Address    State     S/C F/C Freq Inter S/R F/R   d,h:m:s
-- ---------- --------------- -----     --- --- ---- ----- --- ---   -------
 1 ipIcmpEcho 149.49.70.1     up          2   0 5000 1000   2   4    0,0:45:16
 2 tcpConnect 135.64.102.105  up          1   0 1000 1000   1   5    No change
 3 ipIcmpEcho 1.1.1.1         Inactive    0   0 1000 1000   2   4    No change
 4 ipIcmpEcho 1.1.1.2         down        0   0 1000 1000   2   4    No change
```

Output fields:

Field	Description
ID	The ID of the RTR
Type	The configured RTR type. The supported types are: • IP/ICMP Echo • TCP Connection

1 of 2

Field	Description
Dest Address	The destination IP address of the probe packet. That is, the address being monitored.
State	The current operational state of the RTR. Possible options are `up`, `down` or `inactive`.
S/C	Success Counter — the number of successive answered retries
F/C	Failure Counter — the number of successive unanswered retries
Freq	Frequency — the time in milliseconds between successive RTRs
Wait Inter	Wait Interval — the amount of time in milliseconds to wait for a response to a probe before considering it an unanswered probe
S/R	Success Retries — how many successive answered probes will change the status of the RTR operation from down to up
F/R	Failure Retries — how many successive unanswered probes will change the status of the RTR operation from up to down
Last Change d,h:m:s	The time that elapsed since the RTR last changed its operational state

2 of 2

Related Commands

rtr, rtr-schedule, show rtr configuration

show track

Use the **`show track`** command to display tracking information.

Syntax

`show track [`*`object-id`*`] [detail]`

Parameters

Parameter	Description	Possible Values	Default Value
object-id	Object tracker id	**1-50**	
detail	Keyword indicating to display detailed tracking information		

User Level

read-only

Context

general

Examples

To display tracking information:

```
G450-001(super)# show track
ID  Type  rtr-id  State  Clients
--  ----  ------  -----  -------
 1  rtr        1  up           1
 2  rtr        2  up           1
10  list     N/A  up           0

G450-001(super)# show track detail
Track# 1
----------
Type: rtr
RTR id: 1
State: up
Operational Status Last Change (d,h:m:s): 0,0:0:2
Registered Applications:
  FastEthernet 10/2
```

Output fields:

Field	Description
ID	The ID of the object tracker
Type	The type of object tracker: `rtr` or `list`
RTR id	The ID of the RTR associated with this object tracker (if applicable)

1 of 2

Field	Description
State	The current operational state of the object tracker. Possible options are `up` or `down`
Clients	The number of applications registered to receive updates from this object tracker
Operational Status Last Change	The time that elapsed since the object tracker last changed its operational state
Registered Applications	A list of the applications registered to receive updates from this object tracker

2 of 2

Related Commands

rtr, track

track

Use the **`track`** command to configure an object tracker. Use the **`no`** form of this command to delete the object tracker.

You can configure two types of object trackers:

An object tracker which tracks the state of a single RTR object.

A track list which is composed of multiple previously-defined object trackers. Note that when configuring a track list you may also specify how to calculate the state of the list based on the states of the individual object trackers composing the list. If you do not specify how to calculate the state of the list, the boolean AND argument is used.

Note:

You cannot delete an object tracker which is a member of a track list. You must first remove the object tracker from the track list using the **`no object`** command.

You cannot delete an object tracker which was linked to an application using the **`keepalive-track`** command. You must first use the **`no keepalive-track`** command to disable the link.

Syntax

`[no] track` ***`track-id`*** **`rtr`** ***`rtr-id`***

`[no] track` ***`track-id`*** **`list [{boolean {and | or} | threshold count}]`**

Parameters

Parameter	Description	Possible Values	Default Value
track-id	The track list ID	**1-50**	
rtr-id	The RTR operation ID	**1-30**	
boolean	Keyword specifying that the state of the tracked list is based on a Boolean calculation		
and	Keyword specifying that the list is up if all objects are up, or down if one or more of the objects are down. For example, when tracking two interfaces, up means that both interfaces are up, and down means that either interface is down.		
or	Keyword specifying that the list is up if at least one object is up. For example, when tracking two interfaces, up means that either interface is up, and down means that both interfaces are down.		
threshold count	Keyword specifying that the state of the tracked list is based on a threshold calculation, as follows: ● When the list is in the down state, it switches to the up state if the number of the up objects is greater than or equal to the number specified in the **threshold count up** command. ● When the list is in the up state, it switches to the down state if the number of up objects is less than or equal to the number specified in the **threshold count down** command.		

User Level

read-write

Context

general

Example

To configure object tracker 1 which tracks RTR 2:

```
G450-001(config)# track 1 rtr 2
G450-001(config-track rtr 1)#
```

To create Track List 5 and specify that its state should be calculated using the Boolean OR argument:

```
G450-001(config)# track 5 list boolean or
G450-001(config-track list 5)#
```

To create Track List 3 and specify that its state should be calculated using a threshold calculation:

```
G450-001(config)# track 3 list threshold count
G450-001(config-track list 3)#
```

Related Commands

description (object tracking), object, rtr, threshold count, show track

description (object tracking)

Use the **description** command to enter a description of an object tracker. Use the **no** form of this command to use the default description, which is the object tracker's ID.

Syntax

[no] description *text*

Parameters

Parameter	Description	Possible Values	Default Value
text	Description of object tracker	string of 1-255 characters	The object tracker's ID

User Level

read-write

Context

track rtr, track list

Examples

To specify the description for a simple object tracker tracking a single RTR as track rtr-2:

```
G450-001(config-track rtr 1)# description "track rtr-2"
```

To specify the description for a simple object tracker tracking several objects as track list rtr-4 and rtr-5:

```
G450-001(config track list 10)# description "track list rtr-4 and rtr-5"
```

Related Commands

object, threshold count, track, show track

---

object

Use the **object** command to add an object tracker to a track list. Use the **no** form of this command to remove the object tracker from the list of tracked objects.

Syntax

[no] object *track-id* [not]

Parameters

Parameter	Description	Possible Values	Default Value
track-id	The object tracker ID	**1-50**	
not	Keyword that reverses the output value of the object being tracked, i.e., 'up' becomes 'down', and vice-versa		

User Level

read-write

Context

track list

Example

To add object tracker 3 to track list 2:

```
G450-001(config-track list 2)# object 3
```

Related Commands

description (object tracking), threshold count, track, show track

threshold count

Use the **threshold count** command to specify the upper and lower thresholds for the threshold in the **track list** command. Use the **no** form of this command to restore the default values.

Syntax

[no] threshold count [up *up_number*] [down *down_number*]

Parameters

Parameter	Description	Possible Values	Default Value
up_number	The upper threshold for the threshold count in the **track list** command	**1-50**	**1**
down_number	The lower threshold for the threshold count in the **track list** command	**1-50**	**0**

User Level

read-write

Context

track list

Example

To specify that for list 5, the state will change from down to up if 4 or more hosts are up:

```
G450-001(config-track list 5)# threshold count up 4
```

To specify that for list 5, the state will change from up to down if 2 or less hosts are up:

```
G450-001(config-track list 5)# threshold count down 2
```

Related Commands

description (object tracking), object, track, show track

OSPF

bandwidth

Use the **bandwidth** command to set the bandwidth parameter manually for this interface. Use the **no** form of this command to restore the bandwidth parameter to its default value. The manually specified bandwidth value overrides the dynamically calculated bandwidth during route cost calculations.

Syntax

bandwidth *kilobits*

no bandwidth

Parameters

Parameter	Description	Possible Values	Default Value
kilobits	The bandwidth for the interface in kilobits per second	**1-10000000**	**2048** (for Frame Relay)

User Level

read-write

Context

interface:Serial (DS1 PPP L2, DS1 PPP L2-L3, DS1 FR L2, DS1 FR-SUB L2, DS1 FR-SUB L2-L3, USP PPP L2, USP PPP L2-L3, USP FR L2), FastEthernet (L2, L2-L3, PPP L2, PPP L2-L3), VLAN (L2, L2-L3), Loopback (L2, L2-L3), Tunnel (L2, L2-L3), Dialer (L2, L2-L3)

Example

To manually set the bandwidth for the VLAN interface to 100 KB/s:

```
G450-001(if:Vlan 1)# bandwidth 100
```

Related Commands

idle-character, ignore dcd, interface serial, invert txclock, nrzi-encoding, transmitter-delay

ip ospf authentication

Use the **ip ospf authentication** command to specify the authentication type for an interface. Use the **no** form of the command to remove the authentication type for an interface.

Syntax

ip ospf authentication ***auth_type***

no ip ospf authentication

Parameters

Parameter	Description	Possible Values	Default Value
auth_type	The type of authentication	**message-digest**, **null**	**null**

User Level

read-write

Context

interface:Serial (DS1 PPP L2-L3, DS1 PPP L3, DS1 FR-SUB L2-L3, DS1 FR-SUB L3, USP PPP L2-L3, USP PPP L3), FastEthernet (L2-L3, L3, PPP L2-L3, PPP L3), VLAN (L2-L3, L3), Loopback (L2-L3, L3), Tunnel (L2-L3, L3), Dialer (L2-L3, L3)

Example

To set the OSPF authentication for the FastEthernet interface as message-digest:

```
G450-001(if:FastEthernet 10/2)# ip ospf authentication message-digest
```

Related Commands

ip ospf authentication-key, ip ospf cost, ip ospf dead-interval, ip ospf hello-interval, ip ospf message-digest-key, ip ospf network point-to-multipoint, ip ospf priority, ip ospf router-id, router ospf, show ip ospf, show ip ospf database, show ip ospf interface, show ip ospf neighbor, show ip protocols

ip ospf authentication-key

Use the **ip ospf authentication-key** command to configure the interface authentication password. Use the **no** form of this command to remove the OSPF password.

Syntax

ip ospf authentication-key *key*

no ip ospf authentication-key

Parameters

Parameter	Description	Possible Values	Default Value
key	The interface authentication password	string (1-8 chars)	

User Level

read-write

Context

interface:Serial (DS1 PPP L2-L3, DS1 PPP L3, DS1 FR-SUB L2-L3, DS1 FR-SUB L3, USP PPP L2-L3, USP PPP L3), FastEthernet (L2-L3, L3, PPP L2-L3, PPP L3), VLAN (L2-L3, L3), Loopback (L2-L3, L3), Tunnel (L2-L3, L3), Dialer (L2-L3, L3)

Example

To set the authentication password for the VLAN 1 interface as my_pass:

```
G450-001(if:Vlan 1)# ip ospf authentication-key my_pass
```

Related Commands

ip ospf authentication, ip ospf cost, ip ospf dead-interval, ip ospf hello-interval, ip ospf message-digest-key, ip ospf network point-to-multipoint, ip ospf priority, ip ospf router-id, router ospf, show ip ospf, show ip ospf database, show ip ospf interface, show ip ospf neighbor, show ip protocols

ip ospf cost

Use the **ip ospf cost** command to statically configure the interface cost metric. Use the **no** form of this command to return to dynamic calculation of the cost.

Syntax

ip ospf cost *cost*

no ip ospf cost

Parameters

Parameter	Description	Possible Values	Default Value
cost	The price assigned to each interface for the purpose of determining the shortest path	**1-65535**	**1**

User Level

read-write

Context

interface:Serial (DS1 PPP L2-L3, DS1 PPP L3, DS1 FR-SUB L2-L3, DS1 FR-SUB L3, USP PPP L2-L3, USP PPP L3), FastEthernet (L2-L3, L3, PPP L2-L3, PPP L3), VLAN (L2-L3, L3), Loopback (L2-L3, L3), Tunnel (L2-L3, L3), Dialer (L2-L3, L3)

Example

To set the cost metric for the VLAN 1 interface to 10:

```
G450-001(if:Vlan 1)# ip ospf cost 10
```

Related Commands

ip ospf authentication, ip ospf authentication-key, ip ospf dead-interval, ip ospf hello-interval, ip ospf message-digest-key, ip ospf network point-to-multipoint, ip ospf priority, ip ospf router-id, router ospf, show ip ospf, show ip ospf database, show ip ospf interface, show ip ospf neighbor, show ip protocols

ip ospf dead-interval

Use the **ip ospf dead-interval** command to configure the interval before declaring the neighbor as dead. Use the **no** form of this command to set the dead-interval to its default value.

Syntax

ip ospf dead-interval *seconds*

no ip ospf dead-interval

Parameters

Parameter	Description	Possible Values	Default Value
seconds	The interval in seconds	**1-415029**	**40**

User Level

read-write

Context

interface:Serial (DS1 PPP L2-L3, DS1 PPP L3, DS1 FR-SUB L2-L3, DS1 FR-SUB L3, USP PPP L2-L3, USP PPP L3), FastEthernet (L2-L3, L3, PPP L2-L3, PPP L3), VLAN (L2-L3, L3), Loopback (L2-L3, L3), Tunnel (L2-L3, L3), Dialer (L2-L3, L3)

Example

To specify an interval of 15 seconds to wait before declaring a neighbor dead:

```
G450-001(if:Vlan 1)# ip ospf dead-interval 15
```

Related Commands

ip ospf authentication, ip ospf authentication-key, ip ospf cost, ip ospf hello-interval, ip ospf message-digest-key, ip ospf network point-to-multipoint, ip ospf priority, ip ospf router-id, router ospf, show ip ospf, show ip ospf database, show ip ospf interface, show ip ospf neighbor, show ip protocols

ip ospf hello-interval

Use the **ip ospf hello-interval** command to specify the time interval between hello packets the router sends. Use the **no** form of this command to set the hello-interval to its default value.

Syntax

ip ospf hello-interval *seconds*

no ip ospf hello-interval

Parameters

Parameter	Description	Possible Values	Default Value
seconds	The interval in seconds	**1-65535**	**10**

User Level

read-write

Context

interface:Serial (DS1 PPP L2-L3, DS1 PPP L3, DS1 FR-SUB L2-L3, DS1 FR-SUB L3, USP PPP L2-L3, USP PPP L3), FastEthernet (L2-L3, L3, PPP L2-L3, PPP L3), VLAN (L2-L3, L3), Loopback (L2-L3, L3), Tunnel (L2-L3, L3), Dialer (L2-L3, L3)

Example

To specify an interval of 5 seconds between hello packets:

```
G450-001(if:Vlan 1)# ip ospf hello-interval 5
```

Related Commands

ip ospf authentication, ip ospf authentication-key, ip ospf cost, ip ospf dead-interval, ip ospf message-digest-key, ip ospf network point-to-multipoint, ip ospf priority, ip ospf router-id, router ospf, show ip ospf, show ip ospf database, show ip ospf interface, show ip ospf neighbor, show ip protocols

ip ospf message-digest-key

Use the **ip ospf message-digest-key** command to specify the message-digest key for the interface. This command enables OSPF MD5 authentication. Use the **no** form of the command to remove an old MD5 key.

Syntax

ip ospf message-digest-key *key_id algorithm key*

no ip ospf message-digest-key *key_id*

Parameters

Parameter	Description	Possible Values	Default Value
key_id	The OSPF key ID	**1-255**	**10**
algorithm	The authentication algorithm	**md5**	
key	The OSPF password		

User Level

read-write

Context

interface:Serial (DS1 PPP L2-L3, DS1 PPP L3, DS1 FR-SUB L2-L3, DS1 FR-SUB L3, USP PPP L2-L3, USP PPP L3), FastEthernet (L2-L3, L3, PPP L2-L3, PPP L3), VLAN (L2-L3, L3), Loopback (L2-L3, L3), Tunnel (L2-L3, L3), Dialer (L2-L3, L3)

Example

To specify the message-digest key to be 3 with password mypwd:

```
G450-001(if:FastEthernet 10/2)# ip ospf message-digest-key 3 md5 mypwd
```

Related Commands

ip ospf authentication, ip ospf authentication-key, ip ospf cost, ip ospf dead-interval, ip ospf hello-interval, ip ospf network point-to-multipoint, ip ospf priority, ip ospf router-id, router ospf, show ip ospf, show ip ospf database, show ip ospf interface, show ip ospf neighbor, show ip protocols

ip ospf network point-to-multipoint

Use the **ip ospf network point-to-multipoint** command to specify the network type as point-to-multipoint for the interface, and to increase the OSPF timers appropriately. Use the **no** form of the command to return the interface to point-to-point topology.

Syntax

[no] ip ospf network point-to-multipoint

User Level

read-write

Context

interface:Serial (DS1 PPP L2-L3, DS1 PPP L3, DS1 FR-SUB L2-L3, DS1 FR-SUB L3, USP PPP L2-L3, USP PPP L3), FastEthernet (L2-L3, L3, PPP L2-L3, PPP L3), VLAN (L2-L3, L3), Loopback (L2-L3, L3), Tunnel (L2-L3, L3), Dialer (L2-L3, L3)

Example

To specify a network type of point-to-multipoint for the VLAN 1 interface:

```
G450-001(if:Vlan 1)# ip ospf network point-to-multipoint
```

Related Commands

ip ospf authentication, ip ospf authentication-key, ip ospf cost, ip ospf dead-interval, ip ospf hello-interval, ip ospf message-digest-key, ip ospf priority, ip ospf router-id, router ospf, show ip ospf, show ip ospf database, show ip ospf interface, show ip ospf neighbor, show ip protocols

ip ospf priority

Use the **ip ospf priority** command to configure interface priority, which is used during the election of a designated router. Use the **no** form of this command to set the OSPF priority to its default value.

Syntax

ip ospf priority *priority*

no ip ospf priority

Parameters

Parameter	Description	Possible Values	Default Value
priority	The interface priority	**0-255**	**1**

User Level

read-write

Context

interface:Serial (DS1 PPP L2-L3, DS1 PPP L3, DS1 FR-SUB L2-L3, DS1 FR-SUB L3, USP PPP L2-L3, USP PPP L3), FastEthernet (L2-L3, L3, PPP L2-L3, PPP L3), VLAN (L2-L3, L3), Loopback (L2-L3, L3), Tunnel (L2-L3, L3), Dialer (L2-L3, L3)

Example

To set the interface OSPF priority to 17:

```
G450-001(if:Vlan 1)# ip ospf priority 17
```

Related Commands

ip ospf authentication, ip ospf authentication-key, ip ospf cost, ip ospf dead-interval, ip ospf hello-interval, ip ospf message-digest-key, ip ospf network point-to-multipoint, ip ospf router-id, router ospf, show ip ospf, show ip ospf database, show ip ospf interface, show ip ospf neighbor, show ip protocols

ip ospf router-id

Use the **ip ospf router-id** command to configure the IP address of the router interface.

Syntax

ip ospf router-id *router_id*

Parameters

Parameter	Description	Possible Values	Default Value
router_id	The IP address of the router		lowest existing IP interface

User Level

read-write

Context

general

Example

To set the IP address of the router interface to 192.168.49.1:

```
G450-001(super)# ip ospf router-id 192.168.49.1
```

Related Commands

ip ospf authentication, ip ospf authentication-key, ip ospf cost, ip ospf dead-interval, ip ospf hello-interval, ip ospf message-digest-key, ip ospf network point-to-multipoint, ip ospf priority, router ospf, show ip ospf, show ip ospf database, show ip ospf interface, show ip ospf neighbor, show ip protocols

---

router ospf

Use the **router ospf** command to enable OSPF protocol on the system and to enter the router configuration context. Use the **no** form of this command to restore the default value, and disable OSPF globally.

Syntax

[no] router ospf

User Level

read-write

Context

general

Example

To enable OSPF protocol and enter the router configuration context:

```
G450-001(super)# router ospf
G450-001(super router:ospf)#
```

Related Commands

ip ospf authentication, ip ospf authentication-key, ip ospf cost, ip ospf dead-interval, ip ospf hello-interval, ip ospf message-digest-key, ip ospf network point-to-multipoint, ip ospf priority, ip ospf router-id, show ip ospf, show ip ospf database, show ip ospf interface, show ip ospf neighbor, show ip protocols

area

Use the **area** command to configure the area ID of a router. Use the **no** form of the command to delete the area ID.

Syntax

[no] area *area_id* [stub]

Parameters

Parameter	Description	Possible Values	Default Value
area_id	The IP address		
stub	Keyword indicating to configure a stub area		

User Level

read-write

Context

Router OSPF

Example

To configure an area for this OSPF interface with IP address 192.168.49.1:

```
G450-001(router:ospf)# area 192.168.49.1
```

To configure a stub area for this OSPF interface with IP address 176.1.13.12:

```
G450-001(router:ospf)# area 176.1.13.12 stub
```

To remove the area with IP address 192.168.49.1:

```
G450-001(router:ospf)# no area 192.168.49.1
```

Related Commands

default-metric (OSPF), network (OSPF), passive-interface, redistribute (OSPF), timers spf

default-metric (OSPF)

Use the **default-metric** command to set the default metric of redistributed routes for the OSPF protocol. Use the **no** form of this command to restore the default value.

Syntax

default-metric *default_metric*

no default-metric

Parameters

Parameter	Description	Possible Values	Default Value
default_metric	The default metric of redistributed routes	**1-65535**	**20**

User Level

read-write

Context

Router-OSPF

Example

To set the default metric for redistributed routes to 50:

```
G450-001(router:ospf)# default-metric 50
```

Related Commands

area, network (OSPF), passive-interface, redistribute (OSPF), timers spf

network (OSPF)

Use the **network** command to enable OSPF in this network. Use the **no** form of this command to disable OSPF in this network. The default value is disabled.

Syntax

network *net_addr* [*wildcard_mask* [area *area_id*]]

Parameters

Parameter	Description	Possible Values	Default Value
net_addr	The IP address		
wildcard_mask	The wildcard mask		
area	Keyword specifying an area		
area_id	The area ID number		

User Level

read-write

Context

Router: ospf

Example

To enable OPSF on the range of IP addresses from 192.168.0.0 to 192.168.255.255 in area ID 0.0.0.0:

```
G450-001(router:ospf)# network 192.168.0.0 0.0.255.255 area 0.0.0.0
```

Related Commands

area, default-metric (OSPF), passive-interface, redistribute (OSPF), timers spf

passive-interface

Use the **passive-interface** command to suppress OSPF routing updates on the interface.

Syntax

passive-interface {***interface_name*** | ***net_address***}

Parameters

Parameter	Description	Possible Values	Default Value
interface_name	Name of the interface on which to suppress routing updates		
net_address	IP address of the interface on which to suppress routing updates		

User Level

read-write

Context

Router: ospf

Example

To suppress OSPF routing updates on the FastEthernet interface:

```
G450-001(router:ospf)# passive-interface FastEthernet 10/2.1
```

To suppress OSPF routing updates on the interface at IP address 192.168.1.1:

```
G450-001(router:ospf)# passive-interface 192.168.1.1
```

Related Commands

area, default-metric (OSPF), network (OSPF), redistribute (OSPF), timers spf

redistribute (OSPF)

Use the **redistribute** command to redistribute routing information from other protocols into OSPF. Use the **no** form of this command to disable redistribution by OSPF.

Syntax

[no] redistribute ***protocol***

Parameters

Parameter	Description	Possible Values	Default Value
protocol	The protocol to be used	**static**, **connected**, **rip**	

User Level

read-write

Context

Router: ospf

Example

To redistribute static routing information into OSPF:

```
G450-001(router:ospf)# redistribute static
```

Related Commands - OSPF

area, default-metric (OSPF), network (OSPF), passive-interface, timers spf

Related Commands - Route redistribution

default-metric (interface route metric value)

---

timers spf

Use the **timers spf** command to configure the delay between SPF calculations when using OSPF. Use the **no** form of this command to restore the default value.

Syntax

timers spf ***spf_holdtime***

no timers spf

Parameters

Parameter	Description	Possible Values	Default Value
spf_holdtime	The time in seconds of the delay between SPF calculations	**1-3600**	**3**

User Level

read-write

Context

Router: ospf

Example

To set the SPF delay time to 5 seconds:

```
G450-001(router:ospf)# timers spf 5
```

Related Commands

area, default-metric (OSPF), network (OSPF), passive-interface, redistribute (OSPF)

show ip ospf

Use the **show ip ospf** command to display general information about OSPF routing.

Syntax

show ip ospf

User Level

read-only

Context

general

Example

To display IP OSPF routing information:

```
G450-001(super)# show ip ospf

Routing Process OSPF with ID 149.49.75.71
Number of areas in this router is 1
Area 0.0.0.0
Number of Interfaces in this area 0
SPF algorithm executed 1 times
SPF hold time is 3 sec
```

Related Commands

ip ospf authentication, ip ospf authentication-key, ip ospf cost, ip ospf dead-interval, ip ospf hello-interval, ip ospf message-digest-key, ip ospf network point-to-multipoint, ip ospf priority, ip ospf router-id, router ospf, show ip ospf database, show ip ospf interface, show ip ospf neighbor, show ip protocols

show ip ospf database

Use the **show ip ospf database** command to display lists of information related to the OSPF database for a specific router. If no router type is specified, OSPF information is displayed for all routers.

Syntax

show ip ospf database
[asbr-summary|router|network|network-summary|external]

Parameters

Parameter	Description	Possible Values	Default Value
asbr-summary	Keyword specifying to display information about the autonomous system boundary router summary LSAs		
router	Keyword specifying to display information about the router LSAs		
network	Keyword specifying to display information about the network LSAs		
network-summary	Keyword specifying to display information about the network LSAs summary		
external	Keyword specifying to display information about the external LSAs		

User Level

read-only

Context

general

Example

To display OSPF database information for all router types:

```
G450-001(super)# show ip ospf database
Showing 1 rows

Area      Type   LSA ID         Router ID      Sequence  Age   Cksm
-------  -----  ------------  -------------  --------- ----- ------
0.0.0.0   RTR   149.49.75.71   149.49.75.71  80000001  567   139b
```

Related Commands

ip ospf authentication, ip ospf authentication-key, ip ospf cost, ip ospf dead-interval, ip ospf hello-interval, ip ospf message-digest-key, ip ospf network point-to-multipoint, ip ospf priority, ip ospf router-id, router ospf, show ip ospf, show ip ospf interface, show ip ospf neighbor, show ip protocols

show ip ospf interface

Use the **show ip ospf interface** command to display OSPF-related interface information. If no interface name is specified, information for all interfaces is displayed.

Syntax

show ip ospf interface [*interface_name*]

Parameters

Parameter	Description	Possible Values	Default Value
interface_name	The OSPF interface name	string	

Note:

To specify an interface name that includes spaces, enclose the entire name in quotation marks (for example, “New York”).

User Level

read-only

Context

general

Example

To display OSPF information for all interfaces:

```
G450-001(super)# show ip ospf interface

sh ip ospf interface
Showing 1 OSPF Interfaces
Vlan 1.0 is up
Internet Address 1.1.1.1, Mask 255.255.255.0  , Area 0.0.0.0
AS Router ID 1.1.1.1, COST 1
Transmit Delay 1, State DR,  Priority 1
DRId 1.1.1.1, IpAddress 1.1.1.1
```

```
BDRId is 0.0.0.0, IpAddress 0.0.0.0
Timer Intervals Configured:
Hello 10
Dead 40
Retransmit 5
Neighbor count 0
```

Related Commands

ip ospf authentication, ip ospf authentication-key, ip ospf cost, ip ospf dead-interval, ip ospf hello-interval, ip ospf message-digest-key, ip ospf network point-to-multipoint, ip ospf priority, ip ospf router-id, router ospf, show ip ospf, show ip ospf database, show ip ospf neighbor, show ip protocols

show ip ospf neighbor

Use the **show ip ospf neighbor** command to display OSPF neighbor information for a specific interface. If no interface name is specified, information for all interfaces is displayed.

Syntax

show ip ospf neighbor [*interface_name*] [*neighbor_id*]

Parameters

Parameter	Description	Possible Values	Default Value
interface_name	The OSPF interface name	string	
neighbor_id	The OSPF neighbor ID number	an IP address	

Note:

To specify an interface name that includes spaces, enclose the entire name in quotation marks (for example, “New York”).

User Level

read-only

Context

general

Example

To display OSPF neighbor information for all interfaces:

```
G450-001(super)# show ip ospf neighbor
Nbr-Id           Priority   State      Router ID       Time To Live
--------------- ---------- ---------- --------------- -------------
10.0.17.2             1    2 Way      212.150.244.1          36
10.0.17.3            12    Full       10.0.17.3              38
10.0.17.6            18    Full       10.0.17.6              33
10.0.18.2             1    Full       105.1.12.1             107
10.0.20.2             0    Full       62.56.252.253          40
18.18.18.2            1    Full       62.56.255.254          38
192.168.6.173         0    Full       172.18.21.254           4
```

Related Commands

ip ospf authentication, ip ospf authentication-key, ip ospf cost, ip ospf dead-interval, ip ospf hello-interval, ip ospf message-digest-key, ip ospf network point-to-multipoint, ip ospf priority, ip ospf router-id, router ospf, show ip ospf, show ip ospf database, show ip ospf interface, show ip protocols

show ip protocols

Use the **`show ip protocols`** command to display parameters and statistics of a given IP routing protocol. If no protocol is specified, all running protocols are displayed.

Syntax

`show ip protocols [`*`protocol`*`]`

Parameters

Parameter	Description	Possible Values	Default Value
`protocol`	The protocol for which to display statistics	**RIP, OSPF**	

User Level

read-only

Context

general

Example

To display all running protocol details:

```
G450-001(super)# show ip protocols
```

To display RIP details:

```
G450-001(super)# show ip protocols RIP

Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 0 seconds
Invalid after 180 seconds, flushed after 300
Redistributing: rip
Default version control: rip version 1
Interface                        Version   Key
Routing for Networks:
Routing Information Sources:
Gateway                 Last Update
```

Related Commands - OSPF

ip ospf authentication, ip ospf authentication-key, ip ospf cost, ip ospf dead-interval, ip ospf hello-interval, ip ospf message-digest-key, ip ospf network point-to-multipoint, ip ospf priority, ip ospf router-id, router ospf, show ip ospf, show ip ospf database, show ip ospf interface, show ip ospf neighbor

Related Commands - RIP

ip distribution access-list, ip rip authentication key, ip rip authentication mode, ip rip default-route-mode, ip rip poison-reverse, ip rip rip-version, ip rip send-receive-mode, ip rip split-horizon, router rip

Packet sniffing

capture buffer-mode

Use the **capture buffer-mode** command to specify the type of buffer used by the packet sniffer.

Syntax

capture buffer-mode {non_cyclic | cyclic}

Parameters

Parameter	Description	Possible Values	Default Value
non_cyclic	Keyword specifying a linear buffer that is used until it is filled up		
cyclic	Keyword specifying a circular buffer that overwrites the oldest records when it is filled up. Use a cyclic buffer to store the most recent history of packet activity.		

User Level

read-write

Context

general

Example

To specify that the packet sniffer uses cyclic buffer-mode:

```
G450-001(super)# capture buffer-mode cyclic
```

Related Commands

capture buffer-size, capture filter-group, capture interface, capture ipsec, capture max-frame-size, capture-service, capture start, capture stop, capture-service, clear capture-buffer, ip capture-list, name, show capture, show capture-buffer hex

capture buffer-size

Use the **capture buffer-size** command to specify the maximum size of the packet sniffing buffer.

Note:

To activate the change in buffer size, you must run copy running-config startup-config, and reboot the device.

Syntax

capture buffer-size *buffer_size*

Parameters

Parameter	Description	Possible Values	Default Value
buffer_size	The maximum size of the packet sniffing buffer in Kbytes	**256-10000**	**1000**

User Level

read-write

Context

general

Example

To specify the maximum size of the packet sniffing buffer as 2000 Kbytes:

```
G450-001(super)# capture buffer-size 2000
```

Related Commands

capture buffer-mode, capture filter-group, capture interface, capture ipsec, capture max-frame-size, capture start, capture stop, capture-service, clear capture-buffer, ip capture-list, name, show capture, show capture-buffer hex

capture filter-group

Use the **capture filter-group** command to apply the specified filter to the packet sniffer. When a capture filter is applied, packets must match the criteria for a rule whose action is 'capture' in order to be saved to the buffer.

Syntax

capture filter-group ***capture_list_id***

Parameters

Parameter	Description	Possible Values	Default Value
capture_list_id	The capture list number to apply	**500-599**	

User Level

read-write

Context

general

Example

To apply filter group 501 to the packet sniffer:

```
G450-001(super)# capture filter-group 501
```

Related Commands

capture buffer-mode, capture buffer-size, capture interface, capture ipsec, capture max-frame-size, capture start, capture stop, capture-service, clear capture-buffer, ip capture-list, name, show capture, show capture-buffer hex

capture interface

Use the **capture interface** command to specify the interface on which to run the packet sniffing service. Use the **no** form of the command to run packet sniffing on all routing interfaces.

Syntax

capture interface *interface_name*

no capture interface

Parameters

Parameter	Description	Possible Values	Default Value
interface_name	The name of the interface on which to run packet sniffing. If the interface name contains spaces, it must be enclosed in quotes.		

User Level

read-write

Context

general

Example

To specify that the packet sniffing service run on interface FastEthernet 10/2:

```
G450-001(super)# capture interface FastEthernet 10/2
```

Related Commands

capture buffer-mode, capture buffer-size, capture filter-group, capture ipsec, capture max-frame-size, capture start, capture stop, capture-service, clear capture-buffer, ip capture-list, name, show capture, show capture-buffer hex

capture ipsec

Use the **capture ipsec** command to set whether to capture IPSec VPN packets, handled by the internal VPN process, decrypted (plaintext) or encrypted (cyphertext).

Syntax

capture ipsec {cyphertext | plaintext}

no capture ipsec

Parameters

Parameter	Description	Possible Values	Default Value
cyphertext	Keyword specifying to capture IPSec VPN packets encrypted (default)		
plaintext	Keyword specifying to capture IPSec VPN packets decrypted		

User Level

read-write

Context

general

Related Commands

capture buffer-mode, capture buffer-size, capture filter-group, capture interface, capture max-frame-size, capture start, capture stop, capture-service, clear capture-buffer, ip capture-list, name, show capture, show capture-buffer hex

capture max-frame-size

Use the **capture max-frame-size** command to specify the maximum number of bytes captured for each packet by the packet sniffer.

Syntax

capture max-frame-size *max_frame_size*

no capture max-frame-size

Parameters

Parameter	Description	Possible Values	Default Value
max_frame_size	The maximum number of bytes captured for each packet by the packet sniffer	**14-4096**	**128**

User Level

read-write

Context

general

Example

To specify the maximum number of bytes captured for each packet by the packet sniffer as 68 bytes:

```
G450-001(super)# capture max-frame-size 68
```

Related Commands

capture buffer-mode, capture buffer-size, capture filter-group, capture interface, capture ipsec, capture start, capture stop, capture-service, clear capture-buffer, ip capture-list, name, show capture, show capture-buffer hex

capture start

Use the **capture start** command to start the packet sniffing service.

Note:

The capture start command resets the buffer before starting the sniffer.

Note:
In order to upload a capture file, you must first stop the packet sniffing service.

Syntax

capture start

User Level

read-write

Context

general

Examples

If the packet sniffing service has been enabled by the administrator:

```
G450-001(super)# capture start
Starting the packet sniffing process
```

If the packet sniffing service has not been enabled by the administrator:

```
G450-001(super)# capture start
The sniffing service is not available.
To re-enable, use the 'capture-service' command in supervisor mode.
```

Related Commands

capture buffer-mode, capture buffer-size, capture filter-group, capture interface, capture ipsec, capture max-frame-size, capture stop, capture-service, clear capture-buffer, ip capture-list, name, show capture, show capture-buffer hex

capture stop

Use the **capture stop** command to stop the packet sniffing service.

Note:
This command is not saved in the startup configuration file.

Note:
In order to upload a capture file, you must first stop the packet sniffing service.

Syntax

capture stop

User Level

read-write

Context

general

Examples

If the packet sniffing service has been enabled by the administrator:

```
G450-001(super)# capture stop
110 packets captured.
```

If the packet sniffing service has not been enabled by the administrator:

```
G450-001(super)# capture stop
The Packet sniffing process is not running.
```

Related Commands

capture buffer-mode, capture buffer-size, capture filter-group, capture interface, capture ipsec, capture max-frame-size, capture start, capture-service, clear capture-buffer, ip capture-list, name, show capture, show capture-buffer hex

---

capture-service

Use the **capture-service** command to enable the packet sniffing service. Use the **no** form of the command to disable the packet sniffing service. By disabling the service, the administrator can prevent users with read-write access from starting packet sniffing.

Note:

This command can only be executed by an admin user connected via the Console port.

Syntax

[no] capture-service

User Level

admin

Context

general

Example

To enable packet sniffing:

```
G450-001(super)# capture-service
Packet sniffing service enabled
```

To disable packet sniffing:

```
G450-001(super)# no capture-service
Packet sniffing service disabled
```

Related Commands

capture buffer-mode, capture buffer-size, capture filter-group, capture interface, capture ipsec, capture max-frame-size, capture start, capture stop, clear capture-buffer, ip capture-list, name, show capture, show capture-buffer hex

---

clear capture-buffer

Use the **clear capture-buffer** command to clear the packet sniffing buffer.

Syntax

clear capture-buffer

User Level

read-write

Context

general

Example

To clear the packet sniffing buffer:

```
G450-001(super)# clear capture-buffer
```

Related Commands

capture buffer-mode, capture buffer-size, capture filter-group, capture interface, capture ipsec, capture max-frame-size, capture start, capture stop, capture-service, ip capture-list, name, show capture, show capture-buffer hex

copy capture-file ftp

Use the **copy capture-file ftp** command to upload the packet sniffing buffer to a file using the ftp protocol.

Note:

You must stop the packet sniffing service using the **capture stop** command before you can upload the buffer.

Syntax

copy capture-file ftp *filename ip*

Parameters

Parameter	Description	Possible Values	Default Value
filename	The file name on the FTP server		
ip	The IP address of the FTP server		

User Level

read-write

Context

general

Example

To upload the packet sniffing buffer to `g450.cap` on the FTP server at IP address 135.64.10.33:

```
G450-001(super)# copy capture-file ftp g450.cap 135.64.10.33
```

Related Commands

composite-operation, cookie, copy capture-file scp, copy capture-file tftp, copy announcement-file usb, ip-rule (policy, policy-based routing, packet sniffing), owner, show ip capture-list, show upload status

copy capture-file scp

Use the **copy capture-file scp** command to upload the packet sniffing buffer to a file using the scp secure file transfer protocol.

Note:

You must stop the packet sniffing service using the **capture stop** command before you can upload the buffer.

Syntax

copy capture-file scp *filename ip*

Parameters

Parameter	Description	Possible Values	Default Value
filename	The file name on the FTP server		
ip	The IP address of the FTP server		

User Level

read-write

Context

general

Example

To upload the packet sniffing buffer to `g450.cap` on the FTP server at IP address 135.64.10.33:

```
G450-001(super)# copy capture-file scp g450.cap 135.64.10.33
```

Related Commands

composite-operation, cookie, copy capture-file ftp, copy capture-file tftp, copy announcement-file usb, ip-rule (policy, policy-based routing, packet sniffing), owner, show ip capture-list, show upload status

copy capture-file tftp

Use the **copy capture-file tftp** command to upload the packet sniffing buffer to a file using the tftp protocol.

Note:

You must stop the packet sniffing service using the **capture stop** command before you can upload the buffer.

Syntax

copy capture-file tftp *filename ip*

Parameters

Parameter	Description	Possible Values	Default Value
filename	The file name on the TFTP server		
ip	The IP address of the TFTP server		

User Level

read-write

Context

general

Example

To upload the packet sniffing buffer to `g450.cap` on the TFTP server at IP address 135.64.10.33:

```
G450-001(super)# copy capture-file tftp g450.cap 135.64.10.33
```

Related Commands

composite-operation, cookie, copy capture-file ftp, copy capture-file scp, copy announcement-file usb, ip-rule (policy, policy-based routing, packet sniffing), owner, show ip capture-list, show upload status

copy capture-file usb

Use the **copy capture-file usb** command to upload the packet sniffing buffer from the gateway to the USB mass storage device.

Syntax

copy capture-file usb ***source-filename destination-usb-device*** [***destination-filename***]

Parameters

Parameter	Description	Possible Values	Default Value
source-filename	The logical name for the source file		
destination usb-device	The destination USB mass storage device	**usb-device0**	
destination-filename	The destination file name and path		

User Level

admin

Context

general

Example

To upload `g450.cap` from the gateway to usb-device0:

```
G450-001(super)# copy capture-file usb g450.cap usb-device0
```

Related Commands

backup config usb, copy usb announcement-file, erase usb, restore usb, safe-removal usb, show backup status, show restore status, show usb

ip capture-list

Use the **ip capture-list** command to enter the specified capture-list context. If the specified capture-list does not exist, it is created.

Syntax

ip capture-list capture_list_id

no ip capture-list capture_list_id

Parameters

Parameter	Description	Possible Values	Default Value
capture_list_id	The capture list number	**500-599**	

User Level

read-write

Context

general

Example

To enter the capture-list 501 context:

```
G450-001(super)# ip capture-list 501
G450-001(super-Cap 501)#
```

Related Commands

capture buffer-mode, capture buffer-size, capture filter-group, capture interface, capture ipsec, capture max-frame-size, capture start, capture stop, capture-service, clear capture-buffer, name, show capture, show capture-buffer hex

cookie

Use the **cookie** command to set the cookie for the current list.

Syntax

cookie *cookie_number*

Parameters

Parameter	Description	Possible Values	Default Value
cookie_number	The ID number of the cookie	**0-268435455**	

User Level

read-write

Context

ip access-control-list, ip qos-list, ip capture-list, ip pbr-list, ip crypto-list

Example

To specify the cookie for QoS list 440 as 257:

```
G450-001(QoS 440)# cookie 257
```

Related Commands - Packet sniffing

composite-operation, copy capture-file ftp, copy capture-file scp, copy capture-file tftp, ip-rule (policy, policy-based routing, packet sniffing), owner, show ip capture-list, show upload status

Related Commands - Policy

composite-operation, dscp-table, ip-fragments-in, ip-option-in, ip-rule (policy, policy-based routing, packet sniffing), name, owner, show composite-operation, show isdn bri link, show list

ip-rule (policy, policy-based routing, packet sniffing)

Use the **ip-rule** command to enter configuration mode for the specified rule. If the specified rule does not exist, the system creates it and enters its configuration mode.

Syntax

ip-rule {***rule_index*** | **default**}

Parameters

Parameter	Description	Possible Values	Default Value
rule_index	Number of the rule to edit	**1-9999**	
default	Keyword indicating ip-rule number 10,000 (last rule in the ordered list of rules)		

User Level

read-write

Context

ip access-control-list, ip qos-list, ip capture-list, ip pbr-list

Example

To enter configuration mode for ip-rule 22:

```
G450-001(ACL 330)# ip-rule 22
G450-001(ACL 330/ip rule 22)#
```

Related Commands - Packet sniffing

composite-operation, cookie, copy capture-file ftp, copy capture-file scp, copy capture-file tftp, owner, show ip capture-list, show upload status

Related Commands - Policy-based routing

name, owner, show isdn bri link, show list

Related Commands - Policy

composite-operation, cookie, dscp-table, ip-fragments-in, ip-option-in, name, owner, show composite-operation, show isdn bri link, show list

composite-operation

Use the **composite-operation** command to edit the specified composite operation. If the composite operation does not exist, it is created.

Syntax

composite-operation ***index***

Parameters

Parameter	Description	Possible Values	Default Value
index	The composite operation number	**12-19**	

User Level

read-write

Context

ip access-control-list/ip-rule, ip capture-list/ip-rule, ip qos-list, ip qos-list/dscp-table, ip qos-list/ip-rule

Example

To enter configuration mode for composite operation 13:

```
G450-001(QoS 440)# composite-operation 13
G450-001(QoS 440/CompOp 13)#
```

Related Commands - Packet sniffing

cookie, copy capture-file ftp, copy capture-file scp, copy capture-file tftp, ip-rule (policy, policy-based routing, packet sniffing), owner, show ip capture-list, show upload status

Related Commands - Policy

cookie, destination-ip, dscp (policy), dscp-table, icmp, ip-rule (policy, policy-based routing, packet sniffing), name, owner, show composite-operation, show dscp-table, show isdn bri link, show list, source-ip, tcp destination-port, tcp established, tcp source-port, udp destination-port, udp source-port

destination-ip

Use the **destination-ip** command to specify the destination IP address of packets to which the current rule applies.

Use the **not** form of the command to specify that the current rule applies to all packets that *do not* have this destination IP address.

Use the **no** form of the command to set the destination IP address to `any`.

Syntax

[not] destination-ip {host *ip*}|any|{*ip wildcard*}

no destination-ip

Parameters

Parameter	Description	Possible Values	Default Value
host	Keyword that specifies the current rule applies to a single host IP address		
ip	The destination IP address of the rule		
any	Keyword that specifies the current rule applies to any address		
ip wildcard	The range of IP addresses of the rule. The zero bits in the wildcard correspond to bits in the IP address that remain fixed. The one bits in the wildcard correspond to bits in the IP address that can vary. **Note:** This is the opposite of how bits are used in a netmask.		

User Level

read-write

Context

ip capture-list/ip-rule, ip access-control-list/ip-rule, ip pbr-list/ip-rule, ip qos-list/ip-rule, ip crypto-list ip-rule

Example

To specify that rule 22 applies to all packets having destination IP address 135.64.104.102:

```
G450-001(QoS 460/rule 22)# destination-ip host 135.64.104.102
```

To specify that rule 17 applies to packets whose destination IP address is *not* in the range of 176.13.0.0 through 176.13.255.255:

```
G450-001(QoS 460/rule 17)# not destination-ip 176.13.0.0 0.0.255.255
```

Related Commands - Packet sniffing

dscp (policy-based routing, packet sniffing, VPN), icmp, ip-protocol, show ip capture-list, source-ip, tcp destination-port, tcp source-port, udp destination-port, udp source-port

Related Commands - Policy-based routing

dscp (policy-based routing, packet sniffing, VPN), next-hop (policy-based routing), show ip next-hop-list, show isdn bri link

Related Commands - Policy

composite-operation, dscp (policy), show dscp-table, icmp, show composite-operation, show isdn bri link, source-ip, tcp destination-port, tcp established, tcp source-port, udp destination-port, udp source-port

Related Commands - VPN

description (ip rule), ip crypto-list, ip-rule (VPN), local-address, protect crypto map, source-ip, show ip crypto-list

dscp (policy-based routing, packet sniffing, VPN)

Use the **dscp** command to specify the DSCP value that is set by the current policy operation.

Use the **not** form of the command to specify that the current operation set any DSCP value other than requested value.

Use the **no** form of the command to specify that the current operation set the DSCP value to any.

Note:

In crypto-lists, this command is only applicable for rules whose action is **no protect**.

Syntax

dscp {*dscp_value* | any}

not dscp *dscp_value*

no dscp

Parameters

Parameter	Description	Possible Values	Default Value
dscp_value	The DSCP value	**0-63**	
any	Keyword indicating that any DSCP value will match the rule. Using this keyword is equivalent to specifying **no dscp**.		

User Level

read-write

Context

ip capture-list ip-rule, ip pbr-list ip-rule, ip access-control-list ip-rule, ip qos-list ip-rule, ip crypto-list ip-rule

Note:

In ip-rule context, this command tests packets to see if they match the specified DSCP value, but does not change the DSCP value.

Note:

The **not** form of the command is not relevant in the crypto-list ip-rule context.

Example

To specify that ip-rule 10 in crypto-list 901 match a DSCP value of 43:

```
G450-001(Crypto 901/ip rule 10)# dscp 43
```

To specify that ip-rule 10 in crypto-list 901 match any DSCP value:

```
G450-001(Crypto 901/ip rule 10)# no dscp
```

Related Commands - Packet sniffing

destination-ip, icmp, ip-protocol, show ip capture-list, source-ip, tcp destination-port, tcp source-port, udp destination-port, udp source-port

Related Commands - Policy-based routing

destination-ip, next-hop (policy-based routing), show ip next-hop-list, show isdn bri link

Related Commands - VPN

description (ip rule), destination-ip, fragment, icmp, ip crypto-list, ip-protocol, ip-rule (VPN), local-address, protect crypto map, source-ip, show ip crypto-list, tcp destination-port, tcp source-port, udp destination-port, udp source-port

fragment

Use the **fragment** command to apply the current rule for non-initial fragments only.

Note:

You cannot specify TCP/UDP ports or ICMP code/type for a rule when using the **fragment** command.

Syntax

fragment

User Level

read-write

Context

ip qos-list composite-operation, ip capture-list ip-rule, ip pbr-list ip-rule, ip access-control-list ip-rule, ip qos-list ip-rule, ip crypto-list ip-rule

Example

To apply the rule for non-initial fragments:

```
G450-001(super-Capture 520/ip rule 15)# fragment
```

Related Commands - Packet sniffing

dscp (policy-based routing, packet sniffing, VPN), destination-ip, icmp, ip-protocol, show ip capture-list, source-ip, tcp destination-port, tcp source-port, udp destination-port, udp source-port

Related Commands - Policy-based routing

dscp (policy-based routing, packet sniffing, VPN), destination-ip, next-hop (policy-based routing), show ip next-hop-list, show isdn bri link

Related Commands - Policy

composite-operation, dscp (policy), destination-ip, icmp, show composite-operation, show isdn bri link, source-ip, tcp destination-port, tcp established, tcp source-port, udp destination-port, udp source-port, cos, name

Related Commands - VPN

description (ip rule), destination-ip, dscp (policy-based routing, packet sniffing, VPN), icmp, ip crypto-list, ip-protocol, ip-rule (VPN), local-address, protect crypto map, source-ip, show ip crypto-list, tcp destination-port, tcp source-port, udp destination-port, udp source-port

---

icmp

Use the **icmp** command to specify that the current rule applies to a specific type of ICMP packet.

Use the **not** form of this command to specify that the rule applies to all packets *except* those of the requested ICMP attribute. If the IP protocol is not ICMP, it is set to ICMP.

Use the **no** form of the command to specify that the current rule applies to any type of ICMP packet.

Note:

The **icmp** command also sets the IP protocol to ICMP.

Syntax

[not] icmp {*name* | {*icmp_type icmp_code*}}

no icmp

Parameters

Parameter	Description	Possible Values	Default Value
name	Specify that the rule applies to this ICMP name		
icmp_type	Specify that the rule applies to this icmp type	For an ip-rule: **0-256** For a QoS rule: **0-65535**	
icmp_code	Specify that the rule applies to this icmp code	For an ip-rule: **0-256** For a QoS rule: **0-65535**	

User Level

read-write

Context

ip capture-list/ip-rule, ip access-control-list/ip-rule, ip pbr-list/ip-rule, ip qos-list/ip-rule, ip crypto-list ip-rule

Note:

The **not** form of the command is not relevant in the crypto-list ip-rule context.

Example

To specify that rule 27 applies to ICMP error-reply packets:

```
G450-001(ACL 333/ip rule 27)# icmp Echo-Reply
```

To specify that rule 33 applies to any ICMP packet type *except* type 1 code 2:

```
G450-001(ACL 333/ip rule 33)# not icmp 1 2
```

Related Commands - Policy-based routing

destination-ip, dscp (policy-based routing, packet sniffing, VPN), ip-protocol, show ip capture-list, source-ip, tcp destination-port, tcp source-port, udp destination-port, udp source-port

Related Commands - Policy

composite-operation, cookie, destination-ip, dscp (policy), dscp-table, icmp, ip-rule (policy, policy-based routing, packet sniffing), owner, show composite-operation, show dscp-table, show isdn bri link, show list, source-ip, tcp destination-port, tcp established, tcp source-port, udp destination-port, udp source-port

Related Commands - VPN

description (ip rule), destination-ip, dscp (policy-based routing, packet sniffing, VPN), fragment, ip crypto-list, ip-protocol, ip-rule (VPN), local-address, protect crypto map, source-ip, show ip crypto-list, tcp destination-port, tcp source-port, udp destination-port, udp source-port

---

ip-protocol

Use the **ip-protocol** command to specify that the current rule applies to packets having the specified IP protocol.

Use the **no** form of the command to set the IP protocol to its default value.

Use the **not** form of this command to specify that the current rule applies to all packets *except* those having the specified IP protocol.

Syntax

[not] ip-protocol *protocol_name* | *protocol_number*

no ip-protocol

Parameters

Parameter	Description	Possible Values	Default Value
protocol_name	Name of the IP protocol to match		
protocol_number	Number of the IP protocol to match	**1-255**	

User Level

read-write

Context

ip access-control-list/ip-rule, ip capture-list/ip-rule, ip pbr-list/ip-rule, ip qos-list/ip-rule, crypto-list/ip-rule

Note:

The **not** form of the command is not relevant in the crypto-list/ip-rule context.

Example

To specify that rule 22 applies to all packets having an IP protocol of ICMP:

```
G450-001(ACL 330/ip rule 22)# ip-protocol icmp
```

To specify that rule 22 applies to all packets having any IP protocol *except* ICMP:

```
G450-001(ACL 330/ip rule 22)# not ip-protocol icmp
```

Related Commands

destination-ip, dscp (policy-based routing, packet sniffing, VPN), icmp, show ip capture-list, source-ip, tcp destination-port, tcp source-port, udp destination-port, udp source-port

Related Commands - VPN

description (ip rule), destination-ip, dscp (policy-based routing, packet sniffing, VPN), fragment, icmp, ip crypto-list, ip-rule (VPN), local-address, protect crypto map, source-ip, show ip crypto-list, tcp destination-port, tcp source-port, udp destination-port, udp source-port

show ip-rule

Use the **show ip-rule** command to display the attributes of a specific rule. Leave the ***rule_number*** parameter blank to display all rules.

Syntax

show ip-rule [*rule_number*]

Parameters

Parameter	Description	Possible Values	Default Value
rule_number	The specific rule for which attributes are displayed		

User Level

read-write

Context

ip access-control-list, ip access-control-list/ip-rule, ip qos-list, ip qos-list/ip-rule, ip capture-list, ip capture-list/ip-rule, ip pbr-list, ip pbr-list/ip-rule

Example

To display information about ip rule 22 in access-control-list 320:

```
G450-001(ACL 320/ip rule 22)# show ip-rule 22

I.D.  Protocol IP  Wildcard         Port      Operation
----- -------- --- ---------------- --------- ----------
22    Ip       Src                  Any       permit
               Dst                  Any
```

Following is an example of the output that appears if DoS-classification is configured:

```
Index    Protocol      IP                Wildcard   Port       Operation
         DSCP                                                  Fragment rule
-----    ------  ---  ---------   -------------- ------ --------------
123      Any     Src  1.2.3.4         Host          Any          Permit
         Any     Dst  Any                           Any          No

Dos classification: other-attack
234      Any     Src  2.2.2.2         Host          Any          Permit
         Any     Dst  Any                           Any          No

Dos classification: fraggle
345      Any     Src  3.3.3.3         Host          Any          Permit
         Any     Dst  Any                           Any          No

Dos classification: ip-spoofing
Deflt    Any     Src  Any                           Any          Permit
         Any     Dst  Any                           Any          No
```

Related Commands - Policy-based routing: ip pbr-list

destination-ip, dscp (policy-based routing, packet sniffing, VPN), next-hop (policy-based routing), show ip next-hop-list

Related Commands - Policy-based routing: ip pbr-list: ip-rule

ip-rule (policy, policy-based routing, packet sniffing), name, owner, show list

Related Commands - Policy

composite-operation, cookie, dscp-table, ip-fragments-in, ip-option-in, ip-rule (policy, policy-based routing, packet sniffing), name, owner, show composite-operation, show dscp-table, show isdn bri link, show list, composite-operation, destination-ip, dscp (policy), icmp, source-ip, tcp destination-port, tcp established, tcp source-port, udp destination-port, udp source-port

Related Commands - DoS

DoS-classification, show ip access-control-list

source-ip

Use the **source-ip** command to indicate that the current rule applies to packets from the specified source IP address.

Use the **no** form of the command to indicate that the current rule applies to packets from any IP address.

Use the **not** form of the command to indicate that the current rule applies to all packets *except* those coming from the specified IP address.

Syntax

[not] source-ip {host *ip_address* | any | *ip_address wildcard*}

no source-ip

Parameters

Parameter	Description	Possible Values	Default Value
host	Keyword that indicates a specific host IP address		
ip_address	The IP address of the host		
any	Keyword that indicates any IP address		
ip_address ***wildcard***	The range of IP addresses of the rule. The zero bits in the wildcard correspond to bits in the IP address that remain fixed. The one bits in the wildcard correspond to bits in the IP address that can vary. **Note:** This is the opposite of how bits are used in a netmask.		

User Level

read-write

Context

ip pbr-list ip-rule, ip qos-list ip-rule, ip capture-list ip-rule, ip access-control-list ip-rule, ip crypto-list ip-rule

Note:

The **not** form of the command is not relevant in the crypto-list ip-rule context.

Example

To specify that rule 22 of QoS policy list 460 applies to any packet coming from IP address 135.64.104.102:

```
G450-001(QoS 460/rule 22)# source-ip host 135.64.104.102
```

To specify that rule 22 of QoS policy list 460 applies to any packet *except* those coming from IP address 135.64.104.102:

```
G450-001(QoS 460/rule 22)# not source-ip host 135.64.104.102
```

Related Commands - Policy-based routing

destination-ip, dscp (policy-based routing, packet sniffing, VPN), icmp, ip-protocol, show ip capture-list, tcp destination-port, tcp source-port, udp destination-port, udp source-port

Related Commands - Policy

composite-operation, destination-ip, dscp (policy), icmp, show composite-operation, show dscp-table, show isdn bri link, tcp destination-port, tcp established, tcp source-port, udp destination-port, udp source-port

Related Commands - VPN

description (ip rule), destination-ip, ip crypto-list, ip-rule (VPN), local-address, protect crypto map, show ip crypto-list

---

tcp destination-port

Use the **tcp destination-port** command to define a destination port with the TCP protocol for which to apply the current rule.

Use the **no** form of the command to set the TCP destination port to `any`. If the protocol is not TCP, the protocol is set to TCP and the source port is set to its default value.

Use the **not** form of the command to specify that the rule applies to all TCP ports other than the requested ports. If the protocol is not TCP, the protocol is set to TCP and the source port is set to its default value

Note:

Issuing this command also sets the protocol to be TCP, if it is not already.

Syntax

[not] tcp destination-port any | {{eq | lt | gt} {*port_name* | *port_number*}} | {range *start_port end_port*}

no tcp destination-port

Parameters

Parameter	Description	Possible Values	Default Value
any	Keyword that specifies to apply the rule to a port with any name or number		
eq	Keyword that specifies to apply the rule to a port whose name or number matches exactly to the specified name or number		
lt	Keyword that specifies to apply the rule to a port whose name or number is less than the specified name or number		
gt	Keyword that specifies to apply the rule to a port whose name or number is greater than the specified name or number		
port_name	The name of the port for which to apply the rule		
port_number	The number of the port for which to apply the rule		
range	Keyword indicating that a range of ports is specified		
start_port	The start of a port range for which to apply the rule		
end_port	The end of a port range for which to apply the rule		

User Level

read-write

Context

ip pbr-list ip-rule, ip capture-list ip-rule, ip qos-list ip-rule, ip access-control-list ip-rule, crypto-list ip-rule

Note:

The **not** form of the command is not relevant in the crypto-list ip-rule context.

Example

To specify that rule 22 applies to all packets whose destination port is 300:

```
G450-001(ACL 330/ip rule 22)# tcp destination-port eq 300
```

To specify that rule 22 applies to all packets *except* for those whose destination port is 300:

```
G450-001(ACL 330/ip rule 22)# not tcp destination-port eq 300
```

Related Commands - Policy-based routing

destination-ip, dscp (policy-based routing, packet sniffing, VPN), icmp, ip-protocol, show ip capture-list, source-ip, tcp source-port, udp destination-port, udp source-port

Related Commands - Policy

composite-operation, destination-ip, dscp (policy), icmp, show composite-operation, show dscp-table, show isdn bri link, source-ip, tcp established, tcp source-port, udp destination-port, udp source-port

Related Commands - VPN

description (ip rule), destination-ip, dscp (policy-based routing, packet sniffing, VPN), fragment, icmp, ip crypto-list, ip-protocol, ip-rule (VPN), local-address, protect crypto map, source-ip, show ip crypto-list, tcp source-port, udp destination-port, udp source-port

---

tcp source-port

Use the **tcp source-port** command to define a source port with the TCP protocol for which to apply the current rule.

Use the **no** form of the command to set the TCP source port to any. If the protocol is not TCP, the protocol is set to TCP and the destination port is set to its default value.

Use the **not** form of the command to specify that the rule applies to all TCP ports other than the requested ports. If the protocol is not TCP, the protocol is set to TCP and the destination port is set to its default value

Note:

Issuing this command also sets the protocol to be TCP, if it is not already.

Syntax

[not] tcp source-port any | {{eq | lt | gt} {*port_name* | *port_number*}} | {range *start_port end_port*}

no tcp source-port

Parameters

Parameter	Description	Possible Values	Default Value
any	Keyword that specifies to apply the rule to a port with any name or number		
eq	Keyword that specifies to apply the rule to a port whose name or number matches exactly to the specified name or number		
lt	Keyword that specifies to apply the rule to a port whose name or number is less than the specified name or number		
gt	Keyword that specifies to apply the rule to a port whose name or number is greater than the specified name or number		
port_name	The name of the port for which to apply the rule		
port_number	The number of the port for which to apply the rule		
range	Keyword indicating that a range of ports is specified		
start_port	The start of a port range for which to apply the rule		
end_port	The end of a port range for which to apply the rule		

User Level

read-write

Context

ip pbr-list ip-rule, ip capture-list ip-rule, ip qos-list ip-rule, ip access-control-list ip-rule, ip crypto-list ip-rule

Note:

The **not** form of the command is not relevant in the crypto-list ip-rule context.

Example

To specify that rule 22 applies to all packets whose source port is greater than port 95:

```
G450-001(ACL 330/ip rule 22)# tcp source-port gt 95
```

To specify that rule 22 applies to all packets whose source port is less than or equal to port 95:

```
G450-001(ACL 330/ip rule 22)# not tcp source-port gt 95
```

Related Commands - Policy-based routing

destination-ip, dscp (policy-based routing, packet sniffing, VPN), icmp, ip-protocol, show ip capture-list, source-ip, tcp destination-port, udp destination-port, udp source-port

Related Commands - Policy

composite-operation, destination-ip, dscp (policy), icmp, show composite-operation, show dscp-table, show isdn bri link, source-ip, tcp destination-port, tcp established, udp destination-port, udp source-port

Related Commands - VPN

description (ip rule), destination-ip, dscp (policy-based routing, packet sniffing, VPN), fragment, icmp, ip crypto-list, ip-protocol, ip-rule (VPN), local-address, protect crypto map, source-ip, show ip crypto-list, tcp destination-port, udp destination-port, udp source-port

udp destination-port

Use the **udp destination-port** command to define a destination port with the UDP protocol for which to apply the current rule.

Use the **no** form of the command to set the UDP destination port to any. If the protocol is not UDP, the protocol is set to UDP and the source port is set to its default value.

Use the **not** form of the command to specify that the rule applies to all UDP ports other than the requested ports. If the protocol is not UDP, the protocol is set to UDP and the source port is set to its default value

Note:

Issuing this command also sets the protocol to be UDP, if it is not already.

Syntax

udp destination-port any | {{eq | lt | gt} {*port_name* | *port_number*}} | {range *start_port end_port}*

no udp destination-port

Parameters

Parameter	Description	Possible Values	Default Value
any	Keyword that specifies to apply the rule to a port with any name or number		
eq	Keyword that specifies to apply the rule to a port whose name or number matches exactly to the specified name or number		
lt	Keyword that specifies to apply the rule to a port whose name or number is less than the specified name or number		
gt	Keyword that specifies to apply the rule to a port whose name or number is greater than the specified name or number		
port_name	The name of the port for which to apply the rule		
port_number	The number of the port for which to apply the rule		
range	Keyword indicating that a range of ports is specified		
start_port	The start of a port range for which to apply the rule		
end_port	The end of a port range for which to apply the rule		

User Level

read-write

Context

ip pbr-list ip-rule, ip qos-list ip-rule, ip capture-list ip-rule, ip access-control-list ip-rule, ip crypto-list ip-rule

Note:

The **not** form of the command is not relevant in the crypto-list ip-rule context.

Example

To specify that rule 22 applies to all packets whose destination port is port 300:

```
G450-001(ACL 330/ip rule 22)# udp destination-port eq 300
```

To specify that rule 22 applies to all packets *except* for those whose destination port is 300:

```
G450-001(ACL 330/ip rule 22)# not udp destination-port eq 300
```

Related Commands - Policy-based routing

destination-ip, dscp (policy-based routing, packet sniffing, VPN), icmp, ip-protocol, show ip capture-list, source-ip, tcp destination-port, tcp source-port, udp source-port

Related Commands - Policy

composite-operation, destination-ip, dscp (policy), icmp, show composite-operation, show dscp-table, show isdn bri link, source-ip, tcp destination-port, tcp established, tcp source-port, udp source-port

Related Commands - VPN

description (ip rule), destination-ip, dscp (policy-based routing, packet sniffing, VPN), fragment, icmp, ip crypto-list, ip-protocol, ip-rule (VPN), local-address, protect crypto map, source-ip, show ip crypto-list, tcp destination-port, tcp source-port, udp source-port

udp source-port

Use the **udp source-port** command to define a source port with the UDP protocol for which to apply the current rule.

Use the **no** form of the command to set the UDP source port to any. If the protocol is not UDP, the protocol is set to UDP and the destination port is set to its default value.

Use the **not** form of the command to specify that the rule applies to all UDP ports other than the requested ports. If the protocol is not UDP, the protocol is set to UDP and the destination port is set to its default value

Note:

Issuing this command also sets the protocol to be UDP, if it is not already.

Syntax

udp source-port any | {{eq | lt | gt} {*port_name* | *port_number*}} | {range *start_port end_port*}

no udp source-port

Parameters

Parameter	Description	Possible Values	Default Value
any	Keyword that specifies to apply the rule to a port with any name or number		
eq	Keyword that specifies to apply the rule to a port whose name or number matches exactly to the specified name or number		
lt	Keyword that specifies to apply the rule to a port whose name or number is less than the specified name or number		
gt	Keyword that specifies to apply the rule to a port whose name or number is greater than the specified name or number		
port_name	The name of the port for which to apply the rule		
port_number	The number of the port for which to apply the rule		
range	Keyword indicating that a range of ports is specified		
start_port	The start of a port range for which to apply the rule		
end_port	The end of a port range for which to apply the rule		

User Level

read-write

Context

ip pbr-list ip-rule, ip qos-list ip-rule, ip capture-list ip-rule, ip access-control-list ip-rule, ip crypto-list ip-rule

Note:

The **not** form of the command is not relevant in the crypto-list ip-rule context.

Example

To specify that rule 22 applies to all packets whose source port is greater than port 95:

```
G450-001(ACL 330/ip rule 22)# udp source-port gt 95
```

To specify that rule 22 applies to all packets whose source port is less than or equal to port 95:

```
G450-001(ACL 330/ip rule 22)# not udp source-port gt 95
```

Related Commands - Policy-based routing

destination-ip, dscp (policy-based routing, packet sniffing, VPN), icmp, ip-protocol, show ip capture-list, source-ip, tcp destination-port, tcp source-port, udp destination-port

Related Commands - Policy

composite-operation, destination-ip, dscp (policy), icmp, show composite-operation, show dscp-table, show isdn bri link, source-ip, tcp destination-port, tcp established, tcp source-port, udp destination-port

Related Commands - VPN

description (ip rule), destination-ip, dscp (policy-based routing, packet sniffing, VPN), fragment, icmp, ip crypto-list, ip-protocol, ip-rule (VPN), local-address, protect crypto map, source-ip, show ip crypto-list, tcp destination-port, tcp source-port, udp destination-port

name

Use the **name** command to assign a name to the specified list or operation. Use the **no** form of the command to return the name to the default value.

Syntax

[no] name *name*

Parameters

Parameter	Description	Possible Values	Default Value
name	The name of the list or operation. **Note:** If you wish to include spaces in the description, you must enclose the string in quotation marks (“”).	String of 1-31 characters	

User Level

read-write

Context

dhcp pool, dhcp pool vendor specific, dhcp pool option, ip qos-list, ip qos-list dscp-table, ip qos-list composite-operation, ip access-control-list, ip next-hop-list, ip capture-list, ip pbr-list, ip crypto-list.

Example

To specify the name of access control list 330 as “Admin13”:

```
G450-001(ACL 330)# name Admin13
```

Related Commands - DHCP server

bootfile, client-identifier, default-router, dns-server, domain-name, end-ip-addr, lease, next-server, option, server-name, show ip dhcp-pool, start-ip-addr, subnet-mask, value, vendor-specific-option

Related Commands - Packet sniffing

capture buffer-mode, capture buffer-size, capture filter-group, capture interface, capture max-frame-size, capture start, capture stop, capture-service, clear capture-buffer, ip capture-list, show capture, show capture-buffer hex

Related Commands - Policy-based routing

ip-rule (policy, policy-based routing, packet sniffing), owner, show isdn bri link, show list

Related Commands - Policy

composite-operation, cookie, ip-fragments-in, ip-option-in, ip-rule (policy, policy-based routing, packet sniffing), owner, show composite-operation, show dscp-table, show isdn bri link, show list, cos, dscp (policy)

---

owner

Use the **owner** command to specify the owner of the current list.

Syntax

owner *owner_name*

Parameters

Parameter	Description	Possible Values	Default Value
owner_name	Name of the owner	string	

User Level

read-write

Context

ip access-control-list, ip qos-list, ip capture-list, ip pbr-list, ip crypto-list

Example

To set the owner of access control list 330 as MGAdmin3:

```
G450-001(ACL 330)# owner MGAdmin3
```

Related Commands - Packet sniffing

composite-operation, cookie, copy capture-file ftp, copy capture-file scp, copy capture-file tftp, ip-rule (policy, policy-based routing, packet sniffing), show ip capture-list, show upload status

Related Commands - Policy-based routing

ip-rule (policy, policy-based routing, packet sniffing), name, show isdn bri link, show list

Related Commands - Policy

composite-operation, cookie, dscp-table, ip-fragments-in, ip-option-in, ip-rule (policy, policy-based routing, packet sniffing), name, show composite-operation, show isdn bri link, show list

show capture

Use the **`show capture`** command to display information about the currently configured settings for the packet sniffing service.

Note:

Timestamps in the capture file are based on the capture start time that is displayed in the output of the show capture command.

Syntax

`show capture`

User Level

read-only

Context

general

Example

To display information about the currently configured packet sniffing service settings:

```
G450-001(super)# show capture
The sniffing service is enabled
Capturing started at:
21:22:01, February 21, 2003 / 7,9:55:55 (uptime)
stopped at: not-stopped
Buffer size: 1000 KB
Buffer mode is cyclic
Maximum number of bytes captured from
each frame: 128
Packet filter: Capture List 503
Number of frames in buffer: 200
Size of capture file: 50 KB (5%)
```

Related Commands

capture buffer-mode, capture buffer-size, capture filter-group, capture interface, capture ipsec, capture max-frame-size, capture start, capture stop, capture-service, clear capture-buffer, ip capture-list, name, show capture-buffer hex

show capture-buffer hex

Use the **show capture-buffer hex** command to display the contents of the packet sniffing buffer as a hex dump.

Syntax

show capture-buffer hex [frame_id]

Parameters

Parameter	Description	Possible Values	Default Value
frame_id	The ID of the first packet to display in the output		

User Level

read-only

Context

general

Example

To display the contents of the packet sniffing buffer as a hex dump, starting with frame 5:

```
G450-001(super)# show capture-buffer hex 5
Frame number: 5
Frame time: 01/01/1970-23:45:09.10001
Time relative to first frame: 0, 0:0:3.021141
Frame Length: 68 bytes (0x44)
Capture Length: 68 bytes (0x44)
00000: d4c3 b2a1 0200 0400 0000 0000 0000 0000 ................
00010: ffff 0000 0100 0000 348c 913e e5df 0e00 ........4..>....
00020: 2800 0000 2800 0000 2053 454e 4401 2053 (...(... SEND. S
00030: 454e 4401 c021 0100 001a 0506 0b87 16c2 END..!..........
00040: 0d03 0611 ....
Frame number: 6
Frame time: 01/01/1970-23:45:09.100012
Time relative to first frame: 0, 0:0:3.021142
Frame Length: 256 bytes (0x44)
Capture Length: 128 bytes (0x80)
0000000: d4c3 b2a1 0200 0400 0000 0000 0000 0000 ................
0000010: ffff 0000 0100 0000 ea71 8e3e e6ed 0b00 .........q.>....
0000020: e300 0000 e300 0000 ffff ffff ffff 0010 ................
0000030: a498 97ab 0800 4500 00d5 3a7d 0000 8011 ......E...:}....
0000040: ea9a 0a00 0002 0a00 00ff 008a 008a 00c1 ................
--type q to quit or space key to continue--
```

Note:

The right side of the hex dump is the octets converted to characters using ascii code. Octets smaller than 32 or greater than 126 are displayed as a dot (.).

Related Commands

capture buffer-mode, capture buffer-size, capture filter-group, capture interface, capture ipsec, capture max-frame-size, capture start, capture stop, capture-service, clear capture-buffer, ip capture-list, name, show capture

show ip capture-list

Use the **show ip capture-list** command to display details about capture lists.

Syntax

show ip capture-list { *list-number* | all } [detailed]

Parameters

Parameter	Description	Possible Values	Default Value
list_number	The capture list to view	**800-899**	

User Level

read-only

Context

general

Example

To display information about all capture lists:

```
G450-001(super)# show ip capture-list all

Index   Name                    Owner
-------------------------------------
500      Default Capture List    other
501     list #5021            other
```

Related Commands - Packet sniffing: ip capture-list

composite-operation, cookie, copy capture-file ftp, copy capture-file scp, copy capture-file tftp, ip-rule (policy, policy-based routing, packet sniffing), owner, show upload status

Related Commands - Packet sniffing: ip capture-list: ip-rule

destination-ip, dscp (policy-based routing, packet sniffing, VPN), icmp, ip-protocol, show ip capture-list, source-ip, tcp destination-port, tcp source-port, udp destination-port, udp source-port

Password management

Platform information

show platform fans

Use the **show platform fans** command to display information on the fan tray unit.

Syntax

show platform fans

User Level

admin

Context

general

Example

To display information on the fan tray unit:

```
G450-001(super)# show platform fans

FAN TRAY UNIT #1:
------------------------------------------------
Type            : G450 FAN TRAY
Description     : G450 FAN TRAY UNIT
Serial Number   : xxxxxxxxxxxx
HW Vintage      : 1
HW Suffix       : A
Faults          : No Fault Messages
```

Related Commands

show platform power, show platform mainboard

show platform power

Use the **show platform power** command to display the power supply configuration and parameters.

Syntax

show platform power

User Level

admin

Context

general

Example

To display the power supply configuration parameters:

```
G450-001(super)# show platform power
POWER SUPPLY UNIT #1:
------------------------------------------------
Type            : G450 PSU
Description     : G450 FR Power Supply 350W
Serial Number   : xxxxxxxxxxxx
HW Vintage      : 0
HW Suffix       : A
Faults          : No Fault Messages

POWER SUPPLY UNIT #2:
------------------------------------------------
Type            : G450 PSU
Description     : G450 FR Power Supply 350W
Serial Number   : xxxxxxxxxxxx
HW Vintage      : 0
HW Suffix       : A
Faults          : No Fault Messages
```

Related Commands

show platform fans, show platform mainboard

show platform mainboard

Use the **show platform mainboard** command to display the main board parameters and the list of media gateway equipment installed in the sockets on the main board.

Syntax

show platform mainboard

User Level

admin

Context

general

Example

To display the main board parameters and the media gateway equipment list:

```
G450-001(super)# show platform mainboard
MAINBOARD BOARD:
------------------------------------------------
Type           : G450 mainboard
Description    : G450 field replaceable mainboard
Serial Number  : xxxxxxxxxxxx
HW Vintage     : 0
HW Suffix      : A
FW Version     : 1
Faults         : No Fault Messages

MEMORY SOCKET #1:
------------------------------------------------
Type           : DDR SDRAM module
Description    : DDR SDRAM memory with ECC
Serial Number  : xxxxxxxxxxxx
HW Vintage     : 0
Faults         : No Fault Messages

MEMORY SOCKET #2:
------------------------------------------------
Type           : UNKNOWN
Description    : UNKNOWN
Serial Number  : UNKNOWN
HW Vintage     : UNKNOWN
Faults         : NOT PRESENT

MEDIA SOCKET #1:
Type           : MP80 VoIP DSP Module
Description    : VoIP DSP resource with 80 channels
Serial Number  : xxxxxxxxxxxx
HW Vintage     : 0
HW Suffix      : A
Faults         : No Fault Messages

MEDIA SOCKET #2:
Type           : UNKNOWN
Description    : UNKNOWN
Serial Number  : UNKNOWN
HW Vintage     : UNKNOWN
HW Suffix      : UNKNOWN
Faults         :  Not Installed

MEDIA SOCKET #3:
Type           : UNKNOWN
Description    : UNKNOWN
Serial Number  : UNKNOWN
HW Vintage     : UNKNOWN
```

```
HW Suffix       : UNKNOWN
Faults          : Not Installed

MEDIA SOCKET #4:
Type            : MP20 VoIP DSP Module
Description     : VoIP DSP resource with 20 voice channels
Serial Number   : xxxxxxxxxxxx
HW Vintage      : 0
HW Suffix       : A
Faults          : No Fault Messages

FPGA SOCKET:
Type            : UNKNOWN
Description     : UNKNOWN
Serial Number   : UNKNOWN
HW Vintage      : UNKNOWN
HW Suffix       : UNKNOWN
FW Version      : UNKNOWN
Faults          : Not Installed
```

Related Commands

show platform fans, show platform power

PMI

pmi

Use the **pmi** command to define this interface as the Primary Management Interface for the system.

Syntax

pmi

User Level

read-write

Context

interface:Serial (DS1 PPP L2-L3, DS1 PPP L3, DS1 FR-SUB L2-L3, DS1 FR-SUB L3, USP PPP L3, USP PPP L2-L3), FastEthernet (L2-L3, L3), VLAN (L2-L3, L3), Loopback (L2-L3, L3), Tunnel (L2-L3, L3), Dialer (L2-L3, L3)

Example

To define the VLAN 1 interface as the Primary Management Interface:

```
G450-001(super)# interface vlan 1
G450-001(super-if:Vlan 1)# pmi
```

Related Commands

show pmi

---

show pmi

Use the **show pmi** command to view the current Primary Management Interface.

Syntax

show pmi

User Level

read-only

Context

general

Example

To view information about the current PMI:

```
G450-001(super)# show pmi
Active PMI     : interface Vlan 1 (172.16.1.139)
Configured PMI : interface Vlan 1 (172.16.1.139)
```

Related Commands

pmi

Policy - access control lists

ip access-control-list

Use the **ip access-control-list** command to enter configuration mode for the specified policy access control list. If the specified list does not exist, the system creates it and enters its configuration mode. Use the **no** form of the command to delete an access control list.

Syntax

[no] ip access-control-list *list_number*

Parameters

Parameter	Description	Possible Values	Default Value
list_number	The Access Control list number	**300-399**	**300**

User Level

read-write

Context

general

Example

To create access control list 320 and enter its configuration mode:

```
G450-001(super)# ip access-control-list 320
G450-001(ACL 320)#
```

Related Commands

ip access-group, ip policy-list-copy, ip qos-group, ip qos-list, ip simulate, pre-classification, show ip access-control-list, show ip qos-list

cookie

Use the **cookie** command to set the cookie for the current list.

Syntax

cookie *cookie_number*

Parameters

Parameter	Description	Possible Values	Default Value
cookie_number	The ID number of the cookie	**0-268435455**	

User Level

read-write

Context

ip access-control-list, ip qos-list, ip capture-list, ip pbr-list, ip crypto-list

Example

To specify the cookie for QoS list 440 as 257:

```
G450-001(QoS 440)# cookie 257
```

Related Commands - Packet sniffing

composite-operation, copy capture-file ftp, copy capture-file scp, copy capture-file tftp, ip-rule (policy, policy-based routing, packet sniffing), owner, show ip capture-list, show upload status

Related Commands - Policy

composite-operation, dscp-table, ip-fragments-in, ip-option-in, ip-rule (policy, policy-based routing, packet sniffing), name, owner, show composite-operation, show isdn bri link, show list

ip-fragments-in

Use the **ip-fragments-in** command to specify the action taken on incoming IP fragmentation packets for the current access control list. Use the **no** form of the command to return to the default treatment of IP fragmentation packets.

Syntax

ip-fragments-in ***operation***

no ip-fragments-in

Parameters

Parameter	Description	Possible Values	Default Value
operation	The name of the pre-defined composite operation to execute	**Deny**, **Deny-Notify-Rst**, **Permit, Deny-Notify**, **Deny-Rst**	

User Level

read-write

Context

ip access-control-list

Example

To execute the Deny-Notify composite-operation when IP fragmentation packets are received:

```
G450-001(ACL 330)# ip-fragments-in Deny-Notify
```

Related Commands

cookie, ip-option-in, ip-rule (policy, policy-based routing, packet sniffing), name, owner, show composite-operation, show isdn bri link, show list

ip-option-in

Use the **ip-option-in** command to specify the action taken on packets carrying an IP option, for the current access control list. Use the **no** form of the command to return to the default treatment of IP option packets.

Syntax

ip-option-in ***action***

no ip-option-in

Parameters

Parameter	Description	Possible Values	Default Value
action	The action to take	**permit**, **deny**, **deny-notify, deny-rst**, **deny-notify-rst**	

User Level

read-write

Context

ip access-control-list

Example

To specify that incoming packets with an IP option are permitted:

```
G450-001(ACL 330)# ip-option-in permit
```

Related Commands

cookie, ip-fragments-in, ip-rule (policy, policy-based routing, packet sniffing), name, owner, show composite-operation, show isdn bri link, show list

ip-rule (policy, policy-based routing, packet sniffing)

Use the **ip-rule** command to enter configuration mode for the specified rule. If the specified rule does not exist, the system creates it and enters its configuration mode.

Syntax

ip-rule {***rule_index*** | **default**}

Parameters

Parameter	Description	Possible Values	Default Value
rule_index	Number of the rule to edit	**1-9999**	
default	Keyword indicating ip-rule number 10,000 (last rule in the ordered list of rules)		

User Level

read-write

Context

ip access-control-list, ip qos-list, ip capture-list, ip pbr-list

Example

To enter configuration mode for ip-rule 22:

```
G450-001(ACL 330)# ip-rule 22
G450-001(ACL 330/ip rule 22)#
```

Related Commands - Packet sniffing

composite-operation, cookie, copy capture-file ftp, copy capture-file scp, copy capture-file tftp, owner, show ip capture-list, show upload status

Related Commands - Policy-based routing

name, owner, show isdn bri link, show list

Related Commands - Policy

composite-operation, cookie, dscp-table, ip-fragments-in, ip-option-in, name, owner, show composite-operation, show isdn bri link, show list

composite-operation

Use the **composite-operation** command to edit the specified composite operation. If the composite operation does not exist, it is created.

Syntax

composite-operation ***index***

Parameters

Parameter	Description	Possible Values	Default Value
index	The composite operation number	**12-19**	

User Level

read-write

Context

ip access-control-list/ip-rule, ip capture-list/ip-rule, ip qos-list, ip qos-list/dscp-table, ip qos-list/ip-rule

Example

To enter configuration mode for composite operation 13:

```
G450-001(QoS 440)# composite-operation 13
G450-001(QoS 440/CompOp 13)#
```

Related Commands - Packet sniffing

cookie, copy capture-file ftp, copy capture-file scp, copy capture-file tftp, ip-rule (policy, policy-based routing, packet sniffing), owner, show ip capture-list, show upload status

Related Commands - Policy

cookie, destination-ip, dscp (policy), dscp-table, icmp, ip-rule (policy, policy-based routing, packet sniffing), name, owner, show composite-operation, show dscp-table, show isdn bri link, show list, source-ip, tcp destination-port, tcp established, tcp source-port, udp destination-port, udp source-port

destination-ip

Use the **destination-ip** command to specify the destination IP address of packets to which the current rule applies.

Use the **not** form of the command to specify that the current rule applies to all packets that *do not* have this destination IP address.

Use the **no** form of the command to set the destination IP address to `any`.

Syntax

[not] destination-ip {host *ip*}|any**|{*ip wildcard*}**

no destination-ip

Parameters

Parameter	Description	Possible Values	Default Value
host	Keyword that specifies the current rule applies to a single host IP address		
ip	The destination IP address of the rule		
any	Keyword that specifies the current rule applies to any address		
ip wildcard	The range of IP addresses of the rule. The zero bits in the wildcard correspond to bits in the IP address that remain fixed. The one bits in the wildcard correspond to bits in the IP address that can vary. **Note:** This is the opposite of how bits are used in a netmask.		

User Level

read-write

Context

ip capture-list/ip-rule, ip access-control-list/ip-rule, ip pbr-list/ip-rule, ip qos-list/ip-rule, ip crypto-list ip-rule

Example

To specify that rule 22 applies to all packets having destination IP address 135.64.104.102:

```
G450-001(QoS 460/rule 22)# destination-ip host 135.64.104.102
```

To specify that rule 17 applies to packets whose destination IP address is *not* in the range of 176.13.0.0 through 176.13.255.255:

```
G450-001(QoS 460/rule 17)# not destination-ip 176.13.0.0 0.0.255.255
```

Related Commands - Packet sniffing

dscp (policy-based routing, packet sniffing, VPN), icmp, ip-protocol, show ip capture-list, source-ip, tcp destination-port, tcp source-port, udp destination-port, udp source-port

Related Commands - Policy-based routing

dscp (policy-based routing, packet sniffing, VPN), next-hop (policy-based routing), show ip next-hop-list, show isdn bri link

Related Commands - Policy

composite-operation, dscp (policy), show dscp-table, icmp, show composite-operation, show isdn bri link, source-ip, tcp destination-port, tcp established, tcp source-port, udp destination-port, udp source-port

Related Commands - VPN

description (ip rule), ip crypto-list, ip-rule (VPN), local-address, protect crypto map, source-ip, show ip crypto-list

---

dscp (policy)

Use the **dscp** command to specify the DSCP value that is set by the current policy operation.

Use the **not** form of the command to specify that the current operation set any DSCP value other than requested value.

Use the **no** form of the command to specify that the current operation set the DSCP value to no-change.

Syntax

dscp {*dscp_value* | no-change}

not dscp *dscp_value*

no dscp

Parameters

Parameter	Description	Possible Values	Default Value
dscp_value	The DSCP value	**0-63**	
no-change	Keyword indicating that the DSCP value is left unchanged		

User Level

read-write

Context

ip qos-list composite-operation

Example

To specify that composite operation 17 sets the DSCP value of packets to 55:

```
G450-001(QoS 440/CompOp 17)# dscp 55
```

To specify that composite operation 17 sets the DSCP value of packets to a value other than 55:

```
G450-001(QoS 440/CompOp 17)# not dscp 55
```

Related Commands - Policy

composite-operation, destination-ip, icmp, show composite-operation, show isdn bri link, source-ip, tcp destination-port, tcp established, tcp source-port, udp destination-port, udp source-port, cos, name

---

fragment

Use the **fragment** command to apply the current rule for non-initial fragments only.

Note:

You cannot specify TCP/UDP ports or ICMP code/type for a rule when using the **fragment** command.

Syntax

fragment

User Level

read-write

Context

ip qos-list composite-operation, ip capture-list ip-rule, ip pbr-list ip-rule, ip access-control-list ip-rule, ip qos-list ip-rule, ip crypto-list ip-rule

Example

To apply the rule for non-initial fragments:

```
G450-001(super-Capture 520/ip rule 15)# fragment
```

Related Commands - Packet sniffing

dscp (policy-based routing, packet sniffing, VPN), destination-ip, icmp, ip-protocol, show ip capture-list, source-ip, tcp destination-port, tcp source-port, udp destination-port, udp source-port

Related Commands - Policy-based routing

dscp (policy-based routing, packet sniffing, VPN), destination-ip, next-hop (policy-based routing), show ip next-hop-list, show isdn bri link

Related Commands - Policy

composite-operation, dscp (policy), destination-ip, icmp, show composite-operation, show isdn bri link, source-ip, tcp destination-port, tcp established, tcp source-port, udp destination-port, udp source-port, cos, name

Related Commands - VPN

description (ip rule), destination-ip, dscp (policy-based routing, packet sniffing, VPN), icmp, ip crypto-list, ip-protocol, ip-rule (VPN), local-address, protect crypto map, source-ip, show ip crypto-list, tcp destination-port, tcp source-port, udp destination-port, udp source-port

icmp

Use the **icmp** command to specify that the current rule applies to a specific type of ICMP packet.

Use the **not** form of this command to specify that the rule applies to all packets *except* those of the requested ICMP attribute. If the IP protocol is not ICMP, it is set to ICMP.

Use the **no** form of the command to specify that the current rule applies to any type of ICMP packet.

Note:

The **icmp** command also sets the IP protocol to ICMP.

Syntax

[not] icmp {*name* | {*icmp_type icmp_code*}}

no icmp

Parameters

Parameter	Description	Possible Values	Default Value
name	Specify that the rule applies to this ICMP name		

Parameter	Description	Possible Values	Default Value
icmp_type	Specify that the rule applies to this icmp type	For an ip-rule: **0-256** For a QoS rule: **0-65535**	
icmp_code	Specify that the rule applies to this icmp code	For an ip-rule: **0-256** For a QoS rule: **0-65535**	

User Level

read-write

Context

ip capture-list/ip-rule, ip access-control-list/ip-rule, ip pbr-list/ip-rule, ip qos-list/ip-rule, ip crypto-list ip-rule

Note:

The **not** form of the command is not relevant in the crypto-list ip-rule context.

Example

To specify that rule 27 applies to ICMP error-reply packets:

```
G450-001(ACL 333/ip rule 27)# icmp Echo-Reply
```

To specify that rule 33 applies to any ICMP packet type *except* type 1 code 2:

```
G450-001(ACL 333/ip rule 33)# not icmp 1 2
```

Related Commands - Policy-based routing

destination-ip, dscp (policy-based routing, packet sniffing, VPN), ip-protocol, show ip capture-list, source-ip, tcp destination-port, tcp source-port, udp destination-port, udp source-port

Related Commands - Policy

composite-operation, cookie, destination-ip, dscp (policy), dscp-table, icmp, ip-rule (policy, policy-based routing, packet sniffing), owner, show composite-operation, show dscp-table, show isdn bri link, show list, source-ip, tcp destination-port, tcp established, tcp source-port, udp destination-port, udp source-port

Related Commands - VPN

description (ip rule), destination-ip, dscp (policy-based routing, packet sniffing, VPN), fragment, ip crypto-list, ip-protocol, ip-rule (VPN), local-address, protect crypto map, source-ip, show ip crypto-list, tcp destination-port, tcp source-port, udp destination-port, udp source-port

ip-protocol

Use the **ip-protocol** command to specify that the current rule applies to packets having the specified IP protocol.

Use the **no** form of the command to set the IP protocol to its default value.

Use the **not** form of this command to specify that the current rule applies to all packets *except* those having the specified IP protocol.

Syntax

[not] ip-protocol *protocol_name* | *protocol_number*

no ip-protocol

Parameters

Parameter	Description	Possible Values	Default Value
protocol_name	Name of the IP protocol to match		
protocol_number	Number of the IP protocol to match	**1-255**	

User Level

read-write

Context

ip access-control-list/ip-rule, ip capture-list/ip-rule, ip pbr-list/ip-rule, ip qos-list/ip-rule, crypto-list/ip-rule

Note:

The not form of the command is not relevant in the crypto-list/ip-rule context.

Example

To specify that rule 22 applies to all packets having an IP protocol of ICMP:

```
G450-001(ACL 330/ip rule 22)# ip-protocol icmp
```

To specify that rule 22 applies to all packets having any IP protocol *except* ICMP:

```
G450-001(ACL 330/ip rule 22)# not ip-protocol icmp
```

Related Commands - Packet sniffing

destination-ip, dscp (policy-based routing, packet sniffing, VPN), icmp, show ip capture-list, source-ip, tcp destination-port, tcp source-port, udp destination-port, udp source-port

Related Commands - VPN

description (ip rule), destination-ip, dscp (policy-based routing, packet sniffing, VPN), fragment, icmp, ip crypto-list, ip-rule (VPN), local-address, protect crypto map, source-ip, show ip crypto-list, tcp destination-port, tcp source-port, udp destination-port, udp source-port

show composite-operation

Use the **show composite-operation** command to display information about a specific composite-operation. Use the command without a parameter to display information about all composite-operations.

Syntax

show composite-operation [*composite_operation_index*]

Parameters

Parameter	Description	Possible Values	Default Value
composite_operation_index	The composite-operation to display	**0-19**	

User Level

read-write

Context

ip access-control-list, ip access-control-list ip-rule, ip qos-list, ip qos-list ip-rule, ip qos-list composite-operation

Example

To display information about composite-operation 13:

```
G450-001(QoS 440)# show composite-operation 13

Index Name                  CoS       DSCP      Trust
----- -------------------- --------- --------- ------------
13    HSPackets             cos3      1         No
```

Related Commands

composite-operation, cookie, destination-ip, dscp (policy), dscp-table, icmp, ip-rule (policy, policy-based routing, packet sniffing), show composite-operation, show dscp-table, show isdn bri link, show list, source-ip, tcp destination-port, tcp established, tcp source-port, udp destination-port, udp source-port, cos, dscp (policy-based routing, packet sniffing, VPN), name

show ip-rule

Use the **show ip-rule** command to display the attributes of a specific rule. Leave the ***rule_number*** parameter blank to display all rules.

Syntax

show ip-rule [*rule_number*]

Parameters

Parameter	Description	Possible Values	Default Value
rule_number	The specific rule for which attributes are displayed		

User Level

read-write

Context

ip access-control-list, ip access-control-list/ip-rule, ip qos-list, ip qos-list/ip-rule, ip capture-list, ip capture-list/ip-rule, ip pbr-list, ip pbr-list/ip-rule

Example

To display information about ip rule 22 in access-control-list 320:

```
G450-001(ACL 320/ip rule 22)# show ip-rule 22

I.D.  Protocol IP  Wildcard         Port      Operation
----- -------- --- ---------------- --------- ----------
22    Ip       Src                  Any       permit
               Dst                  Any
```

Following is an example of the output that appears if DoS-classification is configured:

```
Index    Protocol      IP          Wildcard        Port   Operation
         DSCP                                             Fragment rule
-----    ------  ---  ---------   -------------- ------ --------------
123      Any     Src  1.2.3.4         Host           Any          Permit
         Any     Dst  Any                            Any          No

Dos classification: other-attack
234      Any     Src  2.2.2.2         Host           Any          Permit
         Any     Dst  Any                            Any          No

Dos classification: fraggle
345      Any     Src  3.3.3.3         Host           Any          Permit
         Any     Dst  Any                            Any          No

Dos classification: ip-spoofing
Deflt    Any     Src  Any                            Any          Permit
         Any     Dst  Any                            Any          No
```

Related Commands - Policy-based routing: ip pbr-list

destination-ip, dscp (policy-based routing, packet sniffing, VPN), next-hop (policy-based routing), show ip next-hop-list

Related Commands - Policy-based routing: ip pbr-list: ip-rule

ip-rule (policy, policy-based routing, packet sniffing), name, owner, show list

Related Commands - Policy

composite-operation, cookie, dscp-table, ip-fragments-in, ip-option-in, ip-rule (policy, policy-based routing, packet sniffing), name, owner, show composite-operation, show dscp-table, show isdn bri link, show list, composite-operation, destination-ip, dscp (policy), icmp, source-ip, tcp destination-port, tcp established, tcp source-port, udp destination-port, udp source-port

Related Commands - DoS

DoS-classification, show ip access-control-list

source-ip

Use the **source-ip** command to indicate that the current rule applies to packets from the specified source IP address.

Use the **no** form of the command to indicate that the current rule applies to packets from any IP address.

Use the **not** form of the command to indicate that the current rule applies to all packets *except* those coming from the specified IP address.

Syntax

[not] source-ip {host *ip_address* | any | *ip_address wildcard*}

no source-ip

Parameters

Parameter	Description	Possible Values	Default Value
host	Keyword that indicates a specific host IP address		
ip_address	The IP address of packets to which the rule is applied		
any	Keyword that indicates any IP address		
ip_address ***wildcard***	The range of IP addresses of the rule. The zero bits in the wildcard correspond to bits in the IP address that remain fixed. The one bits in the wildcard correspond to bits in the IP address that can vary. **Note:** This is the opposite of how bits are used in a netmask.		

User Level

read-write

Context

ip pbr-list ip-rule, ip qos-list ip-rule, ip capture-list ip-rule, ip access-control-list ip-rule, ip crypto-list ip-rule

Note:

The **not** form of the command is not relevant in the crypto-list ip-rule context.

Example

To specify that rule 22 of QoS policy list 460 applies to any packet coming from IP address 135.64.104.102:

```
G450-001(QoS 460/rule 22)# source-ip host 135.64.104.102
```

To specify that rule 22 of QoS policy list 460 applies to any packet *except* those coming from IP address 135.64.104.102:

```
G450-001(QoS 460/rule 22)# not source-ip host 135.64.104.102
```

Related Commands - Policy-based routing

destination-ip, dscp (policy-based routing, packet sniffing, VPN), icmp, ip-protocol, show ip capture-list, tcp destination-port, tcp source-port, udp destination-port, udp source-port

Related Commands - Policy

composite-operation, destination-ip, dscp (policy), icmp, show composite-operation, show dscp-table, show isdn bri link, tcp destination-port, tcp established, tcp source-port, udp destination-port, udp source-port

Related Commands - VPN

description (ip rule), destination-ip, ip crypto-list, ip-rule (VPN), local-address, protect crypto map, show ip crypto-list

---

tcp destination-port

Use the **`tcp destination-port`** command to define a destination port with the TCP protocol for which to apply the current rule.

Use the **`no`** form of the command to set the TCP destination port to `any`. If the protocol is not TCP, the protocol is set to TCP and the source port is set to its default value.

Use the **`not`** form of the command to specify that the rule applies to all TCP ports other than the requested ports. If the protocol is not TCP, the protocol is set to TCP and the source port is set to its default value

Note:

Issuing this command also sets the protocol to be TCP, if it is not already.

Syntax

`[not] tcp destination-port any | {{eq | lt | gt} {`*`port_name`* **`|` *`port_number`***`}} | {range`** *`start_port end_port`***`}`**

`no tcp destination-port`

Parameters

Parameter	Description	Possible Values	Default Value
any	Keyword that specifies to apply the rule to a port with any name or number		
eq	Keyword that specifies to apply the rule to a port whose name or number matches exactly to the specified name or number		
lt	Keyword that specifies to apply the rule to a port whose name or number is less than the specified name or number		
gt	Keyword that specifies to apply the rule to a port whose name or number is greater than the specified name or number		
port_name	The name of the port for which to apply the rule		
port_number	The number of the port for which to apply the rule		
range	Keyword indicating that a range of ports is specified		
start_port	The start of a port range for which to apply the rule		
end_port	The end of a port range for which to apply the rule		

User Level

read-write

Context

ip pbr-list ip-rule, ip capture-list ip-rule, ip qos-list ip-rule, ip access-control-list ip-rule, crypto-list ip-rule

Note:

The **not** form of the command is not relevant in the crypto-list ip-rule context.

Example

To specify that rule 22 applies to all packets whose destination port is 300:

```
G450-001(ACL 330/ip rule 22)# tcp destination-port eq 300
```

To specify that rule 22 applies to all packets *except* for those whose destination port is 300:

```
G450-001(ACL 330/ip rule 22)# not tcp destination-port eq 300
```

Related Commands - Policy-based routing

destination-ip, dscp (policy-based routing, packet sniffing, VPN), icmp, ip-protocol, show ip capture-list, source-ip, tcp source-port, udp destination-port, udp source-port

Related Commands - Policy

composite-operation, destination-ip, dscp (policy), icmp, show composite-operation, show dscp-table, show isdn bri link, source-ip, tcp established, tcp source-port, udp destination-port, udp source-port

Related Commands - VPN

description (ip rule), destination-ip, dscp (policy-based routing, packet sniffing, VPN), fragment, icmp, ip crypto-list, ip-protocol, ip-rule (VPN), local-address, protect crypto map, source-ip, show ip crypto-list, tcp source-port, udp destination-port, udp source-port

tcp established

Use the **tcp established** command to specify that the current rule applies only to packets that are part of an established TCP session. Use the **no** form of the command to specify that the current rule applies to any TCP packets.

Note:

The **tcp established** and **no tcp established** commands also set the IP protocol to TCP.

Syntax

[no] tcp established

User Level

read-write

Context

ip access-control-list ip-rule

Example

To specify that rule 27 applies only to packets from an established TCP session:

```
G450-001(ACL 330/ip rule 27)# tcp established
Rule protocol changed.
```

Related Commands - Policy

composite-operation, destination-ip, dscp (policy), icmp, show composite-operation, show isdn bri link, source-ip, tcp destination-port, tcp source-port, udp destination-port, udp source-port

tcp source-port

Use the **tcp source-port** command to define a source port with the TCP protocol for which to apply the current rule.

Use the **no** form of the command to set the TCP source port to any. If the protocol is not TCP, the protocol is set to TCP and the destination port is set to its default value.

Use the **not** form of the command to specify that the rule applies to all TCP ports other than the requested ports. If the protocol is not TCP, the protocol is set to TCP and the destination port is set to its default value

Note:

Issuing this command also sets the protocol to be TCP, if it is not already.

Syntax

[not] tcp source-port any | {{eq | lt | gt} {*port_name* | *port_number*}} | {range *start_port end_port*}

no tcp source-port

Parameters

Parameter	Description	Possible Values	Default Value
any	Keyword that specifies to apply the rule to a port with any name or number		
eq	Keyword that specifies to apply the rule to a port whose name or number matches exactly to the specified name or number		
lt	Keyword that specifies to apply the rule to a port whose name or number is less than the specified name or number		
gt	Keyword that specifies to apply the rule to a port whose name or number is greater than the specified name or number		
port_name	The name of the port for which to apply the rule		
port_number	The number of the port for which to apply the rule		

Parameter	Description	Possible Values	Default Value
range	Keyword indicating that a range of ports is specified		
start_port	The start of a port range for which to apply the rule		
end_port	The end of a port range for which to apply the rule		

User Level

read-write

Context

ip pbr-list ip-rule, ip capture-list ip-rule, ip qos-list ip-rule, ip access-control-list ip-rule, ip crypto-list ip-rule

Note:

The **not** form of the command is not relevant in the crypto-list ip-rule context.

Example

To specify that rule 22 applies to all packets whose source port is greater than port number 95:

```
G450-001(ACL 330/ip rule 22)# tcp source-port gt 95
```

To specify that rule 22 applies to all packets whose source port is less than or equal to port 95:

```
G450-001(ACL 330/ip rule 22)# not tcp source-port gt 95
```

Related Commands - Policy-based routing

destination-ip, dscp (policy-based routing, packet sniffing, VPN), icmp, ip-protocol, show ip capture-list, source-ip, tcp destination-port, udp destination-port, udp source-port

Related Commands - Policy

composite-operation, destination-ip, dscp (policy), icmp, show composite-operation, show dscp-table, show isdn bri link, source-ip, tcp destination-port, tcp established, udp destination-port, udp source-port

Related Commands - VPN

description (ip rule), destination-ip, dscp (policy-based routing, packet sniffing, VPN), fragment, icmp, ip crypto-list, ip-protocol, ip-rule (VPN), local-address, protect crypto map, source-ip, show ip crypto-list, tcp destination-port, udp destination-port, udp source-port

udp destination-port

Use the **udp destination-port** command to define a destination port with the UDP protocol for which to apply the current rule.

Use the **no** form of the command to set the UDP destination port to any. If the protocol is not UDP, the protocol is set to UDP and the source port is set to its default value.

Use the **not** form of the command to specify that the rule applies to all UDP ports other than the requested ports. If the protocol is not UDP, the protocol is set to UDP and the source port is set to its default value

Note:

Issuing this command also sets the protocol to be UDP, if it is not already.

Syntax

[not] udp destination-port any | {{eq | lt | gt} {*port_name* | *port_number*}} | {range *start_port end_port}*

no udp destination-port

Parameters

Parameter	Description	Possible Values	Default Value
any	Keyword that specifies to apply the rule to a port with any name or number		
eq	Keyword that specifies to apply the rule to a port whose name or number matches exactly to the specified name or number		
lt	Keyword that specifies to apply the rule to a port whose name or number is less than the specified name or number		
gt	Keyword that specifies to apply the rule to a port whose name or number is greater than the specified name or number		
port_name	The name of the port for which to apply the rule		
port_number	The number of the port for which to apply the rule		
range	Keyword indicating that a range of ports is specified		

Parameter	Description	Possible Values	Default Value
start_port	The start of a port range for which to apply the rule		
end_port	The end of a port range for which to apply the rule		

User Level

read-write

Context

ip pbr-list ip-rule, ip qos-list ip-rule, ip capture-list ip-rule, ip access-control-list ip-rule, ip crypto-list ip-rule

Note:

The **not** form of the command is not relevant in the crypto-list ip-rule context.

Example

To specify that rule 22 applies to all packets whose destination port is port 300:

```
G450-001(ACL 330/ip rule 22)# udp destination-port eq 300
```

To specify that rule 22 applies to all packets *except* for those whose destination port is 300:

```
G450-001(ACL 330/ip rule 22)# not udp destination-port eq 300
```

Related Commands - Policy-based routing

destination-ip, dscp (policy-based routing, packet sniffing, VPN), icmp, ip-protocol, show ip capture-list, source-ip, tcp destination-port, tcp source-port, udp source-port

Related Commands - Policy

composite-operation, destination-ip, dscp (policy), icmp, show composite-operation, show dscp-table, show isdn bri link, source-ip, tcp destination-port, tcp established, tcp source-port, udp source-port

Related Commands - VPN

description (ip rule), destination-ip, dscp (policy-based routing, packet sniffing, VPN), fragment, icmp, ip crypto-list, ip-protocol, ip-rule (VPN), local-address, protect crypto map, source-ip, show ip crypto-list, tcp destination-port, tcp source-port, udp source-port

udp source-port

Use the **udp source-port** command to define a source port with the UDP protocol for which to apply the current rule.

Use the **no** form of the command to set the UDP source port to any. If the protocol is not UDP, the protocol is set to UDP and the destination port is set to its default value.

Use the **not** form of the command to specify that the rule applies to all UDP ports other than the requested ports. If the protocol is not UDP, the protocol is set to UDP and the destination port is set to its default value

Note:

Issuing this command also sets the protocol to be UDP, if it is not already.

Syntax

[not] udp source-port any | {{eq | lt | gt} {*port_name* | *port_number*}} | {range *start_port end_port}*

no udp source-port

Parameters

Parameter	Description	Possible Values	Default Value
any	Keyword that specifies to apply the rule to a port with any name or number		
eq	Keyword that specifies to apply the rule to a port whose name or number matches exactly to the specified name or number		
lt	Keyword that specifies to apply the rule to a port whose name or number is less than the specified name or number		
gt	Keyword that specifies to apply the rule to a port whose name or number is greater than the specified name or number		
port_name	The name of the port for which to apply the rule		
port_number	The number of the port for which to apply the rule		

Parameter	Description	Possible Values	Default Value
range	Keyword indicating that a range of ports is specified		
start_port	The start of a port range for which to apply the rule		
end_port	The end of a port range for which to apply the rule		

User Level

read-write

Context

ip pbr-list ip-rule, ip qos-list ip-rule, ip capture-list ip-rule, ip access-control-list ip-rule, ip crypto-list ip-rule

Note:

The **not** form of the command is not relevant in the crypto-list ip-rule context.

Example

To specify that rule 22 applies to all packets whose source port is greater than port 95:

```
G450-001(ACL 330/ip rule 22)# udp source-port gt 95
```

To specify that rule 22 applies to all packets whose source port is less than or equal to port 95:

```
G450-001(ACL 330/ip rule 22)# not udp source-port gt 95
```

Related Commands - Policy-based routing

destination-ip, dscp (policy-based routing, packet sniffing, VPN), icmp, ip-protocol, show ip capture-list, source-ip, tcp destination-port, tcp source-port, udp destination-port

Related Commands - Policy

composite-operation, destination-ip, dscp (policy), icmp, show composite-operation, show dscp-table, show isdn bri link, source-ip, tcp destination-port, tcp established, tcp source-port, udp destination-port

Related Commands - VPN

description (ip rule), destination-ip, dscp (policy-based routing, packet sniffing, VPN), fragment, icmp, ip crypto-list, ip-protocol, ip-rule (VPN), local-address, protect crypto map, source-ip, show ip crypto-list, tcp destination-port, tcp source-port, udp destination-port

name

Use the **name** command to assign a name to the specified list or operation. Use the **no** form of the command to return the name to the default value.

Syntax

[no] name *name*

Parameters

Parameter	Description	Possible Values	Default Value
name	The name of the list or operation. **Note:** If you wish to include spaces in the description, you must enclose the string in quotation marks (“”).	String of 1-31 characters	

User Level

read-write

Context

dhcp pool, dhcp pool vendor specific, dhcp pool option, ip qos-list, ip qos-list dscp-table, ip qos-list composite-operation, ip access-control-list, ip next-hop-list, ip capture-list, ip pbr-list, ip crypto-list.

Example

To specify the name of access control list 330 as Admin13:

```
G450-001(ACL 330)# name Admin13
```

Related Commands - DHCP server

bootfile, client-identifier, default-router, dns-server, domain-name, end-ip-addr, lease, next-server, option, server-name, show ip dhcp-pool, start-ip-addr, subnet-mask, value, vendor-specific-option

Related Commands - Packet sniffing

capture buffer-mode, capture buffer-size, capture filter-group, capture interface, capture max-frame-size, capture start, capture stop, capture-service, clear capture-buffer, ip capture-list, show capture, show capture-buffer hex

Related Commands - Policy-based routing

ip-rule (policy, policy-based routing, packet sniffing), owner, show isdn bri link, show list

Related Commands - Policy

composite-operation, cookie, ip-fragments-in, ip-option-in, ip-rule (policy, policy-based routing, packet sniffing), owner, show composite-operation, show dscp-table, show isdn bri link, show list, cos, dscp (policy)

---

owner

Use the **owner** command to specify the owner of the current list.

Syntax

owner *owner_name*

Parameters

Parameter	Description	Possible Values	Default Value
owner_name	Name of the owner	string	

User Level

read-write

Context

ip access-control-list, ip qos-list, ip capture-list, ip pbr-list, ip crypto-list

Example

To set the owner of access control list 330 as MGAdmin3:

```
G450-001(ACL 330)# owner MGAdmin3
```

Related Commands - Packet sniffing

composite-operation, cookie, copy capture-file ftp, copy capture-file scp, copy capture-file tftp, ip-rule (policy, policy-based routing, packet sniffing), show ip capture-list, show upload status

Related Commands - Policy-based routing

ip-rule (policy, policy-based routing, packet sniffing), name, show isdn bri link, show list

Related Commands - Policy

composite-operation, cookie, dscp-table, ip-fragments-in, ip-option-in, ip-rule (policy, policy-based routing, packet sniffing), name, show composite-operation, show isdn bri link, show list

show composite-operation

Use the **show composite-operation** command to display information about a specific composite-operation. Use the command without a parameter to display information about all composite-operations.

Syntax

show composite-operation [*composite_operation_index*]

Parameters

Parameter	Description	Possible Values	Default Value
composite_operation_index	The composite-operation to display	**0-19**	

User Level

read-write

Context

ip access-control-list, ip access-control-list ip-rule, ip qos-list, ip qos-list ip-rule, ip qos-list composite-operation

Example

To display information about composite-operation 13:

```
G450-001(QoS 440)# show composite-operation 13
Index Name                 CoS       DSCP      Trust
----- -------------------- --------- --------- ------------
13    HSPackets            cos3      1         No
```

Related Commands

composite-operation, cookie, destination-ip, dscp (policy), dscp-table, icmp, ip-rule (policy, policy-based routing, packet sniffing), show composite-operation, show dscp-table, show isdn bri link, show list, source-ip, tcp destination-port, tcp established, tcp source-port, udp destination-port, udp source-port, cos, dscp (policy-based routing, packet sniffing, VPN), name

show ip-rule

Use the **show ip-rule** command to display the attributes of a specific rule. Leave the ***rule_number*** parameter blank to display all rules.

Syntax

show ip-rule [*rule_number*]

Parameters

Parameter	Description	Possible Values	Default Value
rule_number	The specific rule for which attributes are displayed		

User Level

read-write

Context

ip access-control-list, ip access-control-list/ip-rule, ip qos-list, ip qos-list/ip-rule, ip capture-list, ip capture-list/ip-rule, ip pbr-list, ip pbr-list/ip-rule

Example

To display information about ip rule 22 in access-control-list 320:

```
G450-001(ACL 320/ip rule 22)# show ip-rule 22

I.D.  Protocol IP  Wildcard         Port      Operation
----- -------- --- ---------------- --------- ----------
22    Ip       Src                  Any       permit
               Dst                  Any
```

Following is an example of the output that appears if DoS-classification is configured:

```
Index    Protocol      IP         Wildcard        Port   Operation
         DSCP                                             Fragment rule
-----    ------  ---  ---------   -------------- ------ --------------
123      Any     Src  1.2.3.4         Host          Any         Permit
         Any     Dst  Any                           Any         No

Dos classification: other-attack
234      Any     Src  2.2.2.2         Host          Any         Permit
         Any     Dst  Any                           Any         No
```

```
Dos classification: fraggle
345       Any      Src  3.3.3.3          Host          Any          Permit
          Any      Dst  Any                            Any          No

Dos classification: ip-spoofing
Deflt     Any      Src  Any                            Any          Permit
          Any      Dst  Any                            Any          No
```

Related Commands - Policy-based routing: ip pbr-list

destination-ip, dscp (policy-based routing, packet sniffing, VPN), next-hop (policy-based routing), show ip next-hop-list

Related Commands - Policy-based routing: ip pbr-list: ip-rule

ip-rule (policy, policy-based routing, packet sniffing), name, owner, show list

Related Commands - Policy

composite-operation, cookie, dscp-table, ip-fragments-in, ip-option-in, ip-rule (policy, policy-based routing, packet sniffing), name, owner, show composite-operation, show dscp-table, show isdn bri link, show list, composite-operation, destination-ip, dscp (policy), icmp, source-ip, tcp destination-port, tcp established, tcp source-port, udp destination-port, udp source-port

Related Commands - DoS

DoS-classification, show ip access-control-list

---

show list

Use the **`show list`** command to display information about a given list.

Syntax

`show list`

User Level

read-write

Context

ip access-control-list, ip qos-list, ip capture-list, ip pbr-list

Example

To show detailed information about access control list 330:

```
G450-001(ACL 330)# show list
Index Name           Owner
----- -------------- ------------
330   SplitPriority     Admin
ip options: Permit
ip fragments : Permit
Index  Protocol      IP   Wildcard     Port    Operation-
-----  --------      ---  -----------  -----   ----------
22     tcp           Src  Any          Any     Permit
                     Dst  Any          Any
Deflt  Any           Src  Any          Any     Permit
                     Dst  Any          Any
```

Related Commands - Policy-based routing

ip-rule (policy, policy-based routing, packet sniffing), name, owner, show isdn bri link

Related Commands - Policy

composite-operation, cookie, dscp-table, ip-fragments-in, ip-option-in, ip-rule (policy, policy-based routing, packet sniffing), name, owner, show composite-operation, show dscp-table, show isdn bri link, show list

---

ip access-group

Use the **ip access-group** command to activate a specific Access Control list for a specific direction, on the current interface. Use the **no** form of this command to suspend the Access Control list for a specific direction.

Note:

You cannot edit the active Access Control list.

Syntax

ip access-group *policy_list_number direction*

no ip access-group *direction*

Parameters

Parameter	Description	Possible Values	Default Value
policy_list_number	The Access Control list number	**300-399**	**300**
direction	The direction of the packets to which the policy is applied	**in**, **out**	

User Level

read-write

Context

interface:Serial (DS1 PPP L2, DS1 PPP L2-L3, DS1 FR-SUB L2, DS1 FR-SUB L2-L3, USP PPP L2, USP PPP L2-L3), Loopback (L2, L2-L3), FastEthernet (L2, L2-L3, PPP L2, PPP L2-L3, PPP L3), Tunnel (L2, L2-L3), VLAN (L2, L2-L3), Dialer (L2, L2-L3)

Example

To enable access control list 310 for outbound packets on the FastEthernet interface:

```
G450-001(if:FastEthernet 10/2)# ip access-group 310 out
```

Related Commands

ip access-control-list, ip policy-list-copy, ip qos-group, ip qos-list, ip simulate, pre-classification, show ip access-control-list, show ip qos-list

ip policy-list-copy

Use the **ip policy-list-copy** command to copy an existing policy list to a new list.

Note:

The source and destination lists must be of the same type. For example, you cannot copy an access control list to a QoS list.

Syntax

ip policy-list-copy *source_list destination_list*

Parameters

Parameter	Description	Possible Values	Default Value
source_list	The list number of the policy list to copy	For access control lists: **300-399** For QoS lists: **400-499**	
destination_list	The list number of the policy to copy to	For access control lists: **301-399** For QoS lists: **401-499**	

User Level

read-write

Context

general

Example

To copy the settings of access control list 330 to list 340:

```
G450-001(super)# ip policy-list-copy 330 340
```

Related Commands

ip access-control-list, ip access-group, ip qos-group, ip qos-list, ip simulate, pre-classification, show ip access-control-list, show ip qos-list

ip simulate

Use the **ip simulate** command to test the action of a policy on a simulated packet.

Syntax

ip simulate ***policy_list_number direction*** **[*priority*] [*dscp_value*]** ***source destination*** **[*protocol* [*source_port***
destination_port **[*established*]]]**

Parameters

Parameter	Description	Possible Values	Default Value
policy_list_number	The number of the policy	**1-999**	For PBR: **1** For ACL: **300** For Qos: **400** For Capture: **500**
direction	The direction	**in**, **out**	
priority	The priority	**fwd0-fwd7**	
dscp_value	The DSCP value	**dscp0-dscp63**	
source	The source IP address		
destination	The destination IP address		
protocol	The protocol to use	**ip**, **tcp**, **udp**, **1-255**	
source_port	The source port of the simulated packet	**1-65535**	
destination_port	The destination port of the simulated packet	**1-65535**	
established	The value of the TCP established bit		

User Level

read-write

Context

interface:Serial (DS1 PPP L2, DS1 PPP L2-L3, DS1 FR-SUB L2, DS1 FR-SUB L2-L3, USP PPP L2, USP PPP L2-L3), Loopback (L2, L2-L3), FastEthernet (L2-L3, L3, PPP L2, PPP L2-L3, PPP L3), Tunnel (L2, L2-L3), VLAN (L2, L2-L3), Dialer (L2, L2-L3)

Example

To simulate the effects of applying access control list 330 to a packet entering the media gateway through the FastEthernet interface, from IP address 192.67.85.12 to IP address 192.67.54.25:

```
G450-001(if:FastEthernet 10/2)# ip simulate 330 in 192.67.85.12 192.67.54.25
ip
```

Related Commands

ip access-control-list, ip access-group, ip policy-list-copy, ip qos-group, ip qos-list, pre-classification, show ip access-control-list, show ip qos-list

show ip access-control-list

Use the **show ip access-control-list** command to display the attributes of a specific access control list on the current interface or all lists.

Syntax

show ip access-control-list {*list_number* | all | active-list-in | active-list-out | active-list-in-out} [detailed]

Parameters

Parameter	Description	Possible Values	Default Value
list_number	The access control list to display		
all	Keyword specifying to display attributes for all access control lists		
active-list-in	Keyword specifying to display lists for the in direction		
active-list-out	Keyword specifying to display lists for the out direction		
active-list-in-out	Keyword specifying to display lists for in and out directions		
detailed	Keyword specifying to display detailed information		

User Level

read-write

Context

general, interface:Serial (DS1 PPP L2, DS1 PPP L2-L3, DS1 FR-SUB L2, DS1 FR-SUB L2-L3, USP PPP L2, USP PPP L2-L3), FastEthernet (L2, L2-L3), VLAN (L2, L2-L3), Loopback (L2, L2-L3), Tunnel (L2, L2-L3), Dialer (L2, L2-L3)

Example

To display detailed information about all access control lists:

```
G450-001(super)# show ip access-control-list all detailed
List Number: 300
---------------
List Name: Default ACL List
Default Action: permit
Owner: other
List Number: 320
---------------
List Name: Sync1
Default Action: permit
Owner: x9393
List Number: 330
---------------
List Name: Admin13
Default Action: permit
Owner: Charlie
```

To display attributes of access control list 330:

```
G450-001(super)# show ip access-control-list 330
Index Name                            Owner
----- ------------------------------- -------------------------
330   list #330                       other
ip options: Permit
ip fragments : Permit

Index Protocol     IP               Wildcard        Port         Operation
----- -------- --- ---------------- --------------- ------------ --------
22     tcp     Src  Any                              Any          Permit
               Dst  Any                              Any
Deflt  Any     Src  Any                              Any          Permit
               Dst  Any                              Any
```

To display detailed information about all access control lists on the VLAN 1 interface:

```
G450-001(if:Vlan 1)# show ip access-control-list all detailed
List Number: 300
---------------
List Name: Default ACL List
Default Action: permit
Owner: other
List Number: 320
---------------
List Name: Sync1
Default Action: permit
Owner: x9393
List Number: 330
---------------
List Name: Admin13
Default Action: permit
```

```
Owner: Charlie
```

Following is an example of the output that appears if DoS-classification is configured:

```
Index     Protocol      IP          Wildcard       Port   Operation
          DSCP                                             Fragment rule
-----     ------  ---   ---------   -------------- ------ --------------
123       Any     Src   1.2.3.4     Host           Any    Permit
          Any     Dst   Any                        Any    No
Dos classification: other-attack
234       Any     Src   2.2.2.2     Host           Any    Permit
          Any     Dst   Any                        Any    No
Dos classification: fraggle
345       Any     Src   3.3.3.3     Host           Any     Permit
          Any     Dst   Any                        Any     No
Dos classification: ip-spoofing
Deflt     Any     Src   Any                        Any     Permit
          Any     Dst   Any                        Any     No
```

Related Commands

ip access-control-list, ip access-group, ip policy-list-copy, ip qos-group, ip qos-list, ip simulate, pre-classification, show ip qos-list, DoS-classification

Policy - QoS lists

ip policy-list-copy

Use the **ip policy-list-copy** command to copy an existing policy list to a new list.

Note:

The source and destination lists must be of the same type. For example, you cannot copy an access control list to a QoS list.

Syntax

ip policy-list-copy *source_list destination_list*

Parameters

Parameter	Description	Possible Values	Default Value
source_list	The list number of the policy list to copy	For access control lists: **300-399** For QoS lists: **400-499**	
destination_list	The list number of the policy to copy to	For access control lists: **301-399** For QoS lists: **401-499**	

User Level

read-write

Context

general

Example

To copy the settings of access control list 330 to list 340:

```
G450-001(super)# ip policy-list-copy 330 340
```

Related Commands

ip access-control-list, ip access-group, ip qos-group, ip qos-list, ip simulate, pre-classification, show ip access-control-list, show ip qos-list

ip qos-group

Use the **ip qos-group** command to activate the specified QoS list on the given interface. You must first create the QoS list using the **ip qos-list** command.

Syntax

[no] ip qos-group *policy_list direction*

Parameters

Parameter	Description	Possible Values	Default Value
policy_list	The policy list number	**400-499**	**400**
direction	The direction of packets to which the policy applies	**in**, **out**	

User Level

read-write

Context

interface:Serial (DS1 PPP L2, DS1 PPP L2-L3, DS1 FR-SUB L2, DS1 FR-SUB L2-L3, USP PPP L2, USP PPP L2-L3), FastEthernet (L2, L2-L3, PPP L2, PPP L2-L3, PPP L3), VLAN (L2, L2-L3), Loopback (L2, L2-L3), Tunnel (L2, L2-L3), Dialer (L2, L2-L3)

Example

To apply QoS list 440 to all incoming packets on the Vlan 1 interface:

```
G450-001(if:Vlan 1)# ip qos-group 440 in
```

Related Commands

ip access-control-list, ip access-group, ip policy-list-copy, ip qos-list, ip simulate, pre-classification, show ip access-control-list, show ip qos-list

ip qos-list

Use the **ip qos-list** command to enter configuration mode for the specified QoS list. If the QoS list does not exist, the system creates it and enters its configuration mode.

Syntax

ip qos-list *list_number*

Parameters

Parameter	Description	Possible Values	Default Value
list_number	The policy list number	**400-499**	**400**

User Level

read-write

Context

general

Example

To create QoS list 440 and enter its configuration context:

```
G450-001# ip qos-list 440
G450-001(QoS 440)#
```

Related Commands

ip access-control-list, ip access-group, ip policy-list-copy, ip qos-group, ip simulate, pre-classification, show ip access-control-list, show ip qos-list

composite-operation

Use the **composite-operation** command to edit the specified composite operation. If the composite operation does not exist, it is created.

Syntax

composite-operation ***index***

Parameters

Parameter	Description	Possible Values	Default Value
index	The composite operation number	**12-19**	

User Level

read-write

Context

ip access-control-list/ip-rule, ip capture-list/ip-rule, ip qos-list, ip qos-list/dscp-table, ip qos-list/ip-rule

Example

To enter configuration mode for composite operation 13:

```
G450-001(QoS 440)# composite-operation 13
G450-001(QoS 440/CompOp 13)#
```

Related Commands - Packet sniffing

cookie, copy capture-file ftp, copy capture-file scp, copy capture-file tftp, ip-rule (policy, policy-based routing, packet sniffing), owner, show ip capture-list, show upload status

Related Commands - Policy

cookie, destination-ip, dscp (policy), dscp-table, icmp, ip-rule (policy, policy-based routing, packet sniffing), name, owner, show composite-operation, show dscp-table, show isdn bri link, show list, source-ip, tcp destination-port, tcp established, tcp source-port, udp destination-port, udp source-port

---

COS

Use the **cos** command to set the priority value for the current composite operation. Use the **no** form of the command to reset the priority to the default value of **no-change**.

Syntax

cos {*priority* | no-change}

no cos

Parameters

Parameter	Description	Possible Values	Default Value
priority	The priority value of the composite operation	**0-8**	
no-change	Keyword indicating that the priority is not changed		

User Level

read-write

Context

ip qos-list composite-operation

Example

To set the priority for composite operation 12 to 3:

```
G450-001(QoS 440/CompOp 12)# cos 3
```

Related Commands

dscp (policy-based routing, packet sniffing, VPN), name, show composite-operation

dscp (policy)

Use the **dscp** command to specify the DSCP value that is set by the current policy operation.

Use the **not** form of the command to specify that the current operation set any DSCP value other than requested value.

Use the **no** form of the command to specify that the current operation set the DSCP value to `no-change`.

Syntax

dscp {*dscp_value* | no-change}

not dscp *dscp_value*

no dscp

Parameters

Parameter	Description	Possible Values	Default Value
dscp_value	The DSCP value	**0-63**	
no-change	Keyword indicating that the DSCP value is left unchanged		

User Level

read-write

Context

ip qos-list composite-operation

Example

To specify that composite operation 17 sets the DSCP value of packets to 55:

```
G450-001(QoS 440/CompOp 17)# dscp 55
```

To specify that composite operation 17 sets the DSCP value of packets to a value other than 55:

```
G450-001(QoS 440/CompOp 17)# not dscp 55
```

Related Commands - Policy

composite-operation, destination-ip, icmp, show composite-operation, show isdn bri link, source-ip, tcp destination-port, tcp established, tcp source-port, udp destination-port, udp source-port, cos, name

---

name

Use the **name** command to assign a name to the specified list or operation. Use the **no** form of the command to return the name to the default value.

Syntax

[no] name *name*

Parameters

Parameter	Description	Possible Values	Default Value
name	The name of the list or operation. **Note:** If you wish to include spaces in the description, you must enclose the string in quotation marks (“”).	String of 1-31 characters	

User Level

read-write

Context

dhcp pool, dhcp pool vendor specific, dhcp pool option, ip qos-list, ip qos-list dscp-table, ip qos-list composite-operation, ip access-control-list, ip next-hop-list, ip capture-list, ip pbr-list, ip crypto-list.

Example

To specify the name of access control list 330 as Admin13:

```
G450-001(ACL 330)# name Admin13
```

Related Commands - DHCP server

bootfile, client-identifier, default-router, dns-server, domain-name, end-ip-addr, lease, next-server, option, server-name, show ip dhcp-pool, start-ip-addr, subnet-mask, value, vendor-specific-option

Related Commands - Packet sniffing

capture buffer-mode, capture buffer-size, capture filter-group, capture interface, capture max-frame-size, capture start, capture stop, capture-service, clear capture-buffer, ip capture-list, show capture, show capture-buffer hex

Related Commands - Policy-based routing

ip-rule (policy, policy-based routing, packet sniffing), owner, show isdn bri link, show list

Related Commands - Policy

composite-operation, cookie, ip-fragments-in, ip-option-in, ip-rule (policy, policy-based routing, packet sniffing), owner, show composite-operation, show dscp-table, show isdn bri link, show list, cos, dscp (policy)

show composite-operation

Use the **show composite-operation** command to display information about a specific composite-operation. Use the command without a parameter to display information about all composite-operations.

Syntax

show composite-operation [*composite_operation_index*]

Parameters

Parameter	Description	Possible Values	Default Value
composite_operation_index	The composite-operation to display	**0-19**	

User Level

read-write

Context

ip access-control-list, ip access-control-list ip-rule, ip qos-list, ip qos-list ip-rule, ip qos-list composite-operation

Example

To display information about composite-operation 13:

```
G450-001(QoS 440)# show composite-operation 13
Index Name                  CoS       DSCP      Trust
----- -------------------- --------- --------- ------------
13    HSPackets             cos3      1         No
```

Related Commands

composite-operation, cookie, destination-ip, dscp (policy), dscp-table, icmp, ip-rule (policy, policy-based routing, packet sniffing), show composite-operation, show dscp-table, show isdn bri link, show list, source-ip, tcp destination-port, tcp established, tcp source-port, udp destination-port, udp source-port, cos, dscp (policy-based routing, packet sniffing, VPN), name

cookie

Use the **cookie** command to set the cookie for the current list.

Syntax

cookie ***cookie_number***

Parameters

Parameter	Description	Possible Values	Default Value
cookie_number	The ID number of the cookie	**0-268435455**	

User Level

read-write

Context

ip access-control-list, ip qos-list, ip capture-list, ip pbr-list, ip crypto-list

Example

To specify the cookie for QoS list 440 as 257:

```
G450-001(QoS 440)# cookie 257
```

Related Commands - Packet sniffing

composite-operation, copy capture-file ftp, copy capture-file scp, copy capture-file tftp, ip-rule (policy, policy-based routing, packet sniffing), owner, show ip capture-list, show upload status

Related Commands - Policy

composite-operation, dscp-table, ip-fragments-in, ip-option-in, ip-rule (policy, policy-based routing, packet sniffing), name, owner, show composite-operation, show isdn bri link, show list

dscp-table

Use the **dscp-table** command to enter the DSCP table entry context for a particular DSCP value for the current QoS list. If the specified DSCP table entry does not exist, the system creates it.

Syntax

dscp-table *dscp_value*

Parameters

Parameter	Description	Possible Values	Default Value
dscp_value	The specific DSCP value to configure	**0-63**	

User Level

read-write

Context

ip qos-list, capture-list

Example

To enter configuration mode for DSCP table entry 21:

```
G450-001(QoS 440)# dscp-table 21
```

Related Commands

composite-operation, cookie, ip-rule (policy, policy-based routing, packet sniffing), owner, show composite-operation, show dscp-table, show isdn bri link, show list

composite-operation

Use the **composite-operation** command to edit the specified composite operation. If the composite operation does not exist, it is created.

Syntax

composite-operation *index*

Parameters

Parameter	Description	Possible Values	Default Value
index	The composite operation number	**12-19**	

User Level

read-write

Context

ip access-control-list/ip-rule, ip capture-list/ip-rule, ip qos-list, ip qos-list/dscp-table, ip qos-list/ip-rule

Example

To enter configuration mode for composite operation 13:

```
G450-001(QoS 440)# composite-operation 13
G450-001(QoS 440/CompOp 13)#
```

Related Commands - Packet sniffing

cookie, copy capture-file ftp, copy capture-file scp, copy capture-file tftp, ip-rule (policy, policy-based routing, packet sniffing), owner, show ip capture-list, show upload status

Related Commands - Policy

cookie, destination-ip, dscp (policy), dscp-table, icmp, ip-rule (policy, policy-based routing, packet sniffing), name, owner, show composite-operation, show dscp-table, show isdn bri link, show list, source-ip, tcp destination-port, tcp established, tcp source-port, udp destination-port, udp source-port

name

Use the **name** command to assign a name to the specified list or operation. Use the **no** form of the command to return the name to the default value.

Syntax

[no] name *name*

Parameters

Parameter	Description	Possible Values	Default Value
name	The name of the list or operation. **Note:** If you wish to include spaces in the description, you must enclose the string in quotation marks (“”).	String of 1-31 characters	

User Level

read-write

Context

dhcp pool, dhcp pool vendor specific, dhcp pool option, ip qos-list, ip qos-list dscp-table, ip qos-list composite-operation, ip access-control-list, ip next-hop-list, ip capture-list, ip pbr-list, ip crypto-list.

Example

To specify the name of access control list 330 as Admin13:

```
G450-001(ACL 330)# name Admin13
```

Related Commands - DHCP server

bootfile, client-identifier, default-router, dns-server, domain-name, end-ip-addr, lease, next-server, option, server-name, show ip dhcp-pool, start-ip-addr, subnet-mask, value, vendor-specific-option

Related Commands - Packet sniffing

capture buffer-mode, capture buffer-size, capture filter-group, capture interface, capture max-frame-size, capture start, capture stop, capture-service, clear capture-buffer, ip capture-list, show capture, show capture-buffer hex

Related Commands - Policy-based routing

ip-rule (policy, policy-based routing, packet sniffing), owner, show isdn bri link, show list

Related Commands - Policy

composite-operation, cookie, ip-fragments-in, ip-option-in, ip-rule (policy, policy-based routing, packet sniffing), owner, show composite-operation, show dscp-table, show isdn bri link, show list, cos, dscp (policy)

---

show dscp-table

Use the **show dscp-table** command to display a specific entry in the DSCP table. If no DSCP index is specified, the entire DSCP table is displayed.

Syntax

show dscp-table [*index*]

Parameters

Parameter	Description	Possible Values	Default Value
index	The DSCP entry		

User Level

read-write

Context

ip qos-list, ip qos-list dscp-table, ip qos-list ip-rule

Example

To display the entire DSCP table:

```
G450-001(QoS 444)# show dscp-table

Trust configuration is trust-cos
DSCP     Action            Precedence     Name
---- -------------------- ---------- ------------
0    No-Change            mandatory  DSCP#0
1    No-Change            mandatory  DSCP#1
2    No-Change            mandatory  DSCP#2
3    No-Change            mandatory  DSCP#3
4    No-Change            mandatory  DSCP#4
```

```
5     No-Change            mandatory  DSCP#5
6     No-Change            mandatory  DSCP#6
7     No-Change            mandatory  DSCP#7
8     No-Change            mandatory  DSCP#8
9     No-Change            mandatory  DSCP#9
10    No-Change            mandatory  DSCP#10
11    No-Change            mandatory  DSCP#11
.
.
.
63    No-Change            mandatory    DSCP#63
```

Related Commands

composite-operation, cookie, dscp-table, ip-rule (policy, policy-based routing, packet sniffing), name, owner, show composite-operation, show isdn bri link, show list

ip-rule (policy, policy-based routing, packet sniffing)

Use the **ip-rule** command to enter configuration mode for the specified rule. If the specified rule does not exist, the system creates it and enters its configuration mode.

Syntax

ip-rule {***rule_index*** | **default**}

Parameters

Parameter	Description	Possible Values	Default Value
rule_index	Number of the rule to edit	**1-9999**	
default	Keyword indicating ip-rule number 10,000 (last rule in the ordered list of rules)		

User Level

read-write

Context

ip access-control-list, ip qos-list, ip capture-list, ip pbr-list

Example

To enter configuration mode for ip-rule 22:

```
G450-001(ACL 330)# ip-rule 22
G450-001(ACL 330/ip rule 22)#
```

Related Commands - Packet sniffing

composite-operation, cookie, copy capture-file ftp, copy capture-file scp, copy capture-file tftp, owner, show ip capture-list, show upload status

Related Commands - Policy-based routing

name, owner, show isdn bri link, show list

Related Commands - Policy

composite-operation, cookie, dscp-table, ip-fragments-in, ip-option-in, name, owner, show composite-operation, show isdn bri link, show list

composite-operation

Use the **composite-operation** command to edit the specified composite operation. If the composite operation does not exist, it is created.

Syntax

composite-operation *index*

Parameters

Parameter	Description	Possible Values	Default Value
index	The composite operation number	**12-19**	

User Level

read-write

Context

ip access-control-list/ip-rule, ip capture-list/ip-rule, ip qos-list, ip qos-list/dscp-table, ip qos-list/ip-rule

Example

To enter configuration mode for composite operation 13:

```
G450-001(QoS 440)# composite-operation 13
G450-001(QoS 440/CompOp 13)#
```

Related Commands - Packet sniffing

cookie, copy capture-file ftp, copy capture-file scp, copy capture-file tftp, ip-rule (policy, policy-based routing, packet sniffing), owner, show ip capture-list, show upload status

Related Commands - Policy

cookie, destination-ip, dscp (policy), dscp-table, icmp, ip-rule (policy, policy-based routing, packet sniffing), name, owner, show composite-operation, show dscp-table, show isdn bri link, show list, source-ip, tcp destination-port, tcp established, tcp source-port, udp destination-port, udp source-port

destination-ip

Use the **destination-ip** command to specify the destination IP address of packets to which the current rule applies.

Use the **not** form of the command to specify that the current rule applies to all packets that *do not* have this destination IP address.

Use the **no** form of the command to set the destination IP address to any.

Syntax

[not] destination-ip {host *ip*}|any|{*ip wildcard*}

no destination-ip

Parameters

Parameter	Description	Possible Values	Default Value
host	Keyword that specifies the current rule applies to a single host IP address		
ip	The destination IP address of the rule		

Parameter	Description	Possible Values	Default Value
any	Keyword that specifies the current rule applies to any address		
ip wildcard	The range of IP addresses of the rule. The zero bits in the wildcard correspond to bits in the IP address that remain fixed. The one bits in the wildcard correspond to bits in the IP address that can vary. **Note:** This is the opposite of how bits are used in a netmask.		

User Level

read-write

Context

ip capture-list/ip-rule, ip access-control-list/ip-rule, ip pbr-list/ip-rule, ip qos-list/ip-rule, ip crypto-list ip-rule

Example

To specify that rule 22 applies to all packets having destination IP address 135.64.104.102:

```
G450-001(QoS 460/rule 22)# destination-ip host 135.64.104.102
```

To specify that rule 17 applies to packets whose destination IP address is *not* in the range of 176.13.0.0 through 176.13.255.255:

```
G450-001(QoS 460/rule 17)# not destination-ip 176.13.0.0 0.0.255.255
```

Related Commands - Packet sniffing

dscp (policy-based routing, packet sniffing, VPN), icmp, ip-protocol, show ip capture-list, source-ip, tcp destination-port, tcp source-port, udp destination-port, udp source-port

Related Commands - Policy-based routing

dscp (policy-based routing, packet sniffing, VPN), next-hop (policy-based routing), show ip next-hop-list, show isdn bri link

Related Commands - Policy

composite-operation, dscp (policy), show dscp-table, icmp, show composite-operation, show isdn bri link, source-ip, tcp destination-port, tcp established, tcp source-port, udp destination-port, udp source-port

Related Commands - VPN

description (ip rule), ip crypto-list, ip-rule (VPN), local-address, protect crypto map, source-ip, show ip crypto-list

dscp (policy)

Use the **dscp** command to specify the DSCP value that is set by the current policy operation.

Use the **not** form of the command to specify that the current operation set any DSCP value other than requested value.

Use the **no** form of the command to specify that the current operation set the DSCP value to `no-change`.

Syntax

dscp {*dscp_value* | no-change}

not dscp *dscp_value*

no dscp

Parameters

Parameter	Description	Possible Values	Default Value
dscp_value	The DSCP value	**0-63**	
no-change	Keyword indicating that the DSCP value is left unchanged.		

User Level

read-write

Context

ip qos-list composite-operation

Example

To specify that composite operation 17 sets the DSCP value of packets to 55:

```
G450-001(QoS 440/CompOp 17)# dscp 55
```

To specify that composite operation 17 sets the DSCP value of packets to a value other than 55:

```
G450-001(QoS 440/CompOp 17)# not dscp 55
```

Related Commands - Policy

composite-operation, destination-ip, icmp, show composite-operation, show isdn bri link, source-ip, tcp destination-port, tcp established, tcp source-port, udp destination-port, udp source-port, cos, name

---

fragment

Use the **fragment** command to apply the current rule for non-initial fragments only.

Note:

You cannot specify TCP/UDP ports or ICMP code/type for a rule when using the **fragment** command.

Syntax

fragment

User Level

read-write

Context

ip qos-list composite-operation, ip capture-list ip-rule, ip pbr-list ip-rule, ip access-control-list ip-rule, ip qos-list ip-rule, ip crypto-list ip-rule

Example

To apply the rule for non-initial fragments:

```
G450-001(super-Capture 520/ip rule 15)# fragment
```

Related Commands - Packet sniffing

dscp (policy-based routing, packet sniffing, VPN), destination-ip, icmp, ip-protocol, show ip capture-list, source-ip, tcp destination-port, tcp source-port, udp destination-port, udp source-port

Related Commands - Policy-based routing

dscp (policy-based routing, packet sniffing, VPN), destination-ip, next-hop (policy-based routing), show ip next-hop-list, show isdn bri link

Related Commands - Policy

composite-operation, dscp (policy), destination-ip, icmp, show composite-operation, show isdn bri link, source-ip, tcp destination-port, tcp established, tcp source-port, udp destination-port, udp source-port, cos, name

Related Commands - VPN

description (ip rule), destination-ip, dscp (policy-based routing, packet sniffing, VPN), icmp, ip crypto-list, ip-protocol, ip-rule (VPN), local-address, protect crypto map, source-ip, show ip crypto-list, tcp destination-port, tcp source-port, udp destination-port, udp source-port

icmp

Use the **icmp** command to specify that the current rule applies to a specific type of ICMP packet.

Use the **not** form of this command to specify that the rule applies to all packets *except* those of the requested ICMP attribute. If the IP protocol is not ICMP, it is set to ICMP.

Use the **no** form of the command to specify that the current rule applies to any type of ICMP packet.

Note:

The **icmp** command also sets the IP protocol to ICMP.

Syntax

[not] icmp {*name* | {*icmp_type icmp_code*}}

no icmp

Parameters

Parameter	Description	Possible Values	Default Value
name	Specify that the rule applies to this ICMP name		
icmp_type	Specify that the rule applies to this icmp type	For an ip-rule: **0-256** For a QoS rule: **0-65535**	
icmp_code	Specify that the rule applies to this icmp code	For an ip-rule: **0-256** For a QoS rule: **0-65535**	

User Level

read-write

Context

ip capture-list/ip-rule, ip access-control-list/ip-rule, ip pbr-list/ip-rule, ip qos-list/ip-rule, ip crypto-list ip-rule

Note:

The **not** form of the command is not relevant in the crypto-list ip-rule context.

Example

To specify that rule 27 applies to ICMP error-reply packets:

```
G450-001(ACL 333/ip rule 27)# icmp Echo-Reply
```

To specify that rule 33 applies to any ICMP packet type *except* type 1 code 2:

```
G450-001(ACL 333/ip rule 33)# not icmp 1 2
```

Related Commands - Policy-based routing

destination-ip, dscp (policy-based routing, packet sniffing, VPN), ip-protocol, show ip capture-list, source-ip, tcp destination-port, tcp source-port, udp destination-port, udp source-port

Related Commands - Policy

composite-operation, cookie, destination-ip, dscp (policy), dscp-table, icmp, ip-rule (policy, policy-based routing, packet sniffing), owner, show composite-operation, show dscp-table, show isdn bri link, show list, source-ip, tcp destination-port, tcp established, tcp source-port, udp destination-port, udp source-port

Related Commands - VPN

description (ip rule), destination-ip, dscp (policy-based routing, packet sniffing, VPN), fragment, ip crypto-list, ip-protocol, ip-rule (VPN), local-address, protect crypto map, source-ip, show ip crypto-list, tcp destination-port, tcp source-port, udp destination-port, udp source-port

---

ip-protocol

Use the **ip-protocol** command to specify that the current rule applies to packets having the specified IP protocol.

Use the **no** form of the command to set the IP protocol to its default value.

Use the **not** form of this command to specify that the current rule applies to all packets *except* those having the specified IP protocol.

Syntax

[not] ip-protocol *protocol_name* | *protocol_number*

no ip-protocol

Parameters

Parameter	Description	Possible Values	Default Value
protocol_name	Name of the IP protocol to match		
protocol_number	Number of the IP protocol to match	**1-255**	

User Level

read-write

Context

ip access-control-list/ip-rule, ip capture-list/ip-rule, ip pbr-list/ip-rule, ip qos-list/ip-rule, crypto-list/ip-rule

Note:

The **not** form of the command is not relevant in the crypto-list/ip-rule context.

Example

To specify that rule 22 applies to all packets having an IP protocol of ICMP:

```
G450-001(ACL 330/ip rule 22)# ip-protocol icmp
```

To specify that rule 22 applies to all packets having any IP protocol *except* ICMP:

```
G450-001(ACL 330/ip rule 22)# not ip-protocol icmp
```

Related Commands

destination-ip, dscp (policy-based routing, packet sniffing, VPN), icmp, show ip capture-list, source-ip, tcp destination-port, tcp source-port, udp destination-port, udp source-port

Related Commands - VPN

description (ip rule), destination-ip, dscp (policy-based routing, packet sniffing, VPN), fragment, icmp, ip crypto-list, ip-rule (VPN), local-address, protect crypto map, source-ip, show ip crypto-list, tcp destination-port, tcp source-port, udp destination-port, udp source-port

show composite-operation

Use the **show composite-operation** command to display information about a specific composite-operation. Use the command without a parameter to display information about all composite-operations.

Syntax

show composite-operation [*composite_operation_index*]

Parameters

Parameter	Description	Possible Values	Default Value
composite_operation_index	The composite-operation to display	**0-19**	

User Level

read-write

Context

ip access-control-list, ip access-control-list ip-rule, ip qos-list, ip qos-list ip-rule, ip qos-list composite-operation

Example

To display information about composite-operation 13:

```
G450-001(QoS 440)# show composite-operation 13

Index Name                 CoS       DSCP      Trust
----- -------------------- --------- --------- ------------
13    HSPackets            cos3      1         No
```

Related Commands

composite-operation, cookie, destination-ip, dscp (policy), dscp-table, icmp, ip-rule (policy, policy-based routing, packet sniffing), show composite-operation, show dscp-table, show isdn bri link, show list, source-ip, tcp destination-port, tcp established, tcp source-port, udp destination-port, udp source-port, cos, dscp (policy-based routing, packet sniffing, VPN), name

show dscp-table

Use the **show dscp-table** command to display a specific entry in the DSCP table. If no DSCP index is specified, the entire DSCP table is displayed.

Syntax

show dscp-table [*index*]

Parameters

Parameter	Description	Possible Values	Default Value
index	The DSCP entry		

User Level

read-write

Context

ip qos-list, ip qos-list dscp-table, ip qos-list ip-rule

Example

To display the entire DSCP table:

```
G450-001(QoS 444)# show dscp-table

Trust configuration is trust-cos
DSCP     Action            Precedence     Name
---- -------------------- ---------- ------------
0    No-Change            mandatory  DSCP#0
1    No-Change            mandatory  DSCP#1
2    No-Change            mandatory  DSCP#2
3    No-Change            mandatory  DSCP#3
4    No-Change            mandatory  DSCP#4
5    No-Change            mandatory  DSCP#5
6    No-Change            mandatory  DSCP#6
7    No-Change            mandatory  DSCP#7
8    No-Change            mandatory  DSCP#8
9    No-Change            mandatory  DSCP#9
10   No-Change            mandatory  DSCP#10
11   No-Change            mandatory  DSCP#11
.
.
.
63   No-Change              mandatory    DSCP#63
```

Related Commands

composite-operation, cookie, dscp-table, ip-rule (policy, policy-based routing, packet sniffing), name, owner, show composite-operation, show isdn bri link, show list

show ip-rule

Use the **show ip-rule** command to display the attributes of a specific rule. Leave the ***rule_number*** parameter blank to display all rules.

Syntax

show ip-rule [*rule_number*]

Parameters

Parameter	Description	Possible Values	Default Value
rule_number	The specific rule for which attributes are displayed		

User Level

read-write

Context

ip access-control-list, ip access-control-list/ip-rule, ip qos-list, ip qos-list/ip-rule, ip capture-list, ip capture-list/ip-rule, ip pbr-list, ip pbr-list/ip-rule

Example

To display information about ip rule 22 in access-control-list 320:

```
G450-001(ACL 320/ip rule 22)# show ip-rule 22

I.D.  Protocol IP  Wildcard         Port      Operation
----- -------- --- ---------------- --------- ----------
22    Ip       Src                  Any       permit
               Dst                  Any
```

Following is an example of the output that appears if DoS-classification is configured:

```
Index    Protocol      IP          Wildcard        Port   Operation
         DSCP                                             Fragment rule
-----    ------  ---  ---------   -------------- ------ --------------
123      Any     Src  1.2.3.4         Host           Any          Permit
         Any     Dst  Any                            Any          No

Dos classification: other-attack
234      Any     Src  2.2.2.2         Host           Any          Permit
         Any     Dst  Any                            Any          No

Dos classification: fraggle
345      Any     Src  3.3.3.3         Host           Any          Permit
         Any     Dst  Any                            Any          No

Dos classification: ip-spoofing
Deflt    Any     Src  Any                            Any          Permit
         Any     Dst  Any                            Any          No
```

Related Commands - Policy-based routing: ip pbr-list

destination-ip, dscp (policy-based routing, packet sniffing, VPN), next-hop (policy-based routing), show ip next-hop-list

Related Commands - Policy-based routing: ip pbr-list: ip-rule

ip-rule (policy, policy-based routing, packet sniffing), name, owner, show list

Related Commands - Policy

composite-operation, cookie, dscp-table, ip-fragments-in, ip-option-in, ip-rule (policy, policy-based routing, packet sniffing), name, owner, show composite-operation, show dscp-table, show isdn bri link, show list, composite-operation, destination-ip, dscp (policy), icmp, source-ip, tcp destination-port, tcp established, tcp source-port, udp destination-port, udp source-port

Related Commands - DoS

DoS-classification, show ip access-control-list

source-ip

Use the **source-ip** command to indicate that the current rule applies to packets from the specified source IP address.

Use the **no** form of the command to indicate that the current rule applies to packets from any IP address.

Use the **not** form of the command to indicate that the current rule applies to all packets *except* those coming from the specified IP address.

Syntax

[not] source-ip {host *ip_address* | any | *ip_address wildcard*}

no source-ip

Parameters

Parameter	Description	Possible Values	Default Value
host	Keyword that indicates a specific host IP address		
ip_address	The IP address of packets to which the rule is applied		
any	Keyword that indicates any IP address		
ip_address ***wildcard***	The range of IP addresses of the rule. The zero bits in the wildcard correspond to bits in the IP address that remain fixed. The one bits in the wildcard correspond to bits in the IP address that can vary. **Note:** This is the opposite of how bits are used in a netmask.		

User Level

read-write

Context

ip pbr-list ip-rule, ip qos-list ip-rule, ip capture-list ip-rule, ip access-control-list ip-rule, ip crypto-list ip-rule

Note:

The **not** form of the command is not relevant in the crypto-list ip-rule context.

Example

To specify that rule 22 of QoS policy list 460 applies to any packet coming from IP address 135.64.104.102:

```
G450-001(QoS 460/rule 22)# source-ip host 135.64.104.102
```

To specify that rule 22 of QoS policy list 460 applies to any packet *except* those coming from IP address 135.64.104.102:

```
G450-001(QoS 460/rule 22)# not source-ip host 135.64.104.102
```

Related Commands - Policy-based routing

destination-ip, dscp (policy-based routing, packet sniffing, VPN), icmp, ip-protocol, show ip capture-list, tcp destination-port, tcp source-port, udp destination-port, udp source-port

Related Commands - Policy

composite-operation, destination-ip, dscp (policy), icmp, show composite-operation, show dscp-table, show isdn bri link, tcp destination-port, tcp established, tcp source-port, udp destination-port, udp source-port

Related Commands - VPN

description (ip rule), destination-ip, ip crypto-list, ip-rule (VPN), local-address, protect crypto map, show ip crypto-list

---

tcp destination-port

Use the **tcp destination-port** command to define a destination port with the TCP protocol for which to apply the current rule.

Use the **no** form of the command to set the TCP destination port to any. If the protocol is not TCP, the protocol is set to TCP and the source port is set to its default value.

Use the **not** form of the command to specify that the rule applies to all TCP ports other than the requested ports. If the protocol is not TCP, the protocol is set to TCP and the source port is set to its default value.

Note:

Issuing this command also sets the protocol to be TCP, if it is not already.

Syntax

[not] tcp destination-port any | {{eq | lt | gt} {*port_name* | *port_number*}} | {range *start_port end_port*}

no tcp destination-port

Parameters

Parameter	Description	Possible Values	Default Value
any	Keyword that specifies to apply the rule to a port with any name or number		
eq	Keyword that specifies to apply the rule to a port whose name or number matches exactly to the specified name or number		
lt	Keyword that specifies to apply the rule to a port whose name or number is less than the specified name or number		
gt	Keyword that specifies to apply the rule to a port whose name or number is greater than the specified name or number		
port_name	The name of the port for which to apply the rule		
port_number	The number of the port for which to apply the rule		
range	Keyword indicating that a range of ports is specified		
start_port	The start of a port range for which to apply the rule		
end_port	The end of a port range for which to apply the rule		

User Level

read-write

Context

ip pbr-list ip-rule, ip capture-list ip-rule, ip qos-list ip-rule, ip access-control-list ip-rule, crypto-list ip-rule

Note:

The **not** form of the command is not relevant in the crypto-list ip-rule context.

Example

To specify that rule 22 applies to all packets whose destination port is 300:

```
G450-001(ACL 330/ip rule 22)# tcp destination-port eq 300
```

To specify that rule 22 applies to all packets *except* for those whose destination port is 300:

```
G450-001(ACL 330/ip rule 22)# not tcp destination-port eq 300
```

Related Commands - Policy-based routing

destination-ip, dscp (policy-based routing, packet sniffing, VPN), icmp, ip-protocol, show ip capture-list, source-ip, tcp source-port, udp destination-port, udp source-port

Related Commands - Policy

composite-operation, destination-ip, dscp (policy), icmp, show composite-operation, show dscp-table, show isdn bri link, source-ip, tcp established, tcp source-port, udp destination-port, udp source-port

Related Commands - VPN

description (ip rule), destination-ip, dscp (policy-based routing, packet sniffing, VPN), fragment, icmp, ip crypto-list, ip-protocol, ip-rule (VPN), local-address, protect crypto map, source-ip, show ip crypto-list, tcp source-port, udp destination-port, udp source-port

---

tcp source-port

Use the **tcp source-port** command to define a source port with the TCP protocol for which to apply the current rule.

Use the **no** form of the command to set the TCP source port to any. If the protocol is not TCP, the protocol is set to TCP and the destination port is set to its default value.

Use the **not** form of the command to specify that the rule applies to all TCP ports other than the requested ports. If the protocol is not TCP, the protocol is set to TCP and the destination port is set to its default value.

Note:

Issuing this command also sets the protocol to be TCP, if it is not already.

Syntax

[not] tcp source-port any | {{eq | lt | gt} {*port_name* | *port_number*}} | {range *start_port end_port*}

no tcp source-port

Parameters

Parameter	Description	Possible Values	Default Value
any	Keyword that specifies to apply the rule to a port with any name or number		
eq	Keyword that specifies to apply the rule to a port whose name or number matches exactly to the specified name or number		
lt	Keyword that specifies to apply the rule to a port whose name or number is less than the specified name or number		
gt	Keyword that specifies to apply the rule to a port whose name or number is greater than the specified name or number		
port_name	The name of the port for which to apply the rule		
port_number	The number of the port for which to apply the rule		
range	Keyword indicating that a range of ports is specified		
start_port	The start of a port range for which to apply the rule		
end_port	The end of a port range for which to apply the rule		

User Level

read-write

Context

ip pbr-list ip-rule, ip capture-list ip-rule, ip qos-list ip-rule, ip access-control-list ip-rule, ip crypto-list ip-rule

Note:

The **not** form of the command is not relevant in the crypto-list ip-rule context.

Example

To specify that rule 22 applies to all packets whose source port is greater than port number 95:

```
G450-001(ACL 330/ip rule 22)# tcp source-port gt 95
```

To specify that rule 22 applies to all packets whose source port is less than or equal to port 95:

```
G450-001(ACL 330/ip rule 22)# not tcp source-port gt 95
```

Related Commands - Policy-based routing

destination-ip, dscp (policy-based routing, packet sniffing, VPN), icmp, ip-protocol, show ip capture-list, source-ip, tcp destination-port, udp destination-port, udp source-port

Related Commands - Policy

composite-operation, destination-ip, dscp (policy), icmp, show composite-operation, show dscp-table, show isdn bri link, source-ip, tcp destination-port, tcp established, udp destination-port, udp source-port

Related Commands - VPN

description (ip rule), destination-ip, dscp (policy-based routing, packet sniffing, VPN), fragment, icmp, ip crypto-list, ip-protocol, ip-rule (VPN), local-address, protect crypto map, source-ip, show ip crypto-list, tcp destination-port, udp destination-port, udp source-port

udp destination-port

Use the **udp destination-port** command to define a destination port with the UDP protocol for which to apply the current rule.

Use the **no** form of the command to set the UDP destination port to any. If the protocol is not UDP, the protocol is set to UDP and the source port is set to its default value.

Use the **not** form of the command to specify that the rule applies to all UDP ports other than the requested ports. If the protocol is not UDP, the protocol is set to UDP and the source port is set to its default value

Note:

Issuing this command also sets the protocol to be UDP, if it is not already.

Syntax

udp destination-port any | {{eq | lt | gt} {*port_name* | *port_number*}} | {range *start_port end_port}*

no udp destination-port

Parameters

Parameter	Description	Possible Values	Default Value
any	Keyword that specifies to apply the rule to a port with any name or number		
eq	Keyword that specifies to apply the rule to a port whose name or number matches exactly to the specified name or number		
lt	Keyword that specifies to apply the rule to a port whose name or number is less than the specified name or number		
gt	Keyword that specifies to apply the rule to a port whose name or number is greater than the specified name or number		
port_name	The name of the port for which to apply the rule		
port_number	The number of the port for which to apply the rule		
range	Keyword indicating that a range of ports is specified		
start_port	The start of a port range for which to apply the rule		
end_port	The end of a port range for which to apply the rule		

User Level

read-write

Context

ip pbr-list ip-rule, ip qos-list ip-rule, ip capture-list ip-rule, ip access-control-list ip-rule, ip crypto-list ip-rule

Note:

The **not** form of the command is not relevant in the crypto-list ip-rule context.

Example

To specify that rule 22 applies to all packets whose destination port is port 300:

```
G450-001(ACL 330/ip rule 22)# udp destination-port eq 300
```

To specify that rule 22 applies to all packets *except* for those whose destination port is 300:

```
G450-001(ACL 330/ip rule 22)# not udp destination-port eq 300
```

Related Commands - Policy-based routing

destination-ip, dscp (policy-based routing, packet sniffing, VPN), icmp, ip-protocol, show ip capture-list, source-ip, tcp destination-port, tcp source-port, udp source-port

Related Commands - Policy

composite-operation, destination-ip, dscp (policy), icmp, show composite-operation, show dscp-table, show isdn bri link, source-ip, tcp destination-port, tcp established, tcp source-port, udp source-port

Related Commands - VPN

description (ip rule), destination-ip, dscp (policy-based routing, packet sniffing, VPN), fragment, icmp, ip crypto-list, ip-protocol, ip-rule (VPN), local-address, protect crypto map, source-ip, show ip crypto-list, tcp destination-port, tcp source-port, udp source-port

---

udp source-port

Use the **udp source-port** command to define a source port with the UDP protocol for which to apply the current rule.

Use the **no** form of the command to set the UDP source port to `any`. If the protocol is not UDP, the protocol is set to UDP and the destination port is set to its default value.

Use the **not** form of the command to specify that the rule applies to all UDP ports other than the requested ports. If the protocol is not UDP, the protocol is set to UDP and the destination port is set to its default value.

Note:

Issuing this command also sets the protocol to be UDP, if it is not already.

Syntax

udp source-port any | {{**eq** | **lt** | **gt**} {***port_name*** | ***port_number***}} | {**range** ***start_port end_port***}

no udp source-port

Parameters

Parameter	Description	Possible Values	Default Value
any	Keyword that specifies to apply the rule to a port with any name or number		
eq	Keyword that specifies to apply the rule to a port whose name or number matches exactly to the specified name or number		
lt	Keyword that specifies to apply the rule to a port whose name or number is less than the specified name or number		
gt	Keyword that specifies to apply the rule to a port whose name or number is greater than the specified name or number		
port_name	The name of the port for which to apply the rule		
port_number	The number of the port for which to apply the rule		
range	Keyword indicating that a range of ports is specified		
start_port	The start of a port range for which to apply the rule		
end_port	The end of a port range for which to apply the rule		

User Level

read-write

Context

ip pbr-list ip-rule, ip qos-list ip-rule, ip capture-list ip-rule, ip access-control-list ip-rule, ip crypto-list ip-rule

Note:

The **not** form of the command is not relevant in the crypto-list ip-rule context.

Example

To specify that rule 22 applies to all packets whose source port is greater than port 95:

```
G450-001(ACL 330/ip rule 22)# udp source-port gt 95
```

To specify that rule 22 applies to all packets whose source port is less than or equal to port 95:

```
G450-001(ACL 330/ip rule 22)# not udp source-port gt 95
```

Related Commands - Policy-based routing

destination-ip, dscp (policy-based routing, packet sniffing, VPN), icmp, ip-protocol, show ip capture-list, source-ip, tcp destination-port, tcp source-port, udp destination-port

Related Commands - Policy

composite-operation, destination-ip, dscp (policy), icmp, show composite-operation, show dscp-table, show isdn bri link, source-ip, tcp destination-port, tcp established, tcp source-port, udp destination-port

Related Commands - VPN

description (ip rule), destination-ip, dscp (policy-based routing, packet sniffing, VPN), fragment, icmp, ip crypto-list, ip-protocol, ip-rule (VPN), local-address, protect crypto map, source-ip, show ip crypto-list, tcp destination-port, tcp source-port, udp destination-port

name

Use the **name** command to assign a name to the specified list or operation. Use the **no** form of the command to return the name to the default value.

Syntax

[no] name *name*

Parameters

Parameter	Description	Possible Values	Default Value
name	The name of the list or operation. **Note:** If you wish to include spaces in the description, you must enclose the string in quotation marks (“”).	String of 1-31 characters	

User Level

read-write

Context

dhcp pool, dhcp pool vendor specific, dhcp pool option, ip qos-list, ip qos-list dscp-table, ip qos-list composite-operation, ip access-control-list, ip next-hop-list, ip capture-list, ip pbr-list, ip crypto-list.

Example

To specify the name of access control list 330 as Admin13:

```
G450-001(ACL 330)# name Admin13
```

Related Commands - DHCP server

bootfile, client-identifier, default-router, dns-server, domain-name, end-ip-addr, lease, next-server, option, server-name, show ip dhcp-pool, start-ip-addr, subnet-mask, value, vendor-specific-option

Related Commands - Packet sniffing

capture buffer-mode, capture buffer-size, capture filter-group, capture interface, capture max-frame-size, capture start, capture stop, capture-service, clear capture-buffer, ip capture-list, show capture, show capture-buffer hex

Related Commands - Policy-based routing

ip-rule (policy, policy-based routing, packet sniffing), owner, show isdn bri link, show list

Related Commands - Policy

composite-operation, cookie, ip-fragments-in, ip-option-in, ip-rule (policy, policy-based routing, packet sniffing), owner, show composite-operation, show dscp-table, show isdn bri link, show list, cos, dscp (policy)

---

owner

Use the **owner** command to specify the owner of the current list.

Syntax

owner *owner_name*

Parameters

Parameter	Description	Possible Values	Default Value
owner_name	Name of the owner	string	

User Level

read-write

Context

ip access-control-list, ip qos-list, ip capture-list, ip pbr-list, ip crypto-list

Example

To set the owner of access control list 330 as MGAdmin3:

```
G450-001(ACL 330)# owner MGAdmin3
```

Related Commands - Packet sniffing

composite-operation, cookie, copy capture-file ftp, copy capture-file scp, copy capture-file tftp, ip-rule (policy, policy-based routing, packet sniffing), show ip capture-list, show upload status

Related Commands - Policy-based routing

ip-rule (policy, policy-based routing, packet sniffing), name, show isdn bri link, show list

Related Commands - Policy

composite-operation, cookie, dscp-table, ip-fragments-in, ip-option-in, ip-rule (policy, policy-based routing, packet sniffing), name, show composite-operation, show isdn bri link, show list

---

pre-classification

Use the **pre-classification** command to specify which priority tag the current QoS list uses for data flows. Use the **no** form of the command to reset the QoS list to use the default priority tag, **trust-cos-dscp**.

Syntax

pre-classification ***tag_type***

no pre-classification

Parameters

Parameter	Description	Possible Values	Default Value
tag_type	The type of priority tag used with data flows	**untrusted**, **trust-cos**, **trust-dscp**, **trust-cos-dscp**	

User Level

read-write

Context

ip qos-list

Example

To specify that the current QoS list uses the dscp priority tag:

```
G450-001(QoS 440)# pre-classification trust-dscp
```

Related Commands

ip access-control-list, ip access-group, ip policy-list-copy, ip qos-group, ip qos-list, ip simulate, show ip access-control-list, show ip qos-list

show composite-operation

Use the **show composite-operation** command to display information about a specific composite-operation. Use the command without a parameter to display information about all composite-operations.

Syntax

show composite-operation [*composite_operation_index*]

Parameters

Parameter	Description	Possible Values	Default Value
composite_operation_index	The composite-operation to display	**0-19**	

User Level

read-write

Context

ip access-control-list, ip access-control-list ip-rule, ip qos-list, ip qos-list ip-rule, ip qos-list composite-operation

Example

To display information about composite-operation 13:

```
G450-001(QoS 440)# show composite-operation 13

Index Name                 CoS       DSCP      Trust
----- -------------------- --------- --------- ------------
13    HSPackets            cos3      1         No
```

Related Commands

composite-operation, cookie, destination-ip, dscp (policy), dscp-table, icmp, ip-rule (policy, policy-based routing, packet sniffing), show composite-operation, show dscp-table, show isdn bri link, show list, source-ip, tcp destination-port, tcp established, tcp source-port, udp destination-port, udp source-port, cos, dscp (policy-based routing, packet sniffing, VPN), name

show dscp-table

Use the **show dscp-table** command to display a specific entry in the DSCP table. If no DSCP index is specified, the entire DSCP table is displayed.

Syntax

show dscp-table [*index*]

Parameters

Parameter	Description	Possible Values	Default Value
index	The DSCP entry		

User Level

read-write

Context

ip qos-list, ip qos-list dscp-table, ip qos-list ip-rule

Example

To display the entire DSCP table:

```
G450-001(QoS 444)# show dscp-table

Trust configuration is trust-cos
DSCP     Action            Precedence     Name
---- -------------------- ---------- ------------
0    No-Change            mandatory  DSCP#0
1    No-Change            mandatory  DSCP#1
2    No-Change            mandatory  DSCP#2
3    No-Change            mandatory  DSCP#3
4    No-Change            mandatory  DSCP#4
5    No-Change            mandatory  DSCP#5
6    No-Change            mandatory  DSCP#6
7    No-Change            mandatory  DSCP#7
8    No-Change            mandatory  DSCP#8
9    No-Change            mandatory  DSCP#9
10   No-Change            mandatory  DSCP#10
11   No-Change            mandatory  DSCP#11
.
.
.
63   No-Change              mandatory    DSCP#63
```

Related Commands

composite-operation, cookie, dscp-table, ip-rule (policy, policy-based routing, packet sniffing), name, owner, show composite-operation, show isdn bri link, show list

---

show ip-rule

Use the **show ip-rule** command to display the attributes of a specific rule. Leave the ***rule_number*** parameter blank to display all rules.

Syntax

show ip-rule [*rule_number*]

Parameters

Parameter	Description	Possible Values	Default Value
rule_number	The specific rule for which attributes are displayed		

User Level

read-write

Context

ip access-control-list, ip access-control-list/ip-rule, ip qos-list, ip qos-list/ip-rule, ip capture-list, ip capture-list/ip-rule, ip pbr-list, ip pbr-list/ip-rule

Example

To display information about ip rule 22 in access-control-list 320:

```
G450-001(ACL 320/ip rule 22)# show ip-rule 22

I.D.  Protocol IP  Wildcard         Port      Operation
----- -------- --- ---------------- --------- ----------
22    Ip       Src                  Any       permit
               Dst                  Any
```

Following is an example of the output that appears if DoS-classification is configured:

```
Index    Protocol      IP         Wildcard        Port   Operation
         DSCP                                             Fragment rule
-----    ------  ---  ---------   -------------- ------ --------------
123      Any     Src  1.2.3.4         Host          Any         Permit
         Any     Dst  Any                           Any         No

Dos classification: other-attack
234      Any     Src  2.2.2.2         Host          Any         Permit
         Any     Dst  Any                           Any         No

Dos classification: fraggle
345      Any     Src  3.3.3.3         Host          Any         Permit
         Any     Dst  Any                           Any         No

Dos classification: ip-spoofing
Deflt    Any     Src  Any                           Any         Permit
         Any     Dst  Any                           Any         No
```

Related Commands - Policy-based routing: ip pbr-list

destination-ip, dscp (policy-based routing, packet sniffing, VPN), next-hop (policy-based routing), show ip next-hop-list

Related Commands - Policy-based routing: ip pbr-list: ip-rule

ip-rule (policy, policy-based routing, packet sniffing), name, owner, show list

Related Commands - Policy

composite-operation, cookie, dscp-table, ip-fragments-in, ip-option-in, ip-rule (policy, policy-based routing, packet sniffing), name, owner, show composite-operation, show dscp-table, show isdn bri link, show list, composite-operation, destination-ip, dscp (policy), icmp, source-ip, tcp destination-port, tcp established, tcp source-port, udp destination-port, udp source-port

Related Commands - DoS

DoS-classification, show ip access-control-list

---

show list

Use the **`show list`** command to display information about a given list.

Syntax

`show list`

User Level

read-write

Context

ip access-control-list, ip qos-list, ip capture-list, ip pbr-list

Example

To show detailed information about access control list 330:

```
G450-001(ACL 330)# show list
Index Name           Owner
----- -------------- ------------
330   SplitPriority     Admin
ip options: Permit
ip fragments : Permit
```

```
Index   Protocol        IP    Wildcard      Port     Operation-
-----   --------        ---   -----------   -----    ----------
22      tcp             Src   Any           Any      Permit
                        Dst   Any           Any
Deflt   Any             Src   Any           Any      Permit
                        Dst   Any           Any
```

Related Commands - Policy-based routing

ip-rule (policy, policy-based routing, packet sniffing), name, owner, show isdn bri link

Related Commands - Policy

composite-operation, cookie, dscp-table, ip-fragments-in, ip-option-in, ip-rule (policy, policy-based routing, packet sniffing), name, owner, show composite-operation, show dscp-table, show isdn bri link, show list

ip simulate

Use the **ip simulate** command to test the action of a policy on a simulated packet.

Syntax

ip simulate *policy_list_number direction* [*priority*] [*dscp_value*] *source destination* [*protocol* [*source_port destination_port* [*established*]]]

Parameters

Parameter	Description	Possible Values	Default Value
policy_list_number	The number of the policy	**1-999**	For PBR: **1** For ACL: **300** For Qos: **400** For Capture: **500**
direction	The direction	**in**, **out**	
priority	The priority	**fwd0-fwd7**	
dscp_value		**dscp0-dscp63**	
source	The source IP address		
destination	The destination IP address		
protocol	The protocol to use	**ip**, **tcp**, **udp**, **1-255**	

Parameter	Description	Possible Values	Default Value
source_port	The source port of the simulated packet	**1-65535**	
destination_port	The destination port of the simulated packet	**1-65535**	
established	The value of the TCP established bit		

User Level

read-write

Context

interface:Serial (DS1 PPP L2, DS1 PPP L2-L3, DS1 FR-SUB L2, DS1 FR-SUB L2-L3, USP PPP L2, USP PPP L2-L3), Loopback (L2, L2-L3), FastEthernet (L2-L3, L3, PPP L2, PPP L2-L3, PPP L3), Tunnel (L2, L2-L3), VLAN (L2, L2-L3), Dialer (L2, L2-L3)

Example

To simulate the effects of applying access control list 330 to a packet entering the media gateway through the FastEthernet interface, from IP address 192.67.85.12 to IP address 192.67.54.25:

```
G450-001(if:FastEthernet 10/2)# ip simulate 330 in 192.67.85.12 192.67.54.25
ip
```

Related Commands

ip access-control-list, ip access-group, ip policy-list-copy, ip qos-group, ip qos-list, pre-classification, show ip access-control-list, show ip qos-list

show ip qos-list

Use the **show ip qos-list** command to display the attributes about a specific QoS list, or all QoS lists, for the current interface.

Note:

To specify an interface name that includes spaces, enclose the entire name in quotation marks (for example, “FastEthernet 10/2”).

Syntax

show ip qos-list {*list_number* | all | active-list-in | active-list-out | active-list-in-out} [detailed]

Parameters

Parameter	Description	Possible Values	Default Value
list_number	The QoS list to display		
all	Keyword specifying to display all QoS lists		
active-list-in	Keyword specifying to display lists for the in direction		
active-list-out	Keyword specifying to display lists for the out direction		
active-list-in-out	Keyword specifying to display lists for in and out directions		
detailed	Keyword specifying to display detailed information		

User Level

read-write

Context

general, interface:Serial (DS1 PPP L2, DS1 PPP L2-L3, DS1 FR-SUB L2, DS1 FR-SUB L2-L3, USP PPP L2, USP PPP L2-L3), FastEthernet (L2, L2-L3), VLAN (L2, L2-L3), Loopback (L2, L2-L3), Tunnel (L2, L2-L3), Dialer (L2, L2-L3)

Example

To display information about all QoS lists:

```
G450-001(if:Vlan 1)# show ip qos-list all

List Number: 400
---------------
List Name: Default QoS List
Default Action: No-Change
Owner: other
List Trust: trust-cos
```

To display detailed information about all the QoS lists:

```
G450-001(super)# show ip qos-list all detailed

Index Name                            Owner
----- ------------------------------- -------------------------
400   Default QoS List                other

Index Protocol IP  Wildcard         Port            Operation
----- -------- --- ---------------- --------------- --------------
Deflt  Any     Src  Any              Any             Trust-DSCP-CoS
               Dst  Any              Any

Index Name                            Owner
----- ------------------------------- -------------------------
440   list #440                       other

Index Protocol IP  Wildcard         Port            Operation
----- -------- --- ---------------- --------------- --------------
Deflt  Any     Src  Any              Any             Trust-DSCP-CoS
               Dst  Any              Any
```

Related Commands

ip access-control-list, ip access-group, ip policy-list-copy, ip qos-group, ip qos-list, ip simulate, pre-classification, show ip access-control-list, interface fastethernet, interface serial, set qos bearer, set qos bearer, set qos control, set qos signal, show queue, show voip-parameters

Policy-based routing

ip next-hop-list

Use the **ip next-hop-list** command to enter the context of the specified next hop list. If the list does not exist, it is created. Use the **no** form of this command to delete the specified next hop list.

Syntax

ip next-hop-list *next_hop_number*

no ip next-hop-list *next_hop_number*

Parameters

Parameter	Description	Possible Values	Default Value
next_hop_number	The number of the next hop list	**1-20**	

User Level

read-write

Context

general

Example

To enter the context of hop list 2:

```
G450-001(super)# ip next-hop-list 2
G450-001(super-next hop list 2)#
```

Related Commands

ip pbr-group, ip pbr-list, show ip active-lists, show ip active-pbr-lists, show ip pbr-list

next-hop-interface

Use the **next-hop-interface** command to add the specified interface to the next hop path for the current next hop list. Use the **no** form of this command to delete an interface from the next hop list.

Syntax

next-hop-interface {***index*** | ***interface_name***} **[track** ***track-index***]

no next-hop-interface {***index***}

Parameters

Parameter	Description	Possible Values	Default Value
index	The index in the array of next hops belonging to the specific next hop list	**1-20**	
interface_name	The specified next hop interface name	The layer2 interfaces: • **Serial** • **GRE Tunnel** • **Dialer** • **null0** • **WAN FastEthernet (running PPPoE or DHCP client)**	
track	Keyword that applies tracking to monitor the route. **Note:** Object tracking cannot be configured on Null0.		
track-index	The index number of the object tracker	**1-50**	

User Level

read-write

Context

ip next-hop-list

Examples

To add interface Serial 4/1:0 to the next hop path for the current next hop list:

```
G450-001(config-next hop list 1)# next-hop-interface 3 Serial 4/1:0 track 1
```

Related Commands

next-hop-ip, show next-hop

next-hop-ip

Use the **next-hop-ip** command to add the specified ip address to the next hop path for the current next hop list. Use the **no** form of this command to delete an IP address from the next hop list.

Syntax

next-hop-ip {*index* | *ip_address*} [track *track-index*]

no next-hop-ip {*index*}

Parameters

Parameter	Description	Possible Values	Default Value
index	The index in the array of next hops belonging to the specific next hop list	**1-20**	
ip_address	The specified next hop IP address		
track	Keyword that applies tracking to monitor the route		
track-index	The index number of the object tracker	**1-50**	

User Level

read-write

Context

ip next-hop-list

Example

To add the IP address of 149.49.200.2 to the next hop path for the current next-hop list, applying object tracker 3:

```
G450-001(super)# next-hop-ip 2 149.49.200.2 track 3
```

Related Commands

next-hop-interface, show next-hop

show next-hop

Use the **show next-hop** command to show the next-hop entries in the current list.

Syntax

show next-hop

User Level

read-only

Context

ip next-hop-list

Example

To show the next-hop entries in the current list:

```
G450-001(super-next hop list 1)#show next-hop

List index: 1
List name:  NH1

Index   Interface         Next-Hop       Status   Track   Track-Status
-----  ----------------- -------------- ------   -----   ------------
  1     Vlan 78             149.49.78.9      up         1          up
  2     Tunnel 7            7.0.0.2          up       N/A         N/A
```

Related Commands

next-hop-interface, next-hop-ip

ip pbr-group

Use the **ip pbr-group** command to apply the specified PBR list to the current interface. The PBR list is applied to ingress packets only. Use the **no** form of the command to disable the specified PBR list.

Syntax

[no] ip pbr-group *list_number*

Parameters

Parameter	Description	Possible Values	Default Value
list_number	The list number of the PBR list to be applied to ingress packets of the current interface	**801-899**	

User Level

read-write

Context

interface:Serial (DS1 PPP L2, DS1 PPP L2-L3, DS1 FR-SUB L2, DS1 FR-SUB L2-L3, USP PPP L2, USP PPP L2-L3), FastEthernet (L2, L2-L3, PPP L2, PPP L2-L3, PPP L3), VLAN (L2, L2-L3), Loopback (L2, L2-L3), Tunnel (L2, L2-L3), Dialer (L2, L2-L3)

Example

To apply PBR list 811 to the current interface:

```
G450-001(super)# ip pbr-group 811
```

Related Commands

ip next-hop-list, ip pbr-list, show ip active-lists, show ip active-pbr-lists, show ip pbr-list

ip pbr-list

Use the **ip pbr-list** command to enter context of the specified PBR list. If the list does not exist, it is created. Use the **no** form of the command to suspend the specified PBR list.

Syntax

ip pbr-list *list_number*

Parameters

Parameter	Description	Possible Values	Default Value
list_number	The list number of the policy list being entered	**801-899**	

User Level

read-write

Context

general

Example

To enter the context of pbr-list 802:

```
G450-001(super)# ip pbr-list 802
G450-001(super-PBR 802)#
```

Related Commands

ip next-hop-list, ip pbr-group, show ip active-lists, show ip active-pbr-lists, show ip pbr-list

cookie

Use the **cookie** command to set the cookie for the current list.

Syntax

cookie *cookie_number*

Parameters

Parameter	Description	Possible Values	Default Value
cookie_number	The ID number of the cookie	**0-268435455**	

User Level

read-write

Context

ip access-control-list, ip qos-list, ip capture-list, ip pbr-list, ip crypto-list

Example

To specify the cookie for QoS list 440 as 257:

```
G450-001(QoS 440)# cookie 257
```

Related Commands - Packet sniffing

composite-operation, copy capture-file ftp, copy capture-file scp, copy capture-file tftp, ip-rule (policy, policy-based routing, packet sniffing), owner, show ip capture-list, show upload status

Related Commands - Policy

composite-operation, dscp-table, ip-fragments-in, ip-option-in, ip-rule (policy, policy-based routing, packet sniffing), name, owner, show composite-operation, show isdn bri link, show list

icmp

Use the **icmp** command to specify that the current rule applies to a specific type of ICMP packet.

Use the **not** form of this command to specify that the rule applies to all packets *except* those of the requested ICMP attribute. If the IP protocol is not ICMP, it is set to ICMP.

Use the **no** form of the command to specify that the current rule applies to any type of ICMP packet.

Note:

The **icmp** command also sets the IP protocol to ICMP.

Syntax

[not] icmp {*name* | {*icmp_type icmp_code*}}

no icmp

Parameters

Parameter	Description	Possible Values	Default Value
name	Specify that the rule applies to this ICMP name		
icmp_type	Specify that the rule applies to this icmp type	For an ip-rule: **0-256** For a QoS rule: **0-65535**	
icmp_code	Specify that the rule applies to this icmp code	For an ip-rule: **0-256** For a QoS rule: **0-65535**	

User Level

read-write

Context

ip capture-list/ip-rule, ip access-control-list/ip-rule, ip pbr-list/ip-rule, ip qos-list/ip-rule, ip crypto-list ip-rule

Note:

The **not** form of the command is not relevant in the crypto-list ip-rule context.

Example

To specify that rule 27 applies to ICMP error-reply packets:

```
G450-001(ACL 333/ip rule 27)# icmp Echo-Reply
```

To specify that rule 33 applies to any ICMP packet type *except* type 1 code 2:

```
G450-001(ACL 333/ip rule 33)# not icmp 1 2
```

Related Commands - Policy-based routing

destination-ip, dscp (policy-based routing, packet sniffing, VPN), ip-protocol, show ip capture-list, source-ip, tcp destination-port, tcp source-port, udp destination-port, udp source-port

Related Commands - Policy

composite-operation, cookie, destination-ip, dscp (policy), dscp-table, icmp, ip-rule (policy, policy-based routing, packet sniffing), owner, show composite-operation, show dscp-table, show isdn bri link, show list, source-ip, tcp destination-port, tcp established, tcp source-port, udp destination-port, udp source-port

Related Commands - VPN

description (ip rule), destination-ip, dscp (policy-based routing, packet sniffing, VPN), fragment, ip crypto-list, ip-protocol, ip-rule (VPN), local-address, protect crypto map, source-ip, show ip crypto-list, tcp destination-port, tcp source-port, udp destination-port, udp source-port

ip-rule (policy, policy-based routing, packet sniffing)

Use the **ip-rule** command to enter configuration mode for the specified rule. If the specified rule does not exist, the system creates it and enters its configuration mode.

Syntax

ip-rule {***rule_index*** | **default**}

Parameters

Parameter	Description	Possible Values	Default Value
rule_index	Number of the rule to edit	**1-9999**	
default	Keyword indicating ip-rule number 10,000 (last rule in the ordered list of rules)		

User Level

read-write

Context

ip access-control-list, ip qos-list, ip capture-list, ip pbr-list

Example

To enter configuration mode for ip-rule 22:

```
G450-001(ACL 330)# ip-rule 22
G450-001(ACL 330/ip rule 22)#
```

Related Commands - Packet sniffing

composite-operation, cookie, copy capture-file ftp, copy capture-file scp, copy capture-file tftp, owner, show ip capture-list, show upload status

Related Commands - Policy-based routing

name, owner, show isdn bri link, show list

Related Commands - Policy

composite-operation, cookie, dscp-table, ip-fragments-in, ip-option-in, name, owner, show composite-operation, show isdn bri link, show list

destination-ip

Use the **destination-ip** command to specify the destination IP address of packets to which the current rule applies.

Use the **not** form of the command to specify that the current rule applies to all packets that *do not* have this destination IP address.

Use the **no** form of the command to set the destination IP address to `any`.

Syntax

[not] destination-ip {host *ip*}|any|{*ip wildcard*}

no destination-ip

Parameters

Parameter	Description	Possible Values	Default Value
host	Keyword that specifies the current rule applies to a single host IP address		
ip	The destination IP address of the rule		
any	Keyword that specifies the current rule applies to any address		
ip wildcard	The range of IP addresses of the rule. The zero bits in the wildcard correspond to bits in the IP address that remain fixed. The one bits in the wildcard correspond to bits in the IP address that can vary. **Note:** This is the opposite of how bits are used in a netmask.		

User Level

read-write

Context

ip capture-list/ip-rule, ip access-control-list/ip-rule, ip pbr-list/ip-rule, ip qos-list/ip-rule, ip crypto-list ip-rule

Example

To specify that rule 22 applies to all packets having destination IP address 135.64.104.102:

```
G450-001(QoS 460/rule 22)# destination-ip host 135.64.104.102
```

To specify that rule 17 applies to packets whose destination IP address is *not* in the range of 176.13.0.0 through 176.13.255.255:

```
G450-001(QoS 460/rule 17)# not destination-ip 176.13.0.0 0.0.255.255
```

Related Commands - Packet sniffing

dscp (policy-based routing, packet sniffing, VPN), icmp, ip-protocol, show ip capture-list, source-ip, tcp destination-port, tcp source-port, udp destination-port, udp source-port

Related Commands - Policy-based routing

dscp (policy-based routing, packet sniffing, VPN), next-hop (policy-based routing), show ip next-hop-list, show isdn bri link

Related Commands - Policy

composite-operation, dscp (policy), show dscp-table, icmp, show composite-operation, show isdn bri link, source-ip, tcp destination-port, tcp established, tcp source-port, udp destination-port, udp source-port

Related Commands - VPN

description (ip rule), ip crypto-list, ip-rule (VPN), local-address, protect crypto map, source-ip, show ip crypto-list

dscp (policy-based routing, packet sniffing, VPN)

Use the **dscp** command to specify the DSCP value that is set by the current policy operation.

Use the **not** form of the command to specify that the current operation set any DSCP value other than this value.

Use the **no** form of the command to specify that the current operation set the DSCP value to any.

Note:

In crypto-lists, this command is only applicable for rules whose action is **no protect**.

Syntax

dscp {*dscp_value* | any}

not dscp *dscp_value*

no dscp

Parameters

Parameter	Description	Possible Values	Default Value
dscp_value	The DSCP value	**0-63**	
any	Keyword indicating that any DSCP value will match the rule. Using this keyword is equivalent to specifying **no dscp**.		

User Level

read-write

Context

ip capture-list ip-rule, ip pbr-list ip-rule, ip access-control-list ip-rule, ip qos-list ip-rule, ip crypto-list ip-rule

Note:

In ip-rule context, this command tests packets to see if they match the specified DSCP value, but does not change the DSCP value.

Note:

The **not** form of the command is not relevant in the crypto-list ip-rule context.

Example

To specify that ip-rule 10 in crypto-list 901 match a DSCP value of 43:

```
G450-001(Crypto 901/ip rule 10)# dscp 43
```

To specify that ip-rule 10 in crypto-list 901 match any DSCP value:

```
G450-001(Crypto 901/ip rule 10)# not dscp 56
```

Related Commands - Packet sniffing

destination-ip, icmp, ip-protocol, show ip capture-list, source-ip, tcp destination-port, tcp source-port, udp destination-port, udp source-port

Related Commands - Policy-based routing

destination-ip, next-hop (policy-based routing), show ip next-hop-list, show isdn bri link

Related Commands - VPN

description (ip rule), destination-ip, fragment, icmp, ip crypto-list, ip-protocol, ip-rule (VPN), local-address, protect crypto map, source-ip, show ip crypto-list, tcp destination-port, tcp source-port, udp destination-port, udp source-port

fragment

Use the **fragment** command to apply the current rule for non-initial fragments only.

Note:

You cannot specify TCP/UDP ports or ICMP code/type for a rule when using the **fragment** command.

Syntax

fragment

User Level

read-write

Context

ip qos-list composite-operation, ip capture-list ip-rule, ip pbr-list ip-rule, ip access-control-list ip-rule, ip qos-list ip-rule, ip crypto-list ip-rule

Example

To apply the rule for non-initial fragments:

```
G450-001(super-Capture 520/ip rule 15)# fragment
```

Related Commands - Packet sniffing

dscp (policy-based routing, packet sniffing, VPN), destination-ip, icmp, ip-protocol, show ip capture-list, source-ip, tcp destination-port, tcp source-port, udp destination-port, udp source-port

Related Commands - Policy-based routing

dscp (policy-based routing, packet sniffing, VPN), destination-ip, next-hop (policy-based routing), show ip next-hop-list, show isdn bri link

Related Commands - Policy

composite-operation, dscp (policy), destination-ip, icmp, show composite-operation, show isdn bri link, source-ip, tcp destination-port, tcp established, tcp source-port, udp destination-port, udp source-port, cos, name

Related Commands - VPN

description (ip rule), destination-ip, dscp (policy-based routing, packet sniffing, VPN), icmp, ip crypto-list, ip-protocol, ip-rule (VPN), local-address, protect crypto map, source-ip, show ip crypto-list, tcp destination-port, tcp source-port, udp destination-port, udp source-port

ip-protocol

Use the **ip-protocol** command to specify that the current rule applies to packets having the specified IP protocol.

Use the **no** form of the command to set the IP protocol to its default value.

Use the **not** form of this command to specify that the current rule applies to all packets *except* those having the specified IP protocol.

Syntax

[not] ip-protocol *protocol_name* | *protocol_number*

no ip-protocol

Parameters

Parameter	Description	Possible Values	Default Value
protocol_name	Name of the IP protocol to match		
protocol_number	Number of the IP protocol to match	**1-255**	

User Level

read-write

Context

ip access-control-list/ip-rule, ip capture-list/ip-rule, ip pbr-list/ip-rule, ip qos-list/ip-rule, crypto-list/ip-rule

Note:

The not form of the command is not relevant in the crypto-list/ip-rule context.

Example

To specify that rule 22 applies to all packets having an IP protocol of ICMP:

```
G450-001(ACL 330/ip rule 22)# ip-protocol icmp
```

To specify that rule 22 applies to all packets having any IP protocol *except* ICMP:

```
G450-001(ACL 330/ip rule 22)# not ip-protocol icmp
```

Related Commands

destination-ip, dscp (policy-based routing, packet sniffing, VPN), icmp, show ip capture-list, source-ip, tcp destination-port, tcp source-port, udp destination-port, udp source-port

Related Commands - VPN

description (ip rule), destination-ip, dscp (policy-based routing, packet sniffing, VPN), fragment, icmp, ip crypto-list, ip-rule (VPN), local-address, protect crypto map, source-ip, show ip crypto-list, tcp destination-port, tcp source-port, udp destination-port, udp source-port

next-hop (policy-based routing)

Use the **next-hop** command to specify the next hop policy to use when the current rule is applied.

Syntax

next-hop {list *list_number* | DBR}

Parameters

Parameter	Description	Possible Values	Default Value
list	Keyword indicating that a next hop list will be specified to be used for the current rule		
list_number	The next hop list to be used for the current rule	**1-20**	
DBR	Keyword indicating to use destination based routing (not policy based routing) for the current rule		

User Level

read-write

Context

ip-pbr-list/ip-rule

Example

To specify that the next-hop list 1 should be used for the current rule:

```
G450-001(super)# next-hop list 1
G450-001(super)# next-hop DBR
```

Related Commands

destination-ip, dscp (policy-based routing, packet sniffing, VPN), show ip next-hop-list, show isdn bri link

show ip next-hop-list

Use the **show ip next-hop-list** command to show the details of the next hop list.

Syntax

show ip next-hop-list {*next_hop_number* | all}

Parameters

Parameter	Description	Possible Values	Default Value
next_hop_number	The index number of the entry in the next hop list	**1-20**	
all	Keyword indicating the entire next hop list		

User Level

read-only

Context

ip pbr-list ip-rule

Example

To show the details of the entire next hop list:

```
G450-001(super)# show ip next-hop-list all

Index Name
----- ---------
1 list #1
3 list #3
```

To show the details of entry #3 in the next hop list:

```
G450-001(super)# show ip next-hop-list 3
next hop list does not exist
```

Related Commands

destination-ip, dscp (policy-based routing, packet sniffing, VPN), next-hop (policy-based routing), show isdn bri link

show ip-rule

Use the **show ip-rule** command to display the attributes of a specific rule. Leave the ***rule_number*** parameter blank to display all rules.

Syntax

show ip-rule [*rule_number*]

Parameters

Parameter	Description	Possible Values	Default Value
rule_number	The specific rule for which attributes are displayed		

User Level

read-write

Context

ip access-control-list, ip access-control-list/ip-rule, ip qos-list, ip qos-list/ip-rule, ip capture-list, ip capture-list/ip-rule, ip pbr-list, ip pbr-list/ip-rule

Example

To display information about ip rule 22 in access-control-list 320:

```
G450-001(ACL 320/ip rule 22)# show ip-rule 22

I.D.  Protocol IP  Wildcard         Port      Operation
----- -------- --- ---------------- --------- ----------
22    Ip       Src                  Any       permit
               Dst                  Any
```

Following is an example of the output that appears if DoS-classification is configured:

```
Index    Protocol      IP         Wildcard        Port   Operation
         DSCP                                             Fragment rule
-----    ------  ---  ---------   -------------- ------ --------------
123      Any     Src  1.2.3.4         Host          Any         Permit
         Any     Dst  Any                           Any         No

Dos classification: other-attack
234      Any     Src  2.2.2.2         Host          Any         Permit
         Any     Dst  Any                           Any         No
```

```
Dos classification: fraggle
345      Any     Src  3.3.3.3         Host          Any         Permit
         Any     Dst  Any                           Any         No

Dos classification: ip-spoofing
Deflt    Any     Src  Any                           Any         Permit
         Any     Dst  Any                           Any         No
```

Related Commands - Policy-based routing: ip pbr-list

destination-ip, dscp (policy-based routing, packet sniffing, VPN), next-hop (policy-based routing), show ip next-hop-list

Related Commands - Policy-based routing: ip pbr-list: ip-rule

ip-rule (policy, policy-based routing, packet sniffing), name, owner, show list

Related Commands - Policy

composite-operation, cookie, dscp-table, ip-fragments-in, ip-option-in, ip-rule (policy, policy-based routing, packet sniffing), name, owner, show composite-operation, show dscp-table, show isdn bri link, show list, composite-operation, destination-ip, dscp (policy), icmp, source-ip, tcp destination-port, tcp established, tcp source-port, udp destination-port, udp source-port

Related Commands - DoS

DoS-classification, show ip access-control-list

---

source-ip

Use the **source-ip** command to indicate that the current rule applies to packets from the specified source IP address.

Use the **no** form of the command to indicate that the current rule applies to packets from any IP address.

Use the **not** form of the command to indicate that the current rule applies to all packets *except* those coming from the specified IP address.

Syntax

[not] source-ip {host *ip_address* | any | *ip_address wildcard*}

no source-ip

Parameters

Parameter	Description	Possible Values	Default Value
host	Keyword that indicates a specific host IP address		
ip_address	The IP address of packets to which the rule is applied		
any	Keyword that indicates any IP address		
ip_address ***wildcard***	The range of IP addresses of the rule. The zero bits in the wildcard correspond to bits in the IP address that remain fixed. The one bits in the wildcard correspond to bits in the IP address that can vary. **Note:** This is the opposite of how bits are used in a netmask.		

User Level

read-write

Context

ip pbr-list ip-rule, ip qos-list ip-rule, ip capture-list ip-rule, ip access-control-list ip-rule, ip crypto-list ip-rule

Note:

The **not** form of the command is not relevant in the crypto-list ip-rule context.

Example

To specify that rule 22 of QoS policy list 460 applies to any packet coming from IP address 135.64.104.102:

```
G450-001(QoS 460/rule 22)# source-ip host 135.64.104.102
```

To specify that rule 22 of QoS policy list 460 applies to any packet *except* those coming from IP address 135.64.104.102:

```
G450-001(QoS 460/rule 22)# not source-ip host 135.64.104.102
```

Related Commands - Policy-based routing

destination-ip, dscp (policy-based routing, packet sniffing, VPN), icmp, ip-protocol, show ip capture-list, tcp destination-port, tcp source-port, udp destination-port, udp source-port

Related Commands - Policy

composite-operation, destination-ip, dscp (policy), icmp, show composite-operation, show dscp-table, show isdn bri link, tcp destination-port, tcp established, tcp source-port, udp destination-port, udp source-port

Related Commands - VPN

description (ip rule), destination-ip, ip crypto-list, ip-rule (VPN), local-address, protect crypto map, show ip crypto-list

tcp destination-port

Use the **tcp destination-port** command to define a destination port with the TCP protocol for which to apply the current rule.

Use the **no** form of the command to set the TCP destination port to any. If the protocol is not TCP, the protocol is set to TCP and the source port is set to its default value.

Use the **not** form of the command to specify that the rule applies to all TCP ports other than the requested ports. If the protocol is not TCP, the protocol is set to TCP and the source port is set to its default value

Note:

Issuing this command also sets the protocol to be TCP, if it is not already.

Syntax

[not] tcp destination-port any | {{eq | lt | gt} {*port_name* | *port_number*}} | {range *start_port end_port*}

no tcp destination-port

Parameters

Parameter	Description	Possible Values	Default Value
any	Keyword that specifies to apply the rule to a port with any name or number		
eq	Keyword that specifies to apply the rule to a port whose name or number matches exactly to the specified name or number		

Parameter	Description	Possible Values	Default Value
lt	Keyword that specifies to apply the rule to a port whose name or number is less than the specified name or number		
gt	Keyword that specifies to apply the rule to a port whose name or number is greater than the specified name or number		
port_name	The name of the port for which to apply the rule		
port_number	The number of the port for which to apply the rule		
range	Keyword indicating that a range of ports is specified		
start_port	The start of a port range for which to apply the rule		
end_port	The end of a port range for which to apply the rule		

User Level

read-write

Context

ip pbr-list ip-rule, ip capture-list ip-rule, ip qos-list ip-rule, ip access-control-list ip-rule, crypto-list ip-rule

Note:

The **not** form of the command is not relevant in the crypto-list ip-rule context.

Example

To specify that rule 22 applies to all packets whose destination port is 300:

```
G450-001(ACL 330/ip rule 22)# tcp destination-port eq 300
```

To specify that rule 22 applies to all packets *except* for those whose destination port is 300:

```
G450-001(ACL 330/ip rule 22)# not tcp destination-port eq 300
```

Related Commands - Policy-based routing

destination-ip, dscp (policy-based routing, packet sniffing, VPN), icmp, ip-protocol, show ip capture-list, source-ip, tcp source-port, udp destination-port, udp source-port

Related Commands - Policy

composite-operation, destination-ip, dscp (policy), icmp, show composite-operation, show dscp-table, show isdn bri link, source-ip, tcp established, tcp source-port, udp destination-port, udp source-port

Related Commands - VPN

description (ip rule), destination-ip, dscp (policy-based routing, packet sniffing, VPN), fragment, icmp, ip crypto-list, ip-protocol, ip-rule (VPN), local-address, protect crypto map, source-ip, show ip crypto-list, tcp source-port, udp destination-port, udp source-port

---

tcp source-port

Use the **tcp source-port** command to define a source port with the TCP protocol for which to apply the current rule.

Use the **no** form of the command to set the TCP source port to any. If the protocol is not TCP, the protocol is set to TCP and the destination port is set to its default value.

Use the **not** form of the command to specify that the rule applies to all TCP ports other than the requested ports. If the protocol is not TCP, the protocol is set to TCP and the destination port is set to its default value

Note:

Issuing this command also sets the protocol to be TCP, if it is not already.

Syntax

[not] tcp source-port any | {{eq | lt | gt} {*port_name* | *port_number*}} | {range *start_port end_port*}

no tcp source-port

Parameters

Parameter	Description	Possible Values	Default Value
any	Keyword that specifies to apply the rule to a port with any name or number		
eq	Keyword that specifies to apply the rule to a port whose name or number matches exactly to the specified name or number		
lt	Keyword that specifies to apply the rule to a port whose name or number is less than the specified name or number		

Parameter	Description	Possible Values	Default Value
gt	Keyword that specifies to apply the rule to a port whose name or number is greater than the specified name or number		
port_name	The name of the port for which to apply the rule		
port_number	The number of the port for which to apply the rule		
range	Keyword indicating that a range of ports is specified		
start_port	The start of a port range for which to apply the rule		
end_port	The end of a port range for which to apply the rule		

User Level

read-write

Context

ip pbr-list ip-rule, ip capture-list ip-rule, ip qos-list ip-rule, ip access-control-list ip-rule, ip crypto-list ip-rule

Note:

The **not** form of the command is not relevant in the crypto-list ip-rule context.

Example

To specify that rule 22 applies to all packets whose source port is greater than port number 95:

```
G450-001(ACL 330/ip rule 22)# tcp source-port gt 95
```

To specify that rule 22 applies to all packets whose source port is less than or equal to port 95:

```
G450-001(ACL 330/ip rule 22)# not tcp source-port gt 95
```

Related Commands - Policy-based routing

destination-ip, dscp (policy-based routing, packet sniffing, VPN), icmp, ip-protocol, show ip capture-list, source-ip, tcp destination-port, udp destination-port, udp source-port

Related Commands - Policy

composite-operation, destination-ip, dscp (policy), icmp, show composite-operation, show dscp-table, show isdn bri link, source-ip, tcp destination-port, tcp established, udp destination-port, udp source-port

Related Commands - VPN

description (ip rule), destination-ip, dscp (policy-based routing, packet sniffing, VPN), fragment, icmp, ip crypto-list, ip-protocol, ip-rule (VPN), local-address, protect crypto map, source-ip, show ip crypto-list, tcp destination-port, udp destination-port, udp source-port

udp destination-port

Use the **udp destination-port** command to define a destination port with the UDP protocol for which to apply the current rule.

Use the **no** form of the command to set the UDP destination port to any. If the protocol is not UDP, the protocol is set to UDP and the source port is set to its default value.

Use the **not** form of the command to specify that the rule applies to all UDP ports other than the requested ports. If the protocol is not UDP, the protocol is set to UDP and the source port is set to its default value

Note:

Issuing this command also sets the protocol to be UDP, if it is not already.

Syntax

udp destination-port any | {{eq | lt | gt} {*port_name* | *port_number*}} | {range *start_port end_port*}

no udp destination-port

Parameters

Parameter	Description	Possible Values	Default Value
any	Keyword that specifies to apply the rule to a port with any name or number		
eq	Keyword that specifies to apply the rule to a port whose name or number matches exactly to the specified name or number		
lt	Keyword that specifies to apply the rule to a port whose name or number is less than the specified name or number		
gt	Keyword that specifies to apply the rule to a port whose name or number is greater than the specified name or number		
port_name	The name of the port for which to apply the rule		

Parameter	Description	Possible Values	Default Value
port_number	The number of the port for which to apply the rule		
range	Keyword indicating that a range of ports is specified		
start_port	The start of a port range for which to apply the rule		
end_port	The end of a port range for which to apply the rule		

User Level

read-write

Context

ip pbr-list ip-rule, ip qos-list ip-rule, ip capture-list ip-rule, ip access-control-list ip-rule, ip crypto-list ip-rule

Note:

The **not** form of the command is not relevant in the crypto-list ip-rule context.

Example

To specify that rule 22 applies to all packets whose destination port is port 300:

```
G450-001(ACL 330/ip rule 22)# udp destination-port eq 300
```

To specify that rule 22 applies to all packets *except* for those whose destination port is 300:

```
G450-001(ACL 330/ip rule 22)# not udp destination-port eq 300
```

Related Commands - Policy-based routing

destination-ip, dscp (policy-based routing, packet sniffing, VPN), icmp, ip-protocol, show ip capture-list, source-ip, tcp destination-port, tcp source-port, udp source-port

Related Commands - Policy

composite-operation, destination-ip, dscp (policy), icmp, show composite-operation, show dscp-table, show isdn bri link, source-ip, tcp destination-port, tcp established, tcp source-port, udp source-port

Related Commands - VPN

description (ip rule), destination-ip, dscp (policy-based routing, packet sniffing, VPN), fragment, icmp, ip crypto-list, ip-protocol, ip-rule (VPN), local-address, protect crypto map, source-ip, show ip crypto-list, tcp destination-port, tcp source-port, udp source-port

udp source-port

Use the **udp source-port** command to define a source port with the UDP protocol for which to apply the current rule.

Use the **no** form of the command to set the UDP source port to any. If the protocol is not UDP, the protocol is set to UDP and the destination port is set to its default value.

Use the **not** form of the command to specify that the rule applies to all UDP ports other than the requested ports. If the protocol is not UDP, the protocol is set to UDP and the destination port is set to its default value

Note:

Issuing this command also sets the protocol to be UDP, if it is not already.

Syntax

udp source-port any | {**eq** | **lt** | **gt**} {***port_name*** | ***port_number***} | {**range** ***start_port end_port***}

no udp source-port

Parameters

Parameter	Description	Possible Values	Default Value
any	Keyword that specifies to apply the rule to a port with any name or number		
eq	Keyword that specifies to apply the rule to a port whose name or number matches exactly to the specified name or number		
lt	Keyword that specifies to apply the rule to a port whose name or number is less than the specified name or number		
gt	Keyword that specifies to apply the rule to a port whose name or number is greater than the specified name or number		
port_name	The name of the port for which to apply the rule		
port_number	The number of the port for which to apply the rule		

Parameter	Description	Possible Values	Default Value
range	Keyword indicating that a range of ports is specified		
start_port	The start of a port range for which to apply the rule		
end_port	The end of a port range for which to apply the rule		

User Level

read-write

Context

ip pbr-list ip-rule, ip qos-list ip-rule, ip capture-list ip-rule, ip access-control-list ip-rule, ip crypto-list ip-rule

Note:

The **not** form of the command is not relevant in the crypto-list ip-rule context.

Example

To specify that rule 22 applies to all packets whose source port is greater than port 95:

```
G450-001(ACL 330/ip rule 22)# udp source-port gt 95
```

To specify that rule 22 applies to all packets whose source port is less than or equal to port 95:

```
G450-001(ACL 330/ip rule 22)# not udp source-port gt 95
```

Related Commands - Policy-based routing

destination-ip, dscp (policy-based routing, packet sniffing, VPN), icmp, ip-protocol, show ip capture-list, source-ip, tcp destination-port, tcp source-port, udp destination-port

Related Commands - Policy

composite-operation, destination-ip, dscp (policy), icmp, show composite-operation, show dscp-table, show isdn bri link, source-ip, tcp destination-port, tcp established, tcp source-port, udp destination-port

Related Commands - VPN

description (ip rule), destination-ip, dscp (policy-based routing, packet sniffing, VPN), fragment, icmp, ip crypto-list, ip-protocol, ip-rule (VPN), local-address, protect crypto map, source-ip, show ip crypto-list, tcp destination-port, tcp source-port, udp destination-port

name

Use the **name** command to assign a name to the specified list or operation. Use the **no** form of the command to return the name to the default value.

Syntax

[no] name *name*

Parameters

Parameter	Description	Possible Values	Default Value
name	The name of the list or operation. **Note:** If you wish to include spaces in the description, you must enclose the string in quotation marks (“”).	String of 1-31 characters	

User Level

read-write

Context

dhcp pool, dhcp pool vendor specific, dhcp pool option, ip qos-list, ip qos-list dscp-table, ip qos-list composite-operation, ip access-control-list, ip next-hop-list, ip capture-list, ip pbr-list, ip crypto-list

Example

To specify the name of access control list 330 as “Admin13”:

```
G450-001(ACL 330)# name Admin13
```

Related Commands - DHCP server

bootfile, client-identifier, default-router, dns-server, domain-name, end-ip-addr, lease, next-server, option, server-name, show ip dhcp-pool, start-ip-addr, subnet-mask, value, vendor-specific-option

Related Commands - Packet sniffing

capture buffer-mode, capture buffer-size, capture filter-group, capture interface, capture max-frame-size, capture start, capture stop, capture-service, clear capture-buffer, ip capture-list, show capture, show capture-buffer hex

Related Commands - Policy-based routing

ip-rule (policy, policy-based routing, packet sniffing), owner, show isdn bri link, show list

Related Commands - Policy

composite-operation, cookie, ip-fragments-in, ip-option-in, ip-rule (policy, policy-based routing, packet sniffing), owner, show composite-operation, show dscp-table, show isdn bri link, show list, cos, dscp (policy)

---

owner

Use the **owner** command to specify the owner of the current list.

Syntax

owner *owner_name*

Parameters

Parameter	Description	Possible Values	Default Value
owner_name	Name of the owner	string	

User Level

read-write

Context

ip access-control-list, ip qos-list, ip capture-list, ip pbr-list, ip crypto-list

Example

To set the owner of access control list 330 as MGAdmin3:

```
G450-001(ACL 330)# owner MGAdmin3
```

Related Commands - Packet sniffing

composite-operation, cookie, copy capture-file ftp, copy capture-file scp, copy capture-file tftp, ip-rule (policy, policy-based routing, packet sniffing), show ip capture-list, show upload status

Related Commands - Policy-based routing

ip-rule (policy, policy-based routing, packet sniffing), name, show isdn bri link, show list

Related Commands - Policy

composite-operation, cookie, dscp-table, ip-fragments-in, ip-option-in, ip-rule (policy, policy-based routing, packet sniffing), name, show composite-operation, show isdn bri link, show list

show ip-rule

Use the **show ip-rule** command to display the attributes of a specific rule. Leave the ***rule_number*** parameter blank to display all rules.

Syntax

show ip-rule [*rule_number*]

Parameters

Parameter	Description	Possible Values	Default Value
rule_number	The specific rule for which attributes are displayed		

User Level

read-write

Context

ip access-control-list, ip access-control-list/ip-rule, ip qos-list, ip qos-list/ip-rule, ip capture-list, ip capture-list/ip-rule, ip pbr-list, ip pbr-list/ip-rule

Example

To display information about ip rule 22 in access-control-list 320:

```
G450-001(ACL 320/ip rule 22)# show ip-rule 22

I.D.  Protocol IP  Wildcard         Port      Operation
----- -------- --- ---------------- --------- ----------
22    Ip       Src                  Any       permit
               Dst                  Any
```

Following is an example of the output that appears if DoS-classification is configured:

```
Index     Protocol       IP          Wildcard         Port   Operation
          DSCP                                                Fragment rule
-----     ------  ---  ---------   -------------- ------ --------------
123       Any     Src  1.2.3.4         Host           Any          Permit
          Any     Dst  Any                            Any          No

Dos classification: other-attack
234       Any     Src  2.2.2.2         Host           Any          Permit
          Any     Dst  Any                            Any          No

Dos classification: fraggle
345       Any     Src  3.3.3.3         Host           Any          Permit
          Any     Dst  Any                            Any          No

Dos classification: ip-spoofing
Deflt     Any     Src  Any                            Any          Permit
          Any     Dst  Any                            Any          No
```

Related Commands - Policy-based routing: ip pbr-list

destination-ip, dscp (policy-based routing, packet sniffing, VPN), next-hop (policy-based routing), show ip next-hop-list

Related Commands - Policy-based routing: ip pbr-list: ip-rule

ip-rule (policy, policy-based routing, packet sniffing), name, owner, show list

Related Commands - Policy

composite-operation, cookie, dscp-table, ip-fragments-in, ip-option-in, ip-rule (policy, policy-based routing, packet sniffing), name, owner, show composite-operation, show dscp-table, show isdn bri link, show list, composite-operation, destination-ip, dscp (policy), icmp, source-ip, tcp destination-port, tcp established, tcp source-port, udp destination-port, udp source-port

Related Commands - DoS

DoS-classification, show ip access-control-list

show list

Use the **show list** command to display information about a given list.

Syntax

show list

User Level

read-write

Context

ip access-control-list, ip qos-list, ip capture-list, ip pbr-list

Example

To show detailed information about access control list 330:

```
G450-001(ACL 330)# show list
Index Name           Owner
----- -------------- ------------
330   SplitPriority     Admin
ip options: Permit
ip fragments : Permit
Index  Protocol      IP   Wildcard     Port    Operation-
-----  --------      ---  -----------  -----   ----------
22     tcp           Src  Any          Any     Permit
                     Dst  Any          Any
Deflt  Any           Src  Any          Any     Permit
                     Dst  Any          Any
```

Related Commands - Policy-based routing

ip-rule (policy, policy-based routing, packet sniffing), name, owner, show isdn bri link

Related Commands - Policy

composite-operation, cookie, dscp-table, ip-fragments-in, ip-option-in, ip-rule (policy, policy-based routing, packet sniffing), name, owner, show composite-operation, show dscp-table, show isdn bri link, show list

show ip active-lists

Use the **show ip active-lists** command to display information about a specific policy list or all lists.

Syntax

show ip active-lists [*list_index*|*list_type*]

Parameters

Parameter	Description	Possible Values	Default Value
list_index	The index of the policy list to view	**300-499**	
list_type	The type of list	**ACL, Crypto, PBR, QoS**	

User Level

read-only

Context

general

Example

To display information about all lists:

```
G450-001(super)# show ip active-lists

Interface Name                   Dir. Type     Idx List Name
-------------------------------- ---- -------- --- ----------------
FastEthernet 10/2                In   ACL      300 Default ACL List
FastEthernet 10/2                In   QoS      400 Default QoS List
FastEthernet 10/2                Out  ACL      300 Default ACL List
FastEthernet 10/2                Out  QoS      400 Default QoS List
FastEthernet 10/2                ---- Crypto   901 list #901
Vlan 1                           In   ACL      300 Default ACL List
Vlan 1                           In   QoS      400 Default QoS List
Vlan 1                           Out  ACL      300 Default ACL List
Vlan 1                           Out  QoS      400 Default QoS List
```

Output fields

Name	Description
Interface Name	The name of the interface on which the list is operating
Dir.	The direction of traffic on which the list is operating. Options are: • In — The list is operating on incoming traffic • Out — The list is operating on outgoing traffic
Type	The type of list. Options are: • ACL — Access Control List. Controls which packets are authorized to pass through the interface. • QoS — QoS List. Can change the value of the QoS field in a packet. • PBR — Policy-Based Routing List. Determines the routing of packets that match the rules defined in the list. • Crypto — IPSec Crypto List. Provides encryption rules for VPN traffic that needs protection.
Idx	The ID of the list. List IDs must be within the following range: • ACL — 300-399 • QoS — 400-499 • PBR — 800-899 • Crypto — 900-999
List Name	The name of the list, as determined by the name command

Related Commands - Policy-based routing

ip next-hop-list, ip pbr-group, ip pbr-list, show ip active-pbr-lists, show ip pbr-list

Related Commands - VPN

clear crypto isakmp, Use the `clear crypto sa` command to clear all or specific IPSec SAs (Security Association structures)., clear crypto sa counters, ip crypto-list, show crypto ipsec sa, show crypto ipsec transform-set, show crypto isakmp peer, show crypto isakmp peer-group, show crypto isakmp policy, show crypto isakmp sa, show crypto map, show ip crypto-list

show ip active-pbr-lists

Use the **show ip active-pbr-lists** command to display details about a specific PBR list or all PBR lists.

Syntax

show ip active-pbr-lists [list_number]

Parameters

Parameter	Description	Possible Values	Default Value
list_number	The PBR list to view	**800-899**	

User Level

read-only

Context

general

Example

To display information about all PBR lists:

```
G450-001(super)# show ip active-pbr-lists

Interface Name   Index   List Name
-----------------------------------------
Vlan 1           801     Voice PBR List
Vlan 2           803     Data PBR List
```

Related Commands

ip next-hop-list, ip pbr-group, ip pbr-list, show ip active-lists, show ip pbr-list

show ip pbr-list

Use the **show ip pbr-list** command to display information about the specified pbr-list.

Syntax

show ip pbr-list {list_number | all} [detailed]

Parameters

Parameter	Description	Possible Values	Default Value
list_number	The pbr-list number to display	**800-899**	

User Level

read-only

Context

general, interface:Serial (DS1 PPP L2, DS1 PPP L2-L3, DS1 FR-SUB L2, DS1 FR-SUB L2-L3, USP PPP L2, USP PPP L2-L3), FastEthernet (L2, L2-L3), VLAN (L2, L2-L3), Loopback (L2, L2-L3), Tunnel (L2, L2-L3), Dialer (L2, L2-L3)

Example

To display information about pbr-list 801 in detail:

```
G450-001(super)# show ip pbr-list 801 detailed
```

Related Commands

ip next-hop-list, ip pbr-group, ip pbr-list, show ip active-lists, show ip active-pbr-lists

Port classification

set port classification

Use the **set port classification** command to set the port classification to either regular or valuable. Any change in the Spanning Tree state from Forwarding for a valuable port will erase all learned MAC addresses in the media gateway.

Syntax

set port classification ***module/port*** **{regular | valuable}**

Parameters

Parameter	Description	Possible Values	Default Value
module	The module number		
port	Number of the port on the module. You can also specify a range of ports separated by a dash, for example, 10/5-6 for both ETH LAN ports 5-6 on the front panel.		
regular	Keyword specifying that port classification be set to regular		
valuable	Keyword specifying that port classification be set to valuable		

User Level

read-write

Context

general

Example

To set the port classification for port 6/5 to valuable:

```
G450-001(super)# set port classification 6/5 valuable
Port 6/5 classification has been changed.
```

Related Commands

show port classification

show port classification

Use the **show port classification** command to display a port's classification. If no port is specified, information for all ports is displayed.

Syntax

show port classification [module/[port]]

Parameters

Parameter	Description	Possible Values	Default Value
module	Number of the module		
port	Number of the port on the module. You can also specify a range of ports separated by a dash, for example, 10/5-6 for both ETH LAN ports 5-6 on the front panel.		

User Level

read-only

Context

general

Example

To display information for port 6/5:

```
G450-001(super)# show port classification 6/5

Port   Port Classification
------ ---------------------
6/5    regular
```

Related Commands

set port classification

Port mirroring

clear port mirror

Use the **clear port mirror** command to delete a port mirroring pair.

Syntax

clear port mirror ***source_module/source_port dest_module/dest_port***

Parameters

Parameter	Description	Possible Values	Default Value
source_module	The module number of the source (mirrored) port		
source_port	The port number of the source (mirrored) port		
dest_module	The module number of the destination port		
dest_port	The port number of the destination port		

User Level

read-write

Context

general

Example

To disable the mirroring of port 4/1 by port 4/3:

```
G450-001(super)# clear port mirror 4/1 4/3
```

Related Commands

set port mirror, show port mirror

set port mirror

Use the **set port mirror** command to define a port mirroring source-destination pair. The second port receives a copy of all packets sent to and received by the first port.

Syntax

set port mirror source-port *module/port* mirror-port *module/port* sampling *sampling_value* direction *direction_value*

Parameters

Parameter	Description	Possible Values	Default Value
module	Number of the module		
port	Number of the port on the module. You can also specify a range of ports separated by a dash, for example, 10/5-6 for ETH LAN ports 5-6 on the front panel.		
sampling_value	Specifies whether to allow or disable sampling of the transmissions	**always**, **disable**	
direction_value	The direction of transmissions to mirror	**rx**, **tx**, **both**	

User Level

read-write

Context

general

Example

To set up port mirroring from port 10/5 to port 10/6 in the G450 for all packets sent and received:

```
G450-001(super)# set port mirror source-port 10/5 mirror-port 10/6 sampling
always direction both
```

Related Commands

clear port mirror, show port mirror

---

show port mirror

Use the **show port mirror** command to display mirroring information for the specified port. If no port is specified, information for all ports is displayed.

Syntax

show port mirror [*module/port*]

Parameters

Parameter	Description	Possible Values	Default Value
module	Number of the module		
port	Number of the port on the module		

User Level

read-only

Context

general

Example

To display port mirroring information for all ports:

```
G450-001(super)# show port mirror
```

Related Commands

clear port mirror, set port mirror

Port redundancy

set port redundancy

Use the **set port redundancy** command to define or remove redundancy pairs. A redundancy port acts as a backup port in case the primary port fails. The port can be any port that does not belong to a LAG or a LAG interface. Ensure that there is no redundancy scheme already defined on any of the ports.

Syntax

set port redundancy ***prim_module/prim_port second_module/second_port*** **{on|off}** **[*redundancy_name*]**

Parameters

Parameter	Description	Possible Values	Default Value
prim_module	The module number of the primary port		
prim_port	Primary port of the redundancy scheme		
second_module	The module number of the backup port		
second_port	Backup port of the redundancy scheme		
on	Keyword specifying to define the redundancy pair		
off	Keyword specifying to remove the redundancy pair		
redundancy_name	Name for the redundancy scheme		

User Level

read-write

Context

general

Example

To specify that port 10/6 acts as a backup port for port 10/5, and to name the redundancy pair red1:

```
G450-001(super)# set port redundancy 10/5 10/6 on red1
red1: Port 10/6 is redundant to port 10/5.
Port redundancy is active - entry is effective immediately
```

Note:

If you wish to define a name which includes spaces, you must enclose the entire name in quotation marks, for example “new york”.

Related Commands

set port redundancy enable|disable, set port redundancy-intervals, show port redundancy

set port redundancy enable|disable

Use the **set port redundancy enable|disable** command to globally enable or disable port redundancy on the device. Using this command does not delete existing redundancy entries.

Syntax

set port redundancy {enable|disable}

Parameters

Parameter	Description	Possible Values	Default Value
enable	Keyword specifying to enable port redundancy on the device		
disable	Keyword specifying to disable port redundancy on the device		

User Level

read-write

Context

general

Example

To globally enable port redundancy:

```
G450-001(super)# set port redundancy enable
All redundancy schemes are now enabled
```

Related Commands

set port redundancy, set port redundancy-intervals, show port redundancy

set port redundancy-intervals

Use the **set port redundancy-intervals** command to configure the two time constants that determine redundancy switchover parameters.

Syntax

set port redundancy-intervals ***min_time_between_switchovers*** {***switchback_interval*** | **none**}

Parameters

Parameter	Description	Possible Values	Default Value
min_time_between_switchovers	The minimum time, in milliseconds, between redundancy switchovers for each pair	**0-65000**	
switchback_interval	The period, in milliseconds, the primary port link has to be up before the system switches back. Specify **0** to indicate the system never switches back. Specify **1** to indicate that switchback occurs immediately after the primary port link returns.	**0-65000**	
none	Keyword indicating not to switch		

User Level

read-write

Context

general

Example

To specify a delay of 100 milliseconds before switching to the backup port, and a requirement that the primary port be up for 20 milliseconds before control is returned:

```
G450-001(super)# set port redundancy-intervals 100 20
```

Related Commands

set port redundancy, set port redundancy enable|disable, show port redundancy

show port redundancy

Use the **show port redundancy** command to display information about software port redundancy pairs defined on the media gateway.

Syntax

show port redundancy

User Level

read-only

Context

general

Example

To display port redundancy information:

```
G450-001(super)# show port redundancy

Redundancy Name     Primary Port        Secondary Port      Status
-----------------   --------------      ----------------    --------
bud      3/48                   3/47                   secondary
jack     3/46                   3/45                   secondary
tony     3/1                    3/2                    primary
wayne    3/34                   3/33                   secondary
Minimum Time between Switchovers: 1
Switchback interval: 3
```

Related Commands

set port redundancy, set port redundancy enable|disable, set port redundancy-intervals

Port status

show port

Use the **show port** command to display port status on I/O modules. If no port is specified, information for all ports is displayed.

Syntax

show port [*module*[/*port*]]

Parameters

Parameter	Description	Possible Values	Default Value
module	Number of the module		
port	Number of the port on the module. You can also specify a range of ports separated by a dash, for example, 10/5-6 for both ETH LAN ports 5-6 on the front panel.		

User Level

read-only

Context

general

Example

To display port information for all ports:

```
G450-001(super)# show port
Port   Name    Status    Vlan Level  Neg   Dup. Spd. Type
------ ------- --------- ---- ----- ------ ---- ---- ----------------
10/5   NO NAME connected  3     0   enable  full 100M G450 Media Gateway 10/100/
1000BaseT Port
10/6   NO NAME connected  3     0   enable  full 1G   G450 Media Gateway 10/100/
1000BaseT Port
```

Output fields

Name	Description
Port	Module and port number
Name	Name of port
Status	Status of the port — **connected, faulty, disabled, no link**
Vlan	VLAN ID of the port
Level	Priority level of the port — **0-7**
Neg	Auto-negotiation status of the port — **enabled, disabled**
Dup	Duplex setting for the port — **full, half**

1 of 2

Name	Description
Speed	Speed setting for the port — **10, 100, 1000**
Type	Port type, for example: **10/100BASE-TX, GBIC_SX, GBIC_LX, GBIC_not present, GBIC_unknown**
	2 of 2

Related Commands

show port point-to-point status

PPP encapsulation

interface serial

Use the **interface serial** command to enter Serial interface or sub interface configuration mode. If the specified interface or sub interface does not exist, the system creates it and enters its configuration mode.

Use the **no** form of the command to delete the interface. The **no** form can only be used to delete sub L3 and sub frame relay interfaces. The command fails for USP interfaces and when higher or lower layers are defined for that interface.

Syntax

[no] interface Serial *module/if_number* [*if_link_type*]

For USP interfaces ***if_number*** has the syntax:

port[.***ip_interface*** | {.***sub_interface***[.***ip_interface***]}]

For DS1 interfaces ***if_number*** has the syntax:

port:***channel_group***[.***ip_interface*** | {.***sub_interface***[.***ip_interface***]}]

Parameters

Parameter	Description	Possible Values	Default Value
module	The interface module number		
port	The port number of the interface		

Parameter	Description	Possible Values	Default Value
channel_group		For E1: **0-30** For T1: **0-23**	
sub_interface		**1-127**	
ip_interface		**0-1024**	
if_link_type		**point-to-point**	

User Level

read-write

Context

general, interface:Serial (FR SUB)

Example

To create point to point sub-interface number 17 over channel group 2 over E1/T1 controller number 1:

```
G450-001(super)# interface Serial 3/1:2.17 point-to-point
```

Related Commands

description (interface), interface console, interface fastethernet, interface loopback, interface tunnel, interface USB-modem, interface vlan, ip address, ip admin-state, ip broadcast-address, ip crypto-group, load-interval, show ip interface brief

encapsulation

Use the **encapsulation** command to set the encapsulation mode for a Serial interface. By default, the Serial interface has PPP encapsulation. Use the **no** form of this command, which has no parameters, to return to the default.

Use the **encapsulation frame-relay** option to create a frame-relay interface of the IETF (RFC1490/RFC2427) type or non-IETF type. This command deletes the PPP interface associated with the current Serial interface. The PPP interface cannot be deleted if at least one IP interface is defined on it. Instead, the following message appears, “You cannot update this L2 interface since L3 interfaces are defined on it.”

By default, the Frame Relay encapsulation type for the main interface is IETF.

Note:

Non-IETF encapsulation is compatible with other vendors.

Syntax

encapsulation {ppp | frame-relay [*type*]}

no encapsulation

Parameters

Parameter	Description	Possible Values	Default Value
ppp	Keyword indicating that the encapsulation be set to PPP		
frame-relay	Keyword indicating that the encapsulation be set to Frame Relay		
type	The value for the type of Frame Relay encapsulation	**IETF** (RFC1490/RFC2427), **non-IETF**	**IETF**

User Level

read-write

Context

interface:Serial (DS1 PPP L2, DS1 PPP L2-L3, DS1 FR L2, USP PPP L2, USP PPP L2-L3, USP FR L2)

Example

To create a Frame-Relay interface with IETF encapsulation:

```
G450-001(if:Serial 3/1:1)# encapsulation frame-relay ietf
```

Related Commands - Frame relay encapsulation

frame-relay interface-dlci, frame-relay lmi-n391dte, frame-relay lmi-n392dte, frame-relay lmi-n393dte, frame-relay lmi-type, frame-relay priority-dlci-group, frame-relay traffic-shaping, ip address

Related Commands - PPP encapsulation

ip address, keepalive (PPP), ppp timeout ncp, ppp timeout retry, show interfaces

ip address

Use the **ip address** command to assign an IP address and mask to an interface. Use the **no** form of this command to delete an IP interface.

Syntax

ip address {*ip_address mask* [*admin_state*]}|negotiated

no ip address

Parameters

Parameter	Description	Possible Values	Default Value
ip_address	The IP address assigned to the interface		
mask	Mask for the associated IP subnet		
admin_state	The administration status. This parameter is not used with the Console interface.	**up**, **down**	**up**
negotiated	Keyword specifying that the interface receive address and mask from a remote device		

User Level

read-write

Context

Interface: Console, Serial (DS1 PPP L2-L3, DS1 PPP L3, DS1 FR-SUB L2-L3, DS1 FR-SUB L3, USP PPP L2-L3, USP PPP L3), FastEthernet (L2-L3, L3, PPP L2-L3, PPP L3), VLAN (L2-L3, L3), USB-modem, Loopback (L2-L3, L3), Tunnel (L2-L3, L3), Dialer (L2-L3, L3)

Example

To assign the IP address 192.168.22.33 with mask 255.255.255.0 to the FastEthernet interface:

```
G450-001(if:FastEthernet 10/2)# ip address 192.168.22.33 255.255.255.0
```

Related Commands

description (interface), interface console, interface fastethernet, interface loopback, interface serial, interface tunnel, interface USB-modem, interface vlan, ip admin-state, ip broadcast-address, load-interval, show ip interface brief

keepalive (PPP)

Use the **keepalive** command in a PPP interface to enable PPP keepalive, in order to maintain a persistent connection. Entering keepalive without a parameter returns the keepalive to its default value. Use the **no** form of this command to disable PPP keepalive.

Syntax

[no] keepalive [*seconds*]

Parameters

Parameter	Description	Possible Values	Default Value
seconds	The number of seconds between PPP keepalive messages. Entering keepalive 0 disables keepalive.	**0-32767**	**10**

User Level

read-write

Context

interface:Serial (DS1 PPP L2, DS1 PPP L2-L3, DS1 FR L2, USP PPP L2, USP PPP L2-L3, USP FR L2)

Example

To enable PPP keepalive, and generate a message every 300 seconds:

```
G450-001(if:Serial 3/1)# keepalive 300
```

Related Commands

encapsulation, ip address, ppp timeout ncp, ppp timeout retry, show interfaces

ppp timeout ncp

Use the **ppp timeout ncp** command to set the maximum time, in seconds, that PPP allows for negotiation of a network layer protocol. If no network protocol is negotiated within the given time, the connection is terminated. Use the **no** form of the command to disable the timeout feature.

Syntax

[no] ppp timeout ncp *seconds*

Parameters

Parameter	Description	Possible Values	Default Value
seconds	The time in seconds that PPP allows for negotiation of a network layer protocol	**1-65535**	

User Level

read-write

Context

Interface: Console, FastEthernet (PPP L2, PPP L2-L3), Serial (DS1 PPP L2, DS1 PPP L2-L3, USP PPP L2, USP PPP L2-L3), Dialer (L2, L2-L3), USB-modem

Example

To specify that PPP will allow 60 seconds for negotiation of a network protocol:

```
G450-001(super)# ppp timeout ncp 60
```

Related Commands

encapsulation, ip address, keepalive (PPP), ppp timeout retry, show interfaces

ppp timeout retry

Use the **ppp timeout retry** command to set the maximum time to wait for a response during PPP negotiation. Use the **no** form of the command to restore the timeout value to its default.

Syntax

[no] ppp timeout retry *seconds*

Parameters

Parameter	Description	Possible Values	Default Value
seconds	The authentication timeout in seconds	**1-255**	**2**

User Level

read-write

Context

Interface: Console, FastEthernet (PPP L2, PPP L2-L3), Serial (DS1 PPP L2, DS1 PPP L2-L3, USP PPP L2, USP PPP L2-L3), Dialer (L2, L2-L3), USB-modem

Example

To specify that PPP will wait up to 30 seconds for a response during negotiation:

```
G450-001(super)# ppp timeout retry 30
```

Related Commands

encapsulation, ip address, keepalive (PPP), ppp timeout ncp, show interfaces

show interfaces

Use the **show interfaces** command to display interface configuration and statistics for a particular interface or all interfaces. The Frame Relay sub-interface only includes the following counters:

- packets & bytes in
- packets & bytes out
- input errors

- output drops

Syntax

show interfaces [*interface_type interface_identifier*]

Parameters

Parameter	Description	Possible Values	Default Value
interface_type	The type of interface	**Dialer, FastEthernet, Serial, Vlan, Loopback, Console, Tunnel, USB**	
interface_identifier	The interface number. The format varies depending on the value of interface_type: For FastEthernet: **module/port** For Serial: **module/port:channel-group** For Vlan: **Vlan id** For LoopBack: **Loopback number** For Tunnel: **Tunnel number**	For FastEthernet: **10/2 or 10/4** For Serial(USP): **3/1, 4/1, 8/1** For Serial (DS1): module/port: **3/1, 4/1, 8/1** channel-group: E1: **0-30** T1: **0-23** For VLAN: **1-4090** For Loopback: **1-99** For Tunnel: **1-50** For Dialer: **1**	

User Level

read-write

Context

general

Example

To show information about all the interfaces:

```
G450-001(super)# show interfaces
Vlan 1 is up, line protocol is up
Physical address is 00.04.0d.29.c5.11.
Internet address is 172.16.1.139, mask is 255.255.255.240
Primary management interface
MTU 1500 bytes. Bandwidth 100000 kbit.
Reliability 255/255 txLoad 1/255 rxLoad 1/255
```

```
Encapsulation ARPA, ICC-VLAN
Link status trap disabled
Full-duplex, 100Mb/s
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:30, Last output 00:00:30
Last clearing of 'show interface' counters never.
5 minute input rate 144 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 input drops, 0 output drops, 0 unknown protocols
3425 packets input, 323518 bytes
3425 broadcasts received, 0 giants
0 input errors, 0 CRC
32 packets output, 896 bytes
0 output errors, 0 collisions

FastEthernet 10/2 is up, line protocol is down
Physical address is 00.04.0d.29.c5.10.
MTU 1500 bytes. Bandwidth 10000 kbit.
Reliability 1/255 txLoad 255/255 rxLoad 255/255
Encapsulation ARPA
Link status trap disabled
Half-duplex, 10Mb/s, 10BaseTX
ARP type: ARPA, ARP Timeout 04:00:00
Dynamic CAC BBL: 1500 kbps
Dynamic CAC activation priority: 50
Dynamic CAC interface status: active
Last input never, Last output never
Last clearing of 'show interface' counters never.
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 input drops, 0 output drops, 0 unknown protocols
0 packets input, 0 bytes
0 broadcasts received, 0 giants
0 input errors, 0 CRC
0 packets output, 0 bytes
0 output errors, 0 collisions

Tunnel 1 is up, line protocol is up
Internet address is 177.0.0.17, mask is 255.0.0.0
MTU 468 bytes. Bandwidth 9 kbit
Reliability 255/255 txLoad 1/255 rxLoad 1/255
Encapsulation GRE
Link status trap enabled
Keepalive set (10 sec), retries 3
Tunnel source 17.0.0.17, destination 12.0.0.3
Tunnel protocol/transport GRE/IP, key 777
Checksumming of packets enabled
Tunnel DSCP 63, Tunnel TTL 255
Path MTU Discovery, ager 10 mins, MTU 976, expires 00:09:33
Last input never, Last output never
Last clearing of 'show interface' counters never.
```

```
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 input drops, 0 output drops, 0 unknown protocols
0 packets input, 0 bytes
0 broadcasts received, 0 giants
0 input errors, 0 CRC
0 packets output, 0 bytes
0 output errors, 0 collisions

Console asynchronous mode is terminal
Terminal baud rate is 9600
```

Related Commands - Frame relay encapsulation

clear frame-relay counters, frame-relay class-dlci, interface serial, map-class frame-relay, fragment, show frame-relay pvc brief

Related Commands - PPP encapsulation

interface dialer, interface fastethernet, interface serial

Related Commands - Verifying WAN configuration

show controllers, show frame-relay fragment, show frame-relay lmi, show frame-relay pvc, show frame-relay traffic, show interfaces, show ip interface, show map-class frame-relay

PPPoE (PPP over Ethernet)

interface FastEthernet

Use the **interface FastEthernet** command to enter Interface FastEthernet configuration mode. Use the **no** form of this command to delete an IP interface.

If the specified interface does not exist, the system creates it and enters its configuration mode.

Syntax

[no] interface FastEthernet [*module/port*[.*ip_interface*]]

Parameters

Parameter	Description	Possible Values	Default Value
module	The module number of the interface	**10**	
port	The port number of the interface	**3**	
ip_interface	The IP sub-interface number within this interface. A number of IP interfaces may be bound to a Layer 3 interface.	**0-1024**	

User Level

read-write

Context

general

Example

To create a FastEthernet interface and enter its context:

```
G450-001(super)# interface FastEthernet 10/2
```

To create a Level 3 sub-interface on the FastEthernet interface:

```
G450-001(super)# interface FastEthernet 10/2.1
```

Related Commands

description (interface), interface console, interface loopback, interface serial, interface tunnel, interface USB-modem, interface vlan, ip address, ip admin-state, ip broadcast-address, ip crypto-group, load-interval, show ip interface brief

encapsulation pppoe

Use the **encapsulation pppoe** command to enable the PPPoE client. Use the **no** form of the command to return to disable the PPPoE client.

Note:

The **encapsulation pppoe** command fails if:

- ip address is configured on the interface
- The interface is part of a backup scheme
- Dynamic CAC is configured on the interface

Syntax

encapsulation pppoe

no encapsulation

User Level

read-write

Context

interface:FastEthernet

Example

To create a PPPoE interface:

```
G450-001(if:FastEthernet 10/2)# encapsulation pppoe
```

Related Commands

mtu, ppp chap hostname, ppp chap password, ppp pap sent-username, pppoe-client persistent delay, pppoe-client persistent max-attempts, pppoe-client service-name, pppoe-client wait-for-ipcp

ip address negotiated

Use the **ip address negotiated** command to enable obtaining an IP address via PPP/IPCP negotiation. Use the **no** form of this command to disable IP address negotiation.

Note:

The **ip address negotiated** command is intended primarily for PPPoE and dialer modem.

Note:

When you release a negotiated IP address using **no ip address negotiated**, any DNS information is removed as well.

Note:

You cannot configure both DHCP address negotiation and PPP/ICMP address negotiation on the FastEthernet interface.

Syntax

[no] ip address negotiated

User Level

read-write

Context

interface:FastEthernet (PPP L2-L3), Dialer (L2-L3)

Example

To enable obtaining an IP address via PPP/IPCP negotiation:

```
G450-001(config-if:FastEthernet 10/2)# ip address negotiated
```

Related Commands

ppp ipcp dns request

---

mtu

Use the **mtu** command to set the current interface's Maximum Transmission Unit (MTU). Use the **no** form of this command to restore the interface's MTU to its default value.

Note:

The ***size_in_bytes*** parameter specifies the Layer 3 packet size. Layer 2 headers are added to the packet afterwards. The Layer 2 headers vary in size, depending on the type of interface. Thus the total size of the MTU is the sum of the ***size_in_bytes*** value and the Layer 2 headers.

Syntax

[no] mtu *size_in_bytes*

Parameters

Parameter	Description	Possible Values	Default Value
size_in_bytes	The Maximum Transmission Unit in bytes	**64-1500**	**1500**

User Level

read-write

Context

interface:Serial (DS1 PPP L2-L3, DS1 PPP L2, DS1 FR L2, USP FR L2, USP PPP L2, USP PPP L2-L3), FastEthernet (L2, L2-L3), Dialer (L2, L2-L3)

Example

To specify the Maximum Transmission Unit for the Serial 3/1:1 interface to be 1000 bytes:

```
G450-001(if:Serial 3/1:1)# mtu 1000
```

Related Commands - PPPoE

encapsulation pppoe, ppp chap hostname, ppp chap password, ppp pap sent-username, pppoe-client persistent delay, pppoe-client persistent max-attempts, pppoe-client service-name, pppoe-client wait-for-ipcp

ppp chap hostname

Use the **ppp chap hostname** command to override the device hostname for PPP CHAP authentication.

Syntax

ppp chap hostname *string*

no ppp chap hostname

Parameters

Parameter	Description	Possible Values	Default Value
string	The username assigned by the broadband Internet service provider		no

User Level

read-write

Context

interface:FastEthernet, Dialer (L2, L2-L3)

Example

To set the hostname for PPP CHAP authentication to avaya32:

```
G450-001(super-if:FastEthernet 10/2)# ppp chap hostname avaya32
```

Related Commands

encapsulation pppoe, mtu, ppp chap password, ppp pap sent-username, pppoe-client persistent delay, pppoe-client persistent max-attempts, pppoe-client service-name, pppoe-client wait-for-ipcp

ppp chap password

Use the **ppp chap password** command to set the CHAP password for authentication with a remote peer.

Note:

This command is not backward-compatible. If you downgrade to version 3.x or earlier, you need to reconfigure this command on the gateway.

Note:

This command sets the CHAP secret for cases where the device is a CHAP responder, and the console port **ppp chap-secret** command sets the CHAP secret for cases where the device is a CHAP initiator.

Syntax

[no] ppp chap password *secret*

Parameters

Parameter	Description	Possible Values	Default Value
secret	The CHAP password		

User Level

read-write

Context

interface:FastEthernet, Dialer (L2, L2-L3)

Example

To set the CHAP password for authentication with a remote peer to 123456:

```
G450-001(super-if:FastEthernet 10/2)# ppp chap password 123456
```

Related Commands

encapsulation pppoe, interface fastethernet, mtu, ppp chap hostname, ppp pap sent-username, pppoe-client persistent delay, pppoe-client persistent max-attempts, pppoe-client service-name, pppoe-client wait-for-ipcp

ppp chap refuse

Use the **ppp chap refuse** command to prevent authentication with CHAP, even when a chap secret is configured. Use the **no** form of this command to allow authentication with CHAP.

Syntax

[no] ppp chap refuse

User Level

read-write

Context

interface:FastEthernet, Dialer (L2, L2-L3)

Example

To prevent authentication with CHAP:

```
G450-001(super-if:FastEthernet 10/2)# ppp chap refuse
```

Related Commands

ppp pap refuse

ppp ipcp dns request

Use the **ppp ipcp dns request** command to enable requesting DNS information from the remote peer during the PPP/IPCP session. Use the **no** form of this command to restore the default value, which is not to request DNS information during the PPP/IPCP session.

Note:

The DNS Resolver uses the DNS servers discovered using this command.

Syntax

ppp ipcp dns request

no ppp ipcp dns

User Level

read-write

Context

Interface: Console, FastEthernet (PPP L2, PPP L2-L3), Serial (DS1 PPP L2, DS1 PPP L2-L3, USP PPP L2, USP PPP L2-L3) Dialer (L2, L2-L3), USB-modem

Example

To enable DNS information requests from the remote peer during the PPP/IPCP session:

```
G450-001(config-if:FastEthernet 10/2)# ppp ipcp dns request
```

Related Commands

ip address negotiated

---

ppp pap refuse

Use the **ppp pap refuse** command to prevent authentication with PAP, even when a pap-sent password is configured.

Syntax

ppp pap refuse

no ppp pap refuse

User Level

read-write

Context

interface:FastEthernet, Dialer (L2, L2-L3)

Example

To prevent authentication with PAP:

```
G450-001(super-if:FastEthernet 10/2)# ppp pap refuse
```

Related Commands

ppp chap refuse

ppp pap sent-username

Use the **ppp pap sent-username** command to set the Password Authentication Protocol (PAP) password for authentication with the remote peer.

Note:

This command is not backward-compatible. If you downgrade to version 3.x or earlier, you need to reconfigure this command on the gateway.

Syntax

ppp pap sent-username *username* password *password*

no ppp pap sent-username

Parameters

Parameter	Description	Possible Values	Default Value
username	The remote peer PAP username		
password	The remote peer PAP password		

User Level

read-write

Context

interface:FastEthernet, Dialer (L2, L2-L3)

Example

To set the PAP password to avaya32 with password 123456:

```
G450-001(super-if:FastEthernet 10/2)# ppp pap sent-username avaya32 password
123456
```

Related Commands

encapsulation pppoe, mtu, ppp chap hostname, ppp chap password, pppoe-client persistent delay, pppoe-client persistent max-attempts, pppoe-client service-name, pppoe-client wait-for-ipcp

pppoe-client persistent delay

Use the **pppoe-client persistent delay** command to configure the interval between PPPoE-client dial attempts.

Syntax

pppoe-client persistent delay ***seconds***

Parameters

Parameter	Description	Possible Values	Default Value
seconds	The time in seconds to wait	**5-10000**	**30**

User Level

read-write

Context

interface:FastEthernet

Example

To configure the interval between ppp.E-client dial attempts as 1 second:

```
G450-001(super-if:FastEthernet 10/2)# pppoe-client persistent delay 1
```

Related Commands

encapsulation pppoe, mtu, ppp chap hostname, ppp chap password, ppp pap sent-username, pppoe-client persistent max-attempts, pppoe-client service-name, pppoe-client wait-for-ipcp

pppoe-client persistent max-attempts

Use the **pppoe-client persistent max-attempts** command to limit the number of consecutive connection establishment retries. When the number is reached, the PPPoE client stops trying to establish connections. To restart the connection attempts, use the **shutdown** and **no shutdown** command sequence.

Use the **no** form of this command to restore the default value, which is that no limit is imposed on the number of consecutive connection establishment retries. This means the PPPoE client does not stop trying to establish connections.

Syntax

pppoe-client persistent max-attempts *number*

no pppoe-client persistent max-attempts

Parameters

Parameter	Description	Possible Values	Default Value
number	The number of attempts	**0-10000**	**0** (no limit)

User Level

read-write

Context

interface:FastEthernet

Example

To limit the number of consecutive connection establishment retries to 0:

```
G450-001(super-if:FastEthernet 10/2)# pppoe-client persistent max-attempts 0
```

Related Commands

encapsulation pppoe, mtu, ppp chap hostname, ppp chap password, ppp pap sent-username, pppoe-client persistent delay, pppoe-client service-name, pppoe-client wait-for-ipcp

pppoe-client service-name

Use the **pppoe-client service-name** command to set the PPPoE Client service-name. You can use the **pppoe-client service-name** command to force the PPPoE client to connect only to access concentrators that support a specific service-name. If not set, the PPPoE client attempts to automatically discover the service name by initiating PADI frames with a blank service name.

Syntax

[no] pppoe-client service-name *string*

Parameters

Parameter	Description	Possible Values	Default Value
string	The service name		

User Level

read-write

Context

interface:FastEthernet

Example

To set the PPPoE Client service-name to isp1:

```
G450-001(super-if:FastEthernet 10/2)# pppoe-client service-name isp1
```

Related Commands

encapsulation pppoe, mtu, ppp chap hostname, ppp chap password, ppp pap sent-username, pppoe-client persistent delay, pppoe-client persistent max-attempts, pppoe-client wait-for-ipcp

pppoe-client wait-for-ipcp

Use the **pppoe-client wait-for-ipcp** command to configure the amount of time between PPPoE tunnel establishment and IPCP tunnel establishment. The PPPoE client terminates the PPPoE tunnel if this time is exceeded. Use the **no** form of this command to restore the default value, which is 20 seconds.

Note:

The PPP stack has a somewhat similar command: **ppp timeout ncp**. However while this command only terminates the LCP, the **pppoe-client wait-for-ipcp** command terminates the PPPoE tunnel.

Syntax

[no] pppoe-client wait-for-ipcp *seconds*

Parameters

Parameter	Description	Possible Values	Default Value
seconds	The number of seconds to wait	**5-10000**	**20**

User Level

read-write

Context

interface:FastEthernet

Example

To configure the amount of time between PPPoE tunnel establishment and IPCP tunnel establishment as 30 seconds:

```
G450-001(super-if:FastEthernet 10/2)# pppoe-client wait-for-ipcp 30
```

Related Commands

encapsulation pppoe, mtu, ppp chap hostname, ppp chap password, ppp pap sent-username, pppoe-client persistent delay, pppoe-client persistent max-attempts, pppoe-client service-name, show ppp authentication

Priority queueing

priority-queue

Use the **priority-queue** command to enable priority queueing mode in a Serial or FastEthernet interface. By default, priority queueing is off, and WFVQ is enabled on all Serial interfaces and all FastEthernet interfaces for which traffic-shaping is enabled. If you disable priority queueing by using the **no** form of the **priority-queue** command, WFVQ is re-enabled.

Syntax

[no] priority-queue

User Level

read-write

Context

interface:Serial (DS1 PPP L2-L3, DS1 PPP L2, USP PPP L2, USP PPP L2-L3), FastEthernet (L2, L2-L3) - when Frame Relay Traffic Shaping is configured, Serial (DS1 FR L2, USP FR L2) - when Frame Relay Traffic Shaping is not configured, Dialer (L2, L2-L3)

Example

To enable priority queueing:

```
G450-001(if:Serial 3/1:1)# priority-queue
```

Related Commands - Priority queueing

queue-limit, show queueing, voip-queue, voip-queue-delay

Related Commands - WFVQ

fair-queue-limit, fair-voip-queue, priority-queue, show queue, show queueing, voip-queue, voip-queue

queue-limit

Use the **queue-limit** command to set the packet size of any of the four priority queues. Use the **no** form of the command to restore the packet sizes of the queues to their default values, using the interface bandwidth.

Note:

The **queue-limit** command is only applicable if priority queueing mode is enabled.

Syntax

queue-limit *queue_id size*

no queue-limit

Parameters

Parameter	Description	Possible Values	Default Value
queue_id	The queue priority ID	**1** (highest) **4** (lowest)	
size	The size of the queue, in packets	The total number of packets in all queues cannot exceed 5000	

User Level

read-write

Context

interface:Serial (DS1 PPP L2-L3, DS1 PPP L2, USP PPP L2, USP PPP L2-L3), FastEthernet (L2, L2-L3) - when Frame Relay Traffic Shaping is configured, Serial (DS1 FR L2, USP FR L2) - when Frame Relay Traffic Shaping is not configured, Dialer (L2, L2-L3)

Example

To specify a size of 200 for queue 1:

```
G450-001(if:Serial 3/1:1)# queue-limit 1 200
```

Related Commands

priority-queue, show queueing, voip-queue, voip-queue-delay

show queueing

Use the **show queueing** command to display the priority queueing and WFVQ configuration, for a specific interface type or interface, or for all interfaces.

Syntax

show queueing [*interface_type if_number*]

Parameters

Parameter	Description	Possible Values	Default Value
interface_type	The type of interface	**Serial, Fast-Ethernet**	
if_number	The port number of this interface in the form: ***port***[:***channel_group***]	port: **1, 2** channel_group: E1: **0-30** T1: **0-23**	

User Level

read

Context

general

Note:

This command is also used for the FastEthernet interface when traffic shaping has been configured.

Example

To display the priority queue size in packets:

```
G450-001(super)# show queueing
```

```
Current priority queue configuration:

Interface Name  VOIP   Est. Delay    Q.1(High)    Q.2   Q.3   Q.4(Low)    DE Buf
                       [ms]
Serial 3/1      OFF    OFF           524          524   524   524         -
Serial 4/1:1    OFF    OFF           507          507   507   507         507
Current voip fair queue configuration:

 Interface       Total          Flow          Dynamic    Max voip      Priority
 Name            discard        discard       Queue      delay (ms)    queues
                 threshold      threshold
 Serial 3/1:1    256            64            16         20            1
```

Output fields

Field	Description
VOIP	Indicates if VoIP queueing is enabled. VoIP queueing is enabled using the **voip-queue** command.
Est. Delay [ms]	If VoIP queueing is enabled, displays the maximum queue delay for which to estimate the high priority queue size necessary to meet the queueing delay for a specific VoIP codec. By default, this is estimated for the G.729 codec and is 20 ms. It can be configured through the **voip-queue-delay** command. If VoIP queueing is not enabled, the Est. Delay column displays **OFF**.
Q.1	The size, in packets, of the highest priority queue
Q.2	The size, in packets, of the second highest priority queue
Q.3	The size, in packets, of the second lowest priority queue
Q.4	The size, in packets, of the lowest priority queue
Total discard threshold	The total buffer credits limit for WFQ. Configurable through the **fair-queue-limit** command.
Flow discard threshold	Per subqueue buffer credits. Not configurable.
Dynamic queues	The total number of subqueues. Not configurable.
Max voip delay [ms]	Maximum delay for VoIP bearer
Priority queues	The number of priority queues in the system. Not configurable. From the user's point of view control and bearer queues are the same queue.

Related Commands - Priority queueing

priority-queue, queue-limit, voip-queue, voip-queue-delay

Related Commands - WFVQ

fair-queue-limit, fair-voip-queue, priority-queue, show queue, voip-queue, voip-queue

voip-queue

Use the **voip-queue** command to select custom queueing for VoIP traffic. By default, VoIP queueing is off, and Weighted Fair VoIP Queueing (WFVQ) is enabled on all Serial interfaces and all FastEthernet interfaces for which traffic-shaping is enabled. If you disable custom queueing by using the **no** form of the **voip-queue** command, WFVQ is re-enabled.

Syntax

[no] voip-queue

User Level

read-write

Context

interface:Serial (DS1 PPP L2-L3, DS1 PPP L2, DS1 FR L2, USP FR L2, USP PPP L2, USP PPP L2-L3), FastEthernet (L2, L2-L3) - when traffic shaping is configured, Dialer (L2, L2-L3)

Example

To enable VoIP queueing:

```
G450-001(if:Serial 3/1:1)# voip-queue
```

Related Commands - Priority queueing

priority-queue, queue-limit, show queueing, voip-queue-delay

Related Commands - WFVQ

fair-queue-limit, fair-voip-queue, priority-queue, show queue, voip-queue

voip-queue-delay

Use the **voip-queue-delay** command to set the maximum queue delay for which to estimate the high priority queue size necessary to meet the queueing delay for specific VoIP codec parameters. Use the **no** form of this command to return the maximum queue delay introduced for VoIP traffic by egress queueing to the default value of 20ms.

Note:

The command **voip-queue-delay** is not applicable for an interface on which Frame-Relay Traffic-Shaping is enabled. Instead, this command is now applicable under map-class frame-relay context, to control the specific DLCI queueing parameters.

Syntax

[no] voip-queue-delay *queue_delay_ms* [*codec* [*frames-per-packet*]]

Parameters

Parameter	Description	Possible Values	Default Value
queue_delay_ms	The maximum queue delay, in milliseconds, for which to estimate the high priority queue size. The queue delay is the amount of time that voice traffic is allowed to wait in the queue.	**1-1000**	**20**
codec	The codec for which to estimate the high priority queue size	**g711mu** **g711a** **g729** **g729a** **g729b** **g729ab** **g723-5.3** **g723-6.3**	**g729**
frames-per-packet	The number of codec frames per IP packet for which to estimate the high priority queue size	**1-6**	**2**

User Level

admin

Context

interface:Serial (DS1 PPP L2-L3, DS1 PPP L2, USP PPP L2, USP PPP L2-L3), FastEthernet (L2, L2-L3) - when traffic shaping is configured, Serial (DS1 FR L2, USP FR L2) - when Frame Relay Traffic Shaping is not configured, map-class frame-relay, Dialer (L2, L2-L3)

Note:

This command is also used in Serial and WAN FastEthernet context when traffic shaping is configured.

Example

To set the maximum query delay to 30 milliseconds:

```
G450-001(super)# voip-queue-delay 30
```

Related Commands

priority-queue, queue-limit, show queueing, voip-queue

Proxy ARP

ip proxy-arp

Use the **ip proxy-arp** command to enable proxy ARP on an interface. Use the **no** form of this command to disable proxy ARP on an interface.

Syntax

[no] ip proxy-arp

User Level

read-write

Context

interface:FastEthernet (L2-L3, L3), VLAN (L2-L3, L3)

Example

To enable proxy ARP on an interface:

```
G450-001(if:Vlan 1)# ip proxy-arp
```

Related Commands

arp, arp timeout, clear arp-cache, ip max-arp-entries, show ip arp, show ip reverse-arp

QoS

set qos bearer

Use the **set qos bearer** command to permit the setting of VoIP QoS-bearer related parameters for the Media Gateway Processor and VoIP engines. Since Media Gateway Controller and VoIP engines share the same setup, local values are not set to entered values unless **set qos control local** has been executed (refer to set qos control on page 875).

Syntax

set qos bearer {bbedscp | efdscp | 802p | rtpmin | rtpmax} *value*

Parameters

Parameter	Description	Possible Values	Default Value
bbedscp	Keyword specifying that the following value is the BBE differentiated services code point	**0-63**	**43**
efdscp	Keyword specifying that the following value is the EF differentiated services code point	**0-63**	**46**
802p	Keyword specifying that the following value is the 802 priority value	**0-7**	**6**
rtpmin	Keyword specifying that the following value is the RTP port min value. The rtpmin value must be an even number, and the difference between rtpmin and rtpmax must be at least 129.	**2048-65406**	**2048**
rtpmax	Keyword specifying that the following value is the RTP port max value. The rtpmax value must be an odd number and the difference between rtpmax and rtpmin must be at least 129.	**2177-65535**	**65535**
value	A value for the specified keyword		

User Level

read-write

Context

general

Example

To set the BBE differentiated services code point to 43:

```
G450-001(super)# set qos bearer bbedscp 43
```

Related Commands

set qos control, set qos signal, show qos-rtcp

set qos control

Use the **set qos control** command to define the source for QoS control parameters. The source can be either **local** where the user configures the values via the CLI, or **remote** in which case the values are obtained from the media gateway controller. The default value is **remote**.

Syntax

set qos control {local | remote}

Parameters

Parameter	Description	Possible Values	Default Value
local	Keyword that specifies to configure QoS values via the CLI		
remote	Keyword that specifies to obtain QoS values from the media gateway controller		

User Level

read-write

Context

general

Example

To specify that QoS values are configured locally via the CLI:

```
G450-001(super)# set qos control local
```

Related Commands

set qos bearer, set qos signal, show qos-rtcp

---

set qos signal

Use the **set qos signal** command to provide the means to set up QoS signaling parameters, DSCP or 802.1Q, for the Media Gateway Processor.

Syntax

set qos signal {dscp | 802p} ***value***

Parameters

Parameter	Description	Possible Values	Default Value
dscp	Keyword that specifies to setup DSCP parameters		
802p	Keyword that specifies to setup 802.1Q parameters		
value	Parameter value	For dscp: **0-63** For 802p**: 0-7**	For dscp: **34** For 802p: **7**

User Level

read-write

Context

general

Example

To set up DSCP parameter 43:

```
G450-001(super)# set qos signal dscp 43
```

Related Commands

set qos bearer, set qos control, show qos-rtcp

show qos-rtcp

Use the **show qos-rtcp** command to display QoS, RTCP, and RSVP parameters.

Syntax

show qos-rtcp

User Level

admin

Context

general

Example

To display QoS, RSVP and RTCP parameters:

```
G450-001(super)# show qos-rtcp

PARAMETERS IN EFFECT: -- Downloaded --

QOS PARAMETERS          LOCALLY SET        DOWNLOADED
--------------------    ---------------    ---------------
Signal 802 Priority:    7                  0
Signal DSCP         :   34                 0
Bearer 802 Priority:    6                  6
Bearer BBE DSCP     :   43                 43
Bearer EF DSCP      :   46                 46
Minimum RTP Port    :   3                  2048
Maximum RTP Port    :   65535              65535

RSVP PARAMETERS         LOCALLY SET        DOWNLOADED
--------------------    ---------------    ---------------
State               :   Enabled            Disabled
Retry on Failure    :   Yes                Yes
Retry Delay(secs)   :   15                 15
Service Profile     :   Guaranteed         Guaranteed

RTCP MON  PARAMETERS    LOCALLY SET        DOWNLOADED
--------------------    ---------------    ---------------
State               :   Enabled            Disabled
IP Address          :   0.0.0.0            0.0.0.0
Listening Port      :   5005               5005
Report Period(secs):    5                  5
```

Related Commands - QoS

set qos bearer, set qos control, set qos signal

Related Commands - RSVP

set qos rsvp

Related Commands - RTCP

set qos rtcp

---

show voip-parameters

Use the **show voip-parameters** command to display information about the VoIP engine.

Syntax

show voip-parameters

User Level

read-only

Context

general

Examples

To display VoIP information:

```
G450-001(super)# show voip-parameters

VOIP ENGINE PARAMETERS
------------------------------------------------------
IP (PMI)                  : 149.49.78.140
DSP Firmware Version      : N/A
Fault Status              : No Fault Messages
Additional Status         : No Status Messages
```

```
CURRENT STATE
-------------------------------------------------------
In Use     : 20 of  100 channels, 240of 1200 points (0.0% used)

VoIP -DSPs PARAMETERS
VoIP   Child    CODE  SUFFIX     HW       FW          Chan      Admin     Oper     Fault
Slot   Board                  VINTAGE  VINTAGE       InUse     State     State    Status
----   -----    ----  ------  -------  --------      -------   -----     -----    ------
1      VOIP    8122    A       3       235          20/80     Release    InUse  No Error
2      VOIP    7119    A       5       215          0/20      Busyout    Idle   No Error
3      -- Not Installed --
4      SYNC
```

Related Commands - VoIP

busyout voip-dsp, campon-busyout voip-dsp, release voip-dsp, reset voip-dsp, show voip-dsp, test voip-dsp

Related Commands - QoS

set qos bearer, set qos control, set qos signal, show qos-rtcp

RADIUS authentication

clear radius authentication server

Use the **clear radius authentication server** command to clear the primary or secondary RADIUS server IP address.

Syntax

clear radius authentication server {primary|secondary}

Parameters

Parameter	Description	Possible Values	Default Value
primary	Keyword specifying to clear the primary RADIUS server		
secondary	Keyword specifying to clear the secondary RADIUS server		

User Level

admin

Context

general

Example

To clear the secondary RADIUS authentication server:

```
G450-001(super)# clear radius authentication server secondary
```

Related Commands

set radius authentication, set radius authentication retry-number, set radius authentication retry-time, set radius authentication secret, set radius authentication server, set radius authentication udp-port, show radius authentication

set radius authentication

Use the **set radius authentication** command to enable or disable RADIUS authentication.

Syntax

set radius authentication {enable | disable}

Parameters

Parameter	Description	Possible Values	Default Value
enable	Keyword specifying to enable RADIUS authentication		
disable	Keyword specifying to disable RADIUS authentication (default)		

User Level

read-write

Context

general

Example

To enable RADIUS authentication:

```
G450-001(super)# set radius authentication enable
```

Related Commands

clear radius authentication server, set radius authentication retry-number, set radius authentication retry-time, set radius authentication secret, set radius authentication server, set radius authentication udp-port, show radius authentication

set radius authentication retry-number

Use the **set radius authentication retry-number** command to set the number of times to resend an access request when there is no response.

Syntax

set radius authentication retry-number *number*

Parameters

Parameter	Description	Possible Values	Default Value
number	The number of times to resend an access request if there is no response	**1–65535**	

User Level

read-write

Context

general

Example

To set the number of retries for RADIUS authentication to 3:

```
G450-001# set radius authentication retry-number 3
```

Related Commands

clear radius authentication server, set radius authentication, set radius authentication retry-time, set radius authentication secret, set radius authentication server, set radius authentication udp-port, show radius authentication

set radius authentication retry-time

Use the **set radius authentication retry-time** command to set the time to wait before resending an access request.

Syntax

set radius authentication retry-time *seconds*

Parameters

Parameter	Description	Possible Values	Default Value
seconds	The time in seconds to wait before resending an access request	**1–65535**	

User Level

read-write

Context

general

Example

To specify to wait 5 seconds before retrying an access request:

```
G450-001# set radius authentication retry-time 5
```

Related Commands

clear radius authentication server, set radius authentication, set radius authentication retry-number, set radius authentication secret, set radius authentication server, set radius authentication udp-port, show radius authentication

set radius authentication secret

Use the **set radius authentication secret** command to enable secret authentication.

Syntax

set radius authentication secret *string*

Parameters

Parameter	Description	Possible Values	Default Value
string	The text password		

User Level

admin

Context

general

Example

To set the RADIUS authentication password to hush:

```
G450-001# set radius authentication secret hush
```

Related Commands

clear radius authentication server, set radius authentication, set radius authentication retry-number, set radius authentication retry-time, set radius authentication server, set radius authentication udp-port, show radius authentication

set radius authentication server

Use the **set radius authentication server** command to set the IP address of the primary or secondary RADIUS Authentication server.

Syntax

set radius authentication server ***ip_addr*** {**primary** | **secondary**}

Parameters

Parameter	Description	Possible Values	Default Value
ip_addr	IP address of RADIUS authentication server		
primary	Keyword that specifies to set the primary authentication server (default)		
secondary	Keyword that specifies to set the secondary authentication server		

User Level

read-write

Context

general

Example

To set the primary RADIUS authentication server IP address to be 192.40.12.36:

```
G450-001# set radius authentication server 192.40.12.36 primary
```

Related Commands

clear radius authentication server, set radius authentication, set radius authentication retry-number, set radius authentication retry-time, set radius authentication secret, set radius authentication udp-port, show radius authentication

set radius authentication udp-port

Use the **set radius authentication udp-port** command to set the RFC 2138 approved UDP port number.

Normally, the UDP port number should be set to its default value of 1812. Some early implementations of the RADIUS server used port number 1645.

Syntax

set radius authentication udp-port *number*

Parameters

Parameter	Description	Possible Values	Default Value
number	The UDP port number		**1812**

User Level

read-write

Context

general

Example

To set the UDP port number to 1645:

```
G450-001# set radius authentication udp-port number 1645
```

Related Commands

clear radius authentication server, set radius authentication, set radius authentication retry-number, set radius authentication retry-time, set radius authentication secret, set radius authentication server, show radius authentication

show radius authentication

Use the **show radius authentication** command to display all RADIUS authentication configurations. Shared secrets are not displayed.

Syntax

show radius authentication

User Level

read-only

Context

general

Example

To show RADIUS authentication information:

```
G450-001(super)# show radius authentication

Mode:                  Disable
Primary-server:        0.0.0.0
Secondary-server:      0.0.0.0
Retry-number:          4
Retry-time:            5
UDP-port:              1812
```

Related Commands

clear radius authentication server, set radius authentication, set radius authentication retry-number, set radius authentication retry-time, set radius authentication secret, set radius authentication server, set radius authentication udp-port

Recovery password

set terminal recovery password

Use the **set terminal recovery password** command to enable or disable the recovery password.

Note:
This command can only be issued via the console port (not via a modem port).

Syntax

set terminal recovery password ***action***

Parameters

Parameter	Description	Possible Values	Default Value
action	The state of the recovery password	**enable**, **disable**	

User Level

admin

Context

general

Example

To disable the recovery password:

```
G450-001(super)# set terminal recovery password disable
```

Restoring gateway configuration

restore usb

Use the **restore usb** command to restore gateway files from a USB mass storage device.

Note:

The restore operation does not fail if a specific file is missing or incompatible with the MM hardware.

Note:

If you are not restoring to the same machine you backed up from, first delete the VPN license file from the USB device. Otherwise, the restore operation will fail.

Syntax

restore usb *usb-device backup-name*

Parameters

Parameter	Description	Possible Values	Default Value
usb-device	The USB mass storage device	**usb-device0**	
backup-name	The backup directory path and file name		The gateway backup directory on **usb-device0**

User Level

read-write

Context

general

Example

To restore gateway files from directory gatewaybackup1on usb-device0:

```
G450-001(super)# restore usb usb-device0 gatewaybackup1
```

Related Commands

backup config usb, copy announcement-file usb, copy usb announcement-file, erase usb, safe-removal usb, show backup status, show restore status, show usb

show restore status

Use the **show restore status** command to display information regarding the status of a restore operation of gateway files from a USB mass storage device. The output displays the list of files restored so far.

Syntax

show restore status

User Level

read-only

Context

general

Example

To display information regarding the status of a gateway file restore operation:

```
G450-001(super)# show restore status
Files restored:

Type                    FileName                    Status
-----------------------------------------------------------
swComponent             g450_sw_26_23_0.bin         OK
startup-config          startup_config.cfg          OK
auth-file               auth-file.cfg               OK
license-file            vpn_license.cfg             OK
swWebImage              g450_emweb_3_1_8.bin        OK
phone-script            46xxupgrade.scr             OK
phone-script            46xxsettings.txt            OK
phoneImageFile          4602dbte1_82.bin            OK
phoneImageFile          4601dbte1_82.bin            OK
phoneImageFile          4602dape1_82.bin            OK
phoneImageFile          4601dape1_82.bin            OK
announcement            A01100.wav                  OK
announcement            Ann7.wav                    OK
swRuntimeImage          MM710V11.FDL                OK

Files missing/error:
swRuntimeImage          MB 1T+2L Analog             Missing
```

Related Commands

backup config usb, copy announcement-file usb, copy usb announcement-file, erase usb, restore usb, safe-removal usb, show backup status, show usb

RIP

ip distribution access-default-action

Use the **ip distribution access-default-action** command to set the default action for a specific RIP distribution access list.

Syntax

ip distribution access-default-action *list_number default_action*

Parameters

Parameter	Description	Possible Values	Default Value
list_number	The distribution access list number	**1-99**	
default_action	The default action	**default-action-deny, default-action-permit**	

User Level

read-write

Context

general

Example

To specify that the default action for distribution access list 1 is to deny packets:

```
G450-001(super)# ip distribution access-default-action 1
             default-action-deny
```

ip distribution access-list

Use the **ip distribution access-list** command to create a RIP distribution access list or add a distribution access rule to the list. Use the **no** form of this command to delete a distribution access list rule. Apply the distribution rule using the **distribution-list** command.

Syntax

ip distribution access-list *access_list_number access_list_index action* {{*router_ip* [*router_wildcard*]}|any}

no ip distribution access-list *access_list_number* [*access_list_index*]

Note:

If a list index is not given in the **no ip distribution access-list** command, all rules are deleted.

Parameters

Parameter	Description	Possible Values	Default Value
access_list_number	The access list number	**1-99**	
access_list_index	The access list index number	**1–9999**	
action	The action to perform	**permit**, **deny**	
router_ip	The IP router address of the network		
router_wildcard	The IP network wildcard address		
any	Keyword that specifies the value can be any IP address		

User Level

read-write

Context

general

Example

To create distribution list 1, whose default action is to discard information from the network 10.10.0.0:

```
G450-001(super)# ip distribution access-list 1 23 deny 10.10.0.0 0.0.255.255
```

To configure RIP distribution access list number 2 permitting distribution and learning of router 10.1.1.1:

```
G450-001(super)# ip distribution access-list 2 24 permit 10.1.1.1
```

To configure RIP distribution access list number 20 permitting distribution and learning of all networks:

```
G450-001(super)# ip distribution access-list 20 4 permit any
```

Related Commands

ip rip authentication key, ip rip authentication mode, ip rip default-route-mode, ip rip poison-reverse, ip rip rip-version, ip rip send-receive-mode, ip rip split-horizon, router rip, show ip protocols

ip distribution access-list-cookie

Use the **ip distribution access-list-cookie** command to set the list cookie.

Syntax

ip distribution access-list-cookie *list_id cookie*

Parameters

Parameter	Description	Possible Values	Default Value
list_id	The ID of the distribution list	**1-99**	
cookie	The cookie number	integer	

User Level

read-write

Context

general

Example

To set list 4 to have cookie 12345:

```
G450-001(super)# ip distribution access-list-cookie 4 12345
```

ip distribution access-list-copy

Use the **ip distribution access-list-copy** command to copy the distribution access list.

Syntax

ip distribution access-list-copy *source_list destination_list*

Parameters

Parameter	Description	Possible Values	Default Value
source_list	The source distribution access list	**1-99**	
destination_list	The destination distribution access list	**1-99**	

User Level

read-write

Context

general

Example

To copy distribution list 1 to list 3:

```
G450-001(super)# ip distribution access-list-copy 1 3
```

ip distribution access-list-name

Use the **ip distribution access-list-name** command to set the distribution list name.

Syntax

ip distribution access-list-name *distribution_list_number name*

Parameters

Parameter	Description	Possible Values	Default Value
distribution_list_number	The number of the distribution list	**1-99**	
name	The distribution list name		

Note:
To define a name that includes spaces, enclose the entire name in quotation marks (for example, “New York”).

User Level

read-write

Context

general

Example

To name distribution access-list #5 as evening:

```
G450-001(super)# ip distribution access-list-name 5 evening
```

To name distribution access-list #22 as Daily Job:

```
G450-001(super)# ip distribution access-list-name 22 “Daily Job”
```

ip distribution access-list-owner

Use the **ip distribution access-list-owner** command to set the distribution list owner.

Syntax

ip distribution access-list-owner *policy_list_number owner*

Parameters

Parameter	Description	Possible Values	Default Value
policy_list_number	The distribution list number	**1-99**	
owner	The distribution list owner		

Note:

To define a name that includes spaces, enclose the entire name in quotation marks (for example, “New York”).

User Level

read-write

Context

general

Example

To specify Jane Wiley as the owner of distribution list 78:

```
G450-001(super)# ip distribution access-list-owner 78 “Jane Wiley”
```

ip rip authentication key

Use the **ip rip authentication key** command to set the authentication string used on the current interface. Use the **no** form of this command to clear the password.

Syntax

ip rip authentication key *password*

no ip rip authentication key

Parameters

Parameter	Description	Possible Values	Default Value
password	The authentication string for the interface	string (1-16 chars)	

User Level

read-write

Context

interface:Serial (DS1 PPP L2-L3, DS1 PPP L3, DS1 FR-SUB L2-L3, DS1 FR-SUB L3, USP PPP L2-L3, USP PPP L3), FastEthernet (L2-L3, L3, PPP L2-L3, PPP L3), VLAN (L2-L3, L3), Loopback (L2-L3, L3), Tunnel (L2-L3, L3), Dialer (L2-L3, L3)

Example

To set the authentication string on the VLAN 1 interface to hush-hush:

```
G450-001(if:Vlan 1)# ip rip authentication key hush-hush
```

Related Commands

ip distribution access-list, ip rip authentication mode, ip rip default-route-mode, ip rip poison-reverse, ip rip rip-version, ip rip send-receive-mode, ip rip split-horizon, router rip, show ip protocols

ip rip authentication mode

Use the **ip rip authentication mode** command to specify the type of authentication used in RIP Version 2 packets. Use the **no** form of this command to restore the default value, none.

Syntax

ip rip authentication mode [simple|none]

no ip rip authentication mode

Parameters

Parameter	Description	Possible Values	Default Value
simple	Keyword indicating that the clear text authentication should be used		
none	Keyword indicating that no authentication should be used		

User Level

read-write

Context

interface:Serial (DS1 PPP L2-L3, DS1 PPP L3, DS1 FR-SUB L2-L3, DS1 FR-SUB L3, USP PPP L2-L3, USP PPP L3), FastEthernet (L2-L3, L3, PPP L2-L3, PPP L3), VLAN (L2-L3, L3), Loopback (L2-L3, L3), Tunnel (L2-L3, L3), Dialer (L2-L3, L3)

Example

To specify that RIP packets use simple authentication mode:

```
G450-001(if:FastEthernet 10/2)# ip rip authentication mode simple
```

Related Commands

ip distribution access-list, ip rip authentication key, ip rip default-route-mode, ip rip poison-reverse, ip rip rip-version, ip rip send-receive-mode, ip rip split-horizon, router rip, show ip protocols

ip rip default-route-mode

Use the **ip rip default-route-mode** command to enable learning of the default route received by the RIP protocol. Use the **no** form of this command to disable listening to default routes.

Syntax

ip rip default-route-mode *mode*

no ip rip default-route-mode

Parameters

Parameter	Description	Possible Values	Default Value
mode	The default mode	**talk-listen** — RIP sends and receives default route updates on the interface **talk-only** — RIP sends, but does not receive, default route updates on the interface	**talk-listen**

User Level

read-write

Context

interface:Serial (DS1 PPP L2-L3, DS1 PPP L3, DS1 FR-SUB L2-L3, DS1 FR-SUB L3, USP PPP L2-L3, USP PPP L3), FastEthernet (L2-L3, L3, PPP L2-L3, PPP L3), VLAN (L2-L3, L3), Loopback (L2-L3, L3), Tunnel (L2-L3, L3), Dialer (L2-L3, L3)

Example

To specify that the RIP protocol sends, but does not receive, default route updates on the VLAN 1 interface:

```
G450-001(if:Vlan 1)# ip rip default-route-mode talk-only
```

Related Commands

ip distribution access-list, ip rip authentication key, ip rip authentication mode, ip rip poison-reverse, ip rip rip-version, ip rip send-receive-mode, ip rip split-horizon, router rip, show ip protocols

ip rip poison-reverse

Use the **ip rip poison-reverse** command to enable split-horizon with poison-reverse on the current interface. Use the **no** form of this command to disable the poison-reverse mechanism.

The split-horizon technique prevents information about routes from exiting the router interface through which the information was received. This prevents routing loops.

Poison-reverse updates explicitly indicate that a network or subnet is unreachable. Poison-reverse updates are sent to defeat large routing loops.

Syntax

[no] ip rip poison-reverse

User Level

read-write

Context

interface:Serial (DS1 PPP L2-L3, DS1 PPP L3, DS1 FR-SUB L2-L3, DS1 FR-SUB L3, USP PPP L2-L3, USP PPP L3), FastEthernet (L2-L3, L3, PPP L2-L3, PPP L3), VLAN (L2-L3, L3), Loopback (L2-L3, L3), Tunnel (L2-L3, L3), Dialer (L2-L3, L3)

Related Commands

ip distribution access-list, ip rip authentication key, ip rip authentication mode, ip rip default-route-mode, ip rip rip-version, ip rip send-receive-mode, ip rip split-horizon, router rip, show ip protocols

ip rip rip-version

Use the **ip rip rip-version** command to specify the RIP version running on the interface basis.

Syntax

ip rip rip-version [1|2]

Parameters

Parameter	Description	Possible Values	Default Value
`1`	Keyword indicating that RIP version 1 packets should be used		
`2`	Keyword indicating that RIP version 2 packets should be used		

User Level

read-write

Context

interface:Serial (DS1 PPP L2-L3, DS1 PPP L3, DS1 FR-SUB L2-L3, DS1 FR-SUB L3, USP PPP L2-L3, USP PPP L3), FastEthernet (L2-L3, L3, PPP L2-L3, PPP L3), VLAN (L2-L3, L3), Loopback (L2-L3, L3), Tunnel (L2-L3, L3), Dialer (L2-L3, L3)

Example

To specify that RIP version 2 packets should be running on the Serial 3/1:1 interface:

```
G450-001(if:Serial 3/1:1)# ip rip rip-version 2
```

Related Commands

ip distribution access-list, ip rip authentication key, ip rip authentication mode, ip rip default-route-mode, ip rip poison-reverse, ip rip send-receive-mode, ip rip split-horizon, router rip, show ip protocols

ip rip send-receive-mode

Use the **`ip rip send-receive-mode`** command to set the RIP send and receive modes on an interface. Use the **`no`** form of this command to set the RIP to talk (that is, send report).

Syntax

`ip rip send-receive-mode` ***`mode`*** **`[`*** ***`default_route_metric`*** **`]`**

`no ip rip send-receive-mode`

Parameters

Parameter	Description	Possible Values	Default Value
mode	The RIP send and receive mode	**talk-listen** – RIP receives and transmits updates on the interface **talkdefault-listen** – RIP receives updates on the interface and sends only a default route **listen-only** – RIP receives updates on the interface and does not transmit them	**talk-listen**
default_route_metric	The route metric index	**1-15**	

User Level

read-write

Context

interface:Serial (DS1 PPP L2-L3, DS1 PPP L3, DS1 FR-SUB L2-L3, DS1 FR-SUB L3, USP PPP L2-L3, USP PPP L3), FastEthernet (L2-L3, L3, PPP L2-L3, PPP L3), VLAN (L2-L3, L3), Loopback (L2-L3, L3), Tunnel (L2-L3, L3), Dialer (L2-L3, L3)

Example

To set the RIP protocol to receive and transmit updates on the Serial interface:

```
G450-001(if:Serial 3/1:1)# ip rip send-receive-mode talk-listen
```

Related Commands

ip distribution access-list, ip rip authentication key, ip rip authentication mode, ip rip default-route-mode, ip rip poison-reverse, ip rip rip-version, ip rip split-horizon, router rip, show ip protocols

ip rip split-horizon

Use the **ip rip split-horizon** command to enable the split-horizon mechanism on the current interface. Use the **no** form of this command to disable the split-horizon mechanism. By default split-horizon is enabled.

The split-horizon mechanism prevents information about routes from exiting the router interface through which the information was received. This prevents routing loops.

Syntax

[no] ip rip split-horizon

User Level

read-write

Context

interface:Serial (DS1 PPP L2-L3, DS1 PPP L3, DS1 FR-SUB L2-L3, DS1 FR-SUB L3, USP PPP L2-L3, USP PPP L3), FastEthernet (L2-L3, L3, PPP L2-L3, PPP L3), VLAN (L2-L3, L3), Loopback (L2-L3, L3), Tunnel (L2-L3, L3), Dialer (L2-L3, L3)

Related Commands

ip distribution access-list, ip rip authentication key, ip rip authentication mode, ip rip default-route-mode, ip rip poison-reverse, ip rip rip-version, ip rip send-receive-mode, router rip, show ip protocols

router rip

Use the **router rip** command to enable the RIP and to enter the router configuration context. Use the **no** form of this command to restore the default value, and disable RIP.

Syntax

[no] router rip

User Level

read-write

Context

general

Example

To enable RIP and enter the router configuration context:

```
G450-001(super)# router rip
G450-001(super router:rip)#
```

Related Commands

ip distribution access-list, ip rip authentication key, ip rip authentication mode, ip rip default-route-mode, ip rip poison-reverse, ip rip rip-version, ip rip send-receive-mode, ip rip split-horizon, show ip protocols

default-metric (RIP)

Use the **default-metric** command to set the default metric of redistributed routes for the RIP protocol. Use the **no** form of this command to restore the default value.

Syntax

default-metric *default_metric*

no default-metric

Parameters

Parameter	Description	Possible Values	Default Value
default_metric	The interface RIP route metric value	**1-16**	**1**

User Level

read-write

Context

Router-RIP

Example

To set the default metric for redistributed routes to 5:

```
G450-001(router:rip)# default-metric 5
```

Related Commands

default-metric (RIP), distribution-list, network (RIP), redistribute (RIP), timers basic

distribution-list

Use the **distribution-list** command to apply a distribution access list for incoming or outgoing routing information in route updates. Use the **no** form of this command to deactivate the list.

Syntax

[no] distribution-list *access_list_number type* [*interface_type interface_number*|*protocol*]

Parameters

Parameter	Description	Possible Values	Default Value
access_list_number	The number of the access list	**1-99**	
type	The type of the access list	**in**, **out**	
interface_type	The interface type		
interface_number	The interface number		
protocol	The protocol. This parameter is only relevant for outgoing list entries.	**static**, **ospf**	

User Level

read-write

Context

Router: rip

Example

To apply distribution access list 10 to incoming router updates on the VLAN 1 interface:

```
G450-001(router:rip)# distribution-list 10 in "Vlan 1"
```

To apply distribution access list 20 to outgoing router updates on the Serial 3/1:1 interface:

```
G450-001(router:rip)# distribution-list 20 out "Serial 3/1:1":
```

To apply distribution access list 40 to outgoing router updates from OSPF:

```
G450-001(router:rip)# distribution-list 40 out ospf
```

Related Commands

default-metric (RIP), network (RIP), redistribute (RIP), timers basic

network (RIP)

Use the **network** command to specify a list of networks on which the RIP is running. Use the **no** form of this command to remove an entry.

Syntax

[no] network *ip_address* [*wildcard_mask*]

Parameters

Parameter	Description	Possible Values	Default Value
ip_address	The IP address of the network of directly connected networks		
wildcard_mask	The wildcard mask address number		

User Level

read-write

Context

Router: rip

Example

To specify that RIP is used on all interfaces connected to the network 192.168.37.0:

```
G450-001(router:rip)# network 192.168.37.0
```

Related Commands

default-metric (RIP), distribution-list, redistribute (RIP), timers basic

redistribute (RIP)

Use the **redistribute** command to redistribute routing information from another protocol into RIP. Use the **no** form of this command to restore the default value, disable redistribution by RIP.

Syntax

[no] redistribute *protocol*

Parameters

Parameter	Description	Possible Values	Default Value
protocol	The protocol to be used	**static**, **OSPF**	

User Level

read-write

Context

Router-RIP

Example

To redistribute OSPF routing information into RIP:

```
G450-001(router:rip)# redistribute ospf
```

Related Commands - RIP

default-metric (RIP), distribution-list, network (RIP), timers basic

Related Commands - Route redistribution

default-metric (interface route metric value)

timers basic

Use the **timers basic** command to set RIP timers. Use the **no** form of this command to set the RIP timers to their default values.

Syntax

timers basic *update invalid*

no timers basic

Parameters

Parameter	Description	Possible Values	Default Value
update	The RIP update timer, in seconds	**30** or more	
invalid	The RIP invalid route timer, in seconds	**30** or more	

User Level

read-write

Context

Router: rip

Example

To set the update timer to 30 seconds, and the invalid route timer to 180 seconds:

```
G450-001(router:rip)# timers basic 30 180
```

Related Commands

default-metric (RIP), distribution-list, network (RIP), redistribute (RIP)

show ip distribution access-lists

Use the **show ip distribution access-lists** command to display the contents of all current distribution lists or of a specific list.

Syntax

show ip distribution access-lists [*distribution_list_number*]

Parameters

Parameter	Description	Possible Values	Default Value
distribution_list_number	The distribution list number	**1-99**	

User Level

read-only

Context

general

Example

To display the content of distribution list 1:

```
G450-001(super)# show ip distribution access-lists 1
```

To display the content of all current distribution lists:

```
G450-001(super)# show ip distribution access-lists
```

show ip protocols

Use the **show ip protocols** command to display parameters and statistics of a given IP routing protocol. If no protocol is specified, all running protocols are displayed.

Syntax

show ip protocols [*protocol*]

Parameters

Parameter	Description	Possible Values	Default Value
protocol	The protocol for which to display statistics	**RIP, OSPF**	

User Level

read-only

Context

general

Example

To display all running protocol details:

```
G450-001(super)# show ip protocols
```

To display RIP details:

```
G450-001(super)# show ip protocols RIP

Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 0 seconds
Invalid after 180 seconds, flushed after 300
Redistributing: rip
Default version control: rip version 1
Interface                       Version   Key
Routing for Networks:
Routing Information Sources:
Gateway                 Last Update
```

Related Commands - OSPF

ip ospf authentication, ip ospf authentication-key, ip ospf cost, ip ospf dead-interval, ip ospf hello-interval, ip ospf message-digest-key, ip ospf network point-to-multipoint, ip ospf priority, ip ospf router-id, router ospf, show ip ospf, show ip ospf database, show ip ospf interface, show ip ospf neighbor

Related Commands - RIP

ip distribution access-list, ip rip authentication key, ip rip authentication mode, ip rip default-route-mode, ip rip poison-reverse, ip rip rip-version, ip rip send-receive-mode, ip rip split-horizon, router rip

RMON monitoring

clear rmon statistics

Use the **clear rmon statistics** command to clear traffic statistics for an interface. If no module is specified, information for all modules and ports is cleared.

Syntax

clear rmon statistics

User Level

read-write

Context

general

Related Commands

rmon alarm, rmon history, show rmon alarm, show rmon event, show rmon history, show rmon statistics

rmon alarm

Use the **rmon alarm** command to create an RMON alarm entry. Use the **no** form of this command to destroy a specific RMON alarm.

Note:

The ***rising_event*** and ***falling_event*** events must be defined before using the **rmon alarm** command (refer to rmon event on page 909).

Syntax

rmon alarm *alarm_num variable interval sample_type*
rising-threshold *rising_threshold_value rising_event*
falling-threshold *falling_threshold_value falling_event*
startup_alarm owner

no rmon alarm *alarm_num*

Parameters

Parameter	Description	Possible Values	Default Value
alarm_num	The index number of this alarm		
variable	The OID of the statistic to monitor		
interval	The number of seconds		
sample_type	The type of sample used for the alarm	**absolute**, **delta**	
rising_threshold_value	The value above which the rising_event will be triggered		
rising_event	The event index to trigger when rising_threshold_value is exceeded		
falling_threshold_value	The value below which the falling_event will be triggered		
falling_event	The event index to trigger when falling_threshold_value is reached		
startup_alarm	The prerequisite condition for triggering the alarm for the first time	**rising**, **falling**, **risingOrFalling**	
owner	The username of the alarm owner		

User Level

read-write

Context

general

Example

To create an RMON alarm entry number 1 with statistic OID 1.3.6.1.2.1.16.1.1.1.5.16777216 for 20 seconds, of sample type delta, with event 32 triggered above 10000 and event 32 triggered below 1000, initially triggered either by rising or falling, for username root:

```
G450-001(super)# rmon alarm 1 1.3.6.1.2.1.16.1.1.1.5.16777216 20 delta
rising-threshold 10000 32 falling-threshold 1000 32 risingOrFalling root
alarm 1 was created successfully
```

Related Commands

clear rmon statistics, rmon history, show rmon alarm, show rmon event, show rmon history, show rmon statistics

rmon event

Use the **rmon event** command to create an RMON event entry. The RMON event can then be triggered as part of an RMON alarm. To create an RMON alarm, refer to rmon alarm on page 907. Use the **no** form of this command to delete a specific RMON event entity.

Syntax

rmon event *event_num event_type* description *description* owner *owner*

no rmon event *event_num*

Parameters

Parameter	Description	Possible Values	Default Value
event_num	The index number of the event		
event_type	The type of event	**log, trap**, **logAndTrap**, **none**	
description	The event description		
owner	The username of the event owner		

User Level

read-write

Context

general

Example

To create an RMON event entry with a resetTrap trap event number 32 for owner config:

```
G450-001(super)# rmon event 32 trap description resetTrap owner config
event 32 was created successfully
```

Related Commands

clear rmon statistics, rmon alarm, rmon history, show rmon alarm, show rmon event, show rmon history, show rmon statistics

rmon history

Use the **rmon history** command to create an RMON history entry. Use the **no** form of this command to delete an existing history entry.

Syntax

rmon history *history_index module/port* interval *interval* buckets *buckets* owner *owner*

no rmon history *history_index*

Parameters

Parameter	Description	Possible Values	Default Value
history_index	The index of the history item		
module	The module number		
port	The port on the specified module		
interval	The bucket interval for the history item		
buckets	The number of time intervals over which to save history data		
owner	The username of the history item owner		

User Level

read-write

Context

general

Example

To create an RMON history entry of item 32 with module 10 and port 3 for 20 seconds, saved over 100 time intervals for owner config:

```
G450-001(super)# rmon history 32 10/2 interval 20 buckets 100 owner config
history index 32 was created successfully
```

Related Commands

clear rmon statistics, rmon alarm, rmon event, show rmon alarm, show rmon event, show rmon history, show rmon statistics

show rmon alarm

Use the **show rmon alarm** command to display information about existing alarm entries. If no alarm index is specified, information for all alarms is displayed.

Syntax

show rmon alarm [*alarm_index*]

Parameters

Parameter	Description	Possible Values	Default Value
alarm_index	The alarm about which to display information		

User Level

read-only

Context

general

Example

To show information for all existing RMON alarms:

```
G450-001(super)# show rmon alarm

alarm 1 is active, owned by billp
Monitors ifEntry.1.218106371 every 20 seconds
Taking delta samples, last value was 0
Rising threshold is 500, assigned to event # 1
Falling threshold is 100, assigned to event # 2
On startup enable rising or_falling alarms
```

Related Commands

clear rmon statistics, rmon alarm, rmon event, rmon history, show rmon event, show rmon history, show rmon statistics

show rmon event

Use the **show rmon event** command to display information about existing RMON event entries. If no index is specified, information for all events is displayed.

Syntax

show rmon event [*event_index*]

Parameters

Parameter	Description	Possible Values	Default Value
event_index	The index of the event about which to display information		

User Level

read-only

Context

general

Example

To display RMON event information for all events:

```
G450-001(super)# show rmon event

Event 32 is active, owned by config
Description is resetTrap
Event firing causes trap to community public, last fired 0:0:0
```

Related Commands

clear rmon statistics, rmon alarm, rmon event, rmon history, show rmon alarm, show rmon history, show rmon statistics

show rmon history

Use the **show rmon history** command to display information about existing history entries. If no index is specified, information for all history entries is displayed.

Syntax

show rmon history [*history_index*]

Parameters

Parameter	Description	Possible Values	Default Value
history_index	The history entry about which to display information		

User Level

read-only

Context

general

Example

To display RMON history information for entry 32:

```
G450-001(super)# show rmon history 32

history
Entry 32 is active, owned by config
Monitors the port 10/2 every 20 seconds
Requested # of time intervals, ie buckets, is 100
Granted # of time intervals, ie buckets, is 100
Sample # 47 began measuring at 8:32:17
Received 664636 octets, 1912 packets,
2 broadcast and 0 multicast packets,
0 undersize and 0 oversize packets,
22 fragments and 0 jabbers,
0 CRC alignment errors and 3 collisions,
# of dropped packet events (due to a lack of resources): 0
Network utilization is estimated at 0
```

Related Commands

clear rmon statistics, rmon alarm, rmon event, rmon history, show rmon alarm, show rmon event, show rmon statistics

show rmon statistics

Use the **show rmon statistics** command to display traffic statistics for an interface. If no module is specified, information for all modules and ports is displayed.

Syntax

show rmon statistics [*module/port*]

Parameters

Parameter	Description	Possible Values	Default Value
module	The module number of the interface		
port	The port or range of ports of the interface		

User Level

read-only

Context

general

Example

To display traffic statistics for all modules and ports:

```
G450-001(super)# show rmon statistics

Statistics for switch is active, owned by Monitor
Received 1150436284 octets, 1344680977 packets,
3301887234 broadcast and 3286425893 multicast packets,
3088727251 undersize and 3613263278 oversize packets,
1062765319 fragments and 3882972139 jabbers,
1956639312 CRC alignment errors and 725598320 collisions,
# of dropped packet events (due to a lack of resources): 181377479
# of packets received of length (in octets):
64:1508486650, 65-127:3587014782, 128-255:1989866214,
256-511:378421598, 512-1023:2746475436, 1024-1518:3976219609,
```

Related Commands

clear rmon statistics, rmon alarm, rmon event, rmon history, show rmon alarm, show rmon event, show rmon history

Route redistribution

default-metric (interface route metric value)

Use the **default-metric** command to set the interface route metric value. Use the **no** form of this command to restore the default value.

Syntax

default-metric *number*

no default-metric

Parameters

Parameter	Description	Possible Values	Default Value
number	The interface route metric value	**1-15**	**1**

User Level

read-write

Context

interface: Loopback (L2-L3, L3), Serial (DS1 PPP L2-L3, DS1 PPP L3, DS1 FR-SUB L2-L3, DS1 FR-SUB L3, USP PPP L2-L3, USP PPP L3), FastEthernet L2-L3, L3, PPP L2-L3, PPP L3), VLAN (L2-L3, L3), Tunnel (L2-L3, L3), Dialer (L2-L3, L3)

Example

To set the default metric to 10:

```
G450-001(if:FastEthernet 10/2)# default-metric 10
```

default-metric (OSPF)

Use the **default-metric** command to set the default metric of redistributed routes for the OSPF protocol. Use the **no** form of this command to restore the default value.

Syntax

default-metric *default_metric*

no default-metric

Parameters

Parameter	Description	Possible Values	Default Value
default_metric	The default metric of redistributed routes	**1-65535**	**20**

User Level

read-write

Context

Router-OSPF

Example

To set the default metric for redistributed routes to 50:

```
G450-001(router:ospf)# default-metric 50
```

Related Commands

area, network (OSPF), passive-interface, redistribute (OSPF), timers spf

default-metric (RIP)

Use the **default-metric** command to set the default metric of redistributed routes for the RIP protocol. Use the **no** form of this command to restore the default value.

Syntax

default-metric *default_metric*

no default-metric

Parameters

Parameter	Description	Possible Values	Default Value
default_metric	The interface RIP route metric value	**1-16**	**1**

User Level

read-write

Context

Router-RIP

Example

To set the default metric for redistributed routes to 5:

```
G450-001(router:rip)# default-metric 5
```

Related Commands

default-metric (RIP), distribution-list, network (RIP), redistribute (RIP), timers basic

redistribute (OSPF)

Use the **redistribute** command to redistribute routing information from other protocols into OSPF. Use the **no** form of this command to disable redistribution by OSPF.

Syntax

[no] redistribute ***protocol***

Parameters

Parameter	Description	Possible Values	Default Value
protocol	The protocol to be used	**static**, **connected**, **rip**	

User Level

read-write

Context

Router: ospf

Example

To redistribute static routing information into OSPF:

```
G450-001(router:ospf)# redistribute static
```

Related Commands - OSPF

area, default-metric (OSPF), network (OSPF), passive-interface, timers spf

Related Commands - Route redistribution

default-metric (interface route metric value)

redistribute (RIP)

Use the **redistribute** command to redistribute routing information from another protocol into RIP. Use the **no** form of this command to restore the default value, disable redistribution by RIP.

Syntax

[no] redistribute *protocol*

Parameters

Parameter	Description	Possible Values	Default Value
protocol	The protocol to be used	**static**, **OSPF**	

User Level

read-write

Context

Router-RIP

Example

To redistribute OSPF routing information into RIP:

```
G450-001(router:rip)# redistribute ospf
```

Related Commands - RIP

default-metric (RIP), distribution-list, network (RIP), timers basic

Related Commands - Route redistribution

default-metric (interface route metric value)

Routing table configuration

clear ip route

Use the **clear ip route** command to delete all the dynamic routing entries from the routing table.

Syntax

clear ip route {all | *ip_addr* [*ip_mask*]}

Parameters

Parameter	Description	Possible Values	Default Value
all	Keyword specifying to clear the entire routing table		
ip_addr	The IP address of a specific dynamic routing entry to clear		
ip_mask	The IP mask of a specific dynamic routing subnet to clear		

User Level

read-write

Context

general

Example

To clear the entire routing table:

```
G450-001(super)# clear ip route all
```

To clear the routing entry of IP address 192.168.49.1 with IP mask of 255.255.255.0:

```
G450-001(super)# clear ip route 192.168.49.1 255.255.255.0
```

Related Commands

ip default-gateway, ip netmask-format, ip redirects, ip route, ip routing, show ip route, show ip route best-match, show ip route static, show ip route summary, show ip route track-table, traceroute

ip default-gateway

Use the **ip default-gateway** command to define a default gateway (router). Use the **no** form of this command to remove the default gateway.

Syntax

ip default-gateway {*ip_address* | {*interface_type interface_number*}} [*cost*] [*preference*] [permanent | track *track-index*]

no ip default-gateway

Parameters

Parameter	Description	Possible Values	Default Value
ip_address	The IP address of the router		
interface_type	The interface type		
interface_number	The interface number		
cost	The path cost		**1**
preference	The preference	**High**, **Low**	**Low**
permanent	Keyword that specifies not to disable the router if the interface is down		
track	Keyword that specifies to apply tracking to monitor the default gateway. **Note:** Tracking only applies to non-permanent default gateways.		
track-index	The index number of the object tracker	**1-50**	

User Level

read-write

Context

general

Example

To set the default gateway to the IP address 132.55.4.45, having a cost value of 4 with high preference, and applying object tracker 20:

```
G450-001(super)# ip default-gateway 132.55.4.45 4 high track 20
```

To set the default gateway to be the Serial interface:

```
G450-001(super)# ip default-gateway Serial 4/1:1.1 permanent
```

Related Commands

clear ip route, ip netmask-format, ip redirects, ip route, ip routing, show ip route, show ip route best-match, show ip route static, show ip route summary, show ip route track-table, traceroute

ip netmask-format

Use the **ip netmask-format** command to specify the format of netmasks in the **show** command output. Use the **no** form of this command to restore the format to the default format.

Syntax

ip netmask-format *mask_format*

no ip netmask-format

Parameters

Parameter	Description	Possible Values	Default Value
mask_format	The format of the netmasks	**bitcount** - addresses are followed by a slash and the total number of bits in the netmask, such as 17 **decimal** - the network masks are in dotted decimal notation, such as 255.255.255.0 **hexadecimal** - the network masks are in hexadecimal format as indicated by the leading 0X, such as 0XFFFFFF00	**decimal**

User Level

read-write

Context

general

Example

To display netmasks in bitcount format:

```
G450-001(super)# ip netmask-format bitcount
```

Related Commands

clear ip route, ip default-gateway, ip redirects, ip route, ip routing, show ip route, show ip route best-match, show ip route static, show ip route summary, show ip route track-table, traceroute

ip redirects

Use the **ip redirects** command to enable the sending of redirect messages on the current interface. Use the **no** form of this command to disable redirect messages. By default, sending of redirect messages on the interface is enabled.

Syntax

[no] ip redirects

User Level

read-write

Context

interface:Serial (DS1 PPP L2-L3, DS1 PPP L3, DS1 FR-SUB L2-L3, DS1 FR-SUB L3, USP PPP L2-L3, USP PPP L3), FastEthernet (L2-L3, L3, PPP L2, PPP L2-L3, PPP L3), Tunnel (L2-L3, L3), VLAN (L2-L3, L3), Dialer (L2, L2-L3, L3)

Related Commands

clear ip route, ip default-gateway, ip netmask-format, ip route, ip routing, show ip route, show ip route best-match, show ip route static, show ip route summary, show ip route track-table, traceroute

ip route

Use the **ip route** command to establish a static route. Use the **no** form of this command to remove a static route.

Syntax

ip route ***ip_addr mask*** **{{*next_hop* [*next_hop* [*next_hop*]] } | {*interface_type interface_number*}} [*cost*] [*preference*] [permanent | {track *track-index*} | Null0]**

Note:

You may specify up to three next hops. However, if you apply tracking, you may only specify one next hop.

Note:

If you wish to establish a route through the FastEthernet interface on which DHCP address negotiation is configured, you must specify the interface type as the FastEthernet interface.

Note:

When applying tracking to a static route, a PBR next hop, or the DHCP client default route, you must specify the same next hop for the object tracker's RTR (use the **next hop** command in rtr context).

Note:

Object tracking cannot be configured on Null0 or on a permanent route.

Parameters

Parameter	Description	Possible Values	Default Value
ip_addr	The IP address of the network		
mask	The mask of the static route		
next_hop	The next hop address in the network		
interface_type	The interface type		
interface_number	The interface number		
cost	The path cost		**1**
preference	The preference of the route	**High, Low**	**Low**
permanent	Keyword that specifies that the route is not disabled if the interface is down		
track	Keyword specifying to apply tracking to monitor the route		
track-index	The index number of the object tracker	**1-50**	
Null0	Keyword that creates a static discard route. **Note:** Object tracking cannot be configured on Null0 or on a permanent route.		

User Level

read-write

Context

general

Example

To create a static route on IP address 132.55.0.0 with subnet mask 255.255.0.0 following the path 132.55.4.45, with cost of 3, priority of high, and object tracker 6:

```
G450-001(super)# ip route 132.55.0.0 255.255.0.0 132.55.4.45 3 high track 6
```

To create a static discard route on IP address 134.66.0.0:

```
G450-001(super)# ip route 134.66.0.0 255.255.0.0 Null0
```

To create a static route over the WAN Fast Ethernet when running DHCP client:

```
G450-001# ip route 1.1.1.0 255.255.255.0 FastEthernet 10/2
```

Related Commands

clear ip route, ip default-gateway, ip netmask-format, ip redirects, ip routing, show ip route, show ip route best-match, show ip route static, show ip route summary, show ip route track-table, traceroute

ip routing

Use the **ip routing** command to enable IP routing.

Syntax

ip routing

User Level

read-write

Context

general

Related Commands

clear ip route, ip default-gateway, ip netmask-format, ip redirects, ip route, show ip route, show ip route best-match, show ip route static, show ip route summary, show ip route track-table, traceroute

show ip route

Use the **show ip route** command to display information about the IP routing table. If no IP routes are specified, information about all IP routes are displayed.

Syntax

show ip route [*ip_address*[*ip_mask*]]

Parameters

Parameter	Description	Possible Values	Default Value
ip_address	The IP address of the routes		
ip_mask	The IP mask of the routes		

User Level

read-only

Context

general

Example

To display all routes:

```
G450-001(super)# show ip route
Showing 10 rows

Network    Mask Interface        Next-Hop      Cost  TTL  Source
-------    ----  -----------    --------      ----- ----- ---   ------
0.0.0.0    0     FastEth  10/2   10.0.0.1        1     n/a   DHCP
1.0.0.0    8     Vlan     1.0    1.0.0.1         1     n/a   LOCAL
2.2.0.0    16    Dialer   1      9.9.9.50        1     n/a   STAT-LO-P
3.3.0.0    16    Dialer   1      9.9.9.50        1     n/a   STAT-HI-P
7.0.0.0    8     FastEth  10/2   10.0.0.1 DHCP   1     n/a   STAT-LO
8.0.0.0    8     Vlan     1.2    8.0.0.1         1    n/a    LOCAL
9.0.0.0    8     FastEth  10/2   10.0.0.1 DHCP   1     n/a   STAT-LO
10.0.0.0   8     Vlan     1.0    1.0.0.2        20     n/a   OSPF-E2
10.0.0.0   24    FastEth  10/2   10.0.0.2        1      n/a   LOCAL
11.0.0.0   8     Vlan      1.0   1.0.0.2        20     n/a   OSPF-E2
```

Note:

If DHCP address negotiation is enabled on the FastEthernet interface, the Source column displays `DHCP`.

If the ip route was statically established via the FastEthernet interface on which DHCP address negotiation was configured, the Next-Hop column displays `DHCP` in addition to the address.

To display route 137.32.50.13:

```
G450-001(super)# show ip route 137.32.50.13
```

To display a range from route 137.44.50.13 to 255.255.255.0:

```
G450-001(super)# show ip route 137.44.50.13 255.255.255.0
```

Related Commands

clear ip route, ip default-gateway, ip netmask-format, ip redirects, ip route, ip routing, show ip route best-match, show ip route static, show ip route summary, show ip route track-table, traceroute

show ip route best-match

Use the **`show ip route best-match`** command to display a routing table for a destination address.

Syntax

`show ip route best-match` ***`dst_addr`***

Parameters

Parameter	Description	Possible Values	Default Value
`dst_addr`	The destination IP address		

User Level

read-only

Context

general

Example

To display the routing table entries for IP address 199.93.0.0:

```
G450-001(super)# show ip route best-match 199.93.0.0
Searching for: 199.93.0.0
Showing 1 rows
Network      Mask          Interface  Next-Hop       Cost  TTL Source
-----------  ------------  ---------  -------------  ----  --- -------
199.93.0.0   16            e-135new   135.64.76.1      1   n/a STAT-HI
```

Related Commands

clear ip route, ip default-gateway, ip netmask-format, ip redirects, ip route, ip routing, show ip route, show ip route static, show ip route summary, show ip route track-table, traceroute

show ip route static

Use the **show ip route static** command to display static routes. If no routes are specified, all routes are displayed.

Syntax

show ip route static [*ip_addr* [*mask*]]

Parameters

Parameter	Description	Possible Values	Default Value
ip_addr	The IP address of the routes		
mask	The IP mask of the routes		

User Level

read-only

Context

general

Example

To display all static routes:

```
G450-001(super)# show ip route static
```

To display static route 137.32.50.13:

```
G450-001(super)# show ip route static 137.32.50.13
```

To display the range of static routes from 137.44.50.13 to 255.255.255.0:

```
G450-001(super)# show ip route static 137.44.50.13 255.255.255.0
G450-001(super)# show ip route static
Showing 1 rows
Network  Mask Interface   Next-Hop     Cost  Pref  Perm  Active
-------  ---- ----------  -----------  ----  ----  ----  -------
0.0.0.0   0   FastEth 1  149.49.75.1    1   low    No    Yes
where Pref is the preference, and Perm is Permanent.
```

Related Commands

clear ip route, ip default-gateway, ip netmask-format, ip redirects, ip route, ip routing, show ip route, show ip route best-match, show ip route summary, show ip route track-table, traceroute

show ip route summary

Use the **show ip route summary** command to display the number of routes known to the device.

Syntax

show ip route summary

User Level

read-only

Context

general

Example

To display a summary of routes:

```
G450-001(super)# show ip route summary

Route Source        Networks           Subnets
----------------  ----------------  ------------
Local                   0                1
Static                  0                1
Total                   0                2
```

Related Commands

clear ip route, ip default-gateway, ip netmask-format, ip redirects, ip route, ip routing, show ip route, show ip route best-match, show ip route static, traceroute

show ip route track-table

Use the **show ip route track-table** command to display all routes with configured object trackers.

Syntax

show ip route track-table

User Level

read-only

Context

general

Example

To display all routes with configured object trackers:

```
G450-001(super)# show ip route track-table
Showing 1 rows
Network      Mask Interface          Next-Hop     Track Pref State
------------ ---- ------------------ ------------ ----- ---- -----
1.1.1.0      24   Tunnel 8           Via Tun.8    1     low  Down
```

Related Commands

clear ip route, ip default-gateway, ip netmask-format, ip redirects, ip route, ip routing, show ip route, show ip route best-match, show ip route summary, traceroute

traceroute

Use the **traceroute** command to trace the route packets are taking to a particular host by displaying the hops along the path.

Note:

Pressing any key while **traceroute** is operating, terminates the ongoing trace. However, pressing any key while **traceroute** is probing a locally terminated tunnel (GRE, ESP) exits the tunnel without terminating the ongoing trace.

Syntax

traceroute *host* [local-address *ip-addr*] [probe-count *count*] [dest-port-base *dest-port*] [dest-port-increment *increment*] [source-port *source-port*] [timeout *timeout*] [dscp *dscp*] [next-hop {*next-hop-if-name* | *next-hop-ip-addr*}] [max-ttl *max-ttl*] [size *size*] [protocol *protocol*] [include-tunnel-hops] [set-df-bit]

Parameters

Parameter	Description	Possible Values	Default Value
host	The destination host of the traceroute probes, specified as an IP address or host name		
ip_addr	The local IP address of the traceroute probes		The outbound interface address
count	The number of times each TTL value is repeated for a traceroute	**1-5**	**3**
dest-port	The destination port of the first probe sent	**1,024-65,535**	**33,434**
increment	An integer that determines by how much the destination port is incremented for each probe sent, starting from base port	**0-254**	**1**
source-port	The source port of the traceroute probes	**1,024-65,535**	**33,434**
timeout	The duration, in milliseconds, that traceroute waits for a response for each probe sent, until it gives up and marks this probe as unreachable	**10ms-120sec** in milliseconds	**2 seconds** in milliseconds
dscp	The value of the DS field of the traceroute probes	**0-63**	**0**
next-hop-if-name	The interface name of the next hop		
next-hop-ip-addr	The IP address of the next hop		
max-ttl	Do not probe over this TTL value	**1-50**	**30**
size	The L4 payload length, in bytes	**8-4,088**	**40**
protocol	The protocol type of the traceroute probes	**ICMP, UDP**	**UDP**

Parameter	Description	Possible Values	Default Value
include-tunnel-hops	Keyword that specifies that traceroute display the route taken by the probes as they traverse locally terminated tunnels (such as GRE, ESP)		
set-df-bit	Keyword that specifies to set the Don't-Fragment field of the traceroute probes		

User Level

read-only

Context

general

Example

To trace the route to IP address 60.60.60.1, including the route taken by the probes as they traverse locally terminated tunnels:

```
G450-001(super)# traceroute 60.60.60.1 include-tunnel-hops
Tracing route to 60.60.60.1 over a maximum of 30 hops, 40 bytes packets.
Press any key to abort.
  1     3 ms     3 ms     3 ms    111.111.111.114   ESP tunnel
  2     6 ms     5 ms     6 ms    60.60.60.1        GRE tunnel
Trace complete.
```

Related Commands

clear ip route, ip default-gateway, ip netmask-format, ip redirects, ip route, ip routing, show ip route, show ip route best-match, show ip route static, show ip route summary, show ip route track-table

RSVP

set qos rsvp

Use the **set qos rsvp** command to set the current values for the RSVP parameters of the VoIP engines. The parameters that can be set are enabled or disabled, refresh rate in seconds, failure retry yes or no, and service profile (guaranteed-service or controlled load service).

Note:

The **set qos rsvp command** *will not* take effect unless QoS source setup is **local**.

Syntax

set qos rsvp {enable | disable} | {refresh *secs*} | {failure {retry | noretry}} | {profile {guaranteed | controlled}}

Parameters

Parameter	Description	Possible Values	Default Value
enable	Keyword indicating to enable RSVP in the router		
disable	Keyword indicating to disable RSVP in the router		
secs	The refresh time in seconds	**1-99**	**15**
retry	Keyword indicating to retry upon failure		
noretry	Keyword indicating no retry upon failure		
guaranteed	Keyword indicating to use the guaranteed service profile		
controlled	Keyword indicating to use the controlled load service profile		

User Level

read-write

Context

general

Example

To set the refresh rate to 15 seconds:

```
G450-001(super)# set qos rsvp refresh 15
```

To specify no retry upon failure:

```
G450-001(super)# set qos rsvp failure noretry
```

To specify controlled load service:

```
G450-001(super)# set qos rsvp profile controlled
```

To enable RSVP:

```
G450-001(super)# set qos rsvp enable
```

Related Commands

show qos-rtcp

---

show qos-rtcp

Use the **show qos-rtcp** command to display QoS, RTCP, and RSVP parameters.

Syntax

show qos-rtcp

User Level

admin

Context

general

Example

To display QoS, RSVP and RTCP parameters:

```
G450-001(super)# show qos-rtcp
PARAMETERS IN EFFECT: -- Downloaded --

QOS PARAMETERS          LOCALLY SET        DOWNLOADED
--------------------    ---------------    ---------------
Signal 802 Priority:    7                  0
Signal DSCP        :    34                 0
Bearer 802 Priority:    6                  6
Bearer BBE DSCP    :    43                 43
Bearer EF DSCP     :    46                 46
Minimum RTP Port   :    3                  2048
Maximum RTP Port   :    65535              65535
```

```
RSVP PARAMETERS          LOCALLY SET        DOWNLOADED
--------------------     ---------------    ---------------
State               :    Enabled            Disabled
Retry on Failure    :    Yes                Yes
Retry Delay(secs)   :    15                 15
Service Profile     :    Guaranteed         Guaranteed

RTCP MON  PARAMETERS     LOCALLY SET        DOWNLOADED
--------------------     ---------------    ---------------
State               :    Enabled            Disabled
IP Address          :    0.0.0.0            0.0.0.0
Listening Port      :    5005               5005
Report Period(secs):     5                  5
```

Related Commands - RSVP

set qos rsvp

Related Commands - RTCP

set qos rtcp

RTCP

set qos rtcp

Use the **set qos rtcp** command to permit the setup of RTCP parameters. The parameters that can be set are enabling or disabling RTCP reporting capability, setting the IP address of the monitor, setting the reporting period, and defining the listening port number.

Syntax

set qos rtcp {{enable|disable} | monip *ip-address* | reportper *seconds* | listenport *portno*}

Parameters

Parameter	Description	Possible Values	Default Value
enable	Keyword that specifies to enable RTCP reporting capability		
disable	Keyword that specifies to disable RTCP reporting capability		
ip-address	The IP address of the monitor		
seconds	The reporting period in seconds	**5-30**	**5**
portno	The listening port number	**1-65535**	**5005**

User Level

read-write

Context

general

Example

To set the monitoring IP address to 132.123.23.12:

```
G450-001(super)# set qos rtcp monip 132.123.23.12
```

To set the reporting period to 10 seconds:

```
G450-001(super)# set qos rtcp reportper 10
```

To set the listening port number to 5000:

```
G450-001(super)# set qos rtcp listenport 5000
```

To enable reporting capability:

```
G450-001(super)# set qos rtcp enable
```

Related Commands - RTCP

show qos-rtcp

show qos-rtcp

Use the **show qos-rtcp** command to display QoS and RTCP parameters.

Syntax

show qos-rtcp

User Level

admin

Context

general

Example

To display QoS, RSVP and RTCP parameters:

```
G450-001(super)# show qos-rtcp
PARAMETERS IN EFFECT: -- Downloaded --

QOS PARAMETERS          LOCALLY SET        DOWNLOADED
--------------------    ---------------    ---------------
Signal 802 Priority:    7                  0
Signal DSCP         :   34                 0
Bearer 802 Priority:    6                  6
Bearer BBE DSCP     :   43                 43
Bearer EF DSCP      :   46                 46
Minimum RTP Port    :   3                  2048
Maximum RTP Port    :   65535              65535

RSVP PARAMETERS         LOCALLY SET        DOWNLOADED
--------------------    ---------------    ---------------
State               :   Enabled            Disabled
Retry on Failure    :   Yes                Yes
Retry Delay(secs)   :   15                 15
Service Profile     :   Guaranteed         Guaranteed

RTCP MON  PARAMETERS    LOCALLY SET        DOWNLOADED
--------------------    ---------------    ---------------
State               :   Enabled            Disabled
IP Address          :   0.0.0.0            0.0.0.0
Listening Port      :   5005               5005
Report Period(secs):    5                  5
```

Related Commands - RSVP

set qos rsvp

Related Commands - RTCP

set qos rtcp

RTP statistics

rtp-stat clear

Use the **rtp-stat clear** command to reset the RTP statistics application. When you reset the application, all counters are reset and the RTP statistics history is erased.

Syntax

rtp-stat clear

User Level

read-write

Context

general

Example

To reset the RTP statistics application:

```
G450-001(super)# rtp-stat clear
```

Related Commands

rtp-stat event-threshold, rtp-stat fault, rtp-stat min-stat-win, rtp-stat qos-trap, rtp-stat qos-trap-rate-limit, rtp-stat-service, rtp-stat threshold, show rtp-stat config, show rtp-stat detailed, show rtp-stat sessions, show rtp-stat summary, show rtp-stat thresholds, show rtp-stat traceroute

rtp-stat event-threshold

Use the **rtp-stat event-threshold** command to set thresholds on the QoS event counters incremented by the RTP statistics application. If one or more event thresholds are exceeded during an RTP stream and the RTP statistics application is configured to generate QoS SNMP traps, a trap is generated upon termination of the RTP stream. Use the rtp-stat qos-trap command to configure the RTP statistics application to automatically generate QoS traps. Use the rtp-stat threshold command to configure the QoS metric thresholds. Event thresholds should be configured such that the sending of a trap corresponds to a customer's actual experience of QoS problems during the stream.

Syntax

rtp-stat event-threshold
{all|codec-loss|codec-rtt|echo-return-loss|loss|remote-loss|rtt|jitter|remote-jitter|ssrc-change} ***num***

no rtp-stat event-threshold
{all|codec-loss|codec-rtt|echo-return-loss|loss|remote-loss|rtt|jitter|remote-jitter|ssrc-change}

Parameters

Parameter	Description	Possible Values	Default Value
all	Keyword specifying to set all event thresholds to the specified number		
codec-loss	Keyword specifying to set the event threshold for the codec-loss metric		
codec-rtt	Keyword specifying to set the event threshold for the codec-rtt metric		
echo-return-loss	Keyword specifying to set the event threshold for the echo-return-loss metric		
loss	Keyword specifying to set the event threshold for the loss metric		
remote-loss	Keyword specifying to set the event threshold for the remote-loss metric		

Parameter	Description	Possible Values	Default Value
rtt	Keyword specifying to set the event threshold for the rtt metric		
jitter	Keyword specifying to set the event threshold for the jitter metric		
remote-jitter	Keyword specifying to set the event threshold for the remote-jitter metric		
ssrc-change	Keyword specifying to set the event threshold for the ssrc-change metric		
num	The number of events		

User Level

read-write

Context

general

Example

To set RTP-stat echo-return-loss event-threshold to 2:

```
G450-001(super)# rtp-stat event-threshold echo-return-loss 2
```

Related Commands

rtp-stat clear, rtp-stat fault, rtp-stat min-stat-win, rtp-stat qos-trap, rtp-stat qos-trap-rate-limit, rtp-stat-service, rtp-stat threshold, show rtp-stat config, show rtp-stat detailed, show rtp-stat sessions, show rtp-stat summary, show rtp-stat thresholds, show rtp-stat traceroute

rtp-stat fault

Use the **rtp-stat fault** command to configure the RTP statistics application to send QoS fault and/or clear traps. A QoS fault trap is sent when a specified number of active RTP sessions have QoS indicators over the configured thresholds. A QoS clear trap is sent after a QoS fault trap when the number of active RTP sessions with QoS indicators over the configured thresholds reduces to a specified number. QoS fault and clear traps are enabled by default.

Syntax

rtp-stat fault [*fault* [*clear*]]

[no] rtp-stat fault

Parameters

Parameter	Description	Possible Values	Default Value
fault	The fault trap boundary. If the number of active sessions with QoS faults reaches the fault trap boundary, a QoS fault trap is sent.	**1-100**	**3**
clear	The clear trap boundary. If the number of active sessions with QoS faults reduces to the clear trap boundary after a QoS fault trap was sent, a QoS clear trap is sent.	**0-99**	

User Level

read-write

Context

general

Example

To set the fault trap boundary to 1 and the clear trap boundary to 0:

```
G450-001(super)# rtp-stat fault 1 0
The fault trap boundary was set to 1 (default: 3)
The clear trap boundary was set to 0
```

Related Commands

rtp-stat clear, rtp-stat event-threshold, rtp-stat min-stat-win, rtp-stat qos-trap, rtp-stat qos-trap-rate-limit, rtp-stat-service, rtp-stat threshold, show rtp-stat config, show rtp-stat detailed, show rtp-stat sessions, show rtp-stat summary, show rtp-stat thresholds, show rtp-stat traceroute

rtp-stat min-stat-win

Use the **rtp-stat min-stat-win** command to set the minimum statistic window for the RTP statistics application. The minimum statistics window is the minimum number of observed RTP sequence increments for which the application evaluates packet loss. Use the **no** form of this command to reset the minimum statistic window to its default value.

The VoIP engine evaluates the current received packet loss every RTCP interval. The RTCP interval is usually between 5 and 8 seconds. The VoIP engine postpones loss estimation to the next interval if the number of received packets is less than the minimum statistic window.

Syntax

[no] rtp-stat min-stat-win *packets*

Parameters

Parameter	Description	Possible Values	Default Value
packets	The minimum number of observed RTP sequence increments for which the application evaluates packet loss	**10-1000**	

User Level

read-write

Context

general

Example

To set the minimum statistic window to 50:

```
G450-001(super)# rtp-stat min-stat-win 50
```

Related Commands

rtp-stat clear, rtp-stat event-threshold, rtp-stat fault, rtp-stat qos-trap, rtp-stat qos-trap-rate-limit, rtp-stat-service, rtp-stat threshold, show rtp-stat config, show rtp-stat detailed, show rtp-stat sessions, show rtp-stat summary, show rtp-stat thresholds, show rtp-stat traceroute

rtp-stat qos-trap

Use the **rtp-stat qos-trap** command to enable the RTP statistics application to automatically generate QoS traps upon the terminations of RTP streams in which one or more QoS event counters exceeded their configured thresholds. The traps are sent by an SNMP agent to the SNMP trap manager on the Media Gateway Controller (MGC) They are converted to Syslog messages and stored in the messages file on the MGC. Use the **no** form of this command to disable QoS traps. By default, QoS traps are enabled.

Syntax

[no] rtp-stat qos-trap

User Level

read-write

Context

general

Example

To enable QoS traps:

```
G450-001(super)#  rtp-stat qos-trap
The RTP statistics QoS trap is enabled
```

Related Commands

rtp-stat clear, rtp-stat event-threshold, rtp-stat fault, rtp-stat min-stat-win, rtp-stat qos-trap-rate-limit, rtp-stat-service, rtp-stat threshold, show rtp-stat config, show rtp-stat detailed, show rtp-stat sessions, show rtp-stat summary, show rtp-stat thresholds, show rtp-stat traceroute

rtp-stat qos-trap-rate-limit

Use the **rtp-stat qos-trap-rate-limit** command to configure the QoS trap rate limiter. The trap rate limiter limits the rate at which QoS traps are sent to the SNMP trap manager on the MGC. The trap rate limiter uses a token bucket scheme, in which traps are sent only if there are tokens in a virtual bucket. Tokens are added to the bucket every token interval, which sets the maximum long term trap rate. Each time a trap is sent, the number of tokens in the bucket decrements. The bucket size is the maximum number of tokens that the bucket can hold. The bucket size limits the trap burst size.

Syntax

rtp-stat qos-trap-rate-limit ***token-interval bucket-size***

Parameters

Parameter	Description	Possible Values	Default Value
token-interval	The interval, in hundredths of seconds, between additions of a token to the bucket	**10-100000**	**1000**
bucket-size	The maximum number of tokens stored in the bucket	**1-1000**	**5**

User Level

read-write

Context

general

Example

To limit the QoS trap rate to a token every 10 hundredths of a second up to 50 tokens:

```
G450-001(super)# rtp-stat qos-trap-rate-limit 10 50
```

Related Commands

rtp-stat clear, rtp-stat event-threshold, rtp-stat fault, rtp-stat min-stat-win, rtp-stat qos-trap, rtp-stat-service, rtp-stat threshold, show rtp-stat config, show rtp-stat detailed, show rtp-stat sessions, show rtp-stat summary, show rtp-stat thresholds, show rtp-stat traceroute

rtp-stat-service

Use the **rtp-stat-service** command to enable the RTP statistics application. Use the **no** form of this command to disable the RTP statistics application. By default, the RTP statistics application is disabled.

Syntax

[no] rtp-stat-service

User Level

admin

Context

general

Example

To enable the RTP statistics application:

```
G450-001 (super)# rtp-stat-service
The RTP statistics service is enabled.
```

Related Commands

rtp-stat clear, rtp-stat event-threshold, rtp-stat fault, rtp-stat min-stat-win, rtp-stat qos-trap, rtp-stat qos-trap-rate-limit, rtp-stat threshold, show rtp-stat config, show rtp-stat detailed, show rtp-stat sessions, show rtp-stat summary, show rtp-stat thresholds, show rtp-stat traceroute

rtp-stat threshold

Use the **rtp-stat threshold** command to set thresholds for QoS metrics sampled by the RTP statistics application. An event counter for each metric increments every time the metric exceeds its threshold during an RTP session. Use the **rtp-stat threshold** command also to set thresholds on averages of metrics. When an RTP session terminates, the RTP statistics application evaluates the average metrics and generates a QoS trap (if QoS traps are configured) if one or more of them is over its corresponding threshold. See also rtp-stat event-threshold on page 938.

Syntax

rtp-stat threshold
{codec-loss|average-codec-loss|loss|average-loss|remote-loss|
average-remote-loss} ***percentage***

rtp-stat threshold {codec-rtt|rtt|jitter|remote-jitter} ***milliseconds***

rtp-stat threshold echo-return-loss ***db***

no rtp-stat threshold
{all|codec-loss|average-codec-loss|codec-rtt|echo-return-loss|loss|
average-loss|remote-loss|average-remote-loss|rtt|jitter|remote-loss|
echo-return-loss}

Parameters

Parameter	Description	Possible Values	Default Value
codec-loss	Keyword specifying to set the percentage of time the codec plays fill frames due to lack of valid RTP frames. Possible causes include jitter and packet loss.		
average-codec-loss	Keyword specifying to set the average codec loss measurement since the beginning of the RTP stream		
loss	Keyword specifying to set the estimated network RTP packet loss. The VoIP engine evaluates the current received packet loss every RTCP interval — usually 5 to 8 seconds. The VoIP engine postpones loss estimation until the next interval if the number of packets received is less than the minimum statistic window. The minimum statistic window is configured with the CLI command **rtp-stat min-stat-win**.		
average-loss	Keyword specifying to set the average packet loss evaluation since the beginning of the RTP stream		
remote-loss	Keyword specifying to set the network loss according to the remote RTP receiver. The device learns of the remote packet loss from received RTCP messages.		
average-remote-loss	Keyword specifying to set the average remote network loss measurement since the beginning of the RTP stream		
percentage	The percent value	**0.0-100.0**	

Parameter	Description	Possible Values	Default Value
codec-rtt	Keyword specifying to set an estimation of the overall Round Trip Time (RTT) on the voice-channel, including the network delay and internal delays. Round Trip Time is the time taken for a message to get to the remote peer and back to the local receiver.		
rtt	Keyword specifying to set the network RTT. This metric does not include internal delay. The device learns of the RTT from RTCP messages.		
jitter	Keyword specifying to set the variation in delay of packet delivery to the local peer		
remote-jitter	Keyword specifying to set the variation in delay of packet delivery to the remote peer. The device learns of the remote jitter from RTCP messages.		
milliseconds		**0-5000**	
echo-return-loss	Keyword specifying to set the echo cancellation loss on the TDM bus		
db	The db value	**0-100**	
all	Keyword specifying to clear all configured thresholds		

User Level

read-write

Context

general

Example

To set the echo return loss threshold to 5 dB:

```
G450-001(super)# rtp-stat threshold echo-return-loss 5
```

Related Commands

rtp-stat clear, rtp-stat event-threshold, rtp-stat fault, rtp-stat min-stat-win, rtp-stat qos-trap, rtp-stat qos-trap-rate-limit, rtp-stat-service, show rtp-stat config, show rtp-stat detailed, show rtp-stat sessions, show rtp-stat summary, show rtp-stat thresholds, show rtp-stat traceroute

show rtp-stat config

Use the **show rtp-stat config** command to display the RTP statistics application configuration.

Syntax

show rtp-stat config

User Level

read-only

Context

general

Example

To display the configuration of the RTP statistics application:

```
G450-001(super)# show rtp-stat config

RTP Statistic: Enabled
QoS Trap: Enabled
QoS Fault Trap: Enabled
    Fault: 1
    Clear: 0
QoS Trap Rate Limiter:
    Token Interval: 10.00 seconds
    Bucket Size: 5
Session Table:
    Size: 128
    Reserved: 64
Min Stat Win: 50
```

Note:

For an explanation of the output fields, see the table describing the output of the **show rtp-stat config** command in the chapter *Configuring monitoring applications*, in *Administration for the Avaya G450 Media Gateway*, 03-602055.

Related Commands

rtp-stat clear, rtp-stat event-threshold, rtp-stat fault, rtp-stat min-stat-win, rtp-stat qos-trap, rtp-stat qos-trap-rate-limit, rtp-stat-service, rtp-stat threshold, show rtp-stat detailed, show rtp-stat sessions, show rtp-stat summary, show rtp-stat thresholds, show rtp-stat traceroute

show rtp-stat detailed

Use the **show rtp-stat detailed** command to display a detailed QoS log for a specific RTP session.

Syntax

show rtp-stat detailed *session-id*

Parameters

Parameter	Description	Possible Values	Default Value
session-id	The index of a specific RTP session		

User Level

read-only

Context

general

Example

To display RTP statistics for RTP session 35:

```
G450-001(super)#  show rtp-stat detailed 35
Session-ID: 35
Status: Active, QOS: Faulted, EngineId: 0
Start-Time: 2004-10-20,11:09:07, End-Time: -
Duration: 00:03:11
CName: gwp@135.8.118.252
Phone:
Local-Address: 135.8.118.252:2045 SSRC 154611212
Remote-Address: 135.8.76.107:2061 SSRC 2989801899 (0)
Samples: 38 (5 sec)
Codec:
G723 62B 30mS Off, Silence-suppression(Tx/Rx) Disabled/Not-Supported,
Play-Time
186.690sec, Loss 0.0% #1, Avg-Loss 0.1%, RTT 816mS #18, Avg-RTT 463mS,
JBuf-under/overruns 0.2%/0.0%, Jbuf-Delay 60mS, Max-Jbuf-Delay 60mS
Received-RTP:
Packets 6372, Loss 0.0% #0, Avg-Loss 0.0%, RTT 603mS #18, Avg-RTT 267mS, Jitter
0mS #0, Avg-Jitter 0mS, TTL(last/min/max) 63/63/63, Duplicates 0, Seq-Fall 0,
DS
```

```
CP 46, L2Pri 12, RTCP 37
Transmitted-RTP:
VLAN 1, DSCP 184, L2Pri 6, RTCP 43
Remote-Statistics:
Loss 0.0% #0, Avg-Loss 0.0%, Jitter 0mS #0, Avg-Jitter 0mS
Echo-Cancellation:
Loss 45dB #1, Len 32mS
RSVP:
Status Disabled, Failures 0
```

Note:

For an explanation of the output fields, see the table describing the output of the **show rtp-stat detailed** command in the chapter *Configuring monitoring applications*, in *Administration for the Avaya G450 Media Gateway*, 03-602055.

Related Commands

rtp-stat clear, rtp-stat event-threshold, rtp-stat fault, rtp-stat min-stat-win, rtp-stat qos-trap, rtp-stat qos-trap-rate-limit, rtp-stat-service, rtp-stat threshold, show rtp-stat config, show rtp-stat sessions, show rtp-stat summary, show rtp-stat thresholds, show rtp-stat traceroute

show rtp-stat sessions

Use the **show rtp-stat sessions** command to display a summary of the active and/or terminated RTP sessions in the session table. If no parameters are specified, a summary of all RTP session information is displayed.

Syntax

show rtp-stat sessions [active|active-events|history|events] [destination-ip {*remote-subnet remote-subnet-mask*}|{host *rem-addr*}] [last *last-N*]

Parameters

Parameter	Description	Possible Values	Default Value
active	Keyword specifying to display only active sessions		
active-events	Keyword specifying to display only active sessions experiencing bad QoS conditions		
history	Keyword specifying to display only terminated sessions		

Parameter	Description	Possible Values	Default Value
events	Keyword specifying to display only terminated sessions that experienced bad QoS conditions		
destination-ip	Keyword specifying to display only sessions to this destination subnet		
remote-subnet	The destination subnet		
remote-subnet-mask	The destination subnet mask		
host	Keyword specifying to display only sessions to this specific address		
rem-addr	The specific IP address		
last	Keyword specifying to display only the last *N* entries in the history		
last-N	The number of entries in the history to display		

User Level

read-only

Context

general

Example

To display all RTP sessions:

```
G450-001(super)# show rtp-stat sessions

ID    QoS Start date and time End Time  Type      Destination
----- --- ------------------- --------  --------- ---------------
00001  *  2004-10-15,16:57:48 17:00:15   G729      135.8.76.64
00002     2004-10-15,16:59:06 17:00:15   G729      135.8.76.62
00003  *  2004-10-15,17:00:41 17:01:40   G723      135.8.76.107
00004  *  2004-10-18,10:28:33 10:30:29   G729      135.8.76.64
00005  *  2004-10-18,10:39:03 10:42:15   G723      135.8.76.107
00006  *  2004-10-18,10:52:26 10:53:15   G729      135.8.76.64
00007  *  2004-10-18,10:53:42 10:54:29   G723      135.8.76.107
00008  *  2004-10-18,10:56:31 10:57:34   G729      135.8.76.64
00009     2004-10-18,10:57:39 11:02:38   G729      135.8.76.64
00010     2004-10-18,11:03:13 11:06:07   G723      135.8.76.13
00011     2004-10-18,11:13:56 11:16:46   G723      135.8.76.35
00012     2004-10-18,11:13:58 11:16:46   G723      135.8.76.14
00013  *  2004-10-18,11:18:47 11:19:32   G723      135.8.76.107
00014  *  2004-10-18,11:18:50 11:19:59   G723      135.8.76.107
00015  *  2004-10-18,11:20:23 11:20:53   G723      135.8.76.107
00016  *  2004-10-18,11:21:04 11:21:55   G723      135.8.76.107
00017  *  2004-10-18,11:22:11 11:23:02   G729      135.8.76.64
00018     2004-10-18,11:22:42 11:23:02   G729      135.8.76.62
00019  *  2004-10-18,11:40:12 11:42:10   G723      135.8.76.107
00020  *  2004-10-18,11:46:43 11:50:33   G723      135.8.76.107
00021  *  2004-10-18,11:47:07 11:50:33   G723      135.8.76.107
00022  *  2004-10-18,11:47:27 11:50:31   G723      135.8.76.107
00023     2004-10-18,11:48:34 11:50:43   G723      135.8.76.35
00024     2004-10-18,11:48:34 11:50:43   G723      135.8.76.14
00025  *  2004-10-18,11:54:01 11:55:27   G723      135.8.76.13
00026  *  2004-10-18,11:54:02 11:55:27   G729      135.8.76.62
00027  *  2004-10-18,13:43:18 13:54:53   G723      135.8.76.107
00028  *  2004-10-18,13:56:57 08:40:39   G723      135.8.76.107
00029     2004-10-19,17:24:00 17:28:10   G711A     135.8.76.107
00030  *  2004-10-19,17:29:06 09:04:04   G723      135.8.76.107
00031     2004-10-20,10:51:36 10:59:07   G729      135.8.76.64
00032  *  2004-10-20,10:53:42 10:57:36   G723      135.8.76.107
00033  *  2004-10-20,10:58:21 10:59:06   G723      135.8.76.107
00034     2004-10-20,11:08:40         -   G729      135.8.76.64
00035     2004-10-20,11:09:07         -   G723      135.8.76.107
```

To display the last five sessions:

```
G450-001(super)# show rtp-stat sessions last 5

ID    QoS Start date and time End Time Type     Destination
----- --- ------------------- -------- ------- ---------------
00031     2004-10-20,10:51:36 10:59:07 G729     135.8.76.64
00032  *  2004-10-20,10:53:42 10:57:36 G723     135.8.76.107
00033  *  2004-10-20,10:58:21 10:59:06 G723     135.8.76.107
00034     2004-10-20,11:08:40         - G729     135.8.76.64
00035  *  2004-10-20,11:09:07         - G723     135.8.76.107
```

Note:

For an explanation of the output fields, see the explanations in the chapter *Configuring monitoring applications*, in *Administration for the Avaya G450 Media Gateway*, 03-602055.

Related Commands

rtp-stat clear, rtp-stat event-threshold, rtp-stat fault, rtp-stat min-stat-win, rtp-stat qos-trap, rtp-stat qos-trap-rate-limit, rtp-stat-service, rtp-stat threshold, show rtp-stat config, show rtp-stat detailed, show rtp-stat summary, show rtp-stat thresholds, show rtp-stat traceroute

show rtp-stat summary

Use the **`show rtp-stat summary`** command to display a summary of the RTP statistics.

Syntax

`show rtp-stat summary`

User Level

read-write

Context

general

Example

To display a summary of the RTP statistics (in this example, there are two active sessions, one with QoS problems (35)):

```
G450-001(super)# show rtp-stat summary

Total QoS traps: 23
QoS traps Drop : 0
Qos Fault
Engine                          Active   Total    Mean      Tx
```

```
ID   Description     Uptime       Session  Session  Duration  TTL
---  --------------  -----------  -------  -------  --------  ----
000        internal  04,18:15:15    3/1     35/24   01:04:44   64
```

Note:

For an explanation of the output fields, see the table describing the output of the **show rtp-stat summary** command in the chapter *Configuring monitoring applications*, in *Administration for the Avaya G450 Media Gateway*, 03-602055.

Related Commands

rtp-stat clear, rtp-stat event-threshold, rtp-stat fault, rtp-stat min-stat-win, rtp-stat qos-trap, rtp-stat qos-trap-rate-limit, rtp-stat-service, rtp-stat threshold, show rtp-stat config, show rtp-stat detailed, show rtp-stat sessions, show rtp-stat thresholds, show rtp-stat traceroute

show rtp-stat thresholds

Use the **show rtp-stat thresholds** command to display the configured thresholds and event-thresholds for QoS metrics sampled by the RTP statistics application during RTP streams.

Syntax

show rtp-stat thresholds

User Level

read-only

Context

general

Example

To display the configured RTP statistics application thresholds:

```
G450-001(super)# show rtp-stat thresholds

Item                 Threshold      Event Threshold
-------------------  -------------  -----------------
Codec Loss           6.0%           1
Average Codec Loss   3.0%           N/A
Codec RTT            700mS          1
Echo Return Loss     0dB            1
Loss                 6.0%           1
Average Loss         3.0%           N/A
Remote Loss          6.0%           1
```

```
Average Remote Loss    3.0%           N/A
RTT                    500mS          1
Local Jitter           50mS           1
Remote Jitter          50mS           1
SSRC Changes           N/A            1
```

Note:

For an explanation of the output fields, see the table describing the output of the **show rtp-stat thresholds** command in the chapter *Configuring monitoring applications*, in *Administration for the Avaya G450 Media Gateway*, 03-602055.

Related Commands

rtp-stat clear, rtp-stat event-threshold, rtp-stat fault, rtp-stat min-stat-win, rtp-stat qos-trap, rtp-stat qos-trap-rate-limit, rtp-stat-service, rtp-stat threshold, show rtp-stat config, show rtp-stat detailed, show rtp-stat sessions, show rtp-stat summary, show rtp-stat traceroute

show rtp-stat traceroute

If the RTP statistics application is enabled (see rtp-stat-service), the G450 VoIP engine issues a UDP traceroute for every active RTP session. The traceroute is performed 10 seconds after the session begins. A traceroute is not performed if there is another active session to the same destination for which a traceroute was already performed within the last 5 seconds. Use the **show rtp-stat traceroute** command to display the automatic session traceroute result. You can filter the results according to subnet address or rtp-statistics session index.

Syntax

show rtp-stat traceroute [{session *session-id*] | destination-ip *remote-subnet remote-subnet-mask* [last *Last-N*]}]

Parameters

Parameter	Description	Possible Values	Default Value
session-id	The index of a specific RTP statistics session		
remote-subnet	The remote subnet address		
remote-subnet-mask	The remote subnet mask		

Parameter	Description	Possible Values	Default Value
last	Keyword indicating to display only the last *N* entries in the history		
last-N	The number of entries in the history to display		

User Level

read-only

Context

general

Example

To display the automatic session traceroute result, filtered by subnet address with remote subnet 10.2.5.0 and remote subnet mask 255.255.255.0:

```
G450-001(super)# show rtp-stat traceroute destination-ip 10.2.5.0
255.255.255.0
Session ID: 1234
From: 123.21.11.5, To: 10.2.4.15, At: 2004-12-26,12:21:55
TTL HOP ADDRESS       DELAY
--- ---------------  --------
 1  123.21.11.1         2ms
 2  212.201.233.102    65ms
 3  213.21.51.12      110ms
 4  10.2.4.15         175ms

Session ID: 1234
From: 123.21.11.5, To: 10.2.4.5, At: 2004-12-26,13:30:15
TTL HOP ADDRESS       DELAY
--- ---------------  --------
 1  123.21.11.1         2ms
 2  212.201.233.102    65ms
 3  213.21.51.12      110ms
 4  10.2.4.5          145ms
```

Output fields:

Field	Description
Session ID	The RTP statistics index for the RTP session
From	The IP address of the G450
To	The IP address of the session destination (in this case, a destination within the specified subnet)
At	The time the traceroute is performed
TTL	The hop count and TTL field value of probe packets
HOP ADDRESS	The hop IP address
DELAY	The round trip time per probe packet. Three probe packets are sent per hop address, and the displayed value is the average of the three round-trip times. An asterisk (*) indicates that the probe packets timed out.

Related Commands

rtp-stat clear, rtp-stat event-threshold, rtp-stat fault, rtp-stat min-stat-win, rtp-stat qos-trap, rtp-stat qos-trap-rate-limit, rtp-stat-service, rtp-stat threshold, show rtp-stat config, show rtp-stat detailed, show rtp-stat sessions, show rtp-stat summary

SAT

sat

Use the **sat** command to provide a shortcut method to access the System Access Terminal (SAT) so that Avaya Communication Manager translation work can be performed. See the description for session on page 597 for more information. The server must configure the SAT port to 5023.

Syntax

```
sat
```

User Level

read-only

Context

general

Example

To open a connection directly to the Avaya Communication Manager SAT application in the MGC:

```
G450-001(super)# session mgc sat
```

Related Commands

session

SLS survivability

sls

Use the **sls** command to enter the sls context. In this context, you can administer the SLS data set from the G450 CLI. Type **exit** to leave the sls context.

Several second-level subcontexts within the sls context help SLS administration. While in the sls context type these commands to enter the respective subcontexts:

- **station *extension class*** to enter the station context
- **trunk-group *tgnum [group-type]*** to enter the trunk-group context
- **ds1 *port-address*** to enter the ds1 context
- **sig-group *sgnum*** to enter the sig-group context
- **bri *port-address*** to enter the bri context
- **dial-pattern *dialed-string*** to enter the dial-pattern context
- **incoming-routing *tgnum mode* [*pattern length*]** to enter the incoming-routing context

Important:
If you issue this command on a G450 with insufficient memory, the **sls** command aborts and entry into the sls context is denied.

Syntax

sls

User Level

read-write

Context

general

Example

To enter the `sls` context:

```
G450-001(super)# sls
G450-001(super-sls)#
```

Related Commands

bri, clear survivable-config, dial-pattern, ds1, incoming-routing, set sls, show sls, sig-group, station, trunk-group

---

set sls

Use the **set sls** command to enable or disable SLS.

Note:

If the SLS survivable call engine is currently running, you can issue this command to stop SLS from operating.

Note:

If you enabled SLS and then entered additional administration, you must first disable SLS and then re-enable it. This will cause the SLS application to resynchronize its administrative database with the gateway's global CLI command database.

Syntax

set sls {enable | disable}

Parameters

Parameter	Description	Possible Values	Default Value
enable	Keyword indicating to enable SLS		
disable	Keyword indicating to disable SLS		

User Level

read-write

Context

general

Example

To enable SLS:

```
G450-001(super-sls)# set sls enable
Survivable Call Engine is enabled
```

Related Commands

clear survivable-config, show sls, sls

---

show sls

Use the **show sls** command to display SLS status (enabled or disabled).

Syntax

show sls

User Level

read-write

Context

general

Example

To display SLS status:

```
G450-001(super)# show sls
Survivable Call Engine is: enabled
```

Related Commands

clear survivable-config, set sls, sls

bri

Use the **bri** command within the sls context to enter a second-level subcontext for administering ISDN Basic Rate Interface (BRI) for SLS. After issuing this command, the prompt changes to `sls-bri <slot-address>`. Type **exit** to leave the bri context, and return to the sls context.

Syntax

bri *slot-address*

Parameters

Parameter	Description	Possible Values	Default Value
slot-address	The physical module address on the gateway	G450: Table 113	

Note:

The BRI slot address must agree with the slot assignment administration (see set slot-config on page 1028).

Table 113: G450 slot and board matrix for SLS

G450 Media Module	Description	Permitted slots	SLS configured?
MM720	Eight (8) BRI trunk ports	v1, v2, v3, v4, v5, v6, v7, v8	Yes
MM722	Two (8) BRI trunk ports	v1, v2, v3, v4, v5 v6, v7, v8	Yes

User Level

read-write

Context

sls

Example

To enter the second-level subcontext for administering ISDN BRI for slot address v401:

```
G450-001(super-sls)# bri v401
G450-001(sls-bri 401)#
```

Sub-commands

The following commands are available once you are inside the sls > bri context:

BRI sub-commands
set bearer-capability
set country-protocol
set directory-number-a
set directory-number-b
set endpoint-init
set interface
set interface-companding
set layer1-stable
set name
set side
set spid-a
set spid-b
set tei-assignment
show (bri)

Additional SLS commands

clear bri, set sls, show bri, show sls, sls

set bearer-capability

Use the **`set bearer-capability`** command to set the Information Transfer Rate field of the Bearer Capability IE in SLS.

Note:

This command is only valid for a DS1 or BRI circuit employed with ISDN.

Syntax

set bearer-cability *bearer*

Parameters

Parameter	Description	Possible Values	Default Value
bearer	The Information Transfer Rate field of the Bearer Capability IE. • **3khz** – 3.1kHz audio encoding • **speech** – Speech encoding	**3khz** **speech**	**speech**

User Level

read-write

Context

sls > ds1
sls > bri

Example

To set the Information Transfer Rate field to speech for DS1:

```
G450-001 (sls-ds1-<port address>)# set bearer-capability speech
```

To set the Information Transfer Rate field to speech for BRI:

```
G450-001 (sls-bri-<port address>)# set bearer-capability speech
```

Related DS1 commands

clear ds1, set bearer-capability, set channel-numbering, set connect, set country-protocol, set interface, set interface-companding, set long-timer, set name, set protocol-version, set side, set signaling-mode, set sls, show (ds1), show ds1, show sls, sls

set country-protocol

Use the **set country-protocol** command to specify the ISDN Layer-3 country protocol type in SLS.

Note:

This command is only valid for a BRI circuit or DS1 circuit employed with ISDN.

Syntax

set country-protocol *country-code*

Parameters

Parameter	Description	Possible Values	Default Value
country-code	The ISDN Layer-3 country protocol type: • **1** – United States (AT&T mode, also called 5ESS) • **2** – Australia (Australia National PRI) • **3** – Japan • **4** – Italy • **5** – Netherlands • **6** – Singapore • **7** – Mexico • **8** – Belgium • **9** – Saudi Arabia • **10** – United Kingdom (ETSI) • **11** – Spain • **12** – France (ETSI) • **13** – Germany (ETSI) • **14** – Czech Republic • **15** – Russia • **16** – Argentina • **17** – Greece • **18** – China • **19** – Hong Kong • **20** – Thailand • **21** – Macedonia • **22** – Poland • **23** – Brazil • **24** – Nordic countries • **25** – South Africa • **etsi** – ETSI (no use of RESTART message) • **qsig** – QSIG	**1** **2** **3** **4** **5** **6** **7** **8** **9** **10** **11** **12** **13** **14** **15** **16** **17** **18** **19** **20** **21** **22** **23** **24** **25** **etsi** **qsig**	**1**

User Level

read-write

Context

sls > ds1
sls > bri

Example

To specify the ISDN Layer-3 country protocol type as Australia:

```
G450-001 (sls-ds1-<port address>)# set country-protocol 2
```

Related DS1 commands

clear ds1, set bearer-capability, set bit-rate, set channel-numbering, set connect, set interface, set interface-companding, set long-timer, set name, set protocol-version, set side, set signaling-mode, set sls, show (ds1), show ds1, show sls, sls

Related BRI commands

bri, clear bri, set bearer-capability, set directory-number-a, set directory-number-b, set endpoint-init, set interface, set interface-companding, set layer1-stable, set name, set side, set spid-a, set spid-b, set sls, set tei-assignment, show bri, show (bri), show sls, sls

set directory-number-a

Use the **`set directory-number-a`** command to assign a directory number to the B1 channel of the BRI interface in SLS.

Important:
This number must be identical to the provisioned number that the network provider has assigned to this circuit.

Note:
This command is valid only for a BRI circuit employed with ISDN.

Syntax

`set directory-number-a` ***`number`***

Parameters

Parameter	Description	Possible Values	Default Value
`number`	String of 1-10 digits describing the directory number to the B1 channel of the BRI interface	**0-9**	

User Level

read-write

Context

sls > bri

Example

To assign directory number 3035381000 to the B1 channel of the BRI interface:

```
G450-001(sls-bri <port address>)# set directory-number-a 3035381000
```

Related Commands

bri, clear bri, set bearer-capability, set country-protocol, set directory-number-b, set endpoint-init, set interface, set interface-companding, set layer1-stable, set name, set side, set spid-a, set spid-b, set sls, set tei-assignment, show bri, show (bri), show sls, sls

set directory-number-b

Use the **set directory-number-b** command to assign a directory number to the B2 channel of the BRI interface in SLS.

Important:
This number must be identical to the provisioned number that the network provider has assigned to this circuit.

Note:
This command is valid only for a BRI circuit employed with ISDN.

Syntax

set directory-number-b *number*

Parameters

Parameter	Description	Possible Values	Default Value
number	String of 1-10 digits describing the directory number to the B2 channel of the BRI interface	**0-9**	

User Level

read-write

Context

sls > bri

Example

To assign directory number 3035381004 to the B2 channel of the BRI interface:

```
G450-001(sls-bri <port address>)# set directory-number-b 3035381004
```

Related Commands

bri, clear bri, set bearer-capability, set country-protocol, set directory-number-a, set endpoint-init, set interface, set interface-companding, set layer1-stable, set name, set side, set spid-a, set spid-b, set sls, set tei-assignment, show bri, show (bri), show sls, sls

set endpoint-init

Use the **set-endpoint-init** command to determine whether or not the far-end supports endpoint initialization in SLS.

Note:

This command is valid only for a BRI circuit employed with ISDN.

Syntax

set endpoint-init {yes | no}

Note:

The default for this command is **no**.

User Level

read-write

Context

sls > bri

Example

To determine that the far-end does not support endpoint initialization:

```
G450-001(sls-bri <port address>)# set endpoint-init no
```

Related Commands

bri, clear bri, set bearer-capability, set country-protocol, set directory-number-a, set directory-number-b, set interface, set interface-companding, set layer1-stable, set name, set side, set spid-a, set spid-b, set sls, set tei-assignment, show bri, show (bri), show sls, sls

set interface

Use the **set interface** command to specify the glare-handling convention for a DS1 or BRI link in SLS. This command also determines the polarity of the ISDN Layer 2 (LAPD) protocol operation.

Note:

For a DS1 circuit, this command specifies the glare-handling convention for the set connect command that has been administered as ***pbx*** at the far-end of the DS1 link.

Note:

This command is only valid for a DS1 or BRI circuit.

Syntax

set interface *glare-mode*

Parameters

Parameter	Description	Possible Values	Default Value
glare-mode	The glare-handling convention for a DS1 or BRI link. For non-QSIG calls: • **network** – If the gateway is connected to a host computer and encounters glare, it overrides the far-end • **user** – If the gateway is connected to a public network and encounters glare, it releases the circuit For QSIG calls: • **peerMaster** – SLS overrides the other end when glare occurs • **peerSlave** – SLS releases the circuit when glare occurs	**network** **user** **peerMaster** **peerSlave**	**user**

User Level

read-write

Context

sls > ds1
sls > bri

Example

To specify the glare-handling convention as network:

```
G450-001 (sls-ds1-<port address>)# set interface network
```

Related DS1 commands

clear ds1, set bearer-capability, set bit-rate, set channel-numbering, set connect, set country-protocol, set interface-companding, set long-timer, set name, set protocol-version, set side, set signaling-mode, set sls, show ds1, show sls, sls

Related BRI commands

bri, clear bri, set bearer-capability, set country-protocol, set directory-number-a, set directory-number-b, set endpoint-init, set interface-companding, set layer1-stable, set name, set side, set spid-a, set spid-b, set sls, set tei-assignment, show (ds1), show bri, show (bri), sls

set interface-companding

Use the **`set interface-companding`** command to set the interface to agree with the companding method used by the far-end of the DS1 circuit for SLS mode.

Syntax

`set interface-companding` ***`type`***

Parameters

Parameter	Description	Possible Values	Default Value
`type`	The type of interface to agree the companding method used by the far-end of the DS1 circuit. • **alaw** – A-law companding • **ulaw** – U-law companding	**alaw** **ulaw**	**ulaw**

User Level

read-write

Context

sls > ds1
sls > bri

Example

To set the interface to agree with A-law companding for DS1:

```
G450-001 (sls-ds1-<port address>)# set interface-companding alaw
```

to set the interface to agree with A-law companding for BRI:

```
G450-001 (sls-bri-<port address>)# set interface-companding alaw
```

Related DS1 commands

clear ds1, set bearer-capability, set bit-rate, set channel-numbering, set connect, set country-protocol, set interface, set long-timer, set name, set protocol-version, set side, set signaling-mode, set sls, show (ds1), show ds1, show sls, sls

Related BRI commands

bri, clear bri, set bearer-capability, set country-protocol, set directory-number-a, set directory-number-b, set endpoint-init, set interface, set layer1-stable, set name, set side, set spid-a, set spid-b, set sls, set tei-assignment, show bri, show (bri), show sls, sls

set layer1-stable

Use the **set layer1-stable** command to determine whether or not to keep the physical layer active (stable) between calls in SLS. Some European countries, France, for example, require that the physical layer is deactivated when there is no active call.

Note:

This command is valid only for a BRI circuit employed with ISDN.

Syntax

set layer1-stable {yes | no}

Parameters

Parameter	Description	Possible Values	Default Value
yes	Keyword specifying to keep the physical layer active between calls. This is the default.		
no	Keyword specifying not to keep the physical layer active between calls		

User Level

read-write

Context

sls > bri

Example

To not keep the physical layer active between calls:

```
G450-001(sls-bri <port address>)# set layer1-stable no
```

Related Commands

bri, clear bri, set bearer-capability, set country-protocol, set directory-number-a, set directory-number-b, set endpoint-init, set interface, set interface-companding, set name, set side, set spid-a, set spid-b, set sls, set tei-assignment, show bri, show (bri), show sls, sls

set name

Use the **set name** command to identify the username for a station, a trunk group, a DS1, or ISDN facility in SLS.

Syntax

set name *name*

Parameters

Parameter	Description	Possible Values	Default Value
name	The name as specified on the corresponding Communication Manager form (**add trunk-group *n***). This name is typically used to identify an individual, a service provider, or a site. If the file name includes spaces, use quotes. The length of the name is: • DS1 and BRI: 1 -15 characters • station and trunk-group: 1-27 characters		

User Level

read-write

Context

sls > station
sls > trunk-group
sls > ds1
sls > bri

Examples

To set the username Joe Smith for a given station:

```
G450-001 (sls-station-<extension>)# set name "Joe Smith"
```

Related Commands - Station commands

set cor, set expansion-module, set password, set port, set swhook-flash, set trunk-destination, set type (station), show (station), station

Related Commands - Trunk-group commands

add port, clear tac, clear trunk-group, remove port, set channel-preference, set codeset-display, set codeset-national, set dial, set digits, set digit-handling, set digit-treatment, set incoming-destination, set incoming-dialtone, set japan-disconnect, set numbering-format, set send-name, set send-number, set supervision, set tac, set trunk-hunt, show trunk-group, show (trunk-group), trunk-group

Related Commands - DS1 commands

clear ds1, set bearer-capability, set bit-rate, set channel-numbering, set connect, set country-protocol, set interface, set interface-companding, set long-timer, set protocol-version, set side, set signaling-mode, show (ds1), show ds1

Related Commands - BRI commands

bri, clear bri, set bearer-capability, set country-protocol, set directory-number-a, set directory-number-b, set endpoint-init, set interface, set interface-companding, set layer1-stable, set side, set spid-a, set spid-b, set tei-assignment, show bri, show (bri)

Related Commands - SLS commands

set sls, show sls, sls

---

set side

Use the **`set side`** command to specify the glare-handling conditions when the set interface command has been administered as ***`peerMaster`*** or ***`peerSlave`*** for the ISDN link in SLS.

Note:

This command is only valid for ISDN.

Syntax

set side *side*

Parameters

Parameter	Description	Possible Values	Default Value
side	Glare mode	**a** **b**	**a**

User Level

read-write

Context

sls > ds1
sls >bri

Examples

To set the glare-handling conditions to mode a in DS1:

```
G450-001 (sls-ds1-<port address>)# set side a
```

To set the glare-handling conditions to mode a in BRI:

```
G450-001 (sls-bri-<port address>)# set side a
```

Related DS1 commands

clear ds1, set bearer-capability, set bit-rate, set channel-numbering, set connect, set country-protocol, set interface, set interface-companding, set long-timer, set name, set protocol-version, set signaling-mode, set sls, show (ds1), show ds1, show sls, sls

Related BRI commands

bri, clear bri, set bearer-capability, set country-protocol, set directory-number-a, set directory-number-b, set endpoint-init, set interface, set interface-companding, set layer1-stable, set name, set spid-a, set spid-b, set sls, set tei-assignment, show (bri), show bri, show sls, sls

set spid-a

Use the **set spid-a** command to assign a Service Profile Identifier (SPID) to a North American BRI trunk in SLS. The trunk circuit cannot be placed in service unless the SPID initialization is successful.

Note:

On the Communication Manager's **bri-trunk-board** form, page 2, this string is constructed by using the **SPID** field entry (12 digits maximum) as the base, and appending the **Endpt ID** field entry (2 digits) to create a single string (14 digits maximum).

Note:

This command is valid only for a BRI circuit employed with ISDN.

Syntax

set spid-a *spid-number*

Parameters

Parameter	Description	Possible Values	Default Value
spid-number	String of 1-14 digits describing the SPID (Service Profile Identifier) to the circuit	**0-9**	

User Level

read-write

Context

sls > bri

Example

To assign SPID number 30353810041111 to the B1 channel of a North American BRI trunk:

```
G450-001(sls-bri <port address>)# set spid-a 30353810041111
```

Related Commands

bri, clear bri, set bearer-capability, set country-protocol, set directory-number-a, set directory-number-b, set endpoint-init, set interface, set interface-companding, set layer1-stable, set name, set side, set spid-b, set sls, set tei-assignment, show bri, show (bri), show sls, sls

set spid-b

Use the **set spid-b** command to assign a Service Profile Identifier (SPID) to a North American BRI trunk in SLS. The trunk circuit cannot be placed in service unless the SPID initialization is successful.

Note:

On the Communication Manager's **bri-trunk-board** form, page 2, this string is constructed by using the **SPID** field entry (12 digits maximum) as the base, and appending the **Endpt ID** field entry (2 digits) to create a single string (14 digits maximum).

Note:

This command is valid only for a BRI circuit employed with ISDN.

Syntax

set spid-b *spid-number*

Parameters

Parameter	Description	Possible Values	Default Value
spid-number	String of 1-14 digits describing the SPID (Service Profile Identifier) to the circuit	**0-9**	

User Level

read-write

Context

sls > bri

Example

To assign SPID number 30353810041111 to the B2 channel of a North American BRI trunk:

```
G450-001(sls-bri <port address>)# set spid-b 30353810041111
```

Related Commands

bri, clear bri, set bearer-capability, set country-protocol, set directory-number-a, set directory-number-b, set endpoint-init, set interface, set interface-companding, set layer1-stable, set name, set side, set spid-a, set sls, set tei-assignment, show bri, show (bri), show sls, sls

set tei-assignment

Use the **set tei-assignment** command to select the method by which the Layer 2 (LAPD) protocol obtains its Terminal Endpoint Identification (TEI) address in SLS.

Note:

This command is valid only for a BRI circuit employed with ISDN.

Syntax

set tei-assignment *tei*

Parameters

Parameter	Description	Possible Values	Default Value
tei	The method by which the Layer 2 (LAPD) protocol obtains its Terminal Endpoint Identification (TEI) address in SLS. • **auto** – TEI is assigned by the network provider • **zero** – TEI is fixed	**auto** **zero**	**auto**

User Level

read-write

Context

sls > bri

Example

To set the method by which the LAPD protocol obtains its TEI address as automatic:

```
G450-001(sls-bri <port address>)# set tei-assignment auto
```

Related Commands

bri, clear bri, set bearer-capability, set country-protocol, set directory-number-a, set directory-number-b, set endpoint-init, set interface, set interface-companding, set layer1-stable, set name, set side, set spid-a, set spid-b, set sls, show bri, show (bri), show sls, sls

show (bri)

Use the **show** command to list the administered BRI parameters for SLS for this BRI interface port.

Syntax

show

User Level

read-write

Context

sls > bri

Example

To list all of the subcontext parameters in the bri context:

```
G450-001(sls-bri 401)# show

      Name = 'Willow Steet 2'
BRI  Interface Sid  Country  Bearer   Compand TEI  Endpt-Init Layer1-Stable
---- --------- ---- -------- -------- ------- ---- ---------- -------------
v401      user    a country1   speech    ulaw auto     yes           yes

Dir-NumberA Dir-NumberB Spid-A         Spid-B
----------- ----------- -------------- --------------
 3035381002  3035381003 30353810021111 30353810031111
```

Output fields

Field	Description
BRI	The physical module address
Interface	The glare-handling convention if the equipment at the far-end of the link has been administered as **pbx**. Possible values: • **network** (Non-QSIG calls) • **user** (Non-QSIG calls) • **peerMaster** (QSIG calls) • **peerSlave** (QSIG calls)

1 of 2

Field	Description
Sid	The glare-handling condition if the equipment at the far-end of the link has been administered as **peerMaster** or **peerSlave**. Possible values: • **a** • **b**
Country	The ISDN Layer-3 country protocol type
Bearer	The Information Transfer Rate field of the Bearer Capability IE. Possible values: • **3khz** (3.1kHz audio encoding) • **speech** (speech encoding)
Compand	The far-end companding method. Possible values: • **alaw** (A-law companding) • **ulaw** (U-law companding)
TEI	The method by which the Layer 2 (LAPD) protocol obtains its Terminal Endpoint Identification (TEI) address. Possible values: • **auto** (TEI is assigned by the network provider) • **zero** (TEI is fixed)
Endpt-Init	Whether or not the far-end supports endpoint initialization
Layer1-Stable	Whether or not to keep the physical layer active (stable) between calls
Dir-NumberA	The directory number to the B1 channel of the BRI interface
Dir-NumberB	The directory number to the B2 channel of the BRI interface
Spid-A	The Service Profile Identifier (SPID) to a North American BRI trunk
Spid-B	The Service Profile Identifier (SPID) to a North American BRI trunk

2 of 2

Related Commands

bri, dial-pattern, ds1, incoming-routing, set sls, show sls, sig-group, station, sls, trunk-group

clear attendant

Use the **clear attendant** command to delete attendant provisioning in SLS.

Syntax

clear attendant

User Level

read-write

Context

sls

Example

To delete attendant provisioning:

```
G450-001(super-sls)# clear attendant
```

Related Commands

set attendant, show attendant, show sls, sls

clear bri

Use the **clear bri** command to delete the administration for a given BRI channel in SLS.

Syntax

clear bri *slot-address*

Parameters

Parameter	Description	Possible Values	Default Value
slot-address	The administered slot address		

User Level

read-write

Context

sls

Example

To delete the administration for BRI channel v401:

```
G450-001(super-sls)# clear bri v401
```

Related Commands

bri, set bearer-capability, set country-protocol, set directory-number-a, set directory-number-b, set endpoint-init, set interface, set interface-companding, set layer1-stable, set name, set side, set spid-a, set spid-b, set sls, set tei-assignment, show bri, show sls, sls

clear dial-pattern

Use the **clear dial-pattern** command to delete a single dialed string pattern entry in the SLS data set.

Syntax

clear dial-pattern *dialed-string*

Parameters

Parameter	Description	Possible Values	Default Value
dialed-string	Specifies the dialed string pattern	Any defined dial string pattern. Use show dial-pattern to display defined values.	

User Level

read-write

Context

sls

Example

To delete dialed string pattern entry 49139:

```
G450-001(super-sls)# clear dial-pattern 49139
Dial Pattern 49139 was removed.
```

Related Commands

dial-pattern, set delete-digits, set deny, set insert-digits (dial-pattern), set max-length, set min-length, set sls, set tgnum, set type (dial-pattern), show (dial-pattern), show sls, sls

clear ds1

Use the **clear ds1** command to delete the administration for a specific DS1 channel in SLS.

Syntax

clear ds1 ***slot-address***

Note:

See ds1 for valid slot address values.

User Level

read-write

Context

sls

Example

To delete the administration for DS1 channel v4:

```
G450-001(super-sls)# clear ds1 v4
```

Related Commands

set bearer-capability, set bit-rate, set channel-numbering, set connect, set country-protocol, set interface, set interface-companding, set long-timer, set name, set protocol-version, set side, set signaling-mode, set sls, show (ds1), show ds1, show sls, sls

clear extension

Use the **clear extension** command to delete a particular extension number in the SLS data set. The extension number that you want to clear must have been previously administered in the station subcontext.

Note:

It is preferable to use the clear station command, which is equivalent to the **clear extension** command.

Syntax

clear extension *extnum*

Parameters

Parameter	Description	Possible Values	Default Value
extnum	Specifies the extension number to delete	1-13 digit number	

User Level

read-write

Context

sls

Example

To delete extension number 1234:

```
G450-001(super-sls)# clear extension 1234
Extension 1234 was removed.
```

Related Commands

set cor, set expansion-module, set name, set password, set port, set sls, set swhook-flash, set trunk-destination, set type (station), show extension, show sls, station, sls

clear fac

Use the **clear fac** command to delete an administered Feature Access Code for SLS.

Syntax

clear fac *feature*

Parameters

Parameter	Description	Possible Values	Default Value
feature	The type of feature for which the FAC code applies	**ars1** **ars2** **hold** **contact-open** **contact-close** **contact-pulse**	

User Level

read-write

Context

sls

Example

To delete an administered Feature Access Code for feature contact-open:

```
G450-001(super-sls)# clear fac contact-open
Done!
```

Related Commands

set fac, set sls, show fac, show sls, sls

clear incoming-routing

Use the **clear incoming-routing** command to delete an entry for a particular incoming routed string that is associated with a given trunk group in SLS. This removes administration from the incoming-routing subcontext.

Syntax

clear incoming-routing ***tgnum mode*** **[***pattern length***]**

Parameters

Parameter	Description	Possible Values	Default Value
tgnum	ISDN (**t1isdn** or **e1isdn** or **bri**) trunk group number	**1-2000**	
mode	Protocol for receiving incoming digits: • **enbloc** – All digits in SETUP message • **overlap** – Not all digits available in the SETUP message; some digits delivered in subsequent INFO message	**enbloc overlap**	
pattern	Incoming alphanumeric string of 1-16 characters		
length	Numeric string of 0-21 digits	**0-9**	

User Level

read-write

Context

sls

Example

To delete an entry for incoming routed string enbloc protocol associated with trunk group 99:

```
G450-001(super-sls)# clear incoming-routing 99 enbloc
```

Related Commands

set sls, show incoming-routing, show sls, sls

clear sig-group

Use the **clear sig-group** command to delete the administration for a given ISDN signaling group in SLS.

Syntax

clear sig-group ***sgnum***

Parameters

Parameter	Description	Possible Values	Default Value
sgnum	Signaling group number	**1-650**	

User Level

read-write

Context

sls

Example

To delete the administration for ISDN signaling group 99:

```
G450-001(super-sls)# clear sig-group 99
```

Related Commands

add nfas-interface, remove nfas-interface, set associated-signaling, set primary-dchannel, set sls, set trunk-group-chan-select, show (sig-group), show sig-group, show sls, sig-group, sls

clear slot-config

Use the **clear slot-config** command to delete the slot configuration administration in the media gateway for SLS.

Syntax

clear slot-config ***slot-number***

Parameters

Parameter	Description	Possible Values	Default Value
slot-number	Identifies the slot number	The slot number must correspond to Table 115	

Note:

If either trunk or station ports have been previously administered for the media module in this slot, you must remove the port administration (remove port) first before removing the slot-configuration administration.

User Level

read-write

Context

sls

Example

To delete the slot configuration administration for slot v1 in the media gateway:

```
G450-001 (super-sls)# clear slot-config v1
```

Related Commands

set slot-config, set sls, show slot-config, show sls, sls

clear station

Use the **clear station** command to delete a particular extension number in the SLS data set. The extension number that you want to clear must have been previously administered in the station subcontext.

Syntax

clear station ***extension***

Parameters

Parameter	Description	Possible Values	Default Value
extension	1-13 digit number which specifies the extension number to delete	**0-9**	

User Level

read-write

Context

sls

Example

To delete station extension number 1234:

```
G450-001(super-sls)# clear station 1234
Station 1234 was removed.
```

Related Commands

set cor, set expansion-module, set name, set password, set port, set sls, set swhook-flash, set trunk-destination, set type (station), show station, show sls, station, sls

clear survivable-config

Use the **clear survivable-config** command to set the SLS parameters to their default values.

Syntax

clear survivable-config

User Level

read-write

Context

sls

Example

To set the SLS parameters to their default values:

```
G450-001(super-sls)# clear survivable-config
Survivable Configuration is cleared
```

Related Commands

set sls, show sls, sls

clear trunk-group

Use the **clear trunk-group** command to delete a trunk group entry from the SLS data set.

Note:

The trunk group must have already been administered with the trunk-group command before this command will work.

Syntax

clear trunk-group *tgnum*

Parameters

Parameter	Description	Possible Values	Default Value
tgnum	Specifies the trunk group to delete	**1-2000**	

User Level

read-write

Context

sls

Example

To delete trunk group entry 13:

```
G450-001(super-sls)# clear trunk-group 13
Trunk group 13 was removed.
```

Related Commands

add port, clear tac, remove port, set cbc, set cbc-parameter, set cbc-service-feature, set channel-preference, set codeset-display, set codeset-national, set dial, set digits, set digit-handling, set digit-treatment, set incoming-destination, set incoming-dialtone, set japan-disconnect, set name, set numbering-format, set send-name, set send-number, set supervision, set tac, set trunk-hunt, set sls, show (trunk-group), show sls, show trunk-group, sls, trunk-group

dial-pattern

Use the **dial-pattern** command within the sls context to enter a second-level subcontext for administering ARS dial patterns for SLS. After issuing this command, the prompt changes to `sls-dial-pattern <dialed-string>`. Type **exit** to leave the dial-pattern context, and return to the sls context.

Syntax

dial-pattern *dialed string*

Parameters

Parameter	Description	Possible Values	Default Value
dialed string	The dialed string. It can contain a maximum of 28 characters. You can configure a maximum of 30 patterns.	**0-9**, '*' and '**X**' or '**x**' as a pre-string or mid-string replacement. '**X**' or '**x**' cannot be used at the end of a dialed string.	

User Level

read-write

Context

sls

Example

To enter the subcontext for dial-pattern 91:

```
G450-001(super-sls)# dial-pattern 91
G450-001(sls-dial-pattern 91)#
```

Sub-commands

The following commands are available once you are inside the sls > dial-pattern context:

Dial-pattern sub-commands
set delete-digits
set deny
set insert-digits (dial-pattern)
set max-length
set min-length
set tgnum
set type (dial-pattern)
show (dial-pattern)

Additional SLS commands

clear dial-pattern, set sls, show dial-pattern, show sls, sls

set delete-digits

Use the **set delete-digits** command to specify the number of digits to be deleted from the beginning of the dialed string for an outbound call in SLS.

Syntax

set delete-digits ***del-number***

Parameters

Parameter	Description	Possible Values	Default Value
del-number	The number of digits to delete from the beginning of the dialed string	**0-28**	**0**

User Level

read-write

Context

sls > dial-pattern

Example

To specify that 1 digit be deleted from the beginning of the dialed string for an outbound call:

```
G450-001(sls-dial-pattern <dialed-string>)# set delete-digits 1
```

Related Commands

clear dial-pattern, dial-pattern, set deny, set insert-digits (dial-pattern), set max-length, set min-length, set sls, set tgnum, set type (dial-pattern), show (dial-pattern), show dial-pattern, show sls, sls

set deny

Use the **set deny** command to permit or deny access to an outbound trunk in SLS.

Syntax

set deny {yes | no}

Note:

The default value is **no** (access permitted).

User Level

read-write

Context

sls > dial-pattern

Example

To prevent a station from originating an outgoing analog loop-start trunk call:

```
G450-001(sls-dial-pattern <dialed-string>)# set deny yes
Done!
```

Related Commands

clear dial-pattern, dial-pattern, set delete-digits, set insert-digits (dial-pattern), set max-length, set min-length, set sls, set tgnum, set type (dial-pattern), show (dial-pattern), show dial-pattern, show sls, sls

set insert-digits (dial-pattern)

Use the **set insert-digits** command to specify the digits to be inserted at the beginning of the dialed string for an outbound call in SLS.

Syntax

set insert-digits ***digits***

Parameters

Parameter	Description	Possible Values	Default Value
digits	0-36 digits/special characters to insert at the beginning of the dialed string. **Note:** The special character '**,**' (comma) designates that a pause of "X" seconds is to be sent between the digits that are being transmitted out to the PSTN facility. The value of "X" has a default of 1.5 seconds in Avaya Communication Manager administration. This setting may be changed. You may not insert '**,**' as the first character in the dialed string. In addition, you can use '**,**' only on analog and non-ISDN digital trunks.	**" "** (no digits inserted) **0-9** plus '*****' , '#', and '**,**'	**" "**

User Level

read-write

Context

sls > dial-pattern

Examples

To insert the digits "9719" to the dialed string:

```
G450-001(super-sls-incoming-routing <tgnum>)# set insert-digits 9719
```

To remove the digit-treatment (removes data administered with set insert-digits (dial-pattern)):

```
G450-001(super-sls-incoming-routing <tgnum>)# set insert-digits ""
```

Related Commands

clear dial-pattern, dial-pattern, set delete-digits, set deny, set max-length, set min-length, set sls, set tgnum, set type (dial-pattern), show (dial-pattern), show dial-pattern, show sls, sls

set max-length

Use the **`set max-length`** command to establish the maximum length of the dialed string in SLS.

Syntax

set max-length ***length***

Parameters

Parameter	Description	Possible Values	Default Value
length	A numeric value equal to the maximum dialed-string value (see dial-pattern)	**1-28**	The number of digits set by the dial-pattern command.

User Level

read-write

Context

sls > dial-pattern

Example

To set the maximum length of the dialed string to 10:

```
G450-001(sls-dial-pattern <dialed-string>)# set max-length 10
```

Related Commands

clear dial-pattern, dial-pattern, set delete-digits, set deny, set insert-digits (dial-pattern), set min-length, set sls, set tgnum, set type (dial-pattern), show (dial-pattern), show dial-pattern, show sls, sls

set min-length

Use the **`set min-length`** command to establish the minimum length of the dialed string in SLS.

Note:

The maximum length must be set using set max-length prior to setting the minimum length if the minimum length is longer than the default value.

Syntax

set min-length ***length***

Parameters

Parameter	Description	Possible Values	Default Value
length	A numeric value equal to the minimum dialed-string value (see dial-pattern) and a maximum value equal to the number of dialed digits established by the set max-length command	**1-28**	The number of digits set by the dial-pattern command

User Level

read-write

Context

sls > dial-pattern

Example

To set the minimum length of the dialed string to 7:

```
G450-001(sls-dial-pattern <dialed-string>)# set min-length 7
```

Related Commands

clear dial-pattern, dial-pattern, set delete-digits, set deny, set insert-digits (dial-pattern), set max-length, set sls, set tgnum, set type (dial-pattern), show (dial-pattern), show dial-pattern, show sls, sls

set tgnum

Use the **set tgnum** command to designate the trunk-group number in SLS.

Syntax

set tgnum ***tgnum***

Parameters

Parameter	Description	Possible Values	Default Value
tgnum	The trunk group number	**1-2000**	

User Level

read-write

Context

sls > dial-pattern

Example

To designate the trunk-group number as 99:

```
G450-001(sls-dial-pattern <dialed-string>)# set tgnum 99
```

Related Commands

clear dial-pattern, dial-pattern, set delete-digits, set deny, set insert-digits (dial-pattern), set max-length, set min-length, set sls, set type (dial-pattern), show (dial-pattern), show dial-pattern, show sls, sls

set type (dial-pattern)

Use the **set type** command to administer the type of outbound call in SLS. The SLS call-engine uses the dial pattern as part of its ARS routing for outbound trunk calls.

Syntax

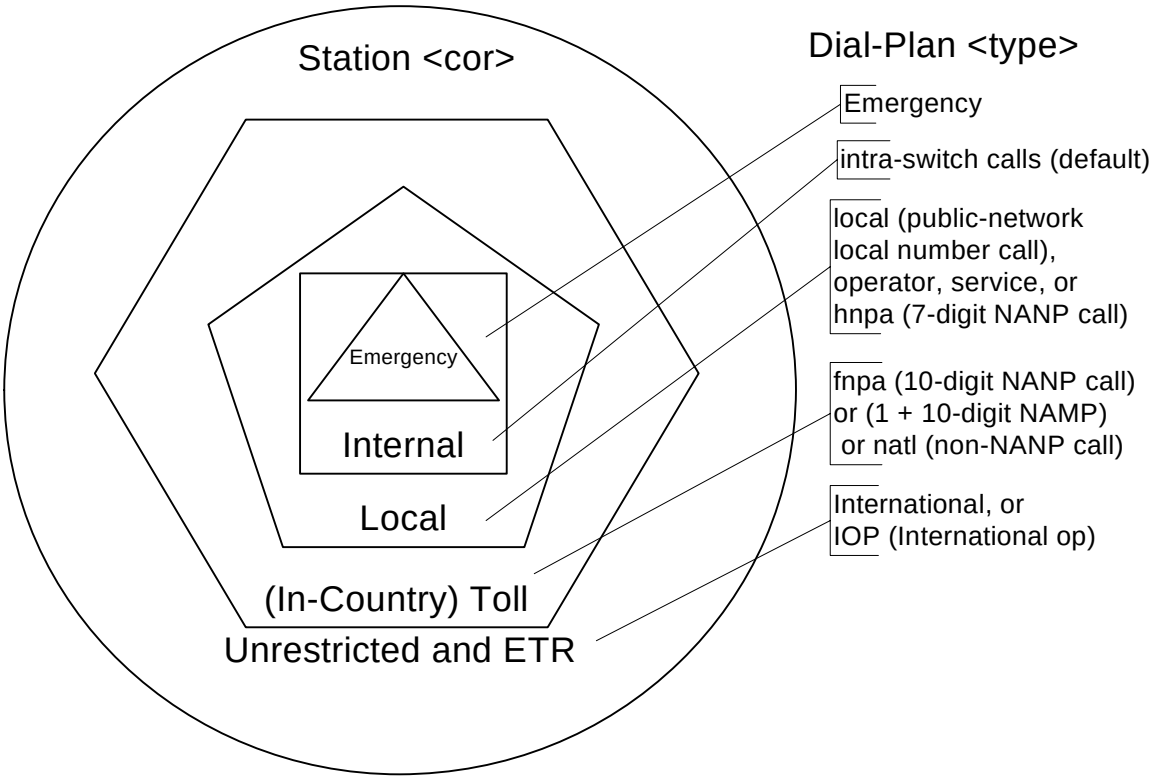
set type ***dial-type***

Parameters

Parameter	Description	Possible Values	Default Value
dial-type	The dial pattern as part of its ARS routing for outbound trunk calls. • **emer** – Emergency call • **fnpa** – 10-digit North American Numbering Plan (NANP) call • **hnpa** – 7-digit NANP call • **intl** – Public-network international number call • **iop** – International operator call • **locl** – Public-network local number call • **natl** – Non-NANP call • **op** – Operator assisted call • **svc** – Service call	**emer** **fnpa** **hnpa** **intl** **iop** **locl** **natl** **op** **svc**	

SLS uses the dial-pattern field as part of its ARS routing for station dialed calls that are to be directed to the other stations and to make outbound trunk calls. Make sure to synchronize your choice of station COR and dial-plan **dial-type**. The following figure illustrates the relationship between the **dial-type** value and the set cor value (configured in station context). Note the following:

- The outer boundary of a station's COR class inherit all the properties of the class symbols encompassed by this class. For example, the 'Local' COR class is also able to dial the 'Emergency' COR.
- COR set to 'Emergency' is the most restricted class. If a station's COR is set to this mode, the only calls that are allowed are those which have an "emergency" type identified in the ARS Analysis table.
- COR set to 'Internal' enables the station to place calls to other stations supported by this gateway. The station is also able to dial calls that match dial patterns with dial-type set to 'emergency'.
- COR set to 'Local' enables the station to place calls that match dial patterns with dial-types set to 'local', 'operator', 'service', or 'hnpa'. In addition, the station may place calls to the 'Emergency' and 'Internal' classes.
- COR set to 'Toll' enables the station to place calls that match dial patterns with dial-types set to 'fnpa' and 'natl'. In addition, the station may place calls to the 'Emergency', 'Internal', and 'Local' classes.
- COR set to 'Unrestricted' enables the station to place calls to any dial patterns that are not explicitly labeled as 'denied' class within the ARS Analysis table. This class of COR effectively inherits the call permission properties of all the other classes.
- The Emergency Transfer Relay (ETR) mode is basically equivalent to the 'Unrestricted' class. When power is lost and the gateway enters ETR mode, the station port is directly connected to the trunk port and receives central office dial tone directly. This ETR station port may dial any number that the central office dialing plan affords for this analog trunk.



User Level

read-write

Context

sls > dial-pattern

Example

To designate the type of outbound call as a public-network local number call:

```
G450-001(sls-dial-pattern <dialed-string>)# set type locl
```

Related Commands

clear dial-pattern, dial-pattern, set delete-digits, set deny, set insert-digits (dial-pattern), set max-length, set min-length, set sls, set tgnum, show dial-pattern, show sls, sls

show (dial-pattern)

Use the **show** command to list all dial-pattern strings in the SLS data set in tabular format.

Syntax

show

User Level

read-write

Context

sls > dial-pattern

Example

To list all dial-pattern strings in tabular format:

```
G450-001(sls-dial-pattern 91)# show

Dialed-String/Deny Min/Max Type Trunk Delete/Insert
                   Length       Group Digits
------------------ ------- ---- ----- ------------------------------------
95381000/n           9/9   locl     2 1/303
```

Output fields

Field	Description
Dialed-String/Deny	The administered ARS dial string and whether the call should be permitted (n) or denied (y)
Min/Max Length	The minimum and maximum number of digits in the dial string
Type	The type of dial string. Possible types include: • **emer** — emergency call • **fnpa** — 10-digit NANP call • **hnpa** — 7-digit NANP call • **intl** — public-network international number call • **iop** — international operator call • **locl** — public-network local number call • **natl** — non-NANP call • **op** — operator • **svc** — service

1 of 2

Field	Description
Trunk group	The trunk-group number
Delete/Insert Digits	The number of digits to add or remove from a dialed string
	2 of 2

Related Commands

bri, dial-pattern, ds1, incoming-routing, set sls, show sls, sig-group, station, sls, trunk-group

ds1

Use the **ds1** command within the sls context to enter a second-level subcontext for administering DS1 trunks for SLS. After issuing this command, the prompt changes to `sls-ds1-<port-address>`. Type **exit** to leave the DS1 context, and return to the `sls` context.

Syntax

ds1 ***slot-address***

Parameters

Parameter	Description	Possible Values	Default Value
slot-address	The physical module address on the gateway	G450: Table 114	

Note:

The DS1 port address must agree with the slot assignment administration (see set slot-config on page 1028).

Table 114: G450 slot and board matrix for SLS

G450 Media Module	Description	Permitted slots	SLS configured?
MM710	One T1/E1 trunk port	v1, v2, v3, v4, v5	Yes

User Level

read-write

Context

sls

Example

To enter the subcontext for administering DS1 trunks for SLS at the port address v4:

```
G450-001 (super-sls)# ds1 v4
G450-001 (sls-ds1-<v4>)#
```

Sub-commands

The following commands are available once you are inside the sls > ds1 context:

DS1 sub-commands
set bearer-capability
set bit-rate
set channel-numbering
set connect
set country-protocol
set interface
set interface-companding
set long-timer
set name
set protocol-version
set side
set signaling-mode
show (ds1)

Additional SLS commands

set sls, show ds1, show sls, sls

set bearer-capability

Use the **set bearer-capability** command to set the Information Transfer Rate field of the Bearer Capability IE in SLS.

Note:

This command is only valid for a DS1 or BRI circuit employed with ISDN.

Syntax

set bearer-cability *bearer*

Parameters

Parameter	Description	Possible Values	Default Value
bearer	The Information Transfer Rate field of the Bearer Capability IE: • **3khz** – 3.1kHz audio encoding • **speech** – Speech encoding	**3khz** **speech**	**speech**

User Level

read-write

Context

sls > ds1
sls > bri

Example

To set the Information Transfer Rate field to speech for DS1:

```
G450-001 (sls-ds1-<port address>)# set bearer-capability speech
```

To set the Information Transfer Rate field to speech for BRI:

```
G450-001 (sls-bri-<port address>)# set bearer-capability speech
```

Related Commands

clear ds1, set bit-rate, set channel-numbering, set connect, set country-protocol, set interface, set interface-companding, set long-timer, set name, set protocol-version, set side, set signaling-mode, set sls, show (ds1), show ds1, show sls, sls

set bit-rate

Use the **set bit-rate** command to set the maximum transmission rate for the DS1 facility in SLS.

Note:

This command is only valid for DS1.

If this command is invoked to change the transmission rate and the DS1 facility and associated signaling group have already been provisioned, the command is blocked and a warning message, "Administrative change is in violation with existing trunk member provisioning", is displayed.

Syntax

set bit-rate *rate*

Parameters

Parameter	Description	Possible Values	Default Value
rate	The maximum transmission rate for the DS1 facility: • **1544** – Sets the transmission rate at 1.544 Mbps (T1) • **2048** – Sets the transmission rate at 2.048 Mbps (E1)	**1544** **2048**	**1544**

User Level

read-write

Context

sls > ds1

Example

To set the maximum transmission rate to 2.048 Mbps:

```
G450-001 (sls-ds1-<port address>)# set bit-rate 2048
```

Related Commands

clear ds1, set bearer-capability, set bit-rate, set channel-numbering, set connect, set country-protocol, set interface, set interface-companding, set long-timer, set name, set protocol-version, set side, set signaling-mode, set sls, show (ds1), show ds1, show sls, sls

set channel-numbering

Use the **set channel-numbering** command to select the channel-numbering method for B-channels on an E1 interface in SLS.

Note:

This command is only valid for DS1.

Syntax

set channel-numbering *method*

Parameters

Parameter	Description	Possible Values	Default Value
method	The channel-numbering method for B-channels on an E1 interface: • **seq** – Sequential codes of B-channels 1-30 in the ISDN Channel Identification IE • **tslot** – Timeslot method	**seq** **tslot**	**tslot**

User Level

read-write

Context

sls > ds1

Example

To select the channel-numbering method for B-channels to seq:

```
G450-001 (sls-ds1-<port address>)# set channel-numbering seq
```

Related Commands

clear ds1, set bearer-capability, set bit-rate, set connect, set country-protocol, set interface, set interface-companding, set long-timer, set name, set protocol-version, set side, set signaling-mode, set sls, show (ds1), show ds1, show sls, sls

set connect

Use the **set connect** command to specify the equipment at the far-end of the DS1 link in SLS.

Note:

This command is only valid for DS1.

Syntax

set connect ***far-end***

Parameters

Parameter	Description	Possible Values	Default Value
far-end	The equipment at the far-end of the DS1 link: • **host** – Data application (computer or server) • **lineside** – Terminal equipment (video multiplexer) • **network** – Central office • **pbx** – Private communication system (another pbx)	**host** **lineside** **network** **pbx**	**network**

User Level

read-write

Context

sls > ds1

Example

To specify that the central office is at the far-end of the DS1 link:

```
G450-001 (sls-ds1-<port address>)# set connect network
```

Related Commands

clear ds1, set bearer-capability, set bit-rate, set channel-numbering, set country-protocol, set interface, set interface-companding, set long-timer, set name, set protocol-version, set side, set signaling-mode, set sls, show (ds1), show ds1, show sls, sls

set country-protocol

Use the **set country-protocol** command to specify the ISDN Layer-3 country protocol type in SLS.

Note:

This command is only valid for a BRI circuit or DS1 circuit employed with ISDN.

Syntax

set country-protocol *country-code*

Parameters

Parameter	Description	Possible Values	Default Value
country-code	The ISDN Layer-3 country protocol type: • **1** – United States (AT&T mode, also called 5ESS) • **2** – Australia (Australia National PRI) • **3** – Japan • **4** – Italy • **5**– Netherlands • **6** – Singapore • **7** – Mexico • **8** – Belgium • **9** – Saudi Arabia • **10** – United Kingdom (ETSI) • **11** – Spain • **12** – France (ETSI) • **13** – Germany (ETSI) • **14** – Czech Republic • **15** – Russia • **16** – Argentina • **17** – Greece • **18** – China • **19** – Hong Kong • **20** – Thailand • **21** – Macedonia • **22** – Poland • **23** – Brazil • **24** – Nordic countries • **25** – South Africa • **etsi** – ETSI (no use of RESTART message) • **qsig** – QSIG	**1** **2** **3** **4** **5** **6** **7** **8** **9** **10** **11** **12** **13** **14** **15** **16** **17** **18** **19** **20** **21** **22** **23** **24** **25** **etsi** **qsig**	**1**

User Level

read-write

Context

sls > ds1
sls > bri

Example

To specify the ISDN Layer-3 country protocol type as Australia:

```
G450-001 (sls-ds1-<port address>)# set country-protocol 2
```

Related DS1 commands

clear ds1, set bearer-capability, set bit-rate, set channel-numbering, set connect, set interface, set interface-companding, set long-timer, set name, set protocol-version, set side, set signaling-mode, set sls, show (ds1), show ds1, show sls, sls

Related BRI commands

bri, clear bri, set bearer-capability, set directory-number-a, set directory-number-b, set endpoint-init, set interface, set interface-companding, set layer1-stable, set name, set side, set spid-a, set spid-b, set sls, set tei-assignment, show bri, show (bri), show sls, sls

---

set interface

Use the **`set interface`** command to specify the glare-handling convention for a DS1 or BRI link in SLS. This command also determines the polarity of the ISDN Layer 2 (LAPD) protocol operation.

Note:

For a DS1 circuit, this command specifies the glare-handling convention for the set connect command that has been administered as ***`pbx`*** at the far-end of the DS1 link.

Note:

This command is only valid for a DS1 or BRI circuit.

Syntax

`set interface` ***`glare-mode`***

Parameters

Parameter	Description	Possible Values	Default Value
glare-mode	The glare-handling convention for a DS1 or BRI link. For non-QSIG calls: • **network** – If the gateway is connected to a host computer and encounters glare, it overrides the far-end • **user** – If the gateway is connected to a public network and encounters glare, it releases the circuit For QSIG calls: • **peerMaster** – SLS overrides the other end when glare occurs • **peerSlave** – SLS releases the circuit when glare occurs	**network** **user** **peerMaster** **peerSlave**	**user**

User Level

read-write

Context

sls > ds1
sls > bri

Example

To specify the glare-handling convention as network:

```
G450-001 (sls-ds1-<port address>)# set interface network
```

Related DS1 commands

clear ds1, set bearer-capability, set bit-rate, set channel-numbering, set connect, set country-protocol, set interface-companding, set long-timer, set name, set protocol-version, set side, set signaling-mode, set sls, show ds1, show sls, sls

Related BRI commands

bri, clear bri, set bearer-capability, set country-protocol, set directory-number-a, set directory-number-b, set endpoint-init, set interface-companding, set layer1-stable, set name, set side, set spid-a, set spid-b, set sls, set tei-assignment, show (ds1), show bri, show (bri), sls

set interface-companding

Use the **set interface-companding** command to set the interface to agree with the companding method used by the far-end of the DS1 circuit for SLS mode.

Syntax

set interface-companding ***type***

Parameters

Parameter	Description	Possible Values	Default Value
type	The interface to agree with the companding method used by the far-end of the DS1 circuit: • **alaw** – A-law companding • **ulaw** – U-law companding	**alaw** **ulaw**	**ulaw**

User Level

read-write

Context

sls > ds1
sls > bri

Example

To set the interface to agree with A-law companding for DS1:

```
G450-001 (sls-ds1-<port address>)# set interface-companding alaw
```

to set the interface to agree with A-law companding for BRI:

```
G450-001 (sls-bri-<port address>)# set interface-companding alaw
```

Related DS1 commands

clear ds1, set bearer-capability, set bit-rate, set channel-numbering, set connect, set country-protocol, set interface, set long-timer, set name, set protocol-version, set side, set signaling-mode, set sls, show (ds1), show ds1, show sls, sls

Related BRI commands

bri, clear bri, set bearer-capability, set country-protocol, set directory-number-a, set directory-number-b, set endpoint-init, set interface, set layer1-stable, set name, set side, set spid-a, set spid-b, set sls, set tei-assignment, show bri, show (bri), show sls, sls

set long-timer

Use the **set long-timer** command to increase the duration of the T303 (call establishment) timer in SLS.

Syntax

```
set long-timer {yes | no}
```

Parameters

Parameter	Description	Possible values	Default value
yes	Keyword specifying to extend the T303 timer from 4 seconds to 13 seconds		
no	Keyword specifying that the T303 timer remain at 4 seconds. This is the default.		

User Level

read-write

Context

sls > ds1

Example

To extend the T303 timer to 13 seconds:

```
G450-001 (sls-ds1-<port address>)# set long-timer yes
```

Related Commands

clear ds1, set bearer-capability, set bit-rate, set channel-numbering, set connect, set country-protocol, set interface, set interface-companding, set name, set protocol-version, set side, set signaling-mode, set sls, show (ds1), show ds1, show sls, sls

set name

Use the **set name** command to identify the username for a station, a trunk group, a DS1, or ISDN facility in SLS.

Syntax

set name *name*

Parameters

Parameter	Description	Possible Values	Default Value
name	The name as specified on the corresponding Communication Manager form (**add trunk-group *n***). This name is typically used to identify an individual, a service provider, or a site. If the file name includes spaces, use quotes. The length of the name is: • DS1 and BRI: 1 -15 characters • station and trunk-group: 1-27 characters		

User Level

read-write

Context

sls > station
sls > trunk-group
sls > ds1
sls > bri

Examples

To set the username Joe Smith for a given station:

```
G450-001 (sls-station-<extension>)# set name "Joe Smith"
```

Related Commands - Station commands

set cor, set expansion-module, set password, set port, set swhook-flash, set trunk-destination, set type (station), show (station), station

Related Commands - Trunk-group commands

add port, clear tac, clear trunk-group, remove port, set channel-preference, set codeset-display, set codeset-national, set dial, set digits, set digit-handling, set digit-treatment, set incoming-destination, set incoming-dialtone, set japan-disconnect, set numbering-format, set send-name, set send-number, set supervision, set tac, set trunk-hunt, show trunk-group, show (trunk-group), trunk-group

Related Commands - DS1 commands

clear ds1, set bearer-capability, set bit-rate, set channel-numbering, set connect, set country-protocol, set interface, set interface-companding, set long-timer, set protocol-version, set side, set signaling-mode, show (ds1), show ds1

Related Commands - BRI commands

bri, clear bri, set bearer-capability, set country-protocol, set directory-number-a, set directory-number-b, set endpoint-init, set interface, set interface-companding, set layer1-stable, set side, set spid-a, set spid-b, set tei-assignment, show bri, show (bri)

Related Commands - SLS commands

set sls, show sls, sls

---

set protocol-version

Use the **`set protocol-version`** command for countries whose public networks allow for multiple ISDN Layer-3 country protocols for ISDN Primary Rate service in SLS.

Note:

This command is only valid for a DS1 circuit employed with ISDN.

Syntax

`set protocol-version` ***`option`***

Parameters

Parameter	Description	Possible Values	Default Value
option	The ISDN Layer-3 country protocols for ISDN Primary Rate service. **Note:** The combination of the country and the protocol versions must match (see set country-protocol). • For Country 1 (United States): - **a** – AT&T mode (also known as 5ESS) - **b** – National ISDN-1 - **c** – Nortel mode (also known as DMS) - **d** – Telecordia (NI-2) • For Country 2 (Australia): - **a** – Australia National PRI - **b** – ETSI - **c** – invalid - **d** – invalid • For Country 10 (United Kingdom): - **a** – DASS - **b** – ETSI - **c** – invalid - **d** – invalid • For Country 12 (France) - **a** – French National PRI - **b** – ETSI - **c** – invalid - **d** – invalid • For Country 13 (Germany): - **a** – German National PRI - **b** – ETSI - **c** – invalid - **d** – invalid • For ETSI: - **a** – Full message set, including RESTART - **b** – No RESTART message - **c** – invalid - **d** – invalid	**a** **b** **c** **d**	**a**

User Level

read-write

Context

sls > ds1

Example

To set the ISDN Layer-3 protocols relative to the country specified by **set country-protocol** to option a:

```
G450-001 (sls-ds1-<port address>)# set protocol-version a
```

Related Commands

clear ds1, set bearer-capability, set bit-rate, set channel-numbering, set connect, set country-protocol, set interface, set interface-companding, set long-timer, set name, set side, set signaling-mode, set sls, show (ds1), show ds1, show sls, sls

set side

Use the **set side** command to specify the glare-handling conditions when the set interface command has been administered as ***peerMaster*** or ***peerSlave*** for the ISDN link in SLS.

Note:

This command is only valid for ISDN.

Syntax

set side *side*

Parameters

Parameter	Description	Possible Values	Default Value
side	Glare mode	**a** **b**	**a**

User Level

read-write

Context

sls > ds1
sls > bri

Examples

To set the glare-handling conditions to mode a in DS1:

```
G450-001 (sls-ds1-<port address>)# set side a
```

To set the glare-handling conditions to mode a in BRI:

```
G450-001 (sls-bri-<port address>)# set side a
```

Related DS1 commands

clear ds1, set bearer-capability, set bit-rate, set channel-numbering, set connect, set country-protocol, set interface, set interface-companding, set long-timer, set name, set protocol-version, set signaling-mode, set sls, show (ds1), show ds1, show sls, sls

Related BRI commands

bri, clear bri, set bearer-capability, set country-protocol, set directory-number-a, set directory-number-b, set endpoint-init, set interface, set interface-companding, set layer1-stable, set name, set spid-a, set spid-b, set sls, set tei-assignment, show (bri), show bri, show sls, sls

---

set signaling-mode

Use the **`set signaling-mode`** command to set the signaling mode for the DS1 facility in SLS.

Note:

This command is only valid for DS1.

If this command is invoked to change the transmission rate and the DS1 facility and associated signaling group have already been provisioned, the command is blocked and a warning message, "Administrative change is in violation with existing trunk member provisioning", is displayed.

Syntax

`set signaling-mode` ***`mode-type`***

Parameters

Parameter	Description	Possible Values	Default Value
mode-type	The signaling mode for the DS1 facility. • **cas** – Out-of-band signaling for E1 service, yielding thirty 64kbps B-channels for voice transmission • **robbedbit** – In-band signaling for T1 service, yielding twenty-four 56kbps B-channels for voice transmission • **idsnpri** – Use this setting for either T1 or E1 ISDN Primary Rate service (supports both FAS and NFAS) • **isdnext** – NFAS T1 or E1 ISDN service for: - T1 facility in which all 24 channels are for bearer transport - E1 facility in which all 31 channels are for bearer transport	**cas** **robbedbit** **idsnpri** **isdnext**	**idsnpri**

User Level

read-write

Context

sls > ds1

Example

To set the signaling mode for the DS1 facility to PRI:

```
G450-001 (sls-ds1-<port address>)# set signaling-mode isdnpri
```

Related Commands

clear ds1, set bearer-capability, set bit-rate, set channel-numbering, set connect, set country-protocol, set interface, set interface-companding, set long-timer, set name, set protocol-version, set side, set sls, show (ds1), show ds1, show sls, sls

show (ds1)

Use the **show** command to list the administered DS1 parameters for SLS for this trunk interface.

Syntax

show

User Level

read-write

Context

sls > ds1

Example

To list the administered DS1 parameters for this trunk interface:

```
G450-001(sls-ds1-<port address>)# show

      Name = 'Willow Steet 2'
DS1  Rate Signaling Channel Connect Interface Side Protocol Ver Bearer Cmpd Ltm
---- ---- --------- ------- ------- --------- ---- -------- --- ------ ---- ---
  v4 1544   isdnpri     seq network      user    a country1   a speech ulaw  no
```

Output fields

Field	Description
DS1	The physical module address on the gateway
Rate	The maximum transmission rate for the DS1 facility. Possible values: • **1.544** Mbps (T1) • **2.048** Mbps (E1)
Signaling	The signaling mode for the DS1 facility. Possible values: • **cas** • **robbedbit** • **idsnpri** • **isdnextshowmgc**
Channel	The channel-numbering method for B-channels on an E1 interface. Possible values: • **seq** (sequential codes of B-channels 1-30 in the ISDN Channel Identification IE) • **tslot** (timeslot method)
Connect	The equipment at the far-end of the DS1 link. Possible values: • **host** (data application – computer or server) • **lineside** (terminal equipment – video multiplexer) • **network** (central office) • **pbx** (private communication system – another pbx)

1 of 2

Field	Description
Interface	The glare-handling convention if the equipment at the far-end of the link has been administered as **pbx**. Possible values: • **network** (Non-QSIG calls) • **user** (Non-QSIG calls) • **peerMaster** (QSIG calls) • **peerSlave** (QSIG calls)
Side	The glare-handling condition if the equipment at the far-end of the link has been administered as **peerMaster** or **peerSlave**. Possible values: • **a** • **b**
Protocol	The ISDN Layer-3 country protocol type
Ver	The protocol version, for countries whose public networks allow for multiple ISDN Layer-3 country protocols for ISDN Primary Rate service
Bearer	The Information Transfer Rate field of the Bearer Capability IE. Possible values: • **3khz** (3.1kHz audio encoding) • **speech** (speech encoding)
Cmpd	The far-end companding method. Possible values: • **alaw** (A-law companding) • **ulaw** (U-law companding)
Ltm	Whether to increase the duration of the T303 (call establishment) timer. Possible values: • **yes** (the T303 timer is extended from 4 seconds to 13 seconds) • **no** (the T303 timer remains at 4 seconds)
	2 of 2

Related Commands

bri, dial-pattern, ds1, incoming-routing, set sls, show sls, sig-group, station, sls, trunk-group

incoming-routing

Use the **incoming-routing** command within the sls context to enter a second-level subcontext for administering digit-treatment for incoming routed calls in SLS. After issuing this command, the prompt changes to sls-incoming-routing <tgnum>. Type **exit** to leave the incoming-routing context, and return to the sls context.

This command applies only to ISDN trunk groups**Syntax**

incoming-routing *tgnum mode* [*pattern length*]

Parameters

Parameter	Description	Possible Values	Default Value
tgnum	ISDN (**t1isdn** or **e1isdn**) trunk group number	**1-2000**	
mode	Protocol for receiving incoming digits: • **enbloc** – All digits in SETUP message • **overlap** – Not all digits available in the SETUP message; some digits delivered in subsequent INFO message	**enbloc*** **overlap**†	
pattern‡	Incoming alphanumeric string of 0-16 characters. If you do not enter a pattern, this is interpreted as a wild card entry.		
length	The length of the received dialed string, expressed as a numeric string of 0-21 digits	**0-9**	

* Each entry must be an enbloc match-pattern entry. If you administer the ***mode*** as **enbloc**, you may use the set insert-digits (dial-pattern) command to administer the inserted dial string, and the set delete-digits command to administer the number of digits to be deleted from the received digit string. There is a maximum of 50 entries for **enbloc** receiving mode.

† Either the **set delete-digits** or the **set insert-digits** subcommand is available for **overlap**, however both of these commands cannot be optioned for the same trunk group. That is, you can either delete or insert digits, not both. There is a maximum of one entry for **overlap** receiving mode.

‡ This field applies only if the ***mode*** is set to **enbloc**.

User Level

read-write

Context

sls

Example

To enter the subcontext for administering digit-treatment for incoming routed calls in SLS for ISDN trunk group 99 with enbloc protocol:

```
G450-001(super-sls)# incoming-routing 99 enbloc
G450-001(super-sls-incoming-routing 99)#
```

Sub-commands

The following commands are available once you are inside the sls >incoming-routing context:

Incoming-routing sub-commands
set delete-digits
set insert-digits (dial-pattern)
set length
set match-pattern
show (incoming-routing)

Additional SLS commands

clear incoming-routing, set sls, show incoming-routing, show sls, sls

---

set delete-digits

Use the **`set delete-digits`** command to specify number of digits to be deleted from the beginning of the dialed string for an inbound trunk call in SLS.

Important:
This command is *required* to complete the incoming-routing administration in which the ***`mode`*** is set to **enbloc**. The command is *optional* when the ***`mode`*** is set to **overlap**.

Syntax

`set delete-digits` ***`count`***

Parameters

Parameter	Description	Possible Values	Default Value
count	The number of digits to be deleted from the beginning of the dialed string. This number ranges from 0 to the maximum length of the received dialed string.	**0-21**	**0**

User Level

read-write

Context

sls > incoming-routing

Example

To specify that 1 digit be deleted from the beginning of the dialed string for an inbound trunk call:

```
G450-001(super-sls-incoming-routing <tgnum>)# set delete-digits 1
```

Related Commands

clear incoming-routing, incoming-routing, set insert-digits (dial-pattern), set length, set match-pattern, set sls, show (incoming-routing), show incoming-routing, show sls, sls

set insert-digits (incoming-routing)

Use the **`set insert-digits`** command to specify number of digits to be inserted at the beginning of the dialed string for an inbound trunk call in SLS.

Important:
This command is *required* to complete the incoming-routing administration in which the ***`mode`*** is set to **enbloc**. The command is *optional* when the ***`mode`*** is set to **overlap**.

Syntax

`set insert-digits` ***`digits`***

Parameters

Parameter	Description	Possible Values	Default Value
digits	0-16 digits/special characters to insert at the beginning of the dialed string	**" "** (no digits inserted) **0-9** plus '*****' and '#'	**" "**

User Level

read-write

Context

sls > incoming-routing

Examples

To insert the digits "9719" to the dialed string:

```
G450-001(sls-dial-pattern <dialed-string>)# set insert-digits 9719
```

To remove the digit-treatment (removes data administered with set insert-digits (incoming-routing)):

```
G450-001(sls-dial-pattern <dialed-string>)# set insert-digits ""
```

Related Commands

clear incoming-routing, incoming-routing, set delete-digits, set length, set match-pattern, set sls, show (incoming-routing), show incoming-routing, show sls, sls

set length

Use the **set length** command to specify the length of the dialed string in SLS.

Note:

There is an actual service offered in some public networks, such as in Japan, where the ISDN Called Party Number IE's 'Number Digits' table entry in octet 4 has no information. In order to program the Incoming Routing Table to handle this case, the ***pattern*** field in **set match-pattern** should be set to "", and the ***length*** field in **set length** should be set to "0". This indicates that there has been a successful match, and that the ***digits*** field in **set insert-digits** will be used to provide the destination number so that the SLS dial plan may route this incoming call.

Syntax

set length ***length***

Parameters

Parameter	Description	Possible Values	Default Value
length	The length of the dialed string, expressed as a numeric string of 0-21 digits. If the ***pattern*** field in set match-pattern is set to the empty string (wild card), then this ***length*** field may be set to **0** to designate a wild card. A wild card designation means that a received digit string of any length (0 to 21 digits) may constitute a length field match.	**0-9**	**0**

User Level

read-write

Context

sls > incoming-routing

Example

To set the dialed string length to 7 digits:

```
G450-001(super-sls-incoming-routing <tgnum>)# set length 7
```

Related Commands

clear incoming-routing, incoming-routing, set delete-digits, set insert-digits (incoming-routing), set match-pattern, set sls, show (incoming-routing), show incoming-routing, show sls, sls

set match-pattern

Use the **set match-pattern** command to specify the beginning digit pattern of the incoming alphanumeric dial string to be matched against in SLS.

Syntax

set match-pattern ***pattern***

Parameters

Parameter	Description	Possible Values	Default Value
pattern	Incoming alphanumeric string of 0-16 characters. The empty string ("") means that any incoming dial pattern may be used to satisfy a correct pattern match for this row entry.	**""** (empty string) Alphanumeric characters	

User Level

read-write

Context

sls > incoming-routing

Example

To specify that alphanumeric dial string 234 be matched against:

```
G450-001(super-sls-incoming-routing <tgnum>)# set match-pattern 234
```

Related Commands

clear incoming-routing, incoming-routing, set delete-digits, set insert-digits (incoming-routing), set length, set sls, show (incoming-routing), show incoming-routing, show sls, sls

show (incoming-routing)

Use the **show** command to display all of the administered dial patterns in SLS.

Syntax

show

User Level

read-write

Context

sls > incoming-routing

Example

To display all the administered dial patterns in SLS:

```
G450-001(super-sls-incoming-routing 99)# show

Match-pattern      Length Del Insert-Digits      Mode    tgnum
------------------ ------ --- ------------------ ------- -----
               234      7   3             5381000  enbloc    99
```

Output fields

Field	Description
Match-pattern	The beginning digit pattern of the incoming alphanumeric dial string to be matched
Length	The length of the dialed string
Del	The number of digits to be deleted from the beginning of the dialed string for an inbound trunk call
Insert-Digits	The number of digits to be inserted from the beginning of the dialed string for an inbound trunk call
Mode	The protocol for receiving incoming digits. Possible values: • **enbloc** (all digits in SETUP message) • **overlap** (not all digits available in the SETUP message; some digits delivered in subsequent INFO message)
tgnum	The ISDN (**t1isdn** or **e1isdn**) trunk group number

Related Commands

bri, dial-pattern, ds1, incoming-routing, set sls, show sls, sig-group, station, sls, trunk-group

set attendant

Use the **set attendant** command to set an attendant access code for the purpose of call routing in SLS. Incoming trunk calls that have dialed strings that can not be completely routed, are routed by SLS to this attendant position. In addition, stations in the branch office may directly dial this attendant using the access-code.

Syntax

set attendant ***access-code extension***

Parameters

Parameter	Description	Possible Values	Default Value
access-code	The dial access code which is recognized as the attendant feature	1-3 digit string	
extension	The station serving as the branch office attendant position. You must enter an extension that was previously administered using the station command.	1-13 digit string	

User Level

read-write

Context

sls

Example

To set the station with extension number 23456 as the attendant station, with access-code 00:

```
G450-001(super-sls)# set attendant 00 23456
```

Related Commands

clear attendant, clear survivable-config, show attendant, show sls, sls

set date-format

Use the **set date-format** command to set a date format for the SLS data set. The default date format is mm/dd/yy.

Syntax

set date format {mm/dd/yy | dd/mm/yy | yy/mm/dd}

User Level

read-write

Context

sls

Example

To set the date format to dd/mm/yy:

```
G450-001(super-sls)# set date-format dd/mm/yy
Date Format is dd/mm/yy
```

Related Commands

set sls, show date-format, show sls, sls

---

set fac

Use the **set fac** command to administer the Feature Access Code for SLS.

Note:

If you are on an active call and issue this command, you will enter the “hard” hold state. If you issue the command again, you will return to the active call.

Syntax

set fac *feature fac*

Parameters

Parameter	Description	Possible Values	Default Value
feature	The type of feature for which the FAC code applies	**ars1** **ars2** **hold** **contact-open** **contact-close** **contact-pulse**	
fac	The unique, 1 to 4 digit dial-string identifier that specifies the feature. **Note:** Rotary-dial, analog phones do not support “*” and “#.”	**0-9** plus “*****” and “**#**” as leading characters only	

User Level

read-write

Context

sls

Example

To administer an ars1 FAC specified by dial-string *88:

```
G450-001(super-sls)# set fac ars1 *88
Done!
```

Related Commands

clear fac, set sls, show fac, show sls, sls

---

set ip-codec-set

Use the **set ip-codec-set** command to configure an IP codec set within the SLS data set.

Note:

When you use this command, silence is set to ***no***, and the frame size is set to ***20 mSec***.

Syntax

set ip-codec-set ***codec***

Parameters

Parameter	Description	Possible Values	Default Value
codec	Codec type	**g.711mu** **g.711a**	

User Level

read-write

Context

sls

Example

To configure IP codec set g.711mu within the SLS data set:

```
G450-001(super-sls)# set ip-codec-set g.711mu
IP codec g.711mu is set
```

Related Commands

set sls, show ip-codec-set, show sls, sls

set max-ip-registrations

Use the **set max-ip-registrations** command to configure the maximum number of IP registrations allowed in the SLS data set.

Syntax

set max-ip-registrations *number*

Parameters

Parameter	Description	Possible Values	Default Value
number	Maximum number of IP registrations	**1-240**	**150**

User Level

read-write

Context

sls

Example

To set the maximum number of IP registrations to 10:

```
G450-001(super-sls)# set max-ip-registrations 10
Maximum IP Registrations is set to 10
```

Related Commands

set sls, show max-ip-registrations, show sls, sls

set pim-lockout

Use the **set pim-lockout** command to prevent or enable Provisioning and Installation Manager (PIM) updates while you are working on SLS administration or the gateway.

Syntax

set pim-lockout {yes | no}

Parameters

Parameter	Description	Possible Values	Default Value
yes	Keyword specifying to prevent PIM updates		
no	Keyword specifying to enable PIM updates. This is the default.		

User Level

read-write

Context

sls

Example

To prevent PIM updates:

```
G450-001(super-sls)# set pim-lockout yes
```

Related Commands

set sls, show pim-lockout, show sls, sls

---

set slot-config

Use the **set slot-config** command to define the slot and the board type in the media gateway for SLS.

Syntax

set slot-config *slot-number board-type*

Parameters

Parameter	Description	Possible Values	Default Value
slot-number	Identifies the slot number	See Table 115	
board-type	Defines the allowable board type		

Table 115: G450 slot and board matrix for SLS

G450 Media Module	Description	Permitted slots	SLS configured?
MM710	One T1/E1 trunk port	v1, v2, v3, v4, v5	Yes
MM711	Eight universal analog ports	v1, v2, v3, v4, v5	Yes
MM712	Eight DCP telephone ports	v1, v2, v3, v4, v5	Yes
MM714	Four analog trunk ports and four analog station ports	v1, v2, v3, v4, v5	Yes
MM716	Twenty-four analog telephone ports. May alternatively be used as DID trunk ports.	v1, v2, v3, v4, v5	Yes
MM717	Twenty-four high density DCP telephone ports	v1, v2, v3, v4, v5	Yes
MM720	Eight BRI trunk ports	v1, v2, v3, v4, v5	Yes
MM722	Two BRI trunk ports	v1, v2, v3, v4, v5	Yes
S8300B	Processor/LSP (display only)	v1	No
S8300C	Processor/LSP (display only)	v1	No
MM340	One T1/E1 WAN routing port (display only)	v3, v4, v5, v8	No
MM342	One Universal Serial WAN routing port (display only)	v3, v4, v5, v8	No

User Level

read-write

Context

sls

Example

To define the slot type as v1 and the board type as MM720 in the media gateway:

```
G450-001 (super-sls)# set slot-config v1 MM720
```

Related Commands

clear slot-config, set sls, show slot-config, show sls, sls

show attendant

Use the **show attendant** command to display attendant provisioning in SLS.

Syntax

show attendant

User Level

read-write

Context

sls

Example

To display attendant provisioning:

```
G450-001(super-sls)# show attendant

Attendant Access-Code Station-extension
--------------------- -----------------
                   00             23456
```

Related Commands

clear attendant, clear survivable-config, set attendant, show sls, sls

show bri

Use the **show bri** command to list the administered BRI parameters for SLS. If no channel parameters are specified, information about all BRI channels is displayed.

Syntax

show bri ***list***

Parameters

Parameter	Description	Possible Values	Default Value
list	The administered BRI parameters to list: • **all** – Lists all administered BRI channels • **port-address** – Lists only the parameters for a single BRI circuit	**all** **port-address**	**all**

User Level

read-write

Context

sls

Example

To list all administered BRI parameters:

```
G450-001(super-sls)# show bri all

      Name = 'Willow Steet 2'
BRI  Interface Side Country  Bearer   Compand TEI  Endpt-Init Layer1-Stable
---- --------- ---- -------- -------- ------- ---- ---------- -------------
v401      user    a country1   speech    ulaw auto        yes           yes

Dir-NumberA Dir-NumberB Spid-A         Spid-B
----------- ----------- -------------- --------------
 3035381002  3035381003 30353810021111 30353810031111


      Name = 'Willow Steet 3'
BRI  Interface Side Country  Bearer   Compand TEI  Endpt-Init Layer1-Stable
---- --------- ---- -------- -------- ------- ---- ---------- -------------
v402      user    a country1   speech    ulaw auto        yes           yes

Dir-NumberA Dir-NumberB Spid-A         Spid-B
----------- ----------- -------------- --------------
 3035381004  3035381005 30353810041111 30353810051111
```

Related Commands

bri, clear bri, set bearer-capability, set country-protocol, set directory-number-a, set directory-number-b, set endpoint-init, set interface, set interface-companding, set layer1-stable, set name, set side, set spid-a, set spid-b, set sls, set tei-assignment, show sls, sls

show date-format

Use the **show date-format** command to display the current date format in effect for the SLS data set.

Syntax

show date-format

User Level

read-write

Context

sls

Example

To display the current date format:

```
G450-001(super-sls)# show date-format
Date Format is mm/dd/yy
```

Related Commands

set date-format, set sls, show sls, sls

show dial-pattern

Use the **show dial-pattern** command to list all dial-pattern strings in the SLS data set in tabular format.

Syntax

show dial-pattern *list*

Parameters

Parameter	Description	Possible Values	Default Value
list	Dial-pattern strings in the SLS data set in tabular format: • **all** – Lists all administered dial patterns • **dialed-string** – Lists only the parameters for a specific dialed string • **dialed-string + *n*** – List starts with the specific dialed string + “n” entries	**all** **dialed-string** **dialed-string + *n***	**all**

User Level

read-write

Context

sls

Example

To list all dial-pattern strings in tabular format:

```
G450-001(super-sls)# show dial-pattern all

Dialed-String/Deny Min/Max Type Trunk Delete/Insert
                   Length       Group Digits
------------------ ------- ---- ----- ------------------------------------
95381000/n           9/9   locl     2 1/303
95350000/n           9/9   locl     3 1/720
```

Output fields

Field	Description
Dialed-String/Deny	The administered ARS dial string and whether the call should be permitted (no) or denied (yes)
Min/Max Length	The minimum and maximum number of digits in the dial string.

1 of 2

Field	Description
Type	The type of dial string. Possible types include: • **emer** — emergency call • **fnpa** — 10-digit NANP call • **hnpa** — 7-digit NANP call • **intl** — public-network international number call • **iop** — international operator call • **locl** — public-network local number call • **natl** — non-NANP call • **op** — operator • **svc** — service
Delete/Insert Digits	The number of digits to add or remove from a dialed string
	2 of 2

Related Commands

clear dial-pattern, dial-pattern, set delete-digits, set deny, set insert-digits (dial-pattern), set max-length, set min-length, set sls, set tgnum, set type (dial-pattern), show sls, sls

show ds1

Use the **`show ds1`** command to list the administered DS1 parameters for SLS.

Syntax

show ds1 ***`list`***

Parameters

Parameter	Description	Possible Values	Default Value
`list`	The DS1 channels to list: • **all** – Lists all administered DS1 channels • **port-address** – Lists only the parameters for a single DS1 channel	**all** **port-address**	**all**

User Level

read-write

Context

sls

Example

To list the administered DS1 parameters:

```
G450-001(super-sls)# show ds1 all

      Name = 'Willow Steet 2'
DS1  Rate Signaling Channel Connect Interface Side Protocol Ver Bearer Cmpd Ltm
---- ---- --------- ------- ------- --------- ---- -------- --- ------ ---- ---
  v4 1544   isdnpri     seq network      user    a country1   a speech ulaw  no


      Name = 'Willow Steet 3'
DS1  Rate Signaling Channel Connect Interface Side Protocol Ver Bearer Cmpd Ltm
---- ---- --------- ------- ------- --------- ---- -------- --- ------ ---- ---
  v5 1544   isdnpri     seq network      user    a country1   a speech ulaw  no
```

Related Commands

clear ds1, set bearer-capability, set bit-rate, set channel-numbering, set connect, set country-protocol, set interface, set interface-companding, set long-timer, set name, set protocol-version, set side, set signaling-mode, set sls, show sls, sls

show extension

Use the **show extension** command to display extension-specific SLS data parameters. If no extension parameters are specified, information for all extensions is displayed.

Note:

It is preferable to use the show station command.

Syntax

show extension *list*

Parameters

Parameter	Description	Possible Values	Default Value
list	The extension-specific SLS data parameters to list: • **all** – Lists all administered extensions • **extension** – Lists only the numbered extension • **extension + *n*** – Lists the numbered extension + “n” entries	**all** **extension** **extension + *n***	

User Level

read-write

Context

sls

Example

To display SLS data parameters for all extensions:

```
G450-001(super-sls)# show extension

Extension Type       Port            Cor        Trk-Des Exp-Mod Flash Passwd
--------- ----       ----            ---        ------- ------- ----- ------
49138     ip4620     xxx.xxx.xxx.xxx unrestr    yes     no        -   ******
49139     ip4610sw   xxx.xxx.xxx.xxx unrestr    yes     yes       -   ******
49140     analog2500 v305            internal   yes      -      yes   ******
Name = Joe Smith
```

Note:

If an IP station or Softphone is currently registered when the command is run, the Port column shows the IP address of the IP station or Softphone.

Output fields

Field	Description
Extension	The extension number of the phone (1-13 digits)
Type	The station type
Port	The module/port location
Cor	The Class of Restriction. Possible classes include: • emergency • internal • local • toll • unrestricted
Trk-Des	Indicates whether to permit (`yes`) or deny (`no`) the call
Exp-Mod	`Yes` means that an expansion module is administered for this station; `no` means that there is no expansion module associated with this station

1 of 2

Field	Description
Flash	`Yes` means that SLS will recognize the switchhook flash on this station; `no` means that flashing the switchhook has no effect
Passwd	Asterisks (*) indicate an administered password. See set password for password requirements on IP endpoints. If the field is blank, no password is administered for this extension.
	2 of 2

Related Commands

clear extension, set cor, set expansion-module, set name, set password, set port, set sls, set swhook-flash, set trunk-destination, set type (station), show sls, station, sls

show fac

Use the **`show fac`** command to list the administered Feature Access Codes for SLS.

Syntax

`show fac`

User Level

read-write

Context

sls

Example

To list the administered Feature Access Codes:

```
G450-001(super-sls)# show fac

Feature        Access Code
-------------  -----------
contact-pulse         *84
contact-close         *85
contact-open          *86
         hold         *87
         ars1         *88
         ars2         *89
Done!
```

Related Commands

clear fac, set fac, set sls, show sls, sls

show incoming-routing

Use the **show incoming-routing** command to show all of the administered dial patterns in SLS for one, several, or all trunk groups.

Syntax

show incoming-routing [***list***]

Parameters

Parameter	Description	Possible Values	Default Value
list	The administered dial patterns to list: • **all** – Lists all administered dial patterns • **tgnum** – Lists the dial pattern parameters for a single trunk group • **tgnum + *n*** – Lists the dial pattern parameters starting with a specific trunk group for a total of "n" entries	**all** **tgnum** **tgnum + *n***	

User Level

read-write

Context

sls

Example

To show all of the administered dial patterns:

```
G450-001(super-sls)# show incoming-routing

Match-pattern      Length Del Insert-Digits      Mode    tgnum
------------------ ------ --- ------------------ ------- -----
               234      7   3            5381000  enbloc    99
               235      7   3            5381001  enbloc    98
```

Related Commands

clear incoming-routing, set sls, show sls, sls

show ip-codec-set

Use the **show ip-codec-set** command to list the codec set entries for SLS.

Syntax

show ip-codec-set

User Level

read-only

Context

sls

Example

To list codec set entries:

```
G450-001(super-sls)# show ip-codec-set
Ip codec g.711 mu, priority 1, frames 2
```

Output fields

Field	Description
IP codec	The administered codec type (g.711 mu or g.711 a)
Priority	The numeric priority of the codec. SLS supports a single priority level (designated as priority 1).
Frames	The frame size. The frames supported are 20 milliseconds in size. Since the incremental building size is in terms of 10 milliseconds, the display reports 2 times the 10 milliseconds.

Related Commands

set ip-codec-set, set sls, show sls, sls

show last-pim-update

Use the **show last-pim-update** command to display when the last Provisioning and Update Manager (PIM) update of the SLS data occurred. The time value is given for the time zone in which the PIM server is located.

Syntax

show last-pim-update

User Level

read-write

Context

sls

Example

To display when the last update occurred:

```
G450-001(super-sls)# show last-pim-update
Last PIM update occured at 15:47:0 on 2/28/2005
```

Related Commands

set sls, show sls, sls

show max-ip-registrations

Use the **show max-ip-registrations** command to display the maximum IP registration administration in the SLS data on the G450.

Syntax

show max-ip-registrations

User Level

read-write

Context

sls

Example

To display the maximum IP registration administration:

```
G450-001(super-sls)# show max-ip-registrations
Maximum IP Registrations is 12
```

Related Commands

set max-ip-registrations, set sls, show sls, sls

show pim-lockout

Use the **show pim-lockout** command to display the current status of the setting for the Provisioning and Installation Manager (PIM) lockout feature.

Syntax

show pim-lockout

User Level

read-only

Context

sls

Example

To display the current status of the PIM lockout feature:

```
G450-001(super-sls)# show pim-lockout
PIM lockout = yes
```

Related Commands

set pim-lockout, set sls, show sls, sls

show sig-group

Use the **show sig-group** command to list all administered signaling groups in SLS.

Syntax

show sig-group *list*

Parameters

Parameter	Description	Possible Values	Default Value
list	The administered signaling groups to list: • **all** – Lists all administered signaling groups • **sgnum** – Lists only the specified signaling group	**all** **sgnum**	**all**

User Level

read-write

Context

sls

Example

To list all administered signaling groups:

(In this example, trunk group 98 is administered on a DS1 module, managed by signaling group 10, in slot v4. Two additional DS1 facilities located in slot v5 and slot v6 share an NFAS managed group, managed by signaling group 12. The NFAS group D-channel is in the slot v5 DS1 module. All trunk members are contained in trunk group 100.)

```
G450-001(super-sls)# show sig-group all

Sig-group Tg-Select Assoc-Sig Prime-Dchan Nfas-Modules/Nfas-Id
--------- --------- --------- ----------- --------------------------------
       10        98       yes     005v424 -
       12       100        no     005v524 005v5:0,005v6:1
```

Related Commands

add nfas-interface, clear sig-group, remove nfas-interface, set associated-signaling, set primary-dchannel, set sls, set trunk-group-chan-select, show sls, sig-group, sls

show slot-config

Use the **show slot-config** command to list the slot and board administration in the media gateway for SLS.

Syntax

show slot-config

User Level

read-write

Context

sls

Examples

To list the slot and board administration in the G450 gateway:

```
G450-001 (super-sls)# show slot-config
Slot  SLS-Configured  Inserted
      Board-type      Board-type
----  --------------  -----------
v1:             -             -
v2:             -         mm340
v3:         mm711         mm711
v4:         mm711         mm711
v5:         mm717         mm717
v6:         mm717         mm717
v7:         mm710         mm710
v8:         mm710         mm710
```

Note:

If there is no module administered for a slot, the display shows "-", and if an unknown media module is inserted, the display shows "unknown".

Related Commands

clear slot-config, set slot-config, set sls, show sls, sls

show station

Use the **show station** command to display extension-specific SLS data parameters. If no extension parameters are specified, information about all extensions is displayed.

Syntax

show station ***list***

Parameters

Parameter	Description	Possible Values	Default Value
list	The extension-specific SLS data parameters to list: • **all** – Lists all administered extensions • **extension** – Lists only the numbered extension • **extension + *n*** – Lists the numbered extension + “n” entries	**all,** **extension** **extension + *n***	**all**

User Level

read-write

Context

sls

Example

To display extension-specific SLS data parameters:

```
G450-001(super-sls)# show station

Extension Type       Port            Cor       Trk-Des Exp-Mod Flash Passwd
--------- ----       ----            ---       ------- ------- ----- ------
49138     ip4620     xxx.xxx.xxx.xxx unrestr    yes     no      - ******
49139     ip4610sw   xxx.xxx.xxx.xxx unrestr    yes     yes     - ******
49140     analog2500 v305            internal   yes     -       yes   ******
Name = Joe Smith
```

Note:

If an IP station or Softphone is currently registered when the command is run, the Port column shows the IP address of the IP station or Softphone.

Output fields

Field	Description
Extension	The extension number of the phone (1-13 digits)
Type	The station type
Port	The module/port location

1 of 2

Field	Description
Cor	The Class of Restriction. Possible classes include: • emergency • internal • local • toll • unrestricted
Trk-Des	Indicates whether to permit (`yes`) or deny (`no`) the call
Exp-Mod	`Yes` means that an expansion module is administered for this station; `no` means that there is no expansion module associated with this station
Flash	`Yes` means that SLS will recognize the switchhook flash on this station; `no` means that flashing the switchhook has no effect
Passwd	Asterisks (*) indicate an administered password. See set password for password requirements on IP endpoints. If the field is blank, no password is administered for this extension.
	2 of 2

Related Commands

clear station, set cor, set expansion-module, set name, set password, set port, set sls, set swhook-flash, set trunk-destination, set type (station), show sls, station, sls

show trunk-group

Use the **`show trunk-group`** command to display trunk group administration in SLS.

Syntax

`show trunk-group` ***`list`***

Parameters

Parameter	Description	Possible Values	Default Value
`list`	The administered trunk groups to list: • **all** – Lists all administered trunk groups • **trunk-group** – Lists only the numbered trunk group • **extension + *n*** – Lists the numbered trunk group + “n” entries	**all** **trunk-group** **extension + *n***	**all**

User Level

read-only

Context

sls

Example

To display trunk group administration for all administered trunk groups:

```
G450-001(super-sls)# show trunk-group all

     Group  Type       Dial  Tac  Ports  Supervision  Treat    Insert
     -----  ----       ----  ---  -----  -----------  -----    ------
     1      loop-start dtmf  99   v301   -            -        -
     2      did        dtmf  88   v305   wink         insert3 538
```

Output fields

Field	Description
Group	The trunk group number (`1-2000`)
Type	The trunk group type (`loop-start`, `did`)
Dial	The dial type (`rotary` or `dtmf`)
Tac	The Trunk Access Code (1 to 4 digits). "#" and "*" are valid entries and are only allowed as the first character of the TAC.
Port	The virtual integrated port assignment
Supervision	Incoming signaling supervision mode (`immediate`, `wink`)
Treat	The digit treatment (`blank`, `absorb 1-5`, `insert 1-4`)
Insert	The digits to insert in the dial string
Codeset Display	The Q.931 codeset that sends display information to the user phone (`codeset0`, `codeset6`, `codeset7`)
Codeset National	The Q.931 codeset that sends National IE display information to the user phone (`codeset6`, `codeset7`)
Channel Preference	Defines how the Channel Identification IE field is encoded (`exclusive`, `preferred`)

1 of 2

Field	Description
Digit Handling	Defines how the inbound/outbound calls handle the transmission/reception of the dialed pattern (`enbloc-enbloc`, `enbloc-overlap`, `overlap-enbloc`, `overlap-overlap`)
Japan Discon	Whether to perform a disconnect sequence (CONNECT message followed by a DISCONNECT message)
Send Name	Whether the calling, connected, called, or busy party's administered name is sent to the network on outgoing or incoming calls (`yes`, `no`, `restricted`)
Send Number	Whether the calling, connected, called, or busy party's administered number is sent to the network on outgoing or incoming calls (`yes`, `no`, `restricted`)
Format Number	The numbering plan for this trunk. The numbering plan encodes the **Numbering Plan Indicator** and **Type of Number** fields in the Calling/Connected Party Number IE in the ISDN protocol (`unknown`, `public`, `private`, `unknownprivate`).
Trunk Hunt	The trunk-hunting search within a facility in an ISDN trunk group or through a non-ISDN digital trunk group (`ascend`, `cyclical`, `descend`)

2 of 2

Related Commands

add port, clear tac, clear trunk-group, remove port, set cbc, set cbc-parameter, set cbc-service-feature, set channel-preference, set codeset-display, set codeset-national, set dial, set digits, set digit-handling, set digit-treatment, set incoming-destination, set incoming-dialtone, set japan-disconnect, set name, set numbering-format, set send-name, set send-number, set supervision, set tac, set trunk-hunt, set sls, show sls, sls, trunk-group

sig-group

Use the **`sig-group`** command within the sls context to enter a second-level subcontext for administering signaling groups for SLS. After issuing this command, the prompt changes to `sls-sig-group <sgnum>`. Type **`exit`** to leave the sig-group context, and return to the sls context.

Syntax

`sig-group` ***`sgnum`***

Parameters

Parameter	Description	Possible Values	Default Value
sgnum	Signaling group number*	**1-650**	

* If you have created more than one trunk group within a single DS1 circuit, it is possible that one signaling group can support multiple trunk groups.

User Level

read-write

Context

sls

Example

To enter the second-level subcontext of `sls-sig-group 100`:

```
G450-001(super-sls)# sig-group 100
G450-001(sls-sig-group 100)#
```

Sub-commands

The following commands are available once you are inside the sig-group context:

Signaling groups sub-commands
add nfas-interface
remove nfas-interface
set associated-signaling
set primary-dchannel
set trunk-group-chan-select
show (sig-group)

Related SLS commands

clear sig-group, set sls, show sig-group, show sls, sls

add nfas-interface

Use the **add nfas-interface** command to identify a list of DS1 modules that are controlled by the primary D-channel in SLS.

Note:

This command applies only to ISDN-PRI trunks in a NFAS-managed group.

Note:

This command is not valid unless the slot configuration has already been administered (see set slot-config) and the set associated-signaling command is set to **no** (NFAS).

Note:

The North American Public Network Service Providers do not allow any part of a T1 to be shared outside of this NFAS-trunk group. In other words, they do not allow one of the T1 interfaces (of this NFAS group) to be fractionalized into 2 or more uses. It must be dedicated to this given customer. Therefore the following usage rules apply:

- All members of an NFAS DS1 (that are administered) must belong to the same trunk-group.
- All members of this trunk-group must belong to a single signaling group.

Syntax

add nfas-interface {*gateway module [interface-id]*}

Parameters

Parameter	Description	Possible Values	Default Value
gateway	3-digit gateway number (for example, 005)		
module	2-character slot number (for example, v4). This number identifies a port on an already-provisioned DS1 board module (see add port).		
interface-id	The DS1 circuit number that is associated with the NFAS group. This number must be coordinated with the public network service provider so that the signaling protocol operates correctly.	**0-31**	

User Level

read-write

Context

sls > sig-group

Example

To identify a list of DS1 modules that are controlled by the primary D-channel for gateway 005, module v5, and DS1 circuit number 0:

```
G450-001(sls-sig-group 100)# add nfas-interface 005v5 0
```

Related Commands

clear sig-group, remove nfas-interface, set associated-signaling, set primary-dchannel, set sls, set trunk-group-chan-select, show (sig-group), show sig-group, show sls, sig-group, sls

remove nfas-interface

Use the **remove nfas-interface** command to remove a member from a NFAS-managed DS1 group in SLS. This command removes the add nfas-interface gateway and module administration.

Note:

This command applies only to ISDN-PRI trunks in a NFAS-managed group.

Note:

This command is not valid unless the slot configuration has already been administered (see set slot-config) and the set associated-signaling command is set to **no** (NFAS).

Syntax

remove nfas-interface *gateway module*

Parameters

Parameter	Description	Possible Values	Default Value
gateway	3-digit gateway number (for example, 005)		
module	2-character slot number (for example, v4). This number identifies a port on an already-provisioned DS1 board module (see add port).		

User Level

read-write

Context

sls > sig-group

Example

To remove gateway 3 with module v5 from the NFAS-managed DS1 group:

```
G450-001(sls-sig-group 100)# remove nfas-interface 005v5
```

Related Commands

add nfas-interface, clear sig-group, set associated-signaling, set primary-dchannel, set sls, set trunk-group-chan-select, show (sig-group), show sig-group, show sls, sig-group, sls

set associated-signaling

Use the **set associated-signaling** command to specify whether the D-channel is physically present in the DS1 interface in SLS.

Note:

If this command is invoked to change the transmission rate and the DS1 facility and associated signaling group have already been provisioned, the command is blocked and a warning message, "Administrative change is in violation with existing trunk member provisioning", is displayed.

Syntax

set associated-signaling {yes | no}

Parameters

Parameter	Description	Default Value
yes	Keyword specifying the D-channel is present in the same DS1 interface. This is the default.	
no	Keyword specifying to use Non-Facility Associated Signaling (NFAS)	

User Level

read-write

Context

sls > sig-group

Example

To specify that the D-channel is present:

```
G450-001(sls-sig-group 100)# set associated-signaling yes
```

Related Commands

add nfas-interface, clear sig-group, remove nfas-interface, set primary-dchannel, set sls, set trunk-group-chan-select, show (sig-group), show sig-group, show sls, sig-group, sls

set primary-dchannel

Use the **set primary-dchannel** command to identify the D-channel number in SLS.

Syntax

set primary-dchannel *circuit-number*

Parameters

Parameter	Description	Possible Values	Default Value
circuit-number	3-digit gateway number (for example, 005) 2-character slot number (for example, v4) 2-digit circuit number: • T1-ISDN: 24 • E1-ISDN: 16		**24**

User Level

read-write

Context

sls > sig-group

Example

To identify the D-channel number for gateway 005, slot v4 in a T1-ISDN line:

```
G450-001(sls-sig-group 100)# set primary-dchannel 005v424
```

Related Commands

add nfas-interface, clear sig-group, remove nfas-interface, set associated-signaling, set sls, set trunk-group-chan-select, show (sig-group), show sig-group, show sls, sig-group, sls

set trunk-group-chan-select

Use the **set trunk-group-chan-select** command to specify the trunk-group number that can accept incoming calls in cases where the Information Channel Selection field does not specify a preferred channel for bearer transport in SLS.

Syntax

set trunk-group-chan-select *tgnum*

Parameters

Parameter	Description	Possible Values	Default Value
tgnum	Trunk group number. **Note:** Use the **0** value to clear any previously set ***tgnum*** value.	**0** **1-2000**	

User Level

read-write

Context

sls > sig-group

Example

- To specify that trunk-group 99 can accept incoming calls:

```
G450-001(sls-sig-group 100)# set trunk-group-chan-select 99
```

- To clear any previously set value for trunk-group selection:

```
G450-001(sls-sig-group 100)# set trunk-group-chan-select 0
```

Related Commands

add nfas-interface, clear sig-group, remove nfas-interface, set associated-signaling, set primary-dchannel, set sls, show (sig-group), show sig-group, show sls, sig-group, sls

show (sig-group)

Use the **show** command to list the parameters of this signaling group.

Syntax

show

User Level

read-write

Context

sls > sig-group

Example

To list all of the subcontext parameters in the sig-group context:

```
G450-001(sls-sig-group 100)# show

Sig-group Tg-Select Assoc-Sig Prime-Dchan Nfas-Modules/Nfas-Id
--------- --------- --------- ----------- --------------------
       10        98       yes     005v424                                -
```

Output fields

Field	Description
Sig-group	Signaling group number
Tg-Select	The trunk-group number that can accept incoming calls in cases where the Information Channel Selection field does not specify a preferred channel for bearer transport
Assoc-Sig	Whether the D-channel is physically present in the DS1 interface
Prime-Dchan	The D-channel number
Nfas-Modules	The DS1 modules that are controlled by the primary D-channel.
Nfas-Id	The DS1 circuit number that is associated with the NFAS group.

Related Commands

bri, dial-pattern, ds1, incoming-routing, set sls, show sls, sig-group, station, sls, trunk-group

station

Use the **station** command within the sls context to enter a second-level subcontext for administering stations for SLS. After issuing this command, the prompt changes to sls-station <extension>. Type **exit** to leave the station context, and return to the sls context.

Syntax

station *extension* [*class*]

Parameters

Parameter	Description	Possible Values	Default Value
extension	A 1-13 digit unique numeric string	"**0**" through "**9**"; an extension can begin with the digit "**0**"	
class	The station class. **Note:** This parameter is only mandatory for the creation of a station administrative instance. Subsequent command accesses to modify/show do not require this parameter to be entered.	**analog** **dcp** **ip**	

User Level

read-write

Context

sls

Example

To enter the second-level context of sls-station for analog station extension 23456:

```
G450-001(super-sls)# station 23456 analog
G450-001(super-sls-station <extension>)#
```

Sub-commands

Depending on the class of station, the following sub-commands are available:

Command	Analog	DCP	IP
set cor	X	X	X
set expansion-module		X	X
set name	X	X	X
set password		X	X
set port	X	X	
set swhook-flash	X		
set trunk-destination	X	X	X
set type (station)	X	X	X
show (station)	X	X	X

Additional SLS commands

set sls, show (station), show sls, sls

---

set cor

Use the **set cor** command to administer the class-of-restriction values for each station that uses SLS.

Syntax

set cor ***cor***

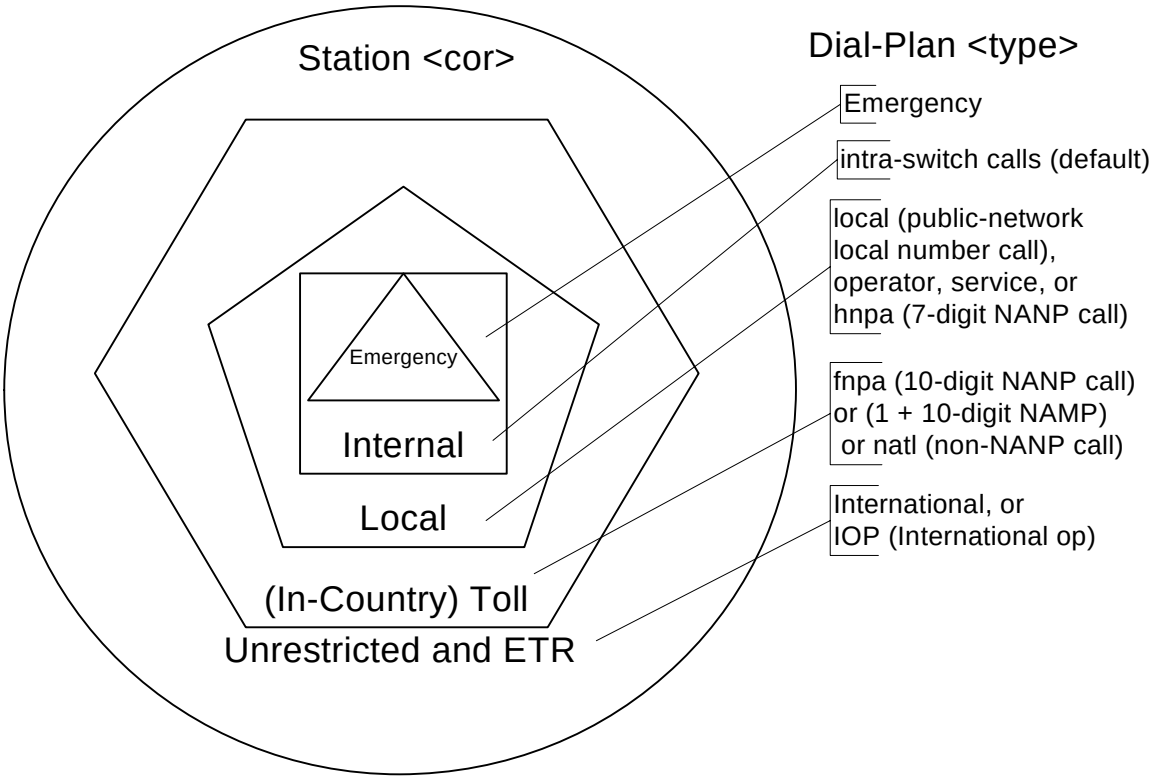
Parameters

Parameter	Description	Possible Values*	Default Value
cor	The class of restriction for a station user's dialing	**emergency** **internal** **local** **toll** **unrestricted**	**internal**

* As the class of restriction moves from "emergency" to "unrestricted," each level increases the range of dialing abilities for this station. For example, "toll" level includes "local," "internal," and "emergency."

SLS uses the dial-pattern field as part of its ARS routing for station dialed calls that are to be directed to the other stations and to make outbound trunk calls. Make sure to synchronize your choice of station COR and dial-plan **dial-type**. The following figure illustrates the relationship between the **set cor** value and the set type (dial-pattern) value (configured in dial-pattern context). Note the following:

- The outer boundary of a station's COR class inherit all the properties of the class symbols encompassed by this class. For example, the 'Local' COR class is also able to dial the 'Emergency' COR.
- COR set to 'Emergency' is the most restricted class. If a station's COR is set to this mode, the only calls that are allowed are those which have an "emergency" type identified in the ARS Analysis table.
- COR set to 'Internal' enables the station to place calls to other stations supported by this gateway. The station is also able to dial calls that match dial patterns with dial-type set to 'emergency'.
- COR set to 'Local' enables the station to place calls that match dial patterns with dial-types set to 'local', 'operator', 'service', or 'hnpa'. In addition, the station may place calls to the 'Emergency' and 'Internal' classes.
- COR set to 'Toll' enables the station to place calls that match dial patterns with dial-types set to 'fnpa' and 'natl'. In addition, the station may place calls to the 'Emergency', 'Internal', and 'Local' classes.
- COR set to 'Unrestricted' enables the station to place calls to any dial patterns that are not explicitly labeled as 'denied' class within the ARS Analysis table. This class of COR effectively inherits the call permission properties of all the other classes.
- The Emergency Transfer Relay (ETR) mode is basically equivalent to the 'Unrestricted' class. When power is lost and the gateway enters ETR mode, the station port is directly connected to the trunk port and receives central office dial tone directly. This ETR station port may dial any number that the central office dialing plan affords for this analog trunk.



User Level

read-write

Context

sls > station

Example

To set the restriction for a station user's dialing to unrestricted:

```
G450-001 (sls-station <extension>)# set cor unrestricted
```

Related Commands

set expansion-module, set name, set password, set port, set sls, set swhook-flash, set trunk-destination, set type (station), show (station), show sls, station, sls

set expansion-module

Use the **set expansion-module** command to administer a DCP or IP station for an expansion module in SLS.

Syntax

set expansion-module {yes | no}

Parameters

Parameter	Description	Possible Values	Default Value
yes	Keyword indicating that this station can have an expansion module		
no	Keyword indicating that this station cannot have an expansion module. This is the default value.		

User Level

read-write

Context

sls > station

Example

To allow the station to have an expansion module:

```
G450-001 (sls-station <extension>)# set expansion-module yes
```

Related Commands

set cor, set name, set password, set port, set sls, set swhook-flash, set trunk-destination, set type (station), show (station), show sls, station, sls

set name

Use the **set name** command to identify the username for a station, a trunk group, a DS1, or ISDN facility in SLS.

Syntax

set name *name*

Parameters

Parameter	Description	Possible Values	Default Value
name	The name as specified on the corresponding Communication Manager form (**add trunk-group *n***). This name is typically used to identify an individual, a service provider, or a site. If the file name includes spaces, use quotes. The length of the name is: • DS1 and BRI: 1 -15 characters • station and trunk-group: 1-27 characters		

User Level

read-write

Context

sls > station
sls > trunk-group
sls > ds1
sls > bri

Examples

To set the username Joe Smith for a given station:

```
G450-001 (sls-station-<extension>)# set name "Joe Smith"
```

Related Commands - Station commands

set cor, set expansion-module, set password, set port, set swhook-flash, set trunk-destination, set type (station), show (station), station

Related Commands - Trunk-group commands

add port, clear tac, clear trunk-group, remove port, set channel-preference, set codeset-display, set codeset-national, set dial, set digits, set digit-handling, set digit-treatment, set incoming-destination, set incoming-dialtone, set japan-disconnect, set numbering-format, set send-name, set send-number, set supervision, set tac, set trunk-hunt, show trunk-group, show (trunk-group), trunk-group

Related Commands - DS1 commands

clear ds1, set bearer-capability, set bit-rate, set channel-numbering, set connect, set country-protocol, set interface, set interface-companding, set long-timer, set protocol-version, set side, set signaling-mode, show (ds1), show ds1

Related Commands - BRI commands

bri, clear bri, set bearer-capability, set country-protocol, set directory-number-a, set directory-number-b, set endpoint-init, set interface, set interface-companding, set layer1-stable, set side, set spid-a, set spid-b, set tei-assignment, show bri, show (bri)

Related Commands - SLS commands

set sls, show sls, sls

---

set password

Use the **set password** command to administer a station password for DCP and IP station sets in SLS. If an IP Softphone in RoadWarrior mode is using the administrative identity of a DCP phone, then the password is required.

Syntax

set password *password*

Parameters

Parameter	Description	Possible Values	Default Value
password	A 4-8 digit numeric password		

User Level

read-write

Context

sls > station

Example

To set a given station password to 12345:

```
G450-001 (sls-station <extension>)# set password 12345
```

Related Commands

set cor, set expansion-module, set name, set port, set sls, set swhook-flash, set trunk-destination, set type (station), show (station), show sls, station, sls

set port

Use the **set port** command to administer a port on a station for SLS.

Syntax

set port *module-port*

Parameters

Parameter	Description	Possible Values	Default Value
module-port	The virtual integrated port assignment for the module in G450	Depends on class administered with the set type (station) command; see below	

Assign a port from this list:

Table 116: Module-port values in SLS station configuration mode

Gateway	Media module	Analog station ports*	DCP
G450	MM711	8 possible ports	
	MM712		8 possible ports
	MM714	4 possible ports (ports 1-4)	
	MM716	24 possible ports	
	MM717		24 possible ports

* You cannot select these modules/ports if they are already assigned as DID trunks.

User Level

read-write

Context

sls > station

Example

To set virtual integrated port v305 to a given station:

```
G450-001 (sls-station-<extension>)# set port v305
```

Related Commands

set cor, set expansion-module, set name, set password, set sls, set swhook-flash, set trunk-destination, set type (station), show (station), show sls, station, sls

set swhook-flash

Use the **set swhook-flash** command to enable SLS to recognize the switchhook flash signal from a particular analog station and to provide subsequent transfer service.

Note:

This command is valid only when the station type is **analog2500**.

Syntax

```
set swhook-flash {yes | no}
```

Parameters

Parameter	Description	Possible Values	Default Value
yes	Keyword indicating that SLS recognizes the switchhook signal and transfers the call. This is the default for analog phone only.		
no	Keyword indicating that SLS does not recognize the switchhook signal and transfers the call. This is the default for IP and DCP phones only.		

User Level

read-write

Context

sls > station

Example

To enable SLS to recognize the switchhook flash signal and to provide subsequent transfer service:

```
G450-001 (sls-station <extension>)# set swhook-flash yes
```

Related Commands

set cor, set expansion-module, set name, set password, set port, set sls, set trunk-destination, set type (station), show (station), show sls, station, sls

set trunk-destination

Use the **set trunk-destination** command to administer a station extension to be included in a pool of stations that can receive incoming analog loop-start trunk calls in circular queueing in SLS.

Note:

This command does not apply to analog DID trunks.

Syntax

set trunk-destination {yes | no}

Parameters

Parameter	Description	Possible Values	Default Value
yes	Keyword indicating that this extension can receive incoming analog loop-start trunk calls as part of the station pool which is available in a circular queueing fashion across the first available idle station. This is the default.		
no	Keyword indicating that this extension cannot receive incoming analog loop-start trunk calls as part of the station pool which is available		

User Level

read-write

Context

sls > station

Example

To designate that a given station extension be included in the station pool:

```
G450-001 (sls-station <extension>)# set trunk-destination yes
```

Related Commands

set cor, set expansion-module, set name, set password, set port, set sls, set swhook-flash, set type (station), show (station), show sls, station, sls

set type (station)

Use the **set type** command to administer specific phone models for SLS.

Note:

The new Avaya 96xx IP phone family is not directly referenced in the CLI. When you administer these phones via the CLI, use the following mapping:

Module name	CLI interface name
9610	4606
9620	4610
9630	4620
9640	4620
9650	4620

Syntax

set type ***model***

Parameters

Parameter	Description	Possible Values			Default Value
model	Model type	**Analog**	**DCP**	**IP**	
		analog 2500	dcp2402 dcp2410 dcp2420 dcp6402 dcp6402D dcp6408 dcp6408+ dcp6408D dcp6408D+ dcp6416D+ dcp6424D+ dcp8403B dcp8405B dcp8405B+ dcp8405D dcp8405D+ dcp8410B dcp8410D dcp8411B dcp8411D dcp8434D	ip4601 ip4602 ip4602sw ip4606 ip4610sw ip4612 ip4620 ip4620sw ip4624 ip4621 ip4622 ip4625	

User Level

read-write

Context

sls > station

Example

To administer phone model ip4625:

```
G450-001 (sls-station <extension>)# set type ip4625
```

Related Commands

set cor, set expansion-module, set name, set password, set port, set sls, set swhook-flash, set trunk-destination, show (station), show sls, station, sls

show (station)

Use the **show** command to list extension-specific SLS data parameters for this station.

Syntax

show

User Level

read-write

Context

sls > station

Example

To list extension-specific SLS data parameters for this station:

```
G450-001 (sls-station <extension>)# show

Extension Type       Port             Co      Trk-Des Exp-Mod Flash Passwd
--------- ---------- ---------------- ------- ------- ------- ----- ------
49138     ip4620     111.222.223.200  unrestr yes     no      -     ******
Name = Joe Smith
```

Note:

If an IP Softphone or an IP phone is currently registered when the command is run, the Port column shows the IP address of the IP Softphone or IP phone.

Output fields

Field	Description
Extension	The extension number of the phone (1-13 digits)
Type	The telephone model
Port	The module/port location

1 of 2

Field	Description
Cor	Class of restriction assigned to the station, which determines the range of dialing ability for the station. Possible values, ranging from most restricted to unrestricted, are: • emergency • internal • local • toll • unrestricted Less restricted classes include all dialing abilities included in more restricted classes.
Trk-Des	Whether or not to permit the station to receive incoming analog loop-start trunk calls in circular queueing
Exp-Mod	`Yes` means that an expansion module is administered for this station; `no` means that there is no expansion module associated with this station
Flash	`Yes` means that SLS will recognize the switchhook flash on this station; `no` means that flashing the switchhook has no effect
Passwd	Asterisks (*) indicate an administered password
	2 of 2

Related Commands

set cor, set expansion-module, set name, set password, set port, set sls, set swhook-flash, set trunk-destination, set type (station), show sls, station, sls

trunk-group

Use the **`trunk-group`** command within the `sls` context to enter a second-level subcontext for administering trunks for SLS. After issuing this command, the prompt changes to `sls-trunk-group-<tgnum>`. Type **`exit`** to leave the trunk-group context, and return to the sls context.

Syntax

`trunk-group` ***`tgnum`*** **`[group-type]`**

Parameters

Parameter	Description	Possible Values	Default Value
tgnum	The required trunk group number	**1-2000**	
group-type	The trunk group type. This argument is required to enter the trunk-group context. See the following for capacities by group type: • G450: Table 117	**loop-start** (analog) **did** (analog) **ground-start** (analog) **bri** (ISDN basic rate) **t1isdn** (ISDN primary rate on 1.544 Mbps facility) **e1isdn** (ISDN primary rate on 2.048 Mbps facility) **t1inband** (non-ISDN rate on 1.544 Mbps facility) **e1inband** (non-ISDN rate on 2.048 Mbps facility)	

You can create a trunk group that does not have any assigned members. Once a valid port is assigned as a trunk group member, this trunk group becomes active and may be employed by SLS call processing for incoming/outgoing trunk operation. The slot-configuration table will be used together with the port capacity for the given module to determine the validity of a port assignment at administration time.

As a corollary to this, there may not be more active trunk groups than there are physical trunk members within a given gateway. Secondly, a combo-port may only be used for one active assignment. For example, the analog station/DID trunk ports may be either allocated to serve as an analog station or as an analog DID trunk, but not BOTH.

The maximum limits for a given trunk type are defined by the slot-configuration assignment for the G450. The maximum number of ports allowed per interface module is defined in Table 117 for the G450.

Table 117: G450 SLS group type assignments

Group type	Media module	Number of ports/channels	Description of trunks that may be assigned
loop-start ground-start did	MM711	Ports 1-8	

1 of 2

Table 117: G450 SLS group type assignments (continued)

Group type	Media module	Number of ports/channels	Description of trunks that may be assigned
loop-start ground-start	MM714	4	Ports 5, 6, 7, 8
did	MM714	4	Ports 1, 2, 3, 4
did	MM716	Ports 1-24	
bri	MM720	16	Eight physical ports, each offering B1 and B2 channels
bri	MM722	4	Two physical ports, each offering B1 and B2 channels
t1-isdn	MM710	23	D-channel is associated with this facility (FAS)
t1-isdn	MM710	24	D-channel is not associated with this facility (NFAS), and the DS1's signaling-mode is set to **isdnext**
e1-isdn	MM710	30	D-channel is associated with this facility (FAS)
e1-isdn	MM710	31	D-channel is not associated with this facility (NFAS), and the DS1's signaling-mode is set to **isdnext**
t1-inband	MM710	24	
e1-inband	MM710	30	
			2 of 2

User Level

read-write

Context

sls

Example

To enter the second-level subcontext of `sls-trunk-group-<tgnum>` where the trunk group is number 200 of type loop-start:

```
G450-001(super-sls)# trunk-group 200 loop-start
G450-001(sls-trunk-group-<200>)#
```

Sub-commands

Depending on the group type, the following commands are available once you are inside the trunk-group context:

Command	ground-start, loop-start	did	t1isdn, e1isdn, bri	e1inband, t1inband
add port	X	X	X	X
clear tac	X	X	X	X
remove port	X	X	X	X
set busy-disconnect	X*			X
set cbc			X	
set cbc-parameter			X	
set cbc-service-feature,			X	
set channel-preference			X	
set codeset-display			X	
set codeset-national			X	
set dial	X	X		X
set digits		X		X
set digit-handling			X	
set digit-treatment		X		X
set incoming-destination	X			X
set incoming-dialtone				X
set japan-disconnect			X	
set name	X	X	X	X
set numbering-format			X	
set send-name			X	
set send-number			X	
set supervision		X		X
set tac	X	X	X	X

Command	ground-start, loop-start	did	t1isdn, e1isdn, bri	e1inband, t1inband
set trunk-hunt			X	X
show (trunk-group)	X	X	X	X

* **Set busy-disconnect** applies only to analog loop-start trunks.

Additional SLS commands

clear trunk-group, set sls, show sls, show trunk-group sls

add port

Use the **add port** command to administer the port appropriate for SLS. The port can belong to one trunk group only, and the port assignment depends on the ***group-type*** parameter for the trunk-group command.

Syntax

add port *module port [sig-group]*

Note:

The ***sig-group*** argument is only necessary for Digital trunks.

Parameters

Parameter	Description	Possible Values	Default Value
module port	The virtual integrated port assignment for this ***group-type***	See either Analog trunks Digital trunks	
sig-group	Specifies the signaling group associated with the management of this trunk member	Number between 1- 650	

Analog trunks

- G450: see Table 118 (255 trunks per trunk group)

Note:

If you attempt to assign more than the maximum number of trunk members, an error message instructs you to delete a trunk member before you can add a new one.

A physical trunk port may only be a member of a single trunk group and cannot be shared across two or more trunk groups.

Table 118: G450 SLS analog port assignments

Group type	Media Module	Number of ports/channels	Description
loop-start did ground-start	MM711*	8	1-8
loop-start ground-start	MM714	4	5, 6, 7, 8
did	MM714	4	1, 2, 3, 4
did	MM716	24	1-24

* If MM711 is used in all five slots, then there are 40 available trunks on a single gateway.

Example (analog trunk port)

To add an analog trunk port:

If an MM711 is inserted into slot V3 and an analog loop-start trunk is to be administered for port 4, then **`add port V304`** administers an analog loop-start trunk through port V304.

```
G450-001 (sls-trunk-group-<tgnum>)# add port v304
```

Digital trunks

- G450: (255 trunks per trunk group (see Table 119). The number of ISDN channels depends on whether the signaling D-channel is associated with this facility (FAS) or not (NFAS).

Note:

You cannot mix BRI and PRI trunk members within the same trunk group.

If you attempt to assign more than the maximum number of trunk members, an error message instructs you to delete a trunk member before you can add a new one.

A physical trunk port may only be a member of a single trunk group and cannot be shared across two or more trunk groups.

Table 119: G450 SLS digital port assignments

Group type	Media Module	Maximum ports/ channels
bri	MM720	8
	MM722	4
t1isdn	MM710	23 (FAS) 24 (NFAS)
e1isdn	MM710	30 (FAS) 31 (NFAS)
t1inband	MM710	24
e1inband1	MM710	30

User Level

read-write

Context

sls > trunk-group

Related Commands

clear tac, clear trunk-group, remove port, set busy-disconnect, set cbc, set cbc-parameter, set cbc-service-feature, set channel-preference, set codeset-display, set codeset-national, set dial, set digits, set digit-handling, set digit-treatment, set incoming-destination, set incoming-dialtone, set japan-disconnect, set name, set numbering-format, set send-name, set send-number, set supervision, set tac, set trunk-hunt, set sls, show (trunk-group), show sls, show trunk-group, sls, trunk-group

clear tac

Use the **clear tac** command to remove a Trunk Access Code (TAC) assignment from a trunk group in SLS. The set tac command establishes the TAC assignment to the trunk group.

Syntax

clear tac

User Level

read-write

Context

sls > trunk-group

Example

To remove TAC assignment from trunk group 200:

```
G450-001 (sls-trunk-group-<200>)# clear tac
Done!
```

Related Commands

add port, clear trunk-group, remove port, set busy-disconnect, set cbc, set cbc-parameter, set cbc-service-feature, set channel-preference, set codeset-display, set codeset-national, set dial, set digits, set digit-handling, set digit-treatment, set incoming-destination, set incoming-dialtone, set japan-disconnect, set name, set numbering-format, set send-name, set send-number, set supervision, set tac, set trunk-hunt, set sls, show (trunk-group), show sls, show trunk-group sls, trunk-group

remove port

Use the **remove port** command to remove the virtual integrated port assignment from a trunk group in SLS. The port assignment is administered with the add port command.

Syntax

remove port *module port*

Parameters

Parameter	Description	Possible Values	Default Value
module port	The virtual integrated port assignment for this ***group-type***	See the add port command for port values	

User Level

read-write

Context

sls > trunk-group

Example

To remove the virtual integrated port assignment of port v301:

```
G450-001 (sls-trunk-group-<tgnum>)# remove port v301
```

Related Commands

add port, clear tac, clear trunk-group, set busy-disconnect, set cbc, set cbc-parameter, set cbc-service-feature, set channel-preference, set codeset-display, set codeset-national, set dial, set digits, set digit-handling, set digit-treatment, set incoming-destination, set incoming-dialtone, set japan-disconnect, set name, set numbering-format, set send-name, set send-number, set supervision, set tac, set trunk-hunt, set sls, show (trunk-group), show sls, show trunk-group sls, trunk-group

set busy-disconnect

Use the **set busy-disconnect** command to specify whether the SLS analog trunk call state machine is to monitor the trunk for the presence of a busy tone for the entire duration of both incoming and outgoing calls. If a busy tone is detected, the SLS call state machine will disconnect the call.

Note:

This command only applies to analog loop-start trunks.

Syntax

set busy-disconnect {yes | no}

Parameters

Parameter	Description	Possible Values	Default Value
yes	Keyword indicating that the SLS Q.931 state machine will connect a tone detector to this time slot for the purpose of detecting the busy tone signal. Upon detecting a busy tone signal, the SLS call processing directs the trunk to initiate a disconnect sequence by opening the loop.		
no	Keyword indicating that no busy tone detection be applied. This is the default value.		

User Level

read-write

Context

sls > trunk-group

Example

To specify that the SLS analog trunk call state machine monitor the analog loop-start trunk for the presence of a busy tone:

```
G450-001 (sls-trunk-group-<tgnum>)# set busy-disconnect yes
```

Related Commands

add port, clear tac, clear trunk-group, remove port, set cbc-parameter, set cbc-service-feature, set channel-preference, set codeset-display, set codeset-national, set dial, set digits, set digit-handling, set digit-treatment, set incoming-destination, set incoming-dialtone, set japan-disconnect, set name, set numbering-format, set send-name, set send-number, set supervision, set tac, set trunk-hunt, set sls, show (trunk-group), show sls, show trunk-group sls, trunk-group

set cbc

Use the **set cbc** command to specify whether the ISDN trunk group is to operate by declaring the service type explicitly on a call-by-call basis in SLS.

Note:

This command only applies to ISDN Primary Rate trunks.

Syntax

```
set cbc {yes | no}
```

Parameters

Parameter	Description	Possible Values	Default Value
yes	Keyword indicating that the SLS Q.931 state machine will define the service type in the Network Specific Facilities information element that is sent with the SETUP message on outbound calls		
no	Keyword indicating that the Network Specific Facilities information element will not be sent. This is the default value.		

User Level

read-write

Context

sls > trunk-group

Example

To specify that the ISDN trunk group will declare the service type explicitly:

```
G450-001 (sls-trunk-group-<tgnum>)# set cbc yes
```

Related Commands

add port, clear tac, clear trunk-group, remove port, set busy-disconnect, set cbc-parameter, set cbc-service-feature, set channel-preference, set codeset-display, set codeset-national, set dial, set digits, set digit-handling, set digit-treatment, set incoming-destination, set incoming-dialtone, set japan-disconnect, set name, set numbering-format, set send-name, set send-number, set supervision, set tac, set trunk-hunt, set sls, show (trunk-group), show sls, show trunk-group sls, trunk-group

set cbc-parameter

Use the **set cbc** command to define what class of service is being specified, as part of the **scocs** service in the Network Services Facility information element sent to the network service provider on outgoing calls in SLS.

Note:

This command only applies to ISDN Primary Rate trunks

Note:

This command is available only if set cbc is set to **yes**, and set cbc-service-feature is set to **scocs**.

Syntax

set cbc-parameter *class*

Parameters

Parameter	Description	Possible Values	Default Value
class	The class of service specified as part of the **scocs** service in the Network Services Facility information element	An integer from **0-99999**	**1**

User Level

read-write

Context

sls > trunk-group

Example

To define the class of service specified as part of the **scocs** service in the Network Services Facility information element:

```
G450-001 (sls-trunk-group-<tgnum>)# set cbc-parameter 2
```

Related Commands

add port, clear tac, clear trunk-group, remove port, set busy-disconnect, set cbc, set cbc-service-feature, set channel-preference, set codeset-display, set codeset-national, set dial, set digits, set digit-handling, set digit-treatment, set incoming-destination, set incoming-dialtone, set japan-disconnect, set name, set numbering-format, set send-name, set send-number, set supervision, set tac, set trunk-hunt, set sls, show (trunk-group), show sls, show trunk-group sls, trunk-group

set cbc-service-feature

Use the **set cbc-service-feature** command to specify the type of service or feature being specified in the Network Services Facility information element (as part of the SETUP message) that is sent to the network service provider on outgoing calls in SLS.

Note:

This command only applies to ISDN Primary Rate trunks.

Note:

This command is available only if set cbc is set to **yes**.

Syntax

set cbc-service-feature *type*

Parameters

Parameter	Description	Possible Values	Default Value
type	The type of service or feature being specified in the Network Services Facility information element. If you specify **scocs** service, use the set cbc-parameter command to define the desired grade of service.	Feature types: • **operator** • **sub-operator** Service types: • **sdn** • **megacom** • **lds** • **scocs**	**sdn**

User Level

read-write

Context

sls > trunk-group

Example

To specify that the **scocs** service will be specified in the Network Services Facility information element:

```
G450-001 (sls-trunk-group-<tgnum>)# set cbc-service-feature scocs
```

Related Commands

add port, clear tac, clear trunk-group, remove port, set busy-disconnect, set cbc, set cbc-parameter, set channel-preference, set codeset-display, set codeset-national, set dial, set digits, set digit-handling, set digit-treatment, set incoming-destination, set incoming-dialtone, set japan-disconnect, set name, set numbering-format, set send-name, set send-number, set supervision, set tac, set trunk-hunt, set sls, show (trunk-group), show sls, show trunk-group sls, trunk-group

set channel-preference

Use the **set channel-preference** command to define how the Channel Identification IE field is encoded in SLS.

Note:

This command only applies to ISDN trunks.

Syntax

set channel-preference *type*

Parameters

Parameter	Description	Possible Values	Default Value
type	Encoding of the Channel Identification IE field: • **exclusive** – The central office must have the ability to grant a call on this channel or reject the call attempt • **preferred** – The central office might offer the call request on another available channel	**exclusive** **preferred**	**preferred**

User Level

read-write

Context

sls > trunk-group

Example

To define that the Channel Identification IE field is encoded to preferred status:

```
G450-001 (sls-trunk-group-<tgnum>)# set channel-preference preferred
```

Related Commands

add port, clear tac, clear trunk-group, remove port, set busy-disconnect, set cbc, set cbc-parameter, set cbc-service-feature, set codeset-display, set codeset-national, set dial, set digits, set digit-handling, set digit-treatment, set incoming-destination, set incoming-dialtone, set japan-disconnect, set name, set numbering-format, set send-name, set send-number, set supervision, set tac, set trunk-hunt, set sls, show (trunk-group), show sls, show trunk-group sls, trunk-group

set codeset-display

Use the **set codeset-display** command to identify which Q.931 codesets are allowed to send display information to the user phone in SLS.

Note:

This command only applies to ISDN trunks.

Syntax

set codeset-display *codeset*

Parameters

Parameter	Description	Possible Values	Default Value
codeset	The Q.931 codeset that sends display information to the user phone	**codeset0** **codeset6** **codeset7**	**codeset6**

User Level

read-write

Context

sls > trunk-group

Example

To identify that codeset6 is allowed to send display information to the user phone:

```
G450-001 (sls-trunk-group-<tgnum>)# set codeset-display codeset6
```

Related Commands

add port, clear tac, clear trunk-group, remove port, set busy-disconnect, set cbc, set cbc-parameter, set cbc-service-feature, set channel-preference, set codeset-national, set dial, set digits, set digit-handling, set digit-treatment, set incoming-destination, set incoming-dialtone,

set japan-disconnect, set name, set numbering-format, set send-name, set send-number, set supervision, set tac, set trunk-hunt, set sls, show (trunk-group), show sls, show trunk-group sls, trunk-group

set codeset-national

Use the **set codeset-national** command to identify which Q.931 codesets are allowed to send National Information Elements (IEs, or display information) to the user phone in SLS.

Note:

This command only applies to ISDN trunks.

Syntax

set codeset-national *codeset*

Parameters

Parameter	Description	Possible Values	Default Value
codeset	The Q.931 codeset that sends National IE display information to the user phone. **Note:** This value depends on the local central office switch.	**codeset6** **codeset7**	**codeset6**

User Level

read-write

Context

sls > trunk-group

Example

To specify that codeset6 is allowed to send National Information Elements to the user phone:

```
G450-001 (sls-trunk-group-<tgnum>)# set codeset-national codeset6
```

Related Commands

add port, clear tac, clear trunk-group, remove port, set busy-disconnect, set cbc, set cbc-parameter, set cbc-service-feature, set channel-preference, set codeset-display, set dial, set digits, set digit-handling, set digit-treatment, set incoming-destination, set incoming-dialtone, set japan-disconnect, set name, set numbering-format, set send-name, set send-number, set supervision, set tac, set trunk-hunt, set sls, show (trunk-group), show sls, show trunk-group sls, trunk-group

set dial

Use the **set dial** command to define the method for sending outbound digits in SLS.

Syntax

set dial *dial-type*

Parameters

Parameter	Description	Possible Values	Default Value
dial-type	The method used to send digits toward the outbound trunk	**rotary** **dtmf**	**dtmf**

User Level

read-write

Context

sls > trunk-group

Example

To define the method for sending outbound digits as DTMF:

```
G450-001 (sls-trunk-group-<200>)# set dial dtmf
```

Related Commands

add port, clear tac, clear trunk-group, remove port, set busy-disconnect, set cbc, set cbc-parameter, set cbc-service-feature, set channel-preference, set codeset-display, set codeset-national, set digits, set digit-handling, set digit-treatment, set incoming-destination, set incoming-dialtone, set japan-disconnect, set name, set numbering-format, set send-name, set send-number, set supervision, set tac, set trunk-hunt, set sls, show (trunk-group), show sls, show trunk-group sls, trunk-group

set digit-handling

Use the **set digit-handling** command to define how the inbound/outbound calls handle the reception/transmission of the dialed pattern in SLS.

Note:

This command only applies to ISDN trunks.

Syntax

set digit-handling *method*

Parameters

Parameter	Description	Possible Values	Default Value
method	How the inbound/outbound calls handle the reception/transmission of the dialed pattern. Enbloc requires sending the entire collected digit string in one block. Overlap sends the digits one at a time as they are collected. **Note:** If you specify **enbloc** for transmission of outbound calls, the dialing technique should be ARS. **Note:** If you are employing TAC dialing for a trunk-group, set the transmission for outbound trunk calls to **overlap**.	**enbloc-enbloc** **enbloc-overlap** **overlap-enbloc** **overlap-overlap**	**enbloc-enbloc**

User Level

read-write

Context

sls > trunk-group

Example

To define that inbound and outbound calls handle reception and transmission as enbloc and enbloc respectively:

```
G450-001 (sls-trunk-group-<tgnum>)# set digit-handling enbloc-enbloc
```

Related Commands

add port, clear tac, clear trunk-group, remove port, set busy-disconnect, set cbc, set cbc-parameter, set cbc-service-feature, set channel-preference, set codeset-display, set codeset-national, set dial, set digits, set digit-treatment, set incoming-destination, set incoming-dialtone, set japan-disconnect, set name, set numbering-format, set send-name, set send-number, set supervision, set tac, set trunk-hunt, set sls, show (trunk-group), show sls, show trunk-group, sls, trunk-group

set digits

Use the **set digits** command to define the inserted dial string that is added to the beginning of the received DID incoming dial string for analog DID trunks or for DS1 TIE trunks using in-band signaling in SLS.

Note:

You must have executed the set digit-treatment command before this command will work.

Syntax

set digits *digits*

Parameters

Parameter	Description	Possible Values*	Default Value
digits	The inserted dial string that is added to the start of the received DID incoming dial string	**0-9** plus ***** and **#**	

* The number of digits must agree with the ***digit-treat*** parameter in the set digit-treatment command. If the ***digit-treat*** parameter is **insert3**, then the ***digits*** parameter for this command must be three digits in length.

User Level

read-write

Context

sls > trunk-group

Example

To define the inserted dial string as 538:

```
G450-001 (sls-trunk-group-<tgnum>)# set digits 538
```

Related Commands

add port, clear tac, clear trunk-group, remove port, set busy-disconnect, set cbc, set cbc-parameter, set cbc-service-feature, set channel-preference, set codeset-display, set codeset-national, set dial, set digit-handling, set digit-treatment, set incoming-destination, set incoming-dialtone, set japan-disconnect, set name, set numbering-format, set send-name, set send-number, set supervision, set tac, set trunk-hunt, set sls, show (trunk-group), show sls, show trunk-group sls, trunk-group

set digit-treatment

Use the **set digit-treatment** command to define the incoming digit treatment for analog DID trunks or for DS1 TIE trunks using in-band signaling in SLS.

Syntax

set digit-treatment *digit-treat*

Parameters

Parameter	Description	Possible Values	Default Value
digit-treat	The incoming digit treatment for analog DID trunks only	**blank** (removes digit treatment), **absorb1** **absorb2** **absorb3** **absorb4** **absorb5** **insert1** **insert2** **insert3** **insert4**	**blank**

User Level

read-write

Context

sls > trunk-group

Examples

To define the incoming digit treatment as absorb 1:

```
G450-001 (sls-trunk-group-<tgnum>)# set digit-treatment absorb 1
```

To remove incoming digit treatment:

```
G450-001 (sls-trunk-group-<tgnum>)# set digit-treatment blank
```

Related Commands

add port, clear tac, clear trunk-group, remove port, set busy-disconnect, set cbc, set cbc-parameter, set cbc-service-feature, set channel-preference, set codeset-display, set codeset-national, set dial, set digits, set digit-handling, set incoming-destination, set incoming-dialtone, set japan-disconnect, set name, set numbering-format, set send-name, set send-number, set supervision, set tac, set trunk-hunt, set sls, show sls, show trunk-group sls,

trunk-group

set incoming-destination

Use the **set incoming-destination** command to identify an extension to directly receive an incoming trunk call, for example, an attendant or a voice response/recording system in SLS.

Note:

This command only applies to non-ISDN digital, analog loop-start, and analog ground-start trunks.

Syntax

set incoming-destination *extension*

Parameters

Parameter	Description	Possible Values	Default Value
extension	The extension to receive an incoming trunk call, for example, an attendant or a voice response/recording system	"**0 - 9**," string may begin with "**0**" 0-13 characters, consistent with the local dial plan Any administered SLS extension	" " (no station administered)*

* To clear the incoming-destination administration use the **set incoming-destination " "** command.

User Level

read-write

Context

sls > trunk-group

Example

To identify extension 5381000 to receive an incoming trunk call:

```
G450-001 (sls-trunk-group-<tgnum>)# set incoming-destination 5381000
```

Related Commands

add port, clear tac, clear trunk-group, remove port, set busy-disconnect, set cbc, set cbc-parameter, set cbc-service-feature, set channel-preference, set codeset-display, set codeset-national, set dial, set digits, set digit-handling, set digit-treatment, set incoming-dialtone, set japan-disconnect, set name, set numbering-format, set send-name, set send-number, set supervision, set tac, set trunk-hunt, set sls, show (trunk-group), show sls, show trunk-group sls,

trunk-group

set incoming-dialtone

Use the **set incoming-dialtone** command to provide a dial tone in response to far-end trunk group seizures in SLS.

Note:

This command only applies to digital DS1 trunks set up for inband signaling.

Syntax

set incoming-dialtone {yes | no}

Parameter	Description	Possible Values	Default Value
yes	A keyword indicating to provide a dial tone		
no	A keyword indicating trunks that are not sending digits, for example, an incoming call on a loop-start central office trunk. This is the default value.		

User Level

read-write

Context

sls > trunk-group

Example

To withhold a dial tone:

```
G450-001 (sls-trunk-group-<tgnum>)# set incoming-dialtone no
```

Related Commands

add port, clear tac, clear trunk-group, remove port, set busy-disconnect, set cbc, set cbc-parameter, set cbc-service-feature, set channel-preference, set codeset-display, set codeset-national, set dial, set digits, set digit-handling, set digit-treatment, set incoming-destination, set japan-disconnect, set name, set numbering-format, set send-name, set send-number, set supervision, set tac, set trunk-hunt, set sls, show (trunk-group), show sls, show trunk-group sls, trunk-group

set japan-disconnect

Use the **set japan-disconnect** command to perform a disconnect sequence (CONNECT message followed by a DISCONNECT message) in SLS.

Note:

This command only applies to ISDN trunks.

Syntax

set japan-disconnect {yes | no}

Parameters

Parameter	Description	Possible Values	Default Value
yes	Keyword specifying to perform a disconnect sequence		
no	Keyword specifying not to perform a disconnect sequence. This is the default.		

User Level

read-write

Context

sls > trunk-group

Example

To choose not to perform a disconnect sequence:

```
G450-001 (sls-trunk-group-<tgnum>)# set japan-disconnect no
```

Related Commands

add port, clear tac, clear trunk-group, remove port, set busy-disconnect, set cbc, set cbc-parameter, set cbc-service-feature, set channel-preference, set codeset-display, set codeset-national, set dial, set digits, set digit-handling, set digit-treatment, set incoming-destination, set incoming-dialtone, set name, set numbering-format, set send-name, set send-number, set supervision, set tac, set trunk-hunt, set sls, show (trunk-group), show sls, show trunk-group sls, trunk-group

set name

Use the **set name** command to identify the username for a station, a trunk group, a DS1, or ISDN facility in SLS.

Syntax

set name *name*

Parameters

Parameter	Description	Possible Values	Default Value
name	The name as specified on the corresponding Communication Manager form (**add trunk-group *n***). This name is typically used to identify an individual, a service provider, or a site. If the file name includes spaces, use quotes. The length of the name is: • DS1 and BRI: 1 -15 characters • station and trunk-group: 1-27 characters		

User Level

read-write

Context

sls > station
sls > trunk-group
sls > ds1
sls > bri

Examples

To set the username Joe Smith for a given station:

```
G450-001 (sls-station-<extension>)# set name "Joe Smith"
```

Related Commands - Station commands

set cor, set expansion-module, set password, set port, set swhook-flash, set trunk-destination, set type (station), show (station), station

Related Commands - Trunk-group commands

add port, clear tac, clear trunk-group, remove port, set busy-disconnect, set cbc, set cbc-parameter, set cbc-service-feature, set channel-preference, set codeset-display, set codeset-national, set dial, set digits, set digit-handling, set digit-treatment, set incoming-destination, set incoming-dialtone, set japan-disconnect, set numbering-format, set send-name, set send-number, set supervision, set tac, set trunk-hunt, show trunk-group, show (trunk-group), trunk-group

Related Commands - DS1 commands

clear ds1, set bearer-capability, set bit-rate, set channel-numbering, set connect, set country-protocol, set interface, set interface-companding, set long-timer, set protocol-version, set side, set signaling-mode, show (ds1), show ds1

Related Commands - BRI commands

bri, clear bri, set bearer-capability, set country-protocol, set directory-number-a, set directory-number-b, set endpoint-init, set interface, set interface-companding, set layer1-stable, set side, set spid-a, set spid-b, set tei-assignment, show bri, show (bri)

Related Commands - SLS commands

set sls, show sls, sls

---

set numbering-format

Use the **`set numbering-format`** command to specify the numbering plan for the current trunk in SLS. The numbering plan encodes the **Numbering Plan Indicator** and **Type of Number** fields in the Calling/Connected Party Number IE in the ISDN protocol.

Note:

Leave the setting of ***`type`*** to be **unknown** since SLS does not currently support an administrative table to calculate the Calling Party Number that is consistent with the numbering plan of the PSTN service provider.

Note:

This command only applies to ISDN trunks.

Syntax

`set numbering-format` ***`type`***

Parameters

Parameter	Description	Possible Values	Default Value
type	The numbering plan for the current trunk. • **unknown** – Both the Numbering Plan Indicator and Type of Number are unknown • **public** – The Numbering Plan Indicator meets the E.164 standard and the Type of Number is national	**unknown** **public**	**unknown**

User Level

read-write

Context

sls > trunk-group

Example

To specify the numbering plan for the current trunk as public:

```
G450-001 (sls-trunk-group-<tgnum>)# set numbering-format public
```

Related Commands

add port, clear tac, clear trunk-group, remove port, set busy-disconnect, set cbc, set cbc-parameter, set cbc-service-feature, set channel-preference, set codeset-display, set codeset-national, set dial, set digits, set digit-handling, set digit-treatment, set incoming-destination, set incoming-dialtone, set japan-disconnect, set name, set send-name, set send-number, set supervision, set tac, set trunk-hunt, set sls, show (trunk-group), show sls, show trunk-group sls, trunk-group

set send-name

Use the **set send-name** command to define whether or not the calling, connected, called, or busy party's administered name is sent to the network on outgoing or incoming calls in SLS.

Note:

Leave the setting of ***method*** to be **no**, since sending a Calling Party Name is a future feature.

Note:

This command only applies to ISDN trunks.

Syntax

set send-name *method*

Parameters

Parameter	Description	Possible Values	Default Value
method	Specifies whether or not the calling, connected, called, or busy party's administered name is sent to the network on outgoing or incoming calls: • **yes** – The name is sent to the network for incoming or outgoing calls • **no** – The name is not sent to the network for incoming or outgoing calls • **restricted** – The name is sent to the network as 'Presentation restricted' **Note:** If the name is not administered for the calling, connected, called, or busy station, the extension number is sent in place of the name.	**yes** **no** **restricted**	**no**

User Level

read-write

Context

sls > trunk-group

Example

To define that the calling, connected, called, or busy party's administered name is sent to the network on outgoing or incoming calls:

```
G450-001 (sls-trunk-group-<tgnum>)# set send-name yes
```

Related Commands

add port, clear tac, clear trunk-group, remove port, set busy-disconnect, set cbc, set cbc-parameter, set cbc-service-feature, set channel-preference, set codeset-display, set codeset-national, set dial, set digits, set digit-handling, set digit-treatment, set incoming-destination, set incoming-dialtone, set japan-disconnect, set name, set numbering-format, set send-number, set supervision, set tac, set trunk-hunt, set sls, show (trunk-group), show sls, show trunk-group sls, trunk-group

set send-number

Use the **set send-number** command to define whether or not the calling, connected, called, or busy party's administered number is sent to the network on outgoing or incoming calls in SLS.

Note:

Leave the setting of ***method*** to be **no**, since sending a Calling Party Number is a future feature.

Note:

This command only applies to ISDN trunks.

Syntax

set send-number *method*

Parameters

Parameter	Description	Possible Values	Default Value
method	Specifies whether or not the calling, connected, called, or busy party's administered number is sent to the network on outgoing or incoming calls: • **yes** – The number is sent to the network for incoming or outgoing calls • **no** – The number is not sent to the network for incoming or outgoing calls • **restricted** – The number is sent to the network as 'Presentation restricted'	**yes** **no** **restricted**	**no**

User Level

read-write

Context

sls > trunk-group

Example

To define that the calling, connected, called, or busy party's administered number is sent to the network on outgoing or incoming calls:

```
G450-001 (sls-trunk-group-<tgnum>)# set send-number yes
```

Related Commands

add port, clear tac, clear trunk-group, remove port, set busy-disconnect, set cbc, set cbc-parameter, set cbc-service-feature, set channel-preference, set codeset-display, set codeset-national, set dial, set digits, set digit-handling, set digit-treatment, set incoming-destination, set incoming-dialtone, set japan-disconnect, set name, set cbc, set cbc-parameter, set cbc-service-feature, set numbering-format, set send-name, set supervision, set tac, set trunk-hunt, set sls, show (trunk-group), show sls, show trunk-group sls, trunk-group

set supervision

Use the **set supervision** command to define the incoming signaling supervision mode for analog DID trunks or DS1 tie trunks only in SLS.

Syntax

set supervision ***sup-type***

Parameters

Parameter	Description	Possible Values	Default Value
sup-type	For analog-did group types: The incoming signaling supervision mode for analog DID trunks	**immediate** **wink**	**wink**
	For t1inband and e1inband group types: Signaling supervision for the non-ISDN digital trunks*	**loop-start** **ground-start** **wink-wink** **wink-immediate** **wink-auto** **immediate-immediate** **auto-auto** **auto-wink**	**wink-wink**

* For TIE trunks you must specify both the incoming and outgoing modes. For example, **wink-immediate** requires the DS1 interface to use wink supervision to answer an incoming call and use an immediate seizure protocol for outbound calls.

User Level

read-write

Context

sls > trunk-group

Example

To define the incoming signaling supervision mode as wink mode:

```
G450-001 (sls-trunk-group-<tgnum>)# set supervision wink
```

To define the incoming signaling supervision mode as wink-wink mode:

```
G450-001 (sls-trunk-group-<tgnum>)# set supervision wink-wink
```

Related Commands

add port, clear tac, clear trunk-group, remove port, set busy-disconnect, set cbc, set cbc-parameter, set cbc-service-feature, set channel-preference, set codeset-display, set codeset-national, set dial, set digits, set digit-handling, set digit-treatment, set incoming-destination, set incoming-dialtone, set japan-disconnect, set name, set numbering-format, set send-name, set send-number, set tac, set trunk-hunt, set sls, show (trunk-group), show sls, show trunk-group sls, trunk-group

set tac

Use the **set tac** command to administer the trunk-access codes for SLS. You must issue this command before the trunk group is enabled in the SLS database.

Syntax

set tac ***tac***

Parameters

Parameter	Description	Possible Values	Default Value
tac	Unique dial string identifies the trunk group* (circumvents normal Automatic Route System dial string analysis)	1-4 digits (can include “#” and “*****” as the leading digit only)	

* This trunk-access code must be unique across all trunk groups, extension numbers, and any ARS Feature Access Code strings.

User Level

read-write

Context

sls > trunk-group

Example

To administer the trunk-access codes for trunk group 88:

```
G450-001 (sls-trunk-group-<200>)# set tac 88
```

Related Commands

add port, clear tac, clear trunk-group, remove port, set busy-disconnect, set cbc, set cbc-parameter, set cbc-service-feature, set channel-preference, set codeset-display, set codeset-national, set dial, set digits, set digit-handling, set digit-treatment, set incoming-destination, set incoming-dialtone, set japan-disconnect, set name, set numbering-format, set send-name, set send-number, set supervision, set trunk-hunt, set sls, show (trunk-group), show sls, show trunk-group sls, trunk-group

set trunk-hunt

Use the **`set trunk-hunt`** command to specify the trunk-hunting search within a facility in an ISDN trunk group or through a non-ISDN digital trunk group in SLS.

Note:

This command only applies to DS1 trunks.

Syntax

`set trunk-hunt` ***`type`***

Parameters

Parameter	Description	Possible Values	Default Value
`type`	The trunk-hunting search type within a facility in an ISDN trunk group, or through a non-ISDN digital trunk group: • **ascend** – A linear search from the lowest to the highest numbered available channels • **cyclical** – A circular search beginning with the point at which the search previously ended. When the search has reached the top of the channel list, it resumes at the bottom of the list in wrap-around fashion. • **descend** – A linear search from the highest to the lowest numbered available channels	**ascend** **cyclical** **descend**	**cyclical**

User Level

read-write

Context

sls > trunk-group

Example

To specify that the trunk-hunting search proceed in a cyclical fashion:

```
G450-001 (sls-trunk-group-<tgnum>)# set trunk-hunt cyclical
```

Related Commands

add port, clear tac, clear trunk-group, remove port, set busy-disconnect, set cbc, set cbc-parameter, set cbc-service-feature, set channel-preference, set codeset-display, set codeset-national, set dial, set digits, set digit-handling, set digit-treatment, set incoming-destination, set incoming-dialtone, set japan-disconnect, set name, set numbering-format, set send-name, set send-number, set supervision, set tac, set sls, show (trunk-group), show sls, show trunk-group sls, trunk-group

show (trunk-group)

Use the **show** command to display trunk group administration in SLS for this trunk group.

Syntax

show

User Level

read-write

Context

sls > trunk-group

Example

This example shows four BRI trunks assigned to one trunk-group

```
G450-001(sls-trunk-group-<tgnum>)# show

Group Type       Dial   Tac  Supervision         Treat   Insert
----- ---------- ------ ---- ------------------- ------- ------
    1        bri      -  *99                   -       -       -
Name = Willow Street 2
Ports = v401,v402,v417,v418
Codeset  Codeset  Channel    Digit           Japan
Display  National Preference Handling        Discon
-------- -------- ---------- --------------- ------
codeset6 codeset6  exclusive   enbloc-enbloc     no

Send Send   Number Trunk
Name Number Format Hunt
---- ------ ------ --------
 yes    yes public   ascend
```

This example shows twelve ports assigned as T1inband signalling

```
G450-001(sls-trunk-group-<tgnum>)# show

Group Type       Dial   Tac  Supervision         Treat   Insert
----- ---------- ------ ---- ------------------- ------- ------
    1  t1-inband   dtmf  *96      wink/immediate       -       -
Name = Willow Street 2
Ports = v401,v402,v403,v404,v405,v406,v407,v408,v409,v410,v411,v412
Incoming-Dest Incoming-Dial Trunk-Hunt
------------- ------------- ----------
            -            no     ascend
```

This example shows twelve ports assigned as t1-isdn signaling:

```
G450-001(sls-trunk-group-<tgnum>)# show
Group Type       Dial   Tac  Supervision         Treat   Insert
----- ---------- ------ ---- ------------------- ------- ------
    1    t1-isdn      -  *99                    -       -       -
Name = Willow Street 2
Ports = v401,v402,v403,v404,v405,v406,v407,v408,v409,v410,v411,v412
Codeset  Codeset  Channel    Digit           Japan
Display  National Preference Handling        Discon
-------- -------- ---------- --------------- ------
codeset6 codeset6  exclusive   enbloc-enbloc     no

Send Send   Number Trunk
Name Number Format Hunt
---- ------ ------ --------
 yes    yes public   ascend

Cbc Cbc-service-feature Cbc-parameter
--- ------------------- -------------
yes                 sdn             -
```

Output fields

Field	Description
Group	The trunk group index
Type	The trunk group type. Possible values: • **loop-start** (analog loopstart) • **did** (analog DID)
Dial	The method for sending outbound digits. Possible values: • **rotary** • **dtmf**
Tac	The trunk-access code - a unique dial string that identifies the trunk group
Ports	The virtual integrated port assignment
Supervision	The incoming signaling supervision mode for analog DID trunks only. Possible values: • **immediate** • **wink**
Treat	The incoming digit treatment for analog DID trunks only

1 of 2

Field	Description
Insert	The dial string that is added to the start of the received DID incoming dial string
Incoming Dest	The extension to receive an incoming trunk call
Incoming-Dial	Whether a dial tone is set in response to far-end trunk group seizures
Trunk-Hunt	The trunk-hunting search within a facility in an ISDN trunk group or through a non-ISDN digital trunk group. Possible values: • **ascend** • **cyclical** • **descend**
	2 of 2

Related Commands

bri, dial-pattern, ds1, incoming-routing, set sls, show sls, sig-group, station, sls, trunk-group

SNMP access configuration

ip snmp

Use the **ip snmp** command to enable the SNMP agent for the G450. Use the **no** form of the command to disable the SNMP agent for the G450. Disabling the SNMP agent also blocks SNMP traps. However, users can change SNMP configuration settings even when the agent is disabled.

Syntax

ip snmp

no ip snmp

User Level

admin

Context

general

Related Commands - SNMP access configuration

set snmp community, set snmp retries, set snmp timeout, show snmp, show snmp engineID, show snmp group, show snmp retries, show snmp timeout, show snmp user, show snmp usertogroup, show snmp view, snmp-server community, snmp-server engineID, snmp-server group, snmp-server remote-user, snmp-server user, snmp-server view

Related Commands - SNMP trap configuration

set port trap, set snmp trap enable | disable auth, set snmp trap enable | disable frame-relay, show port trap, show snmp, snmp trap link-status, snmp-server enable notifications, snmp-server host, snmp-server informs

Related Commands - Dynamic trap manager

snmp-server dynamic-trap-manager

set snmp community

Use the **`set snmp community`** command to set or modify the media gateway's SNMP community strings.

Syntax

`set snmp community {read-only | read-write} [`*`community_string`*`]`

Parameters

Parameter	Description	Possible Values	Default Value
`read-only`	Keyword specifying the read-only access level		
`read-write`	Keyword specifying the read-write access level		
`community_string`	Specifies the name of the SNMP community. If no community string is specified, the community string configured for the specified access type is cleared.		

User Level

read-write

Context

general

Example

To set the read-only community string to read:

```
G450-001(super)# set snmp community read-only read
SNMP read-only community string set
```

Related Commands - SNMP access configuration

ip snmp, set snmp retries, set snmp timeout, show snmp, show snmp engineID, show snmp group, show snmp retries, show snmp timeout, show snmp user, show snmp usertogroup, show snmp view, snmp-server community, snmp-server engineID, snmp-server group, snmp-server remote-user, snmp-server user, snmp-server view

Related Commands - SNMP trap configuration

set port trap, set snmp trap enable | disable auth, set snmp trap enable | disable frame-relay, show port trap, show snmp, snmp trap link-status, snmp-server enable notifications, snmp-server host, snmp-server informs

Related Commands - Dynamic trap manager

snmp-server dynamic-trap-manager

---

set snmp retries

Use the **set snmp retries** command to set the number of times to attempt to communicate with a particular node.

Syntax

set snmp retries *number*

Parameters

Parameter	Description	Possible Values	Default Value
number	The number of retry attempts to make	**1-100000**	

User Level

read-write

Context

general

Example

To set the system to make 100 retry attempts:

```
G450-001(super)# set snmp retries 100
```

Related Commands - SNMP access configuration

ip snmp, set snmp community, set snmp timeout, show snmp, show snmp engineID, show snmp group, show snmp retries, show snmp timeout, show snmp user, show snmp usertogroup, show snmp view, snmp-server community, snmp-server engineID, snmp-server group, snmp-server remote-user, snmp-server user, snmp-server view

Related Commands - SNMP trap configuration

set port trap, set snmp trap enable | disable auth, set snmp trap enable | disable frame-relay, show port trap, show snmp, snmp trap link-status, snmp-server enable notifications, snmp-server host, snmp-server informs

set snmp timeout

Use the **set snmp timeout** command to specify the time to wait for a response before retrying the communication.

Syntax

set snmp timeout *time*

Parameters

Parameter	Description	Possible Values	Default Value
time	The number of seconds to wait	**1-100000**	

User Level

read-write

Context

general

Example

To set the system to wait 60 seconds before retrying communications:

```
G450-001(super)# set snmp timeout 60
```

Related Commands - SNMP access configuration

ip snmp, set snmp community, set snmp retries, show snmp, show snmp engineID, show snmp group, show snmp retries, show snmp timeout, show snmp user, show snmp usertogroup, show snmp view, snmp-server community, snmp-server engineID, snmp-server group, snmp-server remote-user, snmp-server user, snmp-server view

Related Commands - SNMP trap configuration

set port trap, set snmp trap enable | disable auth, set snmp trap enable | disable frame-relay, show port trap, show snmp, snmp trap link-status, snmp-server enable notifications, snmp-server host, snmp-server informs

show snmp

Use the **show snmp** command to display SNMP configuration information.

Syntax

show snmp

User Level

read-only

Context

general

Example

To display SNMP configuration information:

```
G450-001(super)# show snmp

Authentication trap disabled

Community-Access     Community-String
----------------     ----------------
read-only            *****
read-write           *****
```

```
SNMPv3 Notification Status
--------------------------
Traps: Enabled
Informs: Enabled          Retries: 3    Timeout: 3 seconds

SNMP-Rec-Address Model  Level   Notification   Trap/Inform   User name
---------------- -----  ------   ------------   -----------  ----------
149.49.70.137     v1     noauth   all               trap       ReadCommN
 UDP port: 162 DM
```

Related Commands - SNMP access configuration

ip snmp, set snmp community, set snmp retries, set snmp timeout, show snmp engineID, show snmp group, show snmp retries, show snmp timeout, show snmp user, show snmp usertogroup, show snmp view, snmp-server community, snmp-server engineID, snmp-server group, snmp-server remote-user, snmp-server user, snmp-server view

Related Commands - SNMP trap configuration

set port trap, set snmp trap enable | disable auth, set snmp trap enable | disable frame-relay, show port trap, show snmp, snmp trap link-status, snmp-server enable notifications, snmp-server host, snmp-server informs

Related Commands - Dynamic trap manager

snmp-server dynamic-trap-manager

---

show snmp engineID

Use the **show snmp engineID** command to display the SNMP engine ID for the G450.

Syntax

show snmp engineid

User Level

admin

Context

general

Example

To display the SNMP engine ID:

```
G450-001(super)# show snmp engineid
EngineId: 00:00:00:09:00:d0:00:4c:18:00
Engine Boots: 1234455
```

Related Commands - SNMP access configuration

ip snmp, set snmp community, set snmp retries, set snmp timeout, show snmp, show snmp group, show snmp retries, show snmp timeout, show snmp user, show snmp usertogroup, show snmp view, snmp-server community, snmp-server engineID, snmp-server group, snmp-server remote-user, snmp-server user, snmp-server view

Related Commands - SNMP trap configuration

set port trap, set snmp trap enable | disable auth, set snmp trap enable | disable frame-relay, show port trap, show snmp, snmp trap link-status, snmp-server enable notifications, snmp-server host, snmp-server informs

Related Commands - Dynamic trap manager

snmp-server dynamic-trap-manager

---

show snmp group

Use the **show snmp group** command to display configuration information about the SNMP groups or about a specified SNMP group.

Syntax

show snmp group [*group-name*]

User Level

admin

Context

general

Parameters

Parameter	Description	Possible Values	Default Value
group-name	The name of a specific SNMP group		

Example

To display configuration information for the ReadCommG SNMP group:

```
G450-001(super)# show snmp group readcommg
Group Name: ReadCommG
Security Model: v1
Security Level: noauth
Read View: snmpv1View
Write View:
Notify View: snmpv1View
```

Related Commands - SNMP access configuration

ip snmp, set snmp community, set snmp retries, set snmp timeout, show snmp, show snmp engineID, show snmp retries, show snmp timeout, show snmp user, show snmp usertogroup, show snmp view, snmp-server community, snmp-server engineID, snmp-server group, snmp-server remote-user, snmp-server user, snmp-server view

Related Commands - SNMP trap configuration

set port trap, set snmp trap enable | disable auth, set snmp trap enable | disable frame-relay, show port trap, show snmp, snmp trap link-status, snmp-server enable notifications, snmp-server host, snmp-server informs

Related Commands - Dynamic trap manager

snmp-server dynamic-trap-manager

---

show snmp retries

Use the **show snmp retries** command to display the number of retry attempts to make when attempting to communicate with a node.

Syntax

show snmp retries

User Level

read-only

Context

general

Example

To display the number of retry attempts:

```
G450-001(super)# show snmp retries
the SNMP Retries Number is 100
```

Related Commands - SNMP access configuration

ip snmp, set snmp community, set snmp retries, set snmp timeout, show snmp, show snmp engineID, show snmp group, show snmp timeout, show snmp user, show snmp usertogroup, show snmp view, snmp-server community, snmp-server engineID, snmp-server group, snmp-server remote-user, snmp-server user, snmp-server view

Related Commands - SNMP trap configuration

set port trap, set snmp trap enable | disable auth, set snmp trap enable | disable frame-relay, show port trap, show snmp, snmp trap link-status, snmp-server enable notifications, snmp-server host, snmp-server informs

show snmp timeout

Use the **show snmp timeout** command to display the time to wait before resending a communication.

Syntax

show snmp timeout

User Level

read-only

Context

general

Example

To display the timeout value:

```
G450-001(super)# show snmp timeout
the SNMP Timeout is 60
```

Related Commands - SNMP access configuration

ip snmp, set snmp community, set snmp retries, set snmp timeout, show snmp, show snmp engineID, show snmp group, show snmp retries, show snmp user, show snmp usertogroup, show snmp view, snmp-server community, snmp-server engineID, snmp-server group, snmp-server remote-user, snmp-server user, snmp-server view

Related Commands - SNMP trap configuration

set port trap, set snmp trap enable | disable auth, set snmp trap enable | disable frame-relay, show port trap, show snmp, snmp trap link-status, snmp-server enable notifications, snmp-server host, snmp-server informs

show snmp user

Use the **show snmp user** command to display configuration information for all SNMP users or for a specified SNMP user.

Syntax

show snmp user [*username*]

Parameters

Parameter	Description	Possible Values	Default Value
username	The username of the user whose information you wish to display		

User Level

admin

Context

general

Example

To display configuration information for SNMP user john:

```
G450-001(super)# show snmp user john

EngineId: 00:11:22:33:44
User Name: john
Authentication Protocol: md5
Privacy Protocol: des56
Group for Security Model v1:  RestrictedGroup
Group for Security Model v2:  RestrictedGroup
Group for Security Model v3:  RestrictedGroup
Storage Type: volatile
Row status: active
```

Related Commands - SNMP access configuration

ip snmp, set snmp community, set snmp retries, set snmp timeout, show snmp, show snmp engineID, show snmp group, show snmp retries, show snmp timeout, show snmp usertogroup, show snmp view, snmp-server community, snmp-server engineID, snmp-server group, snmp-server remote-user, snmp-server user, snmp-server view

Related Commands - SNMP trap configuration

set port trap, set snmp trap enable | disable auth, set snmp trap enable | disable frame-relay, show port trap, show snmp, snmp trap link-status, snmp-server enable notifications, snmp-server host, snmp-server informs

Related Commands - Dynamic trap manager

snmp-server dynamic-trap-manager

show snmp usertogroup

Use the **show snmp usertogroup** command to show the mapping table between SNMPv3 users and groups.

Syntax

show snmp usertogroup [*username*]

Parameters

Parameter	Description	Possible Values	Default Value
username	Specifies an SNMPv3 username		

User Level

admin

Context

general

Example

To show the mapping table between SNMPv3 users and groups:

```
G450-001(super)# show snmp usertogroup

Security Model: v1
```

```
Security Name: WriteCommN
Group Name: WriteCommG
Security Model: v2c
Security Name: ReadCommN
Group Name: ReadCommG
Security Model: v2c
Security Name: WriteCommN
Group Name: WriteCommG
```

Related Commands - SNMP access configuration

ip snmp, set snmp community, set snmp retries, set snmp timeout, show snmp, show snmp engineID, show snmp group, show snmp retries, show snmp timeout, show snmp user, show snmp view, snmp-server community, snmp-server engineID, snmp-server group, snmp-server remote-user, snmp-server user, snmp-server view

Related Commands - SNMP trap configuration

set port trap, set snmp trap enable | disable auth, set snmp trap enable | disable frame-relay, show port trap, show snmp, snmp trap link-status, snmp-server enable notifications, snmp-server host, snmp-server informs

Related Commands - Dynamic trap manager

snmp-server dynamic-trap-manager

---

show snmp view

Use the **show snmp view** command to display configuration information for all SNMP views or for a specific SNMP view.

Syntax

show snmp view [*view-name*]

Parameters

Parameter	Description	Possible Values	Default Value
view-name	Specifies the view name		

User Level

admin

Context

general

Example

To display configuration information for all SNMP views:

```
G450-001(super)# show snmp view
View Name: iso
Subtree Oid: 1
Subtree Mask:
View Type: include
Storage Type: nonVolatile
Status: active
```

Related Commands - SNMP access configuration

ip snmp, set snmp community, set snmp retries, set snmp timeout, show snmp, show snmp engineID, show snmp group, show snmp retries, show snmp timeout, show snmp user, show snmp usertogroup, snmp-server community, snmp-server engineID, snmp-server group, snmp-server remote-user, snmp-server user, snmp-server view

Related Commands - SNMP trap configuration

set port trap, set snmp trap enable | disable auth, set snmp trap enable | disable frame-relay, show port trap, show snmp, snmp trap link-status, snmp-server enable notifications, snmp-server host, snmp-server informs

Related Commands - Dynamic trap manager

snmp-server dynamic-trap-manager

snmp-server community

Use the **snmp-server community** command to enable read-only and read-write access to SNMP services via community strings. Use the **no** form of the command to prevent access to SNMP services using community strings. By default, community string access is enabled.

Syntax

[no] snmp-server community read-only *community-name* read-write *community-name*

Parameters

Parameter	Description	Possible Values	Default Value
community-name	Assigns a read-only or read-write community string		

User Level

admin

Context

general

Example

To enable read-only access to SNMP services via the read-com community string and read-write access to SNMP services via the write-com community string:

```
G450-001(super)# snmp-server community read-only read-com read-write write-com
```

Related Commands - SNMP access configuration

ip snmp, set snmp community, set snmp retries, set snmp timeout, show snmp, show snmp engineID, show snmp group, show snmp retries, show snmp timeout, show snmp user, show snmp usertogroup, show snmp view, snmp-server engineID, snmp-server group, snmp-server remote-user, snmp-server user, snmp-server view

Related Commands - SNMP trap configuration

set port trap, set snmp trap enable | disable auth, set snmp trap enable | disable frame-relay, show port trap, show snmp, snmp trap link-status, snmp-server enable notifications, snmp-server host, snmp-server informs

Related Commands - Dynamic trap manager

snmp-server dynamic-trap-manager

snmp-server engineID

Use the **`snmp-server engineID`** command to specify the SNMP Engine ID for the G450. Use the **`no`** form of the command to return the device to its default Engine ID.

Note:

The SNMP Engine ID must be unique for all devices on the network.

Note:

When you change the SNMP Engine ID, all users other than the default user are invalidated and must be redefined.

Note:

When the IP address of the G450 changes, the SNMP Engine ID is automatically changed.

Syntax

snmp-server engineID *engineID*

no snmp-server engineID

Parameters

Parameter	Description	Possible Values	Default Value
engineID	12 byte hexadecimal string, with each byte separated by a colon. For example, 00:00:00:81:0a:fe:ff:12:97:33:45:12.		

User Level

admin

Context

general

Example

To specify SNMP Engine 00:02:00:81:00:d0:00:4c:18:00 for the G450:

```
G450-001(super)# snmp-server engineid 00:02:00:81:00:d0:00:4c:18:00
```

Related Commands - SNMP access configuration

ip snmp, set snmp community, set snmp retries, set snmp timeout, show snmp, show snmp engineID, show snmp group, show snmp retries, show snmp timeout, show snmp user, show snmp usertogroup, show snmp view, snmp-server community, snmp-server group, snmp-server remote-user, snmp-server user, snmp-server view

Related Commands - SNMP trap configuration

set port trap, set snmp trap enable | disable auth, set snmp trap enable | disable frame-relay, show port trap, show snmp, snmp trap link-status, snmp-server enable notifications, snmp-server host, snmp-server informs

Related Commands - Dynamic trap manager

snmp-server dynamic-trap-manager

snmp-server group

Use the **snmp-server group** command to define a new SNMPv3 group, or to configure settings for the group. An SNMP group associates users with views. Use the **no** form of the command to remove the specified group.

Note:

If you use the **no** form of the command with no additional parameters, all instances of the specified group are removed. If you specify a particular security group, only that group instance is removed.

Syntax

snmp-server group *groupname* {v1|v2c|{v3 *level*}} [read *read-view*] [write *write-view*] [notify *notify-view*]

no snmp-server group groupname [v1|v2c|{v3 *level*}]

Parameters

Parameter	Description	Possible Values	Default Value
groupname	A character string specifying the group name	A string of up to 32 characters	
v1	Keyword indicating that the group is limited to SNMP v1 functionality		
v2c	Keyword indicating that the group is limited to SNMP v2c functionality		
v3	Keyword indicating that the group has full SNMP v3 functionality. This is the default.		
level	The group's level of authentication	**auth** – the group authenticates packets **noauth** – the group does not authenticate packets **priv** – the group authenticates and encrypts packets	**noauth**

Parameter	Description	Possible Values	Default Value
read-view	A character string specifying the view name for the read view. Users of this group have read access to the set of MIB objects specified in the read view. If no view is specified, the default is an empty view.	A string of up to 64 characters	
write-view	A character string specifying the view name for the write view. Users of this group have write access to the set of MIB objects specified in the write view. If no view is specified, the default is an empty view.	A string of up to 64 characters	
notify-view	A character string specifying the view name for the notify view. Users of this group have notify access to the set of MIB objects specified in the notify view. If no view is specified, the default is an empty view.	A string of up to 64 characters	

User Level

admin

Context

general

Example

To define or edit SNMPv3 group 12groupRO to authenticate packets with read view view1, write view notify, and notify view view2:

```
G450-001(super)# snmp-server group 12groupRO v3 auth read view1 notify view2
```

Related Commands - SNMP access configuration

ip snmp, set snmp community, set snmp retries, set snmp timeout, show snmp, show snmp engineID, show snmp group, show snmp retries, show snmp timeout, show snmp user, show snmp usertogroup, show snmp view, snmp-server community, snmp-server engineID, snmp-server remote-user, snmp-server user, snmp-server view

Related Commands - SNMP trap configuration

set port trap, set snmp trap enable | disable auth, set snmp trap enable | disable frame-relay, show port trap, show snmp, snmp trap link-status, snmp-server enable notifications, snmp-server host, snmp-server informs

Related Commands - Dynamic trap manager

snmp-server dynamic-trap-manager

snmp-server remote-user

Use the **snmp-server remote-user** command to configure settings for a remote SNMPv3 user. If the user does not exist, it is created. Use the **no** form of the command to remove the user from specific groups. If no groups are specified, the user is removed from all groups.

Syntax

snmp-server remote-user *username engineID groupname* [auth {md5|sha} *auth-password* [priv des56 *priv-password*]]

no snmp-server remote-user *username* [*groupname*]

Parameters

Parameter	Description	Possible Values	Default Value
username	A character string specifying the username of this user	A string of up to 32 characters	
engineID	The remote device Engine ID for this user		
groupname	A character string specifying the groupname this user is associated with	A string of up to 32 characters	
md5	Keyword specifying to use the MAC-MD5-96 authentication protocol		
sha	Keyword specifying to use the HMAC-SHA-96 authentication protocol		
auth-password	A character string no longer than 64 characters specifying the authentication password. An authentication password is required if the auth keyword is used. The minimum length is 8 characters.		
priv-password	A character string no longer than 64 characters specifying the privacy password. The minimum length is 8 characters.		

User Level

admin

Context

general

Example

To create or configure a remote SNMPv3 user, with username john, associated with group L2Group, and accessing engine `00:02:00:81:00:d0:00:4c:18:00`:

```
G450-001(super)# snmp-server remote-user john  00:02:00:81:00:d0:00:4c:18:00
L2Group
```

Related Commands - SNMP access configuration

ip snmp, set snmp community, set snmp retries, set snmp timeout, show snmp, show snmp engineID, show snmp group, show snmp retries, show snmp timeout, show snmp user, show snmp usertogroup, show snmp view, snmp-server community, snmp-server engineID, snmp-server group, snmp-server user, snmp-server view

Related Commands - SNMP trap configuration

set port trap, set snmp trap enable | disable auth, set snmp trap enable | disable frame-relay, show port trap, show snmp, snmp trap link-status, snmp-server enable notifications, snmp-server host, snmp-server informs

Related Commands - Dynamic trap manager

snmp-server dynamic-trap-manager

---

snmp-server user

Use the **snmp-server user** command to configure settings for an SNMPv3 user. If the user does not exist, it is created. Use the **no** form of the command to remove the user from specific groups. If no groups are specified, the user is removed from all groups.

Syntax

snmp-server user *username groupname* {{v1|v2c}|{v3 [auth {md5|sha} *auth-password* [priv des56 *priv-password*]]}}

no snmp-server user *username* [*groupname* {v1|v2c|v3}]]

Parameters

Parameter	Description	Possible Values	Default Value
username	A character string specifying the username of this user	A string of up to 32 characters	
groupname	A character string specifying the groupname this user is associated with	A string of up to 32 characters	
v1	Keyword specifying that the user is authorized for SNMP v1 functionality in the specified group		
v2c	Keyword specifying that the user is authorized for SNMP v2c functionality in the specified group		
v3	Keyword specifying that the user is authorized for SNMP v3 functionality in the specified group		
md5	Keyword specifying to use the MAC-MD5-96 authentication protocol		
sha	Keyword specifying to use the HMAC-SHA-96 authentication protocol		
auth-password	A character string specifying the authentication password. An authentication password is required if the auth keyword is used. The minimum length is 8 characters.	A string of between 8 and 64 characters	
priv-password	A character string specifying the privacy password. The minimum length is 8 characters.	A string of between 8 and 64 characters	

User Level

admin

Context

general

Example

To configure settings for an SNMPv3 user with username john and groupname L2Group, authorized for SNMP v3 functionality, using the MAC-MD5-96 authentication protocol, with authentication password katmandu and privacy password uktanatan:

```
G450-001(super)# snmp-server user john L2Group v3 auth md5 katmandu  priv des56
uktanatan
```

Related Commands - SNMP access configuration

ip snmp, set snmp community, set snmp retries, set snmp timeout, show snmp, show snmp engineID, show snmp group, show snmp retries, show snmp timeout, show snmp user, show snmp usertogroup, show snmp view, snmp-server community, snmp-server engineID, snmp-server group, snmp-server remote-user, snmp-server view

Related Commands - SNMP trap configuration

set port trap, set snmp trap enable | disable auth, set snmp trap enable | disable frame-relay, show port trap, show snmp, snmp trap link-status, snmp-server enable notifications, snmp-server host, snmp-server informs

snmp-server view

Use the **snmp-server view** command to configure settings for an SNMP MIB view. If the view does not exist, it is created. An MIB view specifies a particular section or subsection of the MIB tree. You can create a view that includes a particular subsection, or excludes one. Use the **no** form of the command to delete the current view.

Syntax

snmp-server view ***view-name oid-subtree*** **{included|excluded}**

no snmp-server view ***view-name*** **[*oid-subtree*]**

Parameters

Parameter	Description	Possible Values	Default Value
view-name	The name of the view		
oid-subtree	The object identifier subtree to be included in or excluded from this view. Oid-subtree is specified as a series of period-separated numbers. In order to include a subtree family, use an asterisk as a wildcard character. Symbolic MIB object names are not supported.		
included	Keyword indicating that the view includes the specified subtree (this is the default)		
excluded	Keyword indicating that the view excludes the specified subtree		

User Level

admin

Context

general

Example

To configure settings for an SNMP MIB view named internet including Oidtree 1.3.6.1:

```
G450-001(super)# snmp-server view internet 1.3.6.1 included
```

Related Commands - SNMP access configuration

ip snmp, set snmp community, set snmp retries, set snmp timeout, show snmp, show snmp engineID, show snmp group, show snmp retries, show snmp timeout, show snmp user, show snmp usertogroup, show snmp view, snmp-server community, snmp-server engineID, snmp-server group, snmp-server remote-user, snmp-server user

Related Commands - SNMP trap configuration

set port trap, set snmp trap enable | disable auth, set snmp trap enable | disable frame-relay, show port trap, show snmp, snmp trap link-status, snmp-server enable notifications, snmp-server host, snmp-server informs

Related Commands - Dynamic trap manager

snmp-server dynamic-trap-manager

SNMP trap configuration

set port trap

Use the **`set port trap`** command to enable or disable generic SNMP uplink or downlink traps from a port.

Syntax

`set port trap` ***`module/port`*** **{`enable`|`disable`}**

Parameters

Parameter	Description	Possible Values	Default Value
module	Number of the module		
port	Number of the port on the module. You can also specify a range of ports separated by a dash, for example, 10/5-6 for both ETH LAN ports 5-6 on the front panel.		
enable	Keyword specifying to enable uplink/ downlink traps		
disable	Keyword specifying to disable uplink/ downlink traps		

User Level

read-write

Context

general

Example

To enable uplink and downlink traps for port 6/5 on the G450:

```
G450-001(super)# set port trap 6/5 enable
Port 6/5 up/down trap enabled.
```

Related Commands - SNMP access configuration

ip snmp, set snmp community, set snmp retries, set snmp timeout, show snmp, show snmp engineID, show snmp group, show snmp retries, show snmp timeout, show snmp user, show snmp usertogroup, show snmp view, snmp-server community, snmp-server engineID, snmp-server group, snmp-server remote-user, snmp-server user, snmp-server view

Related Commands - SNMP trap configuration

set snmp trap enable | disable auth, set snmp trap enable | disable frame-relay, show port trap, show snmp, snmp trap link-status, snmp-server enable notifications, snmp-server host, snmp-server informs

Related Commands - Dynamic trap manager

snmp-server dynamic-trap-manager

set snmp trap enable | disable auth

Use the **set snmp trap enable|disable auth** command to enable or disable SNMP authentication failure traps for all managers.

Syntax

set snmp trap {enable|disable} auth

User Level

read-write

Context

general

Related Commands - SNMP access configuration

ip snmp, set snmp community, set snmp retries, set snmp timeout, show snmp, show snmp engineID, show snmp group, show snmp retries, show snmp timeout, show snmp user, show snmp usertogroup, show snmp view, snmp-server community, snmp-server engineID, snmp-server group, snmp-server remote-user, snmp-server user, snmp-server view

Related Commands - SNMP trap configuration

set port trap, set snmp trap enable | disable frame-relay, show port trap, show snmp, snmp trap link-status, snmp-server enable notifications, snmp-server host, snmp-server informs

set snmp trap enable | disable frame-relay

Use the **set snmp trap enable|disable frame-relay** command to enable or disable Frame Relay DLCI link status-change traps for all managers.

Syntax

set snmp trap {enable|disable} frame-relay

User Level

read-write

Context

general

Related Commands - SNMP access configuration

ip snmp, set snmp community, set snmp retries, set snmp timeout, show snmp, show snmp engineID, show snmp group, show snmp retries, show snmp timeout, show snmp user, show snmp usertogroup, show snmp view, snmp-server community, snmp-server engineID, snmp-server group, snmp-server remote-user, snmp-server user, snmp-server view

Related Commands - SNMP trap configuration

set port trap, set snmp trap enable | disable auth, show port trap, show snmp, snmp trap link-status, snmp-server enable notifications, snmp-server host, snmp-server informs

show port trap

Use the **show port trap** command to display information on SNMP generic link up/down traps sent for a specific port. If no port is specified, information for all ports is displayed.

Syntax

show port trap [***module***[/***port***]]

Parameters

Parameter	Description	Possible Values	Default Value
module	Number of the module		
port	Number of the port on the module. You can also specify a range of ports separated by a dash, for example, 10/5-6 for both ETH LAN ports 5-6 on the front panel.		

User Level

read-only

Context

general

Example

To display trap information for port 6/5:

```
G450-001(super)# show port trap 6/5
Port 6/5 up/down trap is disabled
```

Related Commands - SNMP access configuration

ip snmp, set snmp community, set snmp retries, set snmp timeout, show snmp, show snmp engineID, show snmp group, show snmp retries, show snmp timeout, show snmp user, show snmp usertogroup, show snmp view, snmp-server community, snmp-server engineID, snmp-server group, snmp-server remote-user, snmp-server user, snmp-server view

Related Commands - SNMP trap configuration

set port trap, set snmp trap enable | disable auth, set snmp trap enable | disable frame-relay, show snmp, snmp trap link-status, snmp-server enable notifications, snmp-server host, snmp-server informs

---

show snmp

Use the **show snmp** command to display SNMP configuration information.

Syntax

show snmp

User Level

read-only

Context

general

Example

To display SNMP configuration information:

```
G450-001(super)# show snmp

 Community-Access     Community-String
 read-only            public
 read-write           private
 trap                 secret

 Trap-Rec-Addr            Status     Traps configured

 SNMPv3 Notifications Status
 Traps: Disabled
 Informs: Disabled      Retries: 3   Timeout: 3 seconds
```

```
SNMP Rec-Addr       Mode    Level     Notification    Trap/     User
                    l                                 Inform    Name
129.22.22.22        v1      noauth    all             trap      ReadCommN
UDP port: 162 DM
129.11.33.44        v2c     noauth    all             inform    WriteCommN
UDP port: 162
```

Related Commands - SNMP access configuration

ip snmp, set snmp community, set snmp retries, set snmp timeout, show snmp, show snmp engineID, show snmp group, show snmp retries, show snmp timeout, show snmp user, show snmp usertogroup, show snmp view, snmp-server community, snmp-server engineID, snmp-server group, snmp-server remote-user, snmp-server user, snmp-server view

Related Commands - SNMP trap configuration

set port trap, set snmp trap enable | disable auth, set snmp trap enable | disable frame-relay, show port trap, snmp trap link-status, snmp-server enable notifications, snmp-server host, snmp-server informs

Related Commands - Dynamic trap manager

snmp-server dynamic-trap-manager

---

snmp trap link-status

Use the **snmp trap link-status** command to enable Link Up and Link Down traps. Use the **no** form of this command to restore the default value, interface traps deactivated.

Syntax

[no] snmp trap link-status

User Level

read-write

Context

Interface: Console, Serial (DS1 PPP L2, DS1 PPP L2-L3, DS1 FR L2, DS1 FR-SUB L2, DS1 FR-SUB L2-L3, USP PPP L2, USP PPP L2-L3, USP FR L2), FastEthernet (L2, L2-L3, PPP L2, PPP L2-L3), Tunnel (L2, L2-L3), Dialer (L2, L2-L3), USB-modem

Example

To enable Link Up and Link Down traps:

```
G450-001(super-if:FastEthernet 10/2)# snmp trap link-status
```

Related Commands - SNMP access configuration

ip snmp, set snmp community, set snmp retries, set snmp timeout, show snmp, show snmp engineID, show snmp group, show snmp retries, show snmp timeout, show snmp user, show snmp usertogroup, show snmp view, snmp-server community, snmp-server engineID, snmp-server group, snmp-server remote-user, snmp-server user, snmp-server view

Related Commands - SNMP trap configuration

set port trap, set snmp trap enable | disable auth, set snmp trap enable | disable frame-relay, show port trap, show snmp, snmp-server enable notifications, snmp-server host, snmp-server informs

snmp-server enable notifications

Use the **snmp-server enable notifications** command to enable the sending of all traps and informs from the G450. Use the **no** form of the command to disable the sending of all traps and informs from the G450.

Note:

This command overrides the enabling of individual notifications using the **snmp-server host** command.

Syntax

[no] snmp-server enable notifications

User Level

admin

Context

general

Example

To enable the sending of all traps and informs from the G450:

```
G450-001(super)# snmp-server enable notifications
```

Related Commands - SNMP access configuration

ip snmp, set snmp community, set snmp retries, set snmp timeout, show snmp, show snmp engineID, show snmp group, show snmp retries, show snmp timeout, show snmp user, show snmp usertogroup, show snmp view, snmp-server community, snmp-server engineID, snmp-server group, snmp-server remote-user, snmp-server user, snmp-server view

Related Commands - SNMP trap configuration

set port trap, set snmp trap enable | disable auth, set snmp trap enable | disable frame-relay, show port trap, show snmp, snmp trap link-status, snmp-server host, snmp-server informs

Related Commands - Dynamic trap manager

snmp-server dynamic-trap-manager

---

snmp-server host

Use the **snmp-server host** command to identify an SNMP management server, and specify the kind of messages it receives. Use the **no** form of the command to remove the specified server, or to disable a particular set of notification types.

Note:

If you use the **no snmp-server host** command without a notification type list, all notification types are disabled.

Syntax

snmp-server host *host_address* {**traps** | **informs**} {{{**v1** | **v2c**} *community-name*} | {**v3** *level username*}} [**udp-port** *port*] [*notification-list*]

no snmp-server host *host_address* [{**traps**|**informs**} *notification-list*]

Parameters

Parameter	Description	Possible Values	Default Value
host_address	The IP address of the SNMP host		
traps	Keyword specifying to send traps to this host (messages not requiring acknowledgement). This is the default.		
informs	Keyword specifying to send informs to this host (messages requiring acknowledgement)		
v1	Keyword specifying to use SNMP v1 functionality with this host		

Parameter	Description	Possible Values	Default Value
v2c	Keyword specifying to use SNMP v2c functionality with this host		
community-name	The community string to use to connect to the specified host (for v1 or v2c)		
v3	Keyword specifying to use SNMP v3 functionality with this host		
level	The level of authentication to apply to messages to this host	**auth** – authenticate messages to this host **noauth** – do not authenticate messages to this host **priv** – authenticate and encrypt messages to this host	**noauth**
username	The username to use for authentication on the specified host		
port	Which port of the target host to use		**162**

Parameter	Description	Possible Values	Default Value
notification-list	List of notification types that are enabled for this host	**all** — all traps **generic** — generic traps **hardware** — hardware faults **rmon** — RMON rising/falling alarm **dhcp server** — DHCP server error **dhcp-clients** — DHCP client error **rtp-stat-faults** — RTP statistics: QoS fault/clear traps **rtp-stat-qos** — RTP statistics: end-of-call QoS traps **wan** — WAN router traps **media-gateway** — media gateway traps **security** — security traps **config** — configuration change notifications **eth-port-faults** — notifications of Ethernet port faults **sw-redundancy** — software redundancy notifications **temperature** — temperature warning notifications **cam-change** — notifications about changes in CAM **l3-events** — notifications about L3 faults (duplicate IP, VLAN violations) **lag-event** — notifications about link aggregation faults and configuration changes **policy** — notifications about changes in policy (for L3 devices) **link-faults** — link-down notifications **supply** — power supply notifications	**all**

User Level

admin

Context

general

Example

To identify an SNMP management server with host 10.1.2.4, connecting through udp-port 789, sending informs to its host using v3 SNMP functionality, authenticating messages with the username John, and having generic traps and configuration change notifications enabled:

```
G450-001(super)# snmp-server host 10.1.2.4 informs v3 auth John udp-port 789
config generic
```

Related Commands - SNMP access configuration

ip snmp, set snmp community, set snmp retries, set snmp timeout, show snmp, show snmp engineID, show snmp group, show snmp retries, show snmp timeout, show snmp user, show snmp usertogroup, show snmp view, snmp-server community, snmp-server engineID, snmp-server group, snmp-server remote-user, snmp-server user, snmp-server view

Related Commands - SNMP trap configuration

set port trap, set snmp trap enable | disable auth, set snmp trap enable | disable frame-relay, show port trap, show snmp, snmp trap link-status, snmp-server enable notifications, snmp-server informs

Related Commands - Dynamic trap manager

snmp-server dynamic-trap-manager

---

snmp-server informs

Use the **snmp-server informs** command to configure settings for SNMP inform messages.

Syntax

snmp-server informs retries *retries-num* timeout *timeout*

Parameters

Parameter	Description	Possible Values	Default Value
retries-num	The maximum number of times to resend an inform message	**0-255**	**3**
timeout	The number of seconds to wait for an acknowledgement before resending an inform message	**1-65536**	**3**

User Level

admin

Context

general

Example

To configure a maximum of 5 retries and a 3 second timeout for SNMP inform messages:

```
G450-001(super)# snmp-server informs retries 5 timeout 3
```

Related Commands - SNMP access configuration

ip snmp, set snmp community, set snmp retries, set snmp timeout, show snmp, show snmp engineID, show snmp group, show snmp retries, show snmp timeout, show snmp user, show snmp usertogroup, show snmp view, snmp-server community, snmp-server engineID, snmp-server group, snmp-server remote-user, snmp-server user, snmp-server view

Related Commands - SNMP trap configuration

set port trap, set snmp trap enable | disable auth, set snmp trap enable | disable frame-relay, show port trap, show snmp, snmp trap link-status, snmp-server enable notifications, snmp-server host

Related Commands - Dynamic trap manager

snmp-server dynamic-trap-manager

Spanning tree

set port edge admin state

Use the **set port edge admin state** command to assign or de-assign RSTP edge-port admin state to a port for Rapid Spanning Tree Protocol (RSTP) treatment.

Syntax

set port edge admin state *module/port admin_state*

Parameters

Parameter	Description	Possible Values	Default Value
module	Number of the module		
port	Number of the port on the module. You can also specify a range of ports separated by a dash, for example, 10/5-6 for both ETH LAN ports 5-6 on the front panel.		
admin_state	The type of the specified port	**edge-port**, **non-edge-port**	

User Level

read-write

Context

general

Example

To specify that port 6/5 is an edge port:

```
G450-001(super)# set port edge admin state 6/5 edge-port
```

Related Commands

set port auto-negotiation-flowcontrol-advertisement, set port duplex, set port enable | disable, set port flowcontrol, set port level, set port name, set port negotiation, set port point-to-point admin status, set port speed, show port auto-negotiation-flowcontrol-advertisement, show port edge state, show port flowcontrol

set port point-to-point admin status

Use the **set port point-to-point admin status** command to manage the connection type of the port.

Syntax

set port point-to-point admin status *module/port admin_status*

Parameters

Parameter	Description	Possible Values	Default Value
module	Number of the module		
port	Number of the port on the module. You can also specify a range of ports separated by a dash, for example, 10/5-6 for both ETH LAN ports 5-6 on the front panel.		
admin_status	The connection type of the port	**force-true** — specify that the port is connected point-to-point **force-false** — specify that this port is shared media **auto** — try to automatically detect the connection type of the port	

User Level

read-write

Context

general

Example

To specify that the connection type of port 6/5 is automatically detected:

```
G450-001(super)# set port point-to-point admin status 6/5 auto
```

Related Commands

set port auto-negotiation-flowcontrol-advertisement, set port enable | disable, set port duplex, set port edge admin state, set port enable | disable, set port flowcontrol, set port level, set port name, set port negotiation, set port speed, show port auto-negotiation-flowcontrol-advertisement, show port edge state, show port flowcontrol

set port spantree

Use the **set port spantree** command to enable or disable spanning tree for specific ports.

Syntax

set port spantree {enable|disable} [*module/port*]

Parameters

Parameter	Description	Possible Values	Default Value
enable	Keyword specifying to enable spanning tree mode		
disable	Keyword specifying to disable spanning tree mode		
module	The module number		
port	The port number		

User Level

read-write

Context

general

Example

To enable spanning tree on port 6/5:

```
G450-001(super)# set port spantree enable 6/5
port 6/5 was enabled on spantree
```

Related Commands

set port spantree cost, set port spantree force-protocol-migration, set port spantree priority, set spantree default-path-cost, set spantree enable | disable, set spantree forward-delay, set spantree hello-time, set spantree max-age, set spantree priority, set spantree tx-hold-count, set spantree version, show spantree

set port spantree cost

Use the **`set port spantree cost`** command to set the spanning tree cost of a port. This value defines which port is allowed to forward traffic if two ports with different costs cause a loop.

Syntax

`set port spantree cost [`*`module/port`*`] [`*`value`*`]`

Parameters

Parameter	Description	Possible Values	Default Value
`module`	The module number		
`port`	The port number		
`value`	Number representing the cost. A lower value specifies precedence of a port to forward traffic.	**1-65535**	

User Level

read-write

Context

general

Example

To set the spanning tree cost of port 6/5 to 4096:

```
G450-001(super)# set port spantree cost 6/5 4096
port 6/5 spantree cost is 4096
```

Related Commands

set port spantree, set port spantree force-protocol-migration, set port spantree priority, set spantree default-path-cost, set spantree enable | disable, set spantree forward-delay, set spantree hello-time, set spantree max-age, set spantree priority, set spantree tx-hold-count, set spantree version, show spantree

set port spantree force-protocol-migration

Use the **`set port spantree force-protocol-migration`** command to force the port to send a rapid spanning tree hello packet (Bridge Protocol Data Unit).

Syntax

`set port spantree force-protocol-migration` ***`module/port`***

Parameters

Parameter	Description	Possible Values	Default Value
`module`	The module number		
`port`	The port number		

User Level

read-write

Context

general

Example

To force port 6/5 to send a hello packet:

```
G450-001(super)# set port spantree force-protocol-migration 6/5
```

Related Commands

set port spantree, set port spantree cost, set port spantree priority, set spantree default-path-cost, set spantree enable | disable, set spantree forward-delay, set spantree hello-time, set spantree max-age, set spantree priority, set spantree tx-hold-count, set spantree version, show spantree

set port spantree priority

Use the **set port spantree priority** command to set the Spanning Tree priority level of a port. This value defines the priority of a port to be blocked in case two ports with the same cost cause a loop.

Syntax

set port spantree priority *module/port value*

Parameters

Parameter	Description	Possible Values	Default Value
module	The module number		
port	The port number		
value	Number representing the priority of the port. 0 is the highest priority. A port with a lower priority will be blocked.	**0-240** (in multiples of 16)	**128**

User Level

read-write

Context

general

Example

To set the priority for port 6/5 to 128:

```
G450-001# set port spantree priority 6/5 128
port 6/5 spantree priority is 128
```

Related Commands

set port spantree, set port spantree cost, set port spantree force-protocol-migration, set spantree default-path-cost, set spantree enable | disable, set spantree forward-delay, set spantree hello-time, set spantree max-age, set spantree priority, set spantree tx-hold-count, set spantree version, show spantree

set spantree default-path-cost

Use the **set spantree default-path-cost** command to set the version of the spanning tree default path cost used by the current bridge.

Syntax

set spantree default-path-cost ***pathcost***

Parameters

Parameter	Description	Possible Values	Default Value
pathcost	The version of the spanning tree default path cost	**common-spanning-tree** - compatible with IEEE802.1D standard **rapid-spanning-tree** - compatible with IEEE802.1W standard	

User Level

read-write

Context

general

Example

To use the rapid-spanning-tree default path cost:

```
G450-001(super)# set spantree default-path-cost rapid-spanning-tree
Spanning tree default path costs is set to rapid spanning tree.
```

Related Commands

set port spantree, set port spantree cost, set port spantree force-protocol-migration, set port spantree priority, set spantree enable | disable, set spantree forward-delay, set spantree hello-time, set spantree max-age, set spantree priority, set spantree tx-hold-count, set spantree version, show spantree

set spantree enable | disable

Use the **set spantree** command to enable or disable the spanning-tree algorithm for the media gateway.

Note:

When you disable spanning tree, blocking ports are disabled in order to prevent loops in the network. As a result, you need to wait 30 seconds before disabling spanning tree if you reset the media gateway, enable spanning tree, or insert a new station.

Syntax

set spantree {enable|disable}

Parameters

Parameter	Description	Possible Values	Default Value
enable	Keyword specifying to enable the spanning-tree algorithm		
disable	Keyword specifying to disable the spanning-tree algorithm		

User Level

read-write

Context

general

Example

To enable spanning tree:

```
G450-001# set spantree enable
bridge spanning tree enabled.
```

Related Commands

set port spantree, set port spantree cost, set port spantree force-protocol-migration, set port spantree priority, set spantree default-path-cost, set spantree forward-delay, set spantree hello-time, set spantree max-age, set spantree priority, set spantree tx-hold-count, set spantree version, show spantree

set spantree forward-delay

Use the **set spantree forward-delay** command to specify the time used when transferring the state of a port to the forwarding state.

Syntax

set spantree forward-delay ***seconds***

Parameters

Parameter	Description	Possible Values	Default Value
seconds	The value must exceed (Bridge Max Age / 2). The recommended value is **15**.	**4-30**	

User Level

read-write

Context

general

Example

To specify a forward delay of 25 seconds:

```
G450-001(super)# set spantree forward-delay 25
bridge forward delay is set to 25.
```

Related Commands

set port spantree, set port spantree cost, set port spantree force-protocol-migration, set port spantree priority, set spantree default-path-cost, set spantree enable | disable, set spantree hello-time, set spantree max-age, set spantree priority, set spantree tx-hold-count, set spantree version, show spantree

set spantree hello-time

Use the **set spantree hello-time** command to specify the time interval between the generation of configuration BPDU's by the root.

Syntax

set spantree hello-time ***seconds***

Parameters

Parameter	Description	Possible Values	Default Value
seconds	The value must not exceed (Bridge Max Age / 2) - 1. The recommended value is **2**.	**1-10**	

User Level

read-write

Context

general

Example

To specify spanning tree hello time is 2 seconds:

```
G450-001# set spantree hello-time 2
bridge hello time is set to 2.
```

Related Commands

set port spantree, set port spantree cost, set port spantree force-protocol-migration, set port spantree priority, set spantree default-path-cost, set spantree enable | disable, set spantree forward-delay, set spantree max-age, set spantree priority, set spantree tx-hold-count, set spantree version, show spantree

set spantree max-age

Use the **`set spantree max-age`** command to specify the time to keep an information message before it is discarded.

Syntax

`set spantree max-age` ***`seconds`***

Parameters

Parameter	Description	Possible Values	Default Value
seconds	The value must be between 2 * (Bridge-hello-time + 1) and 2 * (Bridge-forward-delay - 1). The recommended value is **20**.	**6-40**	

User Level

read-write

Context

general

Example

To keep information messages for 20 seconds before discarding:

```
G450-001(super)# set spantree max-age 20
bridge max age is set to 20.
```

Related Commands

set port spantree, set port spantree cost, set port spantree force-protocol-migration, set port spantree priority, set spantree default-path-cost, set spantree enable | disable, set spantree forward-delay, set spantree hello-time, set spantree priority, set spantree tx-hold-count, set spantree version, show spantree

set spantree priority

Use the **`set spantree priority`** command to set the bridge priority for the spanning tree.

Syntax

`set spantree priority` ***`bridge_priority`***

Parameters

Parameter	Description	Possible Values	Default Value
`bridge_priority`	The number representing the priority of the bridge	**0** (high)-**65535** (low) in increments of 4096	

User Level

read-write

Context

general

Example

To set the bridge priority to 4096:

```
G450-001(super)# set spantree priority 4096
Bridge priority set to 4096.
```

Related Commands

set port spantree, set port spantree cost, set port spantree force-protocol-migration, set port spantree priority, set spantree default-path-cost, set spantree enable | disable, set spantree forward-delay, set spantree hello-time, set spantree max-age, set spantree tx-hold-count, set spantree version, show spantree

set spantree tx-hold-count

Use the **`set spantree tx-hold-count`** command to set the value in packets used by the spanning tree in order to limit the maximum number of BPDU's transmitted during a hello-time period.

Syntax

`set spantree tx-hold-count` ***`rate`***

Parameters

Parameter	Description	Possible Values	Default Value
`rate`	Recommended value is **3**	**1-10**	

User Level

read-write

Context

general

Example

To limit the number of hello packets to 2:

```
G450-001(super)# set spantree tx-hold-count 2
tx hold count is set to 2.
```

Related Commands

set port spantree, set port spantree cost, set port spantree force-protocol-migration, set port spantree priority, set spantree default-path-cost, set spantree enable | disable, set spantree forward-delay, set spantree hello-time, set spantree max-age, set spantree priority, set spantree version, show spantree

set spantree version

Use the **`set spantree version`** command to set the version of the spanning tree protocol used by the device.

Syntax

`set spantree version` ***`version`***

Parameters

Parameter	Description	Possible Values	Default Value
`version`	Version of the spanning tree protocol	**common-spanning-tree** — compatible with IEEE802.1D standard **rapid-spanning-tree** — compatible with IEEE802.1W standard	

User Level

read-write

Context

general

Example

To use the rapid-spanning-tree version of spanning tree:

```
G450-001# set spantree version rapid-spanning-tree
Spanning tree version is set to rapid spanning tree.
```

Related Commands

set port spantree, set port spantree cost, set port spantree force-protocol-migration, set port spantree priority, set spantree default-path-cost, set spantree enable | disable, set spantree forward-delay, set spantree hello-time, set spantree max-age, set spantree priority, set spantree tx-hold-count, show spantree

show port edge state

Use the **show port edge state** command to display the edge state of the specified port. If no port is specified, information for all ports is displayed.

Syntax

show port edge state [*module*/[*port*]]

Parameters

Parameter	Description	Possible Values	Default Value
module	Number of the module		
port	Number of the port on the module. You can also specify a range of ports separated by a dash, for example, 10/5-6 for both ETH LAN ports 5-6 on the front panel.		

User Level

read-only

Context

general

Example

To show edge state for all ports:

```
G450-001(super)# show port edge state
```

Related Commands

set port auto-negotiation-flowcontrol-advertisement, set port enable | disable, set port duplex, set port edge admin state, set port enable | disable, set port flowcontrol, set port level, set port name, set port negotiation, set port point-to-point admin status, set port speed, show port auto-negotiation-flowcontrol-advertisement, show port flowcontrol

show port point-to-point status

Use the **show port point-to-point status** command to display the point-to-point status of the specified port. If no port is specified, information for all ports is displayed.

Syntax

show port point-to-point status [*module/port*]

Parameters

Parameter	Description	Possible Values	Default Value
module	Number of the module		
port	Number of the port on the module		

User Level

read-only

Context

general

Example

To display point-to-point information for all ports:

```
G450-001(super)# show port point-to-point status
```

Related Commands

show port

show spantree

Use the **show spantree** command to display spanning-tree information. If no port is specified, information for all ports is displayed.

Syntax

show spantree [*module*[/*port*]]

Parameters

Parameter	Description	Possible Values	Default Value
module	Number of the module		
port	Number of the port on the module		

User Level

read-only

Context

general

Example

To display spanning tree information for all ports:

```
G450-001(super)# show spantree
Spanning tree state is enabled

Designated Root:  00-04-0d-ea-b0-2d
Designated Root Priority: 32768
Designated Root Cost: 0
Designated Root Port: No root port, Bridge is Designated root
Root Max Age: 20   Hello Time: 2
Root Forward Delay: 15

Bridge ID MAC ADDR: 00-04-0d-ea-b0-2d
Bridge ID priority: 32768
Bridge Max Age: 20        Bridge Hello Time: 2
Bridge Forward Delay: 15  Tx Hold Count 3
Spanning Tree Version is rapid spanning tree
Spanning Tree Default Path Costs is according to common spanning tree

Port   State         Cost       Priority
------ ------------- ---------- ------------
10/5   not-connected 4          128
10/6   not-connected 4          128
```

Output fields:

Field	Description
Spanning tree	Spanning-Tree Protocol status (enabled or disabled)
Designated root	MAC address of the designated spanning-tree root bridge

1 of 2

Field	Description
Designated Root Priority	Priority of the designated root bridge
Designated Root Cost	Total path cost to reach the root
Designated Root Port	Port through which the root bridge can be reached (shown only on non root bridges)
Root Max Age	Amount of time a BPDU packet should be considered valid
Hello Time	Number of times the root bridge sends BPDUs
Bridge ID MAC ADDR	Bridge MAC address used in the sent BPDUs
Bridge ID Priority	Bridge Priority
Port	Port number
State	Spanning-tree port state (disabled, inactive, not-connected, blocking, listening, learning, forwarding, bridging, or type-pvid-inconsistent)
Cost	Cost associated with the port
Priority	Priority associated with the port

2 of 2

Related Commands

set port spantree, set port spantree cost, set port spantree force-protocol-migration, set port spantree priority, set spantree default-path-cost, set spantree enable | disable, set spantree forward-delay, set spantree hello-time, set spantree max-age, set spantree priority, set spantree tx-hold-count, set spantree version

SSH protocol

clear ssh-client known-hosts

Use the **clear ssh-client known-hosts** command to clear the SSH known-host file content. This command is used to unlock the man-in-the-middle attack prevention mechanism, and allow SCP server authentication after an SCP server public key change.

Syntax

clear ssh-client known-hosts

User Level

admin

Context

general

Example

To clear the SSH known-host file content:

```
G450-001(super)# clear ssh-client known-hosts
```

Related Commands

crypto key generate, disconnect ssh, ip ssh, show ip ssh

crypto key generate

Use the **crypto key generate** command to generate an SSH host key pair. You must generate the host key pair before the SSH service can be used. Stations that are currently active receive a warning message that the device public key has changed.

Note:
This command does not close active sessions.

Note:
This command can take several minutes to run (depending on CPU speed).

Syntax

crypto key generate dsa [key-size *bit-number*]

Parameters

Parameter	Description	Possible Values	Default Value
bit-number	Specifies the number of bits in the key	**512-2048**	**1024**

User Level

admin

Context

general

Example

To generate an SSH host key pair:

```
G450-001(super)# crypto key generate dsa
Generating DSA key, This command may take a few minutes
......
Key was created.
Key version: SSH2, DSA
Key Fingerprint: dd:60:59:fa:e0:47:b8:db:e3:1c:17:8d:4c:14:9a:0f root@avaya
```

Related Commands

clear ssh-client known-hosts, disconnect ssh, ip ssh, show ip ssh

disconnect ssh

Use the **disconnect ssh** command to disconnect an existing SSH session.

Syntax

disconnect ssh *session_id*

Parameters

Parameter	Description	Possible Values	Default Value
session_id	The number of the SSH session to disconnect		

User Level

admin

Context

general

Related Commands

clear ssh-client known-hosts, crypto key generate, ip ssh, show ip ssh

hostname

Use the **hostname** command to change the Command Line Interface (CLI) prompt. The prompt is written as **hostname-registration**, where the ***hostname*** is the value entered with the **hostname** command, and ***registration*** is the media gateway registration information. If the device is registered, the current media gateway number appears. If the device is not registered, question marks are displayed.

Use the **hostname** command with no parameters to display the current prompt value. Use the **no** form of this command to return the CLI prompt to the default.

Syntax

hostname [*hostname_string*]

no hostname

Parameters

Parameter	Description	Possible Values	Default Value
hostname_string	The hostname	a string of up to 20 characters	**G450**

User Level

read-write

Context

general

Example

To set the CLI prompt to GTW-HQ:

```
G450-001(super)# hostname GTW-HQ
GTW-HQ-001(super)# hostname
Session hostname is 'GTW-HQ'
```

To reset the CLI prompt to the default:

```
GTW-HQ-001(super)# no hostname
G450-001(super)#
```

Related Commands

banner login, banner post-login, clear screen, line, show banner login, show banner post-login, terminal length, terminal width

---

ip ssh

Use the **ip ssh** command to enable the Secure Shell (SSH) service. SSH is a security protocol that enables you to establish a remote session over a secured tunnel, also called a remote shell. Use the **no** form of the command to disable the SSH service, and close any open connections currently using SSH. When disabling the service, the G450 issues a message listing all current management interfaces. If SSH is currently the only enabled management interface, the user is warned that the remote connection will be lost.

Note:

For normal execution of SSH protocol, the G450 must first be assigned host name identification. Use the **hostname** command to assign host name identification.

Note:

In order to enable SSH to be used, you must configure the server host key. See the **crypto-key generate** command.

Syntax

[no] ip ssh

User Level

admin

Context

general

Example

To disable SSH service:

```
G450-001(super)# no ip ssh
This will prevent future remote SSH sessions and disconnect all active SSH
sessions - do you want to continue (Y/N)? y
```

Related Commands

clear ssh-client known-hosts, crypto key generate, disconnect ssh, show ip ssh

---

show ip ssh

Use the **show ip ssh** command to display general SSH information and information about the currently active connections that are using SSH.

Syntax

show ip ssh

User Level

admin

Context

general

Example

To display SSH information:

```
G450-001(super)# show ip ssh

Max Sessions: 2
Key type: DSA , 512 bit
Listen Port: 22
Ciphers List: 3des-cbc
Session Version Encryption Username IP/Port
0        1.5   3des-cbc   guest   11.11.11.1/34444
```

Output fields

Name	Description
Max Sessions	The maximum number of concurrent sessions
Key type	The type of SSH key (always DSA) and the key length
Listen Port	The SSH server listening port (always 22)
Ciphers List	List of supported ciphers
Session	Session ID of each currently active session
Version	The version of the SSH protocol used by the session
Encryption	The encryption method used by the session
Username	The name of the user that initiated the session
IP/Port	The IP address and port number of the client

Related Commands

clear ssh-client known-hosts, crypto key generate, disconnect ssh, ip ssh

Synchronization

clear sync interface

Use the **clear sync interface** command to disassociate an interface previously specified as the primary or secondary clock synchronization source.

Note:

The primary interface must be disassociated before the secondary interface is disassociated.

Syntax

```
clear sync interface {primary | secondary}
```

Parameters

Parameter	Description	Possible Values	Default Value
primary	Keyword specifying the primary clock synchronization source		
secondary	Keyword specifying the secondary clock synchronization source		

User Level

read-write

Context

general

Example

To disassociate the interface that is specified as the primary clock synchronization source:

```
G450-001(super)# clear sync interface primary
```

Related Commands

set sync interface, set sync source, set sync switching, show sync timing

set sync interface

Use the **set sync interface** command to define the specified module and port as a potential source for clock synchronization for the media gateway.

Syntax

set sync interface {**primary** | **secondary**} ***mmID*** [***portID***]

Parameters

Parameter	Description	Possible Values	Default Value
primary	Keyword that specifies normal failover		
secondary	Keyword that specifies to override normal failover, generate a trap, and assert a fault		

Parameter	Description	Possible Values	Default Value
mmID	The Media Module ID number of a stratum clock source, of the form “vn” where “n” is the slot number		
portID	Port or port range for an ISDN clock source candidate		

User Level

read-write

Context

general

Example

To specify that ports 1, 3, 5, 6, 7, and 8 of media module 2 are used for normal failover:

```
G450-001(super)# set sync interface primary v2 1,3,5-8
```

Related Commands

clear sync interface, set sync source, set sync switching, show sync timing

set sync source

Use the **set sync source** command to specify which clock source is the active clock source. The identity of the current synchronization source is not stored in persistent storage.

Syntax

set sync source {primary | secondary | local}

Parameters

Parameter	Description	Possible Values	Default Value
primary	Keyword specifying to set the primary clock source to be active		

Parameter	Description	Possible Values	Default Value
secondary	Keyword specifying to set the secondary clock source to be active, and the primary clock source on standby		
local	Keyword specifying to set the local clock to be active		

User Level

read-write

Context

general

Example

To set the primary clock as the clock source:

```
G450-001(super)# set sync source primary
```

If the secondary interface is not configured, the sync source set operation will fail:

```
G450-001(super)# set sync source secondary
    Operation Failed
Cannot set the secondary clock source to be the active clock source
```

Related Commands

clear sync interface, set sync interface, set sync switching, show sync timing

set sync switching

Use the **set sync switching** command to toggle automatic failover and failback between designated primary and secondary synchronization sources.

Syntax

set sync switching {enable | disable}

Parameters

Parameter	Description	Possible Values	Default Value
enable	Keyword specifying to enable automatic sync source switching		
disable	Keyword specifying to disable automatic sync source switching		

User Level

read-write

Context

general

Example

To enable sync source switching:

```
G450-001(super)# set sync switching enable
```

Related Commands

clear sync interface, set sync interface, set sync source, show sync timing

show sync timing

Use the **show sync timing** command to display the status of the primary, secondary, and local clock sources.

Syntax

show sync timing

User Level

read-only

Context

general

Example

To display clock source information:

```
G450-001(super)# show sync timing
```

```
SOURCE     MM                   STATUS                   FAILURE
---------  -------------------  -----------------------  -----------
Primary                         Not Configured
Secondary                       Not Configured
Local      v0                   Active                   None

Active Source: v0               Sync Source Switching: Enabled
```

Related Commands

clear sync interface, set sync interface, set sync source, set sync switching

SYN-cookies

clear tcp syn-cookies counters

Use the **clear tcp syn-cookies counters** command to clear the SYN cookies counters.

Syntax

clear tcp syn-cookies counters

User Level

read-only

Context

general

Examples

To clear the SYN cookies counters:

```
G450-001(super)# clear tcp syn-cookies counters
```

Related Commands

show tcp syn-cookies, tcp syn-cookies

show tcp syn-cookies

Use the **show tcp syn-cookies** command to show SYN cookies statistics for inbound TCP connections.

Syntax

show tcp syn-cookies

User Level

read-only

Context

general

Example

To show SYN cookies statistics:

```
G450-001(super)# show tcp syn-cookies
Status: Enabled

Statistics:
SYN rcvd                              10
Connections established                9

local address          remote address        state           Last access (sec)
---------------------  --------------------  --------------  ----------------
192.113.241.201:60342  111.211.131.1:80      IN_PROGRESS              1
192.113.241.201:23     221.2.11.11:432       ESTABLISHED           1200
192.113.241.201:23     121.192.171.121:7311  CLOSING                 10
```

Output fields

Field	Description
Status	The operational status of the TCP SYN cookies defense mechanism: Enabled or Disabled
SYN rcvd	The total number of TCP SYN packets received since the last time the counters were reset
Connections established	The total number of connections that were established since the last time the counters were reset
local address	The local IP address and port of the connection

1 of 2

Field	Description
remote address	The remote IP address and port of the connection
state	The state of the connection: • IN_PROGRESS — connection is in progress • ESTABLISHED — connection is established • CLOSING — connection is closing
Last access	The seconds elapsed since the last time a packet was received on the connection from either side

2 of 2

Related Commands

clear tcp syn-cookies counters, tcp syn-cookies

tcp syn-cookies

Use the **tcp syn-cookies** command to enable the TCP SYN cookies defense mechanism against SYN attacks. Use the **no** form of this command to disable the TCP SYN cookies defense mechanism against SYN attacks.

Note:

SYN cookies are disabled by default.

Note:

When enabling or disabling SYN cookies, you are prompted to copy the running configuration to the start-up configuration using the **copy running-config startup-config** command, and then to **reset** the device.

Syntax

```
[no] tcp syn-cookies
```

User Level

read-write

Context

general

Examples

To enable SYN cookies:

```
G450-001(config)# tcp syn-cookies
To enable tcp syn-cookies copy the running configuration to the
start-upconfiguration file, and reset the device.
G450-001(config)# copy running-config startup-config
G450-001(config)# reset
...
! Coming up from reset - syn-cookies are now enabled
```

To disable SYN cookies:

```
G450-001(config)# no tcp syn-cookies
To disable tcp syn-cookies copy the running configuration to the
start-upconfiguration file, and reset the device.
```

Related Commands

clear tcp syn-cookies counters, show tcp syn-cookies

Syslog files

copy syslog-file ftp

Use the **copy syslog-file ftp** command to copy the Syslog file to a remote server using FTP.

Syntax

copy syslog-file ftp *filename ip*

Parameters

Parameter	Description	Possible Values	Default Value
filename	File name with full path	string	
ip	IP address of the host	IP address	

User Level

admin

Context

general

Example

To copy the syslog file `syslog1` to the host with IP address 192.168.49.10:

```
G450-001(super)# copy syslog-file ftp syslog1 192.168.49.10
```

Related Commands

copy syslog-file scp, copy syslog-file tftp, copy syslog-file usb, show upload syslog-file status

---

copy syslog-file scp

Use the **`copy syslog-file scp`** command to copy the Syslog file to a remote server using SCP.

Syntax

`copy syslog-file scp` ***`filename ip`***

Parameters

Parameter	Description	Possible Values	Default Value
`filename`	File name with full path	string	
`ip`	IP address of the host	IP address	

User Level

admin

Context

general

Example

To copy the Syslog file `syslog1` to the host with IP address 192.168.49.10:

```
G450-001(super)# copy syslog-file scp syslog1 192.168.49.10
```

Related Commands

copy syslog-file ftp, copy syslog-file tftp, copy syslog-file usb, show upload syslog-file status

copy syslog-file tftp

Use the **copy syslog-file tftp** command to copy the Syslog file to a remote server using TFTP.

Syntax

copy syslog-file tftp *filename ip*

Parameters

Parameter	Description	Possible Values	Default Value
filename	File name with full path	string	
ip	IP address of the host	IP address	

User Level

admin

Context

general

Example

To copy the Syslog file `syslog1` to the host with IP address 192.168.49.10:

```
G450-001(super)# copy syslog-file tftp syslog1 192.168.49.10
```

Related Commands

copy syslog-file ftp, copy syslog-file scp, copy syslog-file usb, show upload syslog-file status

copy syslog-file usb

Use the **copy syslog-file usb** command to upload the Syslog file from the gateway to the USB mass storage device.

Syntax

copy syslog-file usb *source-filename destination-usb-device* [*destination-filename*]

Parameters

Parameter	Description	Possible Values	Default Value
source-filename	The logical name for the source file		
destination usb-device	The destination USB mass storage device	**usb-device0**	
destination-filename	The destination file name and path		

User Level

admin

Context

general

Examples

To upload `syslog1` from the gateway to usb-device0:

```
G450-001(super)# copy syslog-file usb syslog1 usb-device0
```

Related Commands

copy syslog-file ftp, copy syslog-file scp, copy syslog-file tftp, copy syslog-file usb, show upload syslog-file status

show upload syslog-file status

Use the **`show upload syslog-file status`** command to view the status of the upload operation of a Syslog file.

Syntax

`show upload syslog-file status`

User Level

read-only

Context

general

Example

To view the status of the upload operation of a Syslog file:

(In this example, an upload command has been issued and the upload succeeds.)

```
G450-001(super)# show upload syslog-file status
Module #10
===========
Module           : 10
Source file      : syslog file
Destination file : 444
Host             : 135.64.102.114
Running state    : Idle
Failure display  : (null)
Last warning     : No-warning
```

(In this example, an upload command has been issued, but the upload fails.)

```
G450-001(super)# Show upload syslog-file status
Module #10
===========
Module           : 10
Source file      : syslog file
Destination file : d:\zion\run.cfg
Host             : 135.64.102.39
Running state    : Idle
Failure display  : SCP - Permission denied
Last warning     : No-warning
```

(In this example, no upload command has been issued.)

```
G450-001(super)# Show upload syslog-file status
Module #10
==========
No source file for upload operation - no upload operation was done.
```

Related Commands

copy syslog-file ftp, copy syslog-file scp, copy syslog-file tftp, copy syslog-file usb

System identification

set system contact

Use the **set system contact** command to set the contact information for this media gateway system.

Syntax

set system contact [*string*]

Parameters

Parameter	Description	Possible Values	Default Value
string	The contact name string should be typed inside double quotes. The name is cleared if you leave this field blank.		

User Level

read-write

Context

general

Example

To set the contact information of the system to Larry Williams:

```
G450-001# set system contact “Larry Williams”
*** Set system contact ***
system contact set
```

Related Commands

set system location, set system name

set system location

Use the **set system location** command to set the location information for this media gateway system.

Syntax

set system location [*string*]

Parameters

Parameter	Description	Possible Values	Default Value
string	The location name string should be typed inside double quotes. The location is cleared if you leave this field blank.		

User Level

read-write

Context

general

Example

To set the location information of the system to tech-support:

```
G450-001# set system location “tech-support”
*** Set system location ***
system location set
```

Related Commands

set system contact, set system name

set system name

Use the **set system name** command to specify the name of the media gateway system.

Note:

Set the name of the media gateway to be consistent with the Name field on the Media Gateway administration form in Avaya Communication Manager (**add media-gateway**).

Syntax

set system name [*string*]

Parameters

Parameter	Description	Possible Values	Default Value
string	The system name string, typed inside quotes. The name is cleared if you leave this field blank.		

User Level

read-write

Context

general

Examples

To set the name of the system to “G450-HQ”:

```
G450-001(super)# set system name “G450-HQ”
*** Set system name ***
system name set
```

Related Commands

set system contact, set system location

Telnet access

ip telnet

Use the **ip telnet** command to enable the Telnet server on all interfaces except the Services interface. Use the **no** form of the command to disable the Telnet server.

Note:

For security reasons, this command can only be executed from the Console port.

Note:

The **ip telnet** command is a secured command and will not be displayed together with the running configuration (using the **show running-config** command). To see the status of this command, use the **show protocol** command (refer to show protocol on page 377).

Syntax

ip telnet [port *port_number*]

no ip telnet

Parameters

Parameter	Description	Possible Values	Default Value
port	Keyword that changes the default port of the Telnet server		
port_number	The number of the new port for the Telnet server	**1-65535**	**23**

User Level

admin

Context

general

Related Commands

ip telnet-client, ip telnet-services, show ip telnet, telnet

ip telnet-client

Use the **ip telnet-client** command to enable the Telnet client. Use the **no** form of the command to disable the Telnet client.

Note:

For security reasons, this command can only be executed from the console port.

Note:

The **ip telnet** command is a secured command and will not be displayed together with the running configuration (using the **show running-config** command). To see the status of this command, use the **show protocol** command (refer to show protocol on page 377).

Syntax

[no] ip telnet-client

User Level

admin

Context

general

Related Commands

ip telnet, ip telnet-services, show ip telnet, telnet

ip telnet-services

Use the **ip telnet-services** command to enable the Telnet server on the Services interface. Use the **no** form of the command to disable the Telnet server on the Services interface.

Syntax

ip telnet-services

no ip telnet-services

User Level

admin

Context

general

Related Commands

ip telnet, ip telnet-client, ip telnet-services, show ip telnet, show protocol, telnet

show ip telnet

Use the **show ip telnet** command to display the configuration and status of the Telnet server and the current Telnet connections.

Syntax

show ip telnet

User Level

read-only

Context

general

Example

To display the configuration and status of the Telnet server and the current Telnet connections:

```
G450-001(super)# show ip telnet

Telnet Engine: Enable
Max Sessions: 5
Listen Port: 23

Session-Id User                                IP:Port
0          root                                135.64.102.29:1059
```

Related Commands

ip telnet, ip telnet-client, ip telnet-services, telnet

---

telnet

Use the **telnet** command to initiate a login session via Telnet to a network host.

Syntax

telnet ***ipaddress*** [***port_number***]

Parameters

Parameter	Description	Possible Values	Default Value
ipaddress	The Telnet IP address		
port_number	The Telnet port number		**23**

User Level

read-only

Context

general

Example

To initiate a Telnet session to IP address 133.23.6.66:

```
G450-001(super)# telnet 133.23.6.66
```

Related Commands

ip telnet, ip telnet-client, ip telnet-services, show ip telnet

TFTP server

clear ip tftp-server statistics

Use the **clear ip tftp-server statistics** command to clear TFTP server statistics.

Syntax

clear ip tftp-server statistics

User Level

read-write

Context

general

Example

To clear TFTP server statistics:

```
G450-001# clear ip tftp-server statistics
```

Related Commands

copy ftp phone-image, copy ftp phone-script, copy running-config startup-config, copy scp phone-script, copy tftp phone-image, copy tftp phone-script, erase phone-image, ip tftp-server file-system size, show application-memory, show download phone-script-file status, show ip tftp-server files, show ip tftp-server statistics, show upload phone-script-file status

ip tftp-server

Use the **ip tftp-server** command to enable the TFTP server. Use the **no ip tftp-server** command to disable the TFTP server.

Syntax

[no] ip tftp-server

User Level

read-write

Context

general

Example

To enable TFTP server:

```
G450-001(super)# ip tftp-server
```

Related Commands

ip tftp-server file-system size

ip tftp-server file-system size

Use the **ip tftp-server file-system-size** command to set the TFTP file system size. Use the **no ip tftp-server file-system-size** command to reset the TFTP file system size to its default size.

Note:

It is possible to increase the memory allocation for the Sniffer cache application at the expense of the TFTP file system size. The Sniffer cache application may have been configured to use up to 1000 Kb of the default TFTP allocation of 18560 Kb, which would cause a conflict when setting the TFTP allocation to a high value.

Syntax

[no] ip tftp-server file-system-size *size*

Parameters

Parameter	Description	Possible Values	Default Value
size	The TFTP server total file size in KB	**256-19456**	**18560**

User Level

read-write

Context

general

Example

To set the TFTP file system size to 18128 KB:

```
G450-001# ip tftp-server file-system-size 18128
To change ip tftp-server file system size, copy the running configuration to
the start-up configuration file, and reset the device
```

Related Commands

copy ftp phone-image, copy ftp phone-script, copy running-config startup-config, copy scp phone-script, copy tftp phone-image, copy tftp phone-script, erase phone-image, show application-memory, show ip tftp-server files, show upload phone-script-file status, ip tftp-server

show application-memory

Use the **show application-memory** CLI command to show the configured and allocated application memory.

Syntax

show application-memory

User Level

read-only

Context

general

Example

To show the configured and allocated application memory:

```
G450-001(super)# show application-memory

Application                                          Memory(KB)
                                                  Allocated  Configured
------------------------------------------------  ---------------------
Sniffer (capture buffer-size)                          1024        1024
TFTP (ip tftp-server file-system-size)                18560       18560
------------------------------------------------  ---------------------
Total used memory                                     19584       19584
Total free memory                                       896         896
Total memory (fixed)                                  20480
```

Related Commands

copy ftp phone-image, copy ftp phone-script, copy running-config startup-config, copy scp phone-script, copy tftp phone-image, copy tftp phone-script, erase phone-image, ip tftp-server file-system size, show ip tftp-server files, show upload phone-script-file status

Traffic shaping

interface serial

Use the **interface serial** command to enter Serial interface or sub interface configuration mode. If the specified interface or sub interface does not exist, the system creates it and enters its configuration mode.

Use the **no** form of the command to delete the interface. The **no** form can only be used to delete sub L3 and sub frame relay interfaces. The command fails for USP interfaces and when higher or lower layers are defined for that interface.

Syntax

[no] interface Serial *module/if_number* [*if_link_type*]

For USP interfaces ***if_number*** has the syntax:

port[.***ip_interface*** | {.***sub_interface***[.***ip_interface***]}]

For DS1 interfaces ***if_number*** has the syntax:

port:***channel_group***[.***ip_interface*** | {.***sub_interface***[.***ip_interface***]}]

Parameters

Parameter	Description	Possible Values	Default Value
module	The interface module number		
port	The port number of the interface		
channel_group		For E1: **0-30** For T1: **0-23**	
sub_interface		**1-127**	
ip_interface		**0-1024**	
if_link_type		**point-to-point**	

User Level

read-write

Context

general, interface:Serial (FR SUB)

Example

To create point to point sub-interface number 17 over channel group 2 over E1/T1 controller number 1:

```
G450-001(super)# interface Serial 3/1:2.17 point-to-point
```

Related Commands - Frame relay encapsulation

clear frame-relay counters, encapsulation, frame-relay class-dlci, frame-relay interface-dlci, frame-relay lmi-n391dte, frame-relay lmi-n392dte, frame-relay lmi-n393dte, frame-relay lmi-type, frame-relay priority-dlci-group, frame-relay traffic-shaping, ip address, map-class frame-relay, bc out, be out, cir out, fragment, show frame-relay map, show frame-relay pvc brief, show interfaces, show traffic-shape, GRE tunneling, show traffic-shape-statistics

Related Commands - Traffic shaping

frame-relay traffic-shaping, map-class frame-relay, bc out, be out, cir out, fragment, show map-class frame-relay, show traffic-shape, show traffic-shape-queue, show traffic-shape-statistics, traffic-shape rate

Related Commands

description (interface), interface console, interface fastethernet, interface loopback, interface tunnel, interface USB-modem, interface vlan, ip address, ip admin-state, ip broadcast-address, ip crypto-group, load-interval, show ip interface brief

frame-relay traffic-shaping

Use the **frame-relay traffic-shaping** command to turn on/off traffic shaping and Frame-Relay fragmentation. Virtual Channels that are not explicitly assigned to a map-class frame-relay, are assigned to the default map-class frame-relay.

Use the **no** form of this command to turn off traffic shaping.

Syntax

[no] frame-relay traffic-shaping

User Level

read-write

Context

interface:Serial (DS1 FR L2, USP FR L2)

Example

To enable traffic shaping on the interface:

```
G450-001(if:Serial 3/1:1)# frame-relay traffic-shaping
```

Related Commands - Traffic shaping

interface serial, map-class frame-relay, bc out, be out, cir out, fragment, show map-class frame-relay, show traffic-shape, show traffic-shape-queue, show traffic-shape-statistics, traffic-shape rate

Related Commands - Frame relay encapsulation

clear frame-relay counters, interface serial, encapsulation, frame-relay class-dlci, frame-relay interface-dlci, frame-relay lmi-n391dte, frame-relay lmi-n392dte, frame-relay lmi-n393dte, frame-relay lmi-type, frame-relay priority-dlci-group, ip address, map-class frame-relay, bc out, be out, cir out, fragment, show frame-relay map, show frame-relay pvc brief, show interfaces, show traffic-shape, GRE tunneling, show traffic-shape-statistics

map-class frame-relay

Use the **map-class frame-relay** command to create a QoS template named ***map_class_name***, which can later be assigned to DLCIs.

Use the **no** form of this command to delete a map class.

Note:

This command fails if the map class is currently associated with a DLCI.

Syntax

[no] map-class frame-relay *map_class_name*

Parameters

Parameter	Description	Possible Values	Default Value
map_class_name	The name of a map class configured by the user		

User Level

read-write

Context

general

Example

To create a map class named mySVoip1:

```
G450-001(super)# map-class frame-relay mySVoip1
G450-001(super-map-class)#
```

Related Commands - Traffic shaping

interface serial, frame-relay traffic-shaping, bc out, be out, cir out, fragment, show map-class frame-relay, show traffic-shape, show traffic-shape-queue, show traffic-shape-statistics, traffic-shape rate

Related Commands - Frame relay encapsulation

clear frame-relay counters, interface serial, encapsulation, frame-relay class-dlci, frame-relay interface-dlci, frame-relay lmi-n391dte, frame-relay lmi-n392dte, frame-relay lmi-n393dte, frame-relay lmi-type, frame-relay priority-dlci-group, frame-relay traffic-shaping, ip address, bc out, be out, cir out, fragment, show frame-relay map, show frame-relay pvc brief, show interfaces, show traffic-shape, GRE tunneling, show traffic-shape-statistics

bc out

Use the **bc out** command to configure the committed burst size in bits, for the outbound direction. Use the **no** form of this command to return the committed burst size to its default value.

Syntax

bc out *bits*

no bc out

Parameters

Parameter	Description	Possible Values	Default Value
bits	The committed burst size in bits	**300-39999999**	**7000**

User Level

read-write

Context

map-class frame-relay

Example

To configure outbound BC to be 64 Kbit:

```
G450-001(map-class)# bc out 64000
```

Related Commands - Traffic shaping

interface serial, frame-relay traffic-shaping, map-class frame-relay, be out, cir out, fragment, show map-class frame-relay, show traffic-shape, show traffic-shape-queue, show traffic-shape-statistics, traffic-shape rate

Related Commands - Frame relay encapsulation

clear frame-relay counters, interface serial, encapsulation, frame-relay class-dlci, frame-relay interface-dlci, frame-relay lmi-n391dte, frame-relay lmi-n392dte, frame-relay lmi-n393dte, frame-relay lmi-type, frame-relay priority-dlci-group, frame-relay traffic-shaping, ip address, map-class frame-relay, be out, cir out, fragment, show frame-relay map, show frame-relay pvc brief, show interfaces, show traffic-shape, GRE tunneling, show traffic-shape-statistics

be out

Use the **be out** command to configure the excess burst size in bits, for the outbound direction. Use the **no** form of this command to return the excess burst size to its default value.

Note:

The Excess Information Rate (EIR) is equal to: (BC+BE)/Tc/1000, where Tc is the Frame Relay meter time interval in mSec, BC is the committed burst rate and BE is the excess burst size.

Syntax

be out *bits*

no be out

Parameters

Parameter	Description	Possible Values	Default Value
bits	The excess burst size in bits	**0-39999999**	**7000**

User Level

read-write

Context

map-class frame-relay

Example

To configure outbound BE to be 64 Kbit:

```
G450-001(map-class)# be out 64000
```

Related Commands - Traffic shaping

interface serial, frame-relay traffic-shaping, map-class frame-relay, bc out, cir out, fragment, show map-class frame-relay, show traffic-shape, show traffic-shape-queue, show traffic-shape-statistics, traffic-shape rate

Related Commands - Frame relay encapsulation

clear frame-relay counters, interface serial, encapsulation, frame-relay class-dlci, frame-relay interface-dlci, frame-relay lmi-n391dte, frame-relay lmi-n392dte, frame-relay lmi-n393dte, frame-relay lmi-type, frame-relay priority-dlci-group, frame-relay traffic-shaping, ip address, map-class frame-relay, bc out, cir out, fragment, show frame-relay map, show frame-relay pvc brief, show interfaces, show traffic-shape, GRE tunneling, show traffic-shape-statistics

cir out

Use the **cir out** command to configure the Committed Information Rate (CIR) in bits per second, for the outbound direction. Use the **no** form of this command to return the CIR to its default value.

Note:
This command fails if the map class is currently associated with a DLCI.

Syntax

cir out *cir*

no cir out

Parameters

Parameter	Description	Possible Values	Default Value
cir	The CIR in bits per second	**1000-39999999**	**56000**

User Level

read-only

Context

map-class frame-relay

Example

To configure outbound CIR to be 64 Kbps:

```
G450-001(map-class)# cir out 64000
```

Related Commands - Traffic shaping

interface serial, frame-relay traffic-shaping, map-class frame-relay, bc out, be out, fragment, show map-class frame-relay, show traffic-shape, show traffic-shape-queue, show traffic-shape-statistics, traffic-shape rate

Related Commands - Frame relay encapsulation

clear frame-relay counters, interface serial, encapsulation, frame-relay class-dlci, frame-relay interface-dlci, frame-relay lmi-n391dte, frame-relay lmi-n392dte, frame-relay lmi-n393dte, frame-relay lmi-type, frame-relay priority-dlci-group, frame-relay traffic-shaping, ip address, map-class frame-relay, bc out, be out, fragment, show frame-relay map, show frame-relay pvc brief, show interfaces, show traffic-shape, GRE tunneling, show traffic-shape-statistics

fragment

Use the **fragment** command to enable FRF.12 fragmentation and configure the fragment size. Use the **no** form of this command to disable FRF.12 fragmentation. By default, FRF.12 fragmentation is disabled.

Syntax

[no] fragment *size*

Parameters

Parameter	Description	Possible Values	Default Value
size	The size of the fragment in octets, including the Frame Relay Header (2 octets) and Fragmentation header (4 octets)	**16-1600**	**88**

User Level

read-write

Context

map-class frame-relay

Example

To enable FRF.12 fragmentation and set the fragment size to 63:

```
G450-001(super-map-class)# fragment 63
```

Related Commands - Traffic shaping

interface serial, frame-relay traffic-shaping, map-class frame-relay, bc out, be out, cir out, show map-class frame-relay, show traffic-shape, show traffic-shape-queue, show traffic-shape-statistics, traffic-shape rate

Related Commands - Frame relay encapsulation

clear frame-relay counters, interface serial, encapsulation, frame-relay class-dlci, frame-relay interface-dlci, frame-relay lmi-n391dte, frame-relay lmi-n392dte, frame-relay lmi-n393dte, frame-relay lmi-type, frame-relay priority-dlci-group, frame-relay traffic-shaping, ip address, map-class frame-relay, bc out, be out, cir out, show frame-relay map, show frame-relay pvc brief, show interfaces, show traffic-shape, GRE tunneling, show traffic-shape-statistics

show map-class frame-relay

Use the **show map-class frame-relay** command to display the map-class Frame Relay table.

Syntax

show map-class frame-relay

User Level

read-only

Context

general

Example

To display the map class Frame Relay table:

```
G450-001(super)# show map-class frame-relay
```

Showing 3 frame-relay map-class entries

Map Class Name	CIR	BC	BE	Fragment
default	56000	7000	0	OFF
orna1	56000	7000	0	OFF
stam	56000	7000	0	OFF

Related Commands - Frame relay encapsulation

clear frame-relay counters, interface serial, encapsulation, frame-relay class-dlci, frame-relay interface-dlci, frame-relay lmi-n391dte, frame-relay lmi-n392dte, frame-relay lmi-n393dte, frame-relay lmi-type, frame-relay priority-dlci-group, frame-relay traffic-shaping, ip address, map-class frame-relay, bc out, be out, cir out, fragment, show frame-relay map, show frame-relay pvc brief, show interfaces, show traffic-shape, GRE tunneling, show traffic-shape-statistics

Related Commands - Traffic shaping

interface serial, frame-relay traffic-shaping, map-class frame-relay, bc out, be out, cir out, fragment, show traffic-shape, show traffic-shape-queue, show traffic-shape-statistics, traffic-shape rate

Related Commands - Verifying WAN configuration

show frame-relay fragment, show frame-relay lmi, show frame-relay map, show frame-relay pvc, show frame-relay traffic, show interfaces

show traffic-shape

Use the **show traffic-shape** command to display traffic shaping and Frame Relay Traffic Shaping configuration information.

Syntax

show traffic-shape [*interface-name-number*]

Parameters

Parameter	Description	Possible Values	Default Value
interface-name-number	Interface or sub-interface type and number		

User Level

read-only

Context

general

Example

To display traffic shaping and Frame Relay Traffic Shaping information for the G450:

```
G450-001(super)# show traffic-shape
                     Target    Byte   Sustain   Excess    Interval Increment
Interface         VC Rate      Limit  bits/int  bits/int  (ms)     (bytes)
----------------- --- --------- ------ --------- --------- -------- ---------
Serial 5/0:11.11  16      24000  12375     24000     96000      125       375
Serial 5/0:11.11  20      24000  12375     24000     96000      125       375
Serial 3/1:1.2    30      24000  12375     24000     96000      125       375
FastEthernet 10/2        128000   1518    128000         0        1        16
```

To display traffic shaping and Frame Relay Traffic Shaping information for the Serial 5/0 interface:

```
G450-001(super)# show traffic-shape interface Serial 5/0:11.11
                     Target    Byte   Sustain   Excess    Interval Increment
Interface         VC Rate      Limit  bits/int  bits/int  (ms)     (bytes)
----------------- --- --------- ------ --------- --------- -------- ---------
Serial 5/0:11.11  16      24000  12375     24000     96000      125       375
Serial 5/0:11.11  20      24000  12375     24000     96000      125       375
```

Output fields:

Field	Description
Interface	Interface or sub-interface type and number
VC	Virtual circuit, which is the DLCI number
Target Rate	Rate that traffic is shaped to, in bits per second. This is the CIR.
Byte Limit	Maximum number of bytes sent per internal interval. This is the high-watermark, which is equivalent to (inBc + Be)/8.
Sustain bits/int	Configured sustained bits per interval. This is the Bc.
Excess bits/int	Configured excess bits in the first interval. This is the Be.
Interval (ms)	The internal interval being used, in milliseconds. This is the inTc.
Increment (bytes)	Number of bytes that will be sustained per internal interval. This is inBc/8.

Related Commands - Traffic shaping

interface serial, frame-relay traffic-shaping, map-class frame-relay, bc out, be out, cir out, fragment, show map-class frame-relay, show traffic-shape-queue, show traffic-shape-statistics, traffic-shape rate

Related Commands - Frame relay encapsulation

clear frame-relay counters, interface serial, encapsulation, frame-relay class-dlci, frame-relay interface-dlci, frame-relay lmi-n391dte, frame-relay lmi-n392dte, frame-relay lmi-n393dte, frame-relay lmi-type, frame-relay priority-dlci-group, frame-relay traffic-shaping, ip address, map-class frame-relay, bc out, be out, cir out, fragment, show frame-relay map, show frame-relay pvc brief, show interfaces, GRE tunneling, show traffic-shape-statistics

show traffic-shape-queue

Use the **show traffic-shape-queue** command to display information about the real-time status of traffic-shaping and Frame Relay Traffic Shaping queues.

Syntax

show traffic-shape-queue [*interface-name-number*]

Parameters

Parameter	Description	Possible Values	Default Value
interface-name-number	Interface or sub-interface type and number		

User Level

read-only

Context

general

Example

To display traffic shaping and Frame Relay Traffic Shaping queueing data for the G450:

```
G450-001(super)# show traffic-shape-queue
  Traffic queued in shaping queue on 4/1:11.11 dlci 16
  Queueing strategy: weighted fair voip
   Voip queue: 0/0/20/0/0 (size/max size/threshold-ms/drops/tx)
```

```
   Weighted fair queue: 1/2/64/0/127 (size/max size/threshold/drops/tx)
        Conversations 1/1/256 (active/max active/max total)
   Available Bandwidth 64 kilobits/sec

Voip queue:
 Voip queue is empty

Weighted fair queue:
 Idx Source ip       Destination ip  Prot Sport Dport Cnt Total drop Total tx
 --- --------------- --------------- ---- ----- ----- --- ---------- --------
 228 149.49.70.155   135.64.102.240  tcp     23  2515   1          0         127
```

Related Commands - Traffic shaping

interface serial, frame-relay traffic-shaping, map-class frame-relay, bc out, be out, cir out, fragment, show map-class frame-relay, show traffic-shape, show traffic-shape-statistics, traffic-shape rate

Related Commands - Frame relay encapsulation

clear frame-relay counters, interface serial, encapsulation, frame-relay class-dlci, frame-relay interface-dlci, frame-relay lmi-n391dte, frame-relay lmi-n392dte, frame-relay lmi-n393dte, frame-relay lmi-type, frame-relay priority-dlci-group, frame-relay traffic-shaping, ip address, map-class frame-relay, bc out, be out, cir out, fragment, show frame-relay map, show frame-relay pvc brief, show interfaces, show traffic-shape, show traffic-shape-statistics

show traffic-shape-statistics

Use the **show traffic-shape-statistics** command to display traffic shaping and Frame Relay Traffic Shaping statistics.

Syntax

show traffic-shape-statistics [*interface-name-number*]

Parameters

Parameter	Description	Possible Values	Default Value
interface-name-number	Interface or sub-interface type and number		

User Level

read-only

Context

general

Example

To display traffic shaping and Frame Relay Traffic Shaping statistics for the G450:

```
G450-001(super)# show traffic-shape-statistics
                        Queue Packets   Bytes     Packets   Bytes     Shaping
Interface         VC    Depth                     Delayed   Delayed   Active
----------------- ---- ----- -------- ---------- --------- -------- ---------
Serial 4/1:11.11    16     0      455     220218       375    182250    No
Serial 3/1:1.2      30    50      455     220218       375    182250    yes
FastEthernet 10/2            0     1031    1938990       534    938270    No
```

To display traffic shaping and Frame Relay Traffic Shaping statistics for the Serial 4/1 interface:

```
G450-001(super)# show traffic-shape statistics Serial 4/1:11.11
                        Queue Packets   Bytes     Packets   Bytes     Shaping
Interface         VC    Depth                     Delayed   Delayed   Active
----------------- ---- ----- -------- ---------- --------- -------- ---------
Serial 4/1:11.11    16     0      455     220218       375    182250    No
```

Output fields:

Field	Description
Interface	Interface or sub-interface type and number
VC	Virtual circuit, which is the DLCI number
Queue Depth	Number of frames currently in the VC (Virtual Circuit) queue
Packets	Number of packets sent through the VC
Bytes	Number of bytes sent through the VC
Packets Delayed	Number of packets sent through the VC that were delayed in the traffic-shaping queue
Bytes Delayed	Number of bytes sent through the VC that were delayed in the traffic-shaping queue
Shaping Active	Whether traffic shaping is active. Possible values: • **Yes** — traffic shaping is occurring, i.e. VC-Q is not empty • **No** — traffic shaping is not occurring, i.e. VC-Q is empty

Related Commands - Traffic shaping

interface serial, frame-relay traffic-shaping, map-class frame-relay, bc out, be out, cir out, fragment, show map-class frame-relay, show traffic-shape, show traffic-shape-queue, traffic-shape rate

Related Commands - Frame relay encapsulation

clear frame-relay counters, interface serial, encapsulation, frame-relay class-dlci, frame-relay interface-dlci, frame-relay lmi-n391dte, frame-relay lmi-n392dte, frame-relay lmi-n393dte, frame-relay lmi-type, frame-relay priority-dlci-group, frame-relay traffic-shaping, ip address, map-class frame-relay, bc out, be out, cir out, fragment, show frame-relay map, show frame-relay pvc brief, show interfaces, show traffic-shape, GRE tunneling

---

traffic-shape rate

Use the **`traffic-shape rate`** command to configure traffic shaping for outbound traffic on the current interface.

Syntax

`traffic-shape rate` ***`bit_rate`***

Parameters

Parameter	Description	Possible Values	Default Value
`bit_rate`	The bit-rate that traffic is shaped to, in bits per second	**64000-10240000**	

User Level

read-write

Context

interface:FastEthernet(L2, L2-L3)

Example

To set the traffic-shaping rate to 128000:

```
G450-001(if:FastEthernet 10/2)# traffic-shape rate 128000
```

Related Commands - Traffic shaping

interface serial, frame-relay traffic-shaping, map-class frame-relay, bc out, be out, cir out, fragment, show map-class frame-relay, show traffic-shape, show traffic-shape-queue, show traffic-shape-statistics

Related Commands - WAN Ethernet port configuration

interface FastEthernet, autoneg, duplex, keepalive-track, speed (interface)

USB mass storage device

backup config usb

Use the **backup config usb** command to back up the gateway configuration to a USB mass storage device.

Syntax

backup config usb *usb-device backup-name*

Parameters

Parameter	Description	Possible Values	Default Value
usb-device	The destination USB mass storage device	**usb-device0**	
backup-name	The destination backup database path and file name on the USB device	string of up to 64 characters	

User Level

read-write

Context

general

Example

To back up the gateway configuration in the form of file `gatewaybackup1` to usb-device0:

```
G450-001(super)# backup config usb usb-device0 gatewaybackup1
```

Related Commands

copy announcement-file usb, copy usb announcement-file, erase usb, restore usb, safe-removal usb, show backup status, show restore status, show usb

dir

Use the **dir** command to show either:

- The files that have been downloaded to the media gateway using the G450-001 Download interface and the SNMP MIB.
- The files in the USB mass storage device.

Syntax

dir {[*module_number*] | [*file-system* [*directory*]]}

Parameters

Parameter	Description	Possible Values	Default Value
module_number	Displays downloaded files for the specified module only		
file-system	Displays files on the USB mass storage device	**usbdevice0**	
directory	Displays files for the specified directory on the USB mass storage device		

User Level

read-write

Context

general

Example

To display a list of downloaded files:

```
G450-001(super)# dir
M# file              ver num   file type    file location  file description
-- ----              --------  ----------   -------------  ----------------
1  MM712             5         SW RT Image  Nv-Ram         MM712 - image
3  MM711             17        SW RT Image  Nv-Ram         MM711 - image
4  MM722             2         SW RT Image  Nv-Ram         MM722 - image
9  hi.wav            N/A       Annc files   Nv-Ram         Announcement files
9  hi1.wav           N/A       Annc files   Nv-Ram         Announcement files
9  hi2.wav           N/A       Annc files   Nv-Ram         Announcement files
10 startup-config    N/A       Startup Conf Nv-Ram         Startup Config
10 running-config    N/A       Running Conf Ram            Running Config
10 G450-A           24.6.0    SW RT Image  Flash Bank A   Software Image Bank A
10 G450-B           24.8.0    SW Component Flash Bank B   Software Image Bank B
10 G450              2.2.4     SW Web Image Nv-Ram          EmWeb application
10 G450-Booter       21.12.0   SW BootImage Nv-Ram          Booter Image
10 sniffer           N/A       Other        Ram             Sniffer Capture
10 phone-ScriptA     N/A       Phone Script Nv-Ram          N/A
10 phone-ScriptB     N/A       Phone Script Nv-Ram          46xxupgrade.scr
10 phone-ScriptC     N/A       Phone Script Nv-Ram          N/A
10 phone-ScriptD     N/A       Phone Script Nv-Ram          N/A
10 phone-ImageA      N/A       Phone Image  Ram             N/A
10 phone-ImageB      N/A       Phone Image  Ram             N/A
10 phone-ImageC      N/A       Phone Image  Ram             4601dbte1_82.bin
10 phone-ImageD      N/A       Phone Image  Ram             4602dbte1_82.bin
10 phone-ImageE      N/A       Phone Image  Ram             4602dape1_82.bin
10 phone-ImageF      N/A       Phone Image  Ram             4601dape1_82.bin
10 dhcp-binding      N/A       DHCP Binding Nv-Ram          Ip Address Binding
```

To display a list of the files in the USB mass storage device:

```
G450-001(super)# dir usbdevice0 1
  Date                 Type        Size(Bytes)       Filename
  -------              --------     ----------        --------
2006-11-13,14:56:58    <DIR>              1024        IPPHONE
2006-11-13,14:57:22    <DIR>              1024        GWANNC
2006-11-13,14:56:58    <DIR>              1024        MM
2006-11-13,14:56:58    file               3146        startup_config.cfg
2006-11-13,14:56:58    file                953        vpn_license.cfg
2006-11-13,14:57:22    file                718        readme.txt
```

Related Commands

copy ftp EW_archive, copy ftp module, copy ftp SW_imageA, copy ftp SW_imageB, copy tftp EW_archive, copy tftp module, copy tftp SW_imageA, copy tftp SW_imageB, copy usb announcement-file, set boot bank, show boot bank, show download software status, show image version

erase usb

Use the **erase usb** command to erase a file or directory on the USB mass storage device.

Syntax

erase usb *usb-device file-name*

Parameters

Parameter	Description	Possible Values	Default Value
usb-device	The USB mass storage device	**usb-device0**	
file-name	The name of the file or directory to be deleted	A string of up to 64 characters	

User Level

read-write

Context

general

Example

To delete `backupgateway1` on usb-device0:

```
G450-001(super)# erase usb usb-device0 backupgateway1
```

Related Commands

backup config usb, copy announcement-file usb, copy usb announcement-file, restore usb, safe-removal usb, show backup status, show restore status, show usb

restore usb

Use the **restore usb** command to restore gateway files from a USB mass storage device.

Note:

The restore operation does not fail if a specific file is missing or incompatible with the MM hardware.

Note:

If you are restoring to a different machine than the one from which you backed up, first delete the VPN license file from the USB device. Otherwise, the restore operation will fail.

Syntax

`restore usb` ***`usb-device backup-name`***

Parameters

Parameter	Description	Possible Values	Default Value
`usb-device`	The USB mass storage device	**usb-device0**	
`backup-name`	The backup directory path and file name		The gateway backup directory on **usb-device0**

User Level

read-write

Context

general

Example

To restore gateway files from directory `gatewaybackup1` on usb-device0:

```
G450-001(super)# restore usb usb-device0 gatewaybackup1
```

Related Commands

backup config usb, copy announcement-file usb, copy usb announcement-file, erase usb, safe-removal usb, show backup status, show restore status, show usb

safe-removal usb

Use the **`safe-removal usb`** command to safely remove the USB mass storage device. Use the command before unplugging the USB mass storage device.

Syntax

`safe-removal usb` ***`file-system`***

Parameters

Parameter	Description	Possible Values	Default Value
file-system	USB mass storage file system name		

User Level

read-only

Context

general

Example

To safely remove usb-device0:

```
G450-001(super)# safe-removal usb usb-device0
```

Related Commands

backup config usb, copy announcement-file usb, copy usb announcement-file, erase usb, restore usb, show backup status, show restore status, show usb

show backup status

Use the **show backup status** command to display information regarding the status of a backup of the gateway configuration to a USB mass storage device.

Syntax

show backup status

User Level

read-only

Context

general

Example

To display information regarding the status of a backup:

```
G450-001(super)# show backup status
Backup operation in progress. Do not remove usb mass storage device until the
```

```
end of operation.
Files backup:
Type              FileName            Status
------            ----------------    -----------
Startup-config    startup-config.cfg  OK
```

Related Commands

backup config usb, copy announcement-file usb, copy usb announcement-file, erase usb, restore usb, safe-removal usb, show restore status, show usb

show restore status

Use the **show restore status** command to display information regarding the status of a restore operation of gateway files from a USB mass storage device. The output displays the list of files restored so far.

Syntax

show restore status

User Level

read-only

Context

general

Example

To display information regarding the status of a gateway file restore operation:

```
G450-001(super)# show restore status
Files restored:
```

```
Type                      FileName                     Status
-----------------------------------------------------------
swComponent               g450_sw_26_23_0.bin         OK
startup-config            startup_config.cfg           OK
auth-file                 auth-file.cfg                OK
license-file              vpn_license.cfg              OK
swWebImage                g450_emweb_3_1_8.bin        OK
phone-script              46xxupgrade.scr              OK
phone-script              46xxsettings.txt             OK
phoneImageFile            4602dbte1_82.bin             OK
phoneImageFile            4601dbte1_82.bin             OK
phoneImageFile            4602dape1_82.bin             OK
phoneImageFile            4601dape1_82.bin             OK
announcement              A01100.wav                   OK
announcement              Ann7.wav                     OK
swRuntimeImage            MM710V11.FDL                 OK

Files missing/error:
swRuntimeImage            MB 1T+2L Analog              Missing
```

Related Commands

backup config usb, copy announcement-file usb, copy usb announcement-file, erase usb, restore usb, safe-removal usb, show backup status, show usb

show usb

Use the **show usb** command to display the USB devices connected to the gateway.

Syntax

show usb {**all** | ***usb-device-id***}

Parameters

Parameter	Description	Possible Values	Default Value
all	Keyword specifying to show information about all USB mass storage devices		
usb-device-id	Specifies a USB device ID for which to display information	**1-512**	

User Level

read-only

Context

general

Example

To display all USB devices connected to the gateway:

```
G450-001(super)# show usb all
USB  Description      Manufacturer USB Power Max       Speed
Dev Id                            Ver Mode  Power(mA)
---- ---------------- ------------ --- ----- --------- -----
1    Root Hub         N/A          1.1 Self  0         Full
2    DiskOnKey        M-Sys        1.1 Bus   94        Full
257  Root Hub         N/A          2.0 Self  0         High

USB  Vendor Product Device Serial Number    FileSystem  Storage Free    FS
Dev Id ID     ID      Ver                               (MB)    (MB)
---- ------ ------- ------ ---------------- ----------- ------- ------- -----
1    0x0    0x0     0.0    N/A              N/A         N/A     N/A     N/A
2    0x8ec  0x12    2.0    0870974092E3A8D8 /usbdevice0 61      44      FAT32
257  0x0    0x0     0.0    N/A              N/A         N/A     N/A     N/A
```

Related Commands

backup config usb, copy announcement-file usb, copy usb announcement-file, erase usb, restore usb, safe-removal usb, show backup status, show restore status

User accounts

login authentication inactivity-period

Use the **login authentication inactivity-period** command to disable a local user account after a specified inactivity period. Use the **no** form of the command to deactivate the inactivity period policy. By default, the inactivity period policy is deactivated to be backward compatible.

Note:

The **no** form of the command does not re-enable accounts deactivated because of the inactivity period policy. To re-enable an account, an administrator must run the username command and re-configure the account using the same user name and password.

Note:

This command does not apply to the root account or to Service accounts.

Syntax

login authentication inactivity-period *days*

no login authentication inactivity-period

Parameters

Parameter	Description	Possible Values	Default Value
days	The number of days during which the account is inactive, after which the account will be disabled	**2-365**	

User Level

admin

Context

general

Example

To set the login inactivity period to two months:

```
G450-001(super)# login authentication inactivity-period 60
```

Related Commands

login authentication lockout, login authentication min-password-digit-chars, login authentication min-password-length, login authentication min-password-lower-chars, login authentication min-password-special-chars, login authentication min-password-upper-chars, login authentication password-expire, password, show login authentication, show username, username

login authentication lockout

Use the **login authentication lockout** command to lockout or disable a local user account after successive failed login attempts. When an account is disabled it requires administrator intervention to re-enable the account.

Use the **no** form of the command to return the lockout or disable threshold counts to their default values.

Note:

As soon as you use the **login authentication lockout** command, the new lockout settings immediately override previous settings, for all user accounts.

Note:

The root account can only be locked, it cannot be disabled.

Syntax

login authentication { [lockout <*time*> | disable | unset] | attempt <*count*> }

Parameters

Parameter	Description	Possible Values	Default Value
lockout	A keyword indicating to implement a policy of locking out an account for a specified time period if ***count*** is exceeded		
time	The lockout time, in seconds	**30-3600** **0** disables the lockout function	**180**
disable	A keyword indicating to implement a policy of disabling an account if ***count*** is exceeded		

Parameter	Description	Possible Values	Default Value
unset	A keyword indicating not to implement account lockout or account disabling		
count	The number of successive failed login attempts before account lockout or account disabling is enforced	**1-10** **0** disables the timeout function	**3**

User Level

admin

Context

general

Example

To disable access to the device following 8 failed login attempts:

```
G450-001(super)# login authentication disable attempt 8
```

Related Commands

login authentication inactivity-period, login authentication min-password-digit-chars, login authentication min-password-length, login authentication min-password-lower-chars, login authentication min-password-special-chars, login authentication min-password-upper-chars, login authentication password-expire, password, show login authentication, show username, username

login authentication min-password-digit-chars

Use the **login authentication min-password-digit-chars** command to set the minimum number of digit characters that a password must contain. Use the **no** form of the command to return the minimum number to the default value.

Syntax

login authentication min-password-digit-chars ***length***

no login authentication min-password-digit-chars

Parameters

Parameter	Description	Possible Values	Default Value
length	The minimum number of digit characters in a user password	0-30	0

User Level

admin

Context

general

Example

To set the minimum number of digit characters that a password must contain, to 0:

```
G450-001(super)# login authentication min-password-digit-chars 0
```

Related Commands

login authentication inactivity-period, login authentication lockout, login authentication min-password-length, login authentication min-password-lower-chars, login authentication min-password-special-chars, login authentication min-password-upper-chars, login authentication password-expire, password, show login authentication, show username, username

login authentication min-password-length

Use the **login authentication min-password-length** command to set the minimum password length during configuration of local users accounts. Use the **no** form of the command to return the minimum password length to the default value of 8.

Note:

The minimum password length must be at least as great as the sum of the min-password-upper-chars, min-password-lower-chars, min-password-digit-chars, and min-password-special-chars.

Syntax

login authentication min-password-length *length*

no login authentication min-password-length

Parameters

Parameter	Description	Possible Values	Default Value
length	The minimum length of a user password	8-31	8

User Level

admin

Context

general

Example

To set the minimum password length to 10 characters:

```
G450-001(super)# login authentication min-password-length 10
```

Related Commands

login authentication inactivity-period, login authentication lockout, login authentication min-password-digit-chars, login authentication min-password-lower-chars, login authentication min-password-special-chars, login authentication min-password-upper-chars, login authentication password-expire, password, show login authentication, show username, username

login authentication min-password-lower-chars

Use the **login authentication min-password-lower-chars** command to set the minimum number of lowercase characters that a password must contain. Use the **no** form of the command to return the minimum number to the default value.

Syntax

login authentication min-password-lower-chars ***length***

no login authentication min-password-lower-chars

Parameters

Parameter	Description	Possible Values	Default Value
length	The minimum number of lowercase characters in a user password	1-31	1

User Level

admin

Context

general

Example

To set the minimum number of lowercase characters that a password must contain, to 5:

```
G450-001(super)# login authentication min-password-lower-chars 5
```

Related Commands

login authentication inactivity-period, login authentication lockout, login authentication min-password-digit-chars, login authentication min-password-length, login authentication min-password-special-chars, login authentication min-password-upper-chars, login authentication password-expire, password, show login authentication, show username, username

login authentication min-password-special-chars

Use the **login authentication min-password-special-chars** command to set the minimum number of special characters that a password must contain. Special characters are any printable non-alphanumeric characters, except for white characters (blank or tab), and a double quote ("), which is ascii character 34.

Use the **no** form of the command to return the minimum number to the default value.

Syntax

login authentication min-password-special-chars *length*

no login authentication min-password-special-chars

Parameters

Parameter	Description	Possible Values	Default Value
length	The minimum number of digit characters in a user password	0-30	0

User Level

admin

Context

general

Example

To set the minimum number of special characters that a password must contain, to 1:

```
G450-001(super)# login authentication min-password-special-chars 1
```

Related Commands

login authentication inactivity-period, login authentication lockout, login authentication min-password-digit-chars, login authentication min-password-length, login authentication min-password-lower-chars, login authentication min-password-upper-chars, login authentication password-expire, password, show login authentication, show username, username

login authentication min-password-upper-chars

Use the **login authentication min-password-upper-chars** command to set the minimum number of uppercase characters that a password must contain. Use the **no** form of the command to return the minimum number to the default value.

Syntax

login authentication min-password-upper-chars ***length***

no login authentication min-password-upper-chars

Parameters

Parameter	Description	Possible Values	Default Value
length	The minimum number of uppercase characters in a user password	0-30	0

User Level

admin

Context

general

Example

To set the minimum number of uppercase characters that a password must contain, to 3:

```
G450-001(super)# login authentication min-password-upper-chars 3
```

Related Commands

login authentication inactivity-period, login authentication lockout, login authentication min-password-digit-chars, login authentication min-password-length, login authentication min-password-lower-chars, login authentication min-password-special-chars, login authentication password-expire, password, show login authentication, show username, username

login authentication password-expire

Use the **login authentication password-expire** command to cause all local user passwords to expire after a specified number of days. For existing accounts, the expiration policy starts on the day you use this command; for new accounts, the expiration policy starts on the day they are created. Accounts with expired passwords are locked and require an administrator to reset the account using the username command. However, a user can change the password before it expires using the password command. Starting 10 days before password expiration, every time the user logs on a message appears, informing the user that the password will expire in *n* days.

Use the **no** form of the command to deactivate the password expiration policy. By default, the password expiration policy is deactivated for backward compatibility.

Note:

The **no** form of the command does not re-enable accounts deactivated because of the password expiration policy. To re-enable an account, an administrator must run the username command and re-configure the account using the same user name and password.

Note:

This command does not apply to the root account.

Syntax

login authentication password-expire *days*

no login authentication password-expire

Parameters

Parameter	Description	Possible Values	Default Value
days	The number of days after which an account's password expires	**2-365**	

User Level

admin

Context

general

Example

To set password expiration to six months:

```
G450-001(super)# login authentication inactivity-period 180
```

Related Commands

login authentication inactivity-period, login authentication lockout, login authentication min-password-digit-chars, login authentication min-password-length, login authentication min-password-lower-chars, login authentication min-password-special-chars, login authentication min-password-upper-chars, password, show login authentication, show username, username

password

Use the **password** command to change your password. If a password expiration policy is being implemented, then starting from 10 days before password expiration, a warning appears every time you log on, informing you that your password will expire in *n* days.

The new password you enter must match the password policies determined by login authentication min-password-length, login authentication min-password-upper-chars, login authentication min-password-lower-chars, login authentication min-password-digit-chars, and login authentication min-password-special-chars.

Note:

For the new password to take effect, run the copy running-config startup-config command.

Note:

This command applies only to local user accounts. It does not apply to a Services account or a remote Radius account.

Syntax

password

User Level

read-write

Context

general

Example

To change your user password:

```
G450-001(super)# password

  Enter new password: xxxxxxx
  Confirm new password:  xxxxxxx

Password was changed; please commit changes to have the change permanent.
```

Related Commands

login authentication inactivity-period, login authentication lockout, login authentication min-password-digit-chars, login authentication min-password-length, login authentication min-password-lower-chars, login authentication min-password-special-chars, login authentication min-password-upper-chars, login authentication password-expire, show login authentication, show username, username

show login authentication

Use the **show login authentication** command to view the login authentication settings and information.

Syntax

show login authentication

User Level

admin

Context

general

Example

To view the login authentication settings and information:

```
G450-001(super)# show login authentication
Services logins: On
Local craft: On
Lockout time: 180 seconds
Lockout attempt threshold: 3
Authentication response time: 120 seconds
CLI logout timeout: Off
Inactivity period:  90 days
Password expiration period Off
Min password length: 10
Min lower case chars: 1
Min upper case chars: 0 (default)
Min digit chars: 1
Min special chars: 0 (default)
```

Related Commands

login authentication inactivity-period, login authentication lockout, login authentication min-password-digit-chars, login authentication min-password-length, login authentication min-password-lower-chars, login authentication min-password-special-chars, login authentication min-password-upper-chars, login authentication password-expire, password, show username, username

show username

Use the **show username** command to display local user accounts.

Syntax

show username

User Level

admin

Context

general

Example

To display all defined user accounts:

```
G450-001(super)# show username

User          Access        Account     Active
account       level         type
------------------------------  -----------  ----------  ----------------
root          admin         local       yes
flori         admin         local       yes (8 days left)
flori_new     admin         local       yes (8 days left)
craft         read-only     local       no
udi1          read-only     local       yes (8 days left)
flori111      read-only     local       yes (8 days left)
flori_lock    read-only     local       yes (8 days left)
floriram      admin         local       yes (8 days left)
init          admin         local       no
flori_11      read-only     local       yes (8 days left)
flori_admin   read-only     local       yes (8 days left)
craft         admin         Services    yes
inads         tech          Services    yes
init          dev           Services    yes
rasaccess     read-only     Services    yes
sroot         dev           Services    yes
```

Output fields

Name	Description
User account	The user name of the account
Access level	The access level granted to this user account. This can be one of the following: • **read-only** • **read-write** • **admin**
Account type	The account type - local or remote. This can be one of the following: • **local** • **Services**
Active	Whether the account is active.

Related Commands

login authentication inactivity-period, login authentication lockout, login authentication min-password-digit-chars, login authentication min-password-length, login authentication min-password-lower-chars, login authentication min-password-special-chars, login authentication min-password-upper-chars, login authentication password-expire, password, show login authentication, username

username

Use the **username** command to add a local user account. Use the **no** form of the command to remove the user account from the system.

By default there is only a single user account, named **root**, with password **root**, which accesses the administrator level. You cannot delete this basic user account, nor modify its access level. However, you can modify its basic password.

Note:

For security reasons, you should change the **root** password immediately.

Syntax

username ***name*** **[password** ***passwd*** **| asg-secret** ***secret*****] access-type** ***access_type***

no username ***name***

Parameters

Parameter	Description	Possible Values	Default Value
name	New user name or **dadmin**	Minimum four character string	
passwd	User's password	The minimum password length, minimum number of uppercase characters, minimum number of lowercase characters, minimum number of digit characters, and minimum number of special characters must comply with the settings in: login authentication min-password-length, login authentication min-password-upper-chars, login authentication min-password-lower-chars, login authentication min-password-digit-chars, and login authentication min-password-special-chars.	
secret	ASG secret key of a dadmin user	32 hexadecimal characters	
access_type	Access type definition	**read-only**, **read-write**, **admin** **Note:** A dadmin user and a root user must be assigned an **admin** access type.	

User Level

admin

Context

general

Example

To create a new user account with username john, password john7Long, and a read-write access:

```
G450-001(super)# username john password john7Long access-type read-write
User account added.
```

To change the password of the root user:

```
G450-001(super)# username root password mY1secret access-type admin
User account modified.
```

Note:

You cannot change the access type of the root user:

```
G450-001(super)# username root password VerySecret3 access-type read-write
ERROR: User account root has always an administrator access type.
```

Note:

If you wish to define a username which includes spaces, you must enclose the entire name in quotation marks, for example “new york”.

Related Commands

login authentication inactivity-period, login authentication lockout, login authentication min-password-digit-chars, login authentication min-password-length, login authentication min-password-lower-chars, login authentication min-password-special-chars, login authentication min-password-upper-chars, login authentication password-expire, password, show login authentication, show username

USP configuration

interface serial

Use the **interface serial** command to enter Serial interface or sub interface configuration mode. If the specified interface or sub interface does not exist, the system creates it and enters its configuration mode.

Use the **no** form of the command to delete the interface. The **no** form can only be used to delete sub L3 and sub frame relay interfaces. The command fails for USP interfaces and when higher or lower layers are defined for that interface.

Syntax

[no] interface Serial *module/if_number* [*if_link_type*]

For USP interfaces ***if_number*** has the syntax:

port[.***ip_interface*** | {.***sub_interface***[.***ip_interface***]}]

For DS1 interfaces ***if_number*** has the syntax:

port:***channel_group***[.***ip_interface*** | {.***sub_interface***[.***ip_interface***]}]

Parameters

Parameter	Description	Possible Values	Default Value
module	The interface module number		
port	The port number of the interface		
channel_group		For E1: **0-30** For T1: **0-23**	
sub_interface		**1-127**	
ip_interface		**0-1024**	
if_link_type		**point-to-point**	

User Level

read-write

Context

general, interface:Serial (FR SUB)

Example

To create point to point sub-interface number 17 over channel group 2 over E1/T1 controller number 1:

```
G450-001(super)# interface Serial 3/1:2.17 point-to-point
```

Related Commands

description (interface), interface console, interface fastethernet, interface loopback, interface tunnel, interface USB-modem, interface vlan, ip address, ip admin-state, ip broadcast-address, ip crypto-group, load-interval, show ip interface brief

bandwidth

Use the **bandwidth** command to set the bandwidth parameter manually for this interface. Use the **no** form of this command to restore the bandwidth parameter to its default value. The manually specified bandwidth value overrides the dynamically calculated bandwidth during route cost calculations.

Syntax

bandwidth *kilobits*

no bandwidth

Parameters

Parameter	Description	Possible Values	Default Value
kilobits	The bandwidth for the interface in kilobits per second	**1-10000000**	**2048** (for Frame Relay)

User Level

read-write

Context

interface:Serial (DS1 PPP L2, DS1 PPP L2-L3, DS1 FR L2, DS1 FR-SUB L2, DS1 FR-SUB L2-L3, USP PPP L2, USP PPP L2-L3, USP FR L2), FastEthernet (L2, L2-L3, PPP L2, PPP L2-L3), VLAN (L2, L2-L3), Loopback (L2, L2-L3), Tunnel (L2, L2-L3), Dialer (L2, L2-L3)

Example

To manually set the bandwidth for the VLAN interface to 100 KB/s:

```
G450-001(if:Vlan 1)# bandwidth 100
```

Related Commands

idle-character, ignore dcd, interface serial, invert txclock, nrzi-encoding, transmitter-delay

idle-character

Use the **idle-character** command to set the bit pattern used to indicate an idle line. Use the **no** form of this command to restore the default value. For E1 and USP interfaces, the default value is **flags**. For T1 interfaces, the default is **marks**.

Syntax

idle-character {flags|marks}

no idle-character

Parameters

Parameter	Description	Possible Values	Default Value
flags	Keyword specifying that flags are transmitted to indicate an idle line		
marks	Keyword specifying that marks are transmitted to indicate an idle line		

User Level

read-write

Context

interface:Serial (DS1 PPP L2, DS1 PPP L2-L3, DS1 FR L2, USP PPP L2, USP PPP L2-L3, USP FR L2)

Example

To set the idle-character to marks:

```
G450-001(if:Serial 3/1)# idle-character marks
```

Related Commands

bandwidth, ignore dcd, interface serial, invert txclock, nrzi-encoding, transmitter-delay

ignore dcd

Use the **ignore dcd** command to specify how the system monitors the line to determine if it is up or down. Specify **ignore dcd** to ignore DCD signals, and instead use DSR/CTS signals to determine the line's status. Use the **no** form of the command to specify that DCD signals are used to determine line status.

Syntax

[no] ignore dcd

User Level

read-write

Context

interface:Serial (USP FR-L2, USP PPP-L2, USP PPP L2-L3)

Example

To ignore DCD signals on an interface:

```
G450-001(if:Serial 3/1:1)# ignore dcd
```

Related Commands

bandwidth, idle-character, interface serial, invert txclock, nrzi-encoding, transmitter-delay

invert txclock

Use the **invert txclock** command to invert the transmit clock signal from the data communications equipment (DCE). Use the **no** form of the command to restore the signal to not inverted.

Syntax

[no] invert txclock

User Level

read-write

Context

interface:Serial (USP FR L2, USP PPP L2, USP PPP L2-L3)

Example

To invert the transmit clock signal on an interface:

```
G450-001(if:Serial 3/1:1)# invert txclock
```

Related Commands

bandwidth, idle-character, ignore dcd, interface serial, nrzi-encoding, transmitter-delay

nrzi-encoding

Use the **nrzi-encoding** command to enable the non-return-to-zero inverted (NRZI) line coding format on the specified interface. Use the **no** form of the command to disable NRZI encoding.

Syntax

[no] nrzi-encoding

User Level

read-write

Context

interface:Serial (USP FR L2, USP PPP L2, USP PPP L2-L3)

transmitter-delay

Use the **transmitter-delay** command to set the minimum number of flags to be sent between successive packets. Use the **no** form of the command to restore the transmitter-delay value to the default of 0.

Syntax

transmitter-delay *number*

no transmitter-delay

Parameters

Parameter	Description	Possible Values	Default Value
number	The number of flags	**0-15**	

User Level

read-write

Context

interface:Serial (USP FR L2, USP PPP L2, USP PPP L2-L3)

Example

To set the transmitter-delay to send at least 10 flags between packets:

```
G450-001(if:Serial 4/1)# transmitter-delay 10
```

Related Commands

bandwidth, idle-character, ignore dcd, interface serial, invert txclock, nrzi-encoding

Van Jacobson header compression

clear ip tcp header-compression

Use the **clear ip tcp header-compression** command to clear TCP compression statistics either for all enabled interfaces or for a specific interface. To clear TCP compression statistics for all enabled interfaces, do not enter an interface type and number.

Note:

There is no renegotiation of parameters.

Syntax

clear ip tcp header-compression [*interface_type interface_number*]

Parameters

Parameter	Description	Possible Values	Default Value
interface_type	The type of interface		
interface_number	The interface number		

User Level

read-only

Context

general

Example

To clear TCP compression statistics for all enabled interfaces:

```
G450-001(super)# clear ip tcp header-compression
```

Related Commands

clear ip rtp header-compression, ip rtp compression-connections, ip rtp header-compression, ip rtp max-period, ip rtp max-time, ip rtp non-tcp-mode, ip rtp port-range, ip tcp compression-connections, ip tcp header-compression, show ip rtp header-compression, show ip rtp header-compression brief, show ip tcp header-compression

ip tcp compression-connections

Use the **ip tcp compression-connections** command to specify the total number of TCP header compression connections supported on the current interface. Use the **no** form of this command to restore the default value of 16 connections.

Syntax

[no] ip tcp compression-connections *number*

Parameters

Parameter	Description	Possible Values	Default Value
number	The number of TCP compression connections	**3-256**	**16**

User Level

read-write

Context

interface:Serial (DS1 PPP L2, DS1 PPP L2-L3, DS1 FR-SUB L2, DS1 FR-SUB L2-L3, USP PPP L2, USP PPP L2-L3), Dialer (L2, L2-L3, L3)

Example

To specify that 20 TCP header compression connections are to be supported in the current interface:

```
G450-001(super-if:Dialer 1)# ip tcp compression-connections 20
```

Related Commands

clear ip rtp header-compression, clear ip tcp header-compression, ip rtp compression-connections, ip rtp header-compression, ip rtp max-period, ip rtp max-time, ip rtp non-tcp-mode, ip rtp port-range, ip tcp header-compression, show ip rtp header-compression, show ip rtp header-compression brief, show ip tcp header-compression

ip tcp header-compression

Use the **ip tcp header-compression** command to enable TCP header compression on the current interface. Use the **no** form of this command to disable both RTP and TCP compression on the current interface.

Syntax

[no] ip tcp header-compression [iphc-format]

Parameters

Parameter	Description	Possible Values	Default Value
iphc-format	Keyword specifying the header compression format. **Note:** • For a PPP or Dialer interface, specifying the **iphc-format** parameter activates IPHC compression, while not specifying the command activates VJ compression (unless IPHC compression is already active) • For a Frame Relay IETF interface, you must specify the **iphc-format** parameter in order to activate compression. IPHC compression is then activated. • For a Frame Relay non-IETF interface, the **ip tcp header-compression** command activates VJ compression. The **iphc-format** parameter is not accessible since IPHC compression is not supported.		

User Level

read-write

Context

interface:Serial (DS1 PPP L2, DS1 PPP L2-L3, DS1 FR-SUB L2, DS1 FR-SUB L2-L3, USP PPP L2, USP PPP L2-L3), Dialer (L2, L2-L3, L3)

Example

To enable TCP header compression on Serial interface 3/1:1.1:

```
G450-001(if:Serial 3/1:1.1) ip tcp header-compression
```

Related Commands

clear ip rtp header-compression, clear ip tcp header-compression, ip rtp compression-connections, ip rtp header-compression, ip rtp max-period, ip rtp max-time, ip rtp non-tcp-mode, ip rtp port-range, ip tcp compression-connections, show ip rtp header-compression, show ip rtp header-compression brief, show ip tcp header-compression

show ip tcp header-compression

Use the **show ip tcp header-compression** command to display TCP header compression statistics for a specific interface. If no interface is specified, it shows TCP header compression statistics for all interfaces.

Syntax

show ip tcp header-compression [*interface_name*]

Parameters

Parameter	Description	Possible Values	Default Value
interface_name	The name of the interface		

User Level

read-only

Context

general

Example

To display TCP header compression statistics for all interfaces:

```
G450-001(super)# show ip tcp header-compression
IP TCP header compression statistics:
Interface Serial 3/1:1.1:
  Rcvd:    0 Full Headers, 0 Compressed, 0 Errors
  Sent:    85 Full Headers, 34 Compressed,
           1139 Bytes Saved, 4335 Bytes Sent,
           1.26 Efficiency Improvement Factor
  Connect: Active, 3 Rx Slots, 3 Tx Slots
```

Output fields

Name	Description
Rcvd	Information on received TCP packets, as follows: • Full Headers — the number of TCP packets with full headers received • Compressed — the number of TCP packets with compressed headers received • Errors — the number of packets discarded during de-compression due to errors
Sent	Information on sent TCP packets, as follows: • Full Headers — the number of TCP packets with full headers sent • Compressed — the number of TCP packets with compressed headers sent • Bytes Saved — the total saving in bytes due to compression • Bytes Sent — the total number of bytes sent after compression • Efficiency Improvement Factor — the improvement factor, calculated as *(bytes saved + bytes sent)/ bytes sent* (rounded to two decimal places)
Connect	Connection information, as follows: • Active/Inactive — whether TCP header compression is negotiated and working on this interface • Rx Slots — the number of TCP sessions to decompress • Tx Slots — the number of TCP sessions to compress

Related Commands

clear ip rtp header-compression, clear ip tcp header-compression, ip rtp compression-connections, ip rtp header-compression, ip rtp max-period, ip rtp max-time, ip rtp non-tcp-mode, ip rtp port-range, ip tcp compression-connections, ip tcp header-compression, show ip rtp header-compression, show ip rtp header-compression brief

show ip tcp header-compression brief

Use the **`show ip tcp header-compression brief`** command to display a subset of TCP header compression statistics for a specific interface. If no interface is specified, it shows TCP header compression statistics for all interfaces.

Syntax

`show ip tcp header-compression brief [`*`interface_name`*`]`

Parameters

Parameter	Description	Possible Values	Default Value
interface_name	The name of the interface		

User Level

read-only

Context

general

Example

To display concise TCP header compression statistics for all interfaces:

```
G450-001(super)# show ip tcp header-compression brief

Interface   Active   Slots  Packets   Bytes     Improvement
                           Sent      Saved       Factor
---------- -------- ------  --------  --------- -----------
Serial 1:0   NO      16      0           0          1.00
```

Output fields

Name	Description
Interface	The interface on which TCP header compressions is being applied
Active	Whether TCP header compression is active and working on this interface
Slots	The number of Rx and Tx slots. That is, the total number of TCP header compression connections supported on this interface.
Packets Sent	The number of compressed packets sent + the number of full headers sent
Bytes Saved	The total saving in bytes due to compression
Improvement Factor	The efficiency of the compression, calculated as *(bytes saved + bytes sent) / bytes sent* (rounded to two decimal places)

Related Commands

clear ip rtp header-compression, clear ip tcp header-compression, ip rtp compression-connections, ip rtp header-compression, ip rtp max-period, ip rtp max-time, ip rtp non-tcp-mode, ip rtp port-range, ip tcp compression-connections, show ip rtp header-compression, show ip rtp header-compression brief, show ip tcp header-compression

VLAN configuration

clear port static-vlan

Use the **clear port static-vlan** command to delete statically configured VLANs from the port.

Syntax

clear port static-vlan *module/port_range vlan_id*

Parameters

Parameter	Description	Possible Values	Default Value
module	The module number		
port_range	The port or range of ports which are being bound		
vlan_id	The VLAN ID to remove		

User Level

read-write

Context

general

Example

To remove VLAN 5 from port 6/5:

```
G450-001(super)# clear port static-vlan 6/5 5
VLAN 5 is unbound from port 6/5
```

Related Commands

clear vlan, icc-vlan, interface vlan, set port static-vlan, set port vlan, set port vlan-binding-mode, set trunk, set vlan, show cam vlan, show port vlan-binding-mode, show trunk, show vlan

clear vlan

Use the **clear vlan** command to delete an existing VLAN and its interface. When you clear a VLAN, all ports assigned to that VLAN are returned to the default VLAN.

Syntax

clear vlan ***vlan_id*** | {**name** ***vlan_name***}

Parameters

Parameter	Description	Possible Values	Default Value
vlan_id	The VLAN number		
name	Keyword specifying to identify the VLAN by the VLAN name		
vlan_name	The VLAN name. If you wish to enter a name which includes spaces, you must enclose the entire name in quotation marks, for example “new york”.		

User Level

read-write

Context

general

Example

To delete VLAN 100:

```
G450-001(super)# clear vlan 100
This command will assign all ports on vlan 100 to their default in the entire
management domain - do you want to continue (Y/N)?  y
VLAN 100 deletion successful
```

Related Commands

clear port static-vlan, icc-vlan, interface vlan, set port static-vlan, set port vlan, set port vlan-binding-mode, set trunk, set vlan, show cam vlan, show port vlan-binding-mode, show trunk, show vlan

interface vlan

Use the **interface vlan** command to enter interface VLAN configuration mode. Use the **no** form of this command to delete the interface.

If the specified interface does not exist, the system creates it and enters its configuration mode.

Syntax

[no] interface vlan *vlan_id*[.*ip_interface*]

Parameters

Parameter	Description	Possible Values	Default Value
vlan_id	The VLAN ID number of this interface	**1-4090**	
ip_interface	The IP sub-interface number within this interface. A number of IP interfaces may be bound to a Layer 3 interface.	**0-1024**	

User Level

read-write

Context

general

Example

To create VLAN 2 and enter its configuration context:

```
G450-001(super)# interface Vlan 2
```

To create a sub interface 1 on VLAN 2:

```
G450-001(if:Vlan 2)# interface Vlan 2.1
```

Related Commands - IP interface configuration

description (interface), interface console, interface fastethernet, interface loopback, interface serial, interface tunnel, interface USB-modem, ip address, ip admin-state, ip broadcast-address, load-interval, show ip interface brief

Related Commands - VLAN configuration

clear port static-vlan, clear vlan, icc-vlan, set port static-vlan, set port vlan, set port vlan-binding-mode, set trunk, set vlan, show cam vlan, show port vlan-binding-mode, show trunk, show vlan

---

icc-vlan

Use the **icc-vlan** command to set the current VLAN as the ICC-VLAN.

Syntax

icc-vlan

User Level

read-write

Context

interface: VLAN (L2, L2-L3)

Example

To set VLAN 2 as the ICC VLAN:

```
G450-001(super)# interface vlan 2
G450-001(if:Vlan 2)# icc-vlan
```

Related Commands - ICC configuration

show icc-vlan

Related Commands - VLAN configuration

clear port static-vlan, clear vlan, interface vlan, set port static-vlan, set port vlan, set port vlan-binding-mode, set trunk, set vlan, show cam vlan, show port vlan-binding-mode, show trunk, show vlan

set port static-vlan

Use the **set port static-vlan** command to assign a static VLAN to a port.

Syntax

set port static-vlan *module/port vlan_num*

Parameters

Parameter	Description	Possible Values	Default Value
module	The module number		
port	The port or range of ports which are being bound		
vlan_num	VLAN to bind to the port		

User Level

read-write

Context

general

Example

To bind ports 10/5 through 10/6 in the G450 to VLAN 2:

```
G450-001# set port static-vlan 10/5-6 2
VLAN 2 is bound to port 10/5
VLAN 2 is bound to port 10/6
```

Related Commands

clear port static-vlan, clear vlan, icc-vlan, interface vlan, set port vlan, set port vlan-binding-mode, set trunk, set vlan, show cam vlan, show port vlan-binding-mode, show trunk, show vlan

set port vlan

Use the **set port vlan** command to set the port VLAN ID (PVID).

Note:
You need to define a VLAN before setting a port VLAN ID.

Syntax

set port vlan *vlan_num module/port*

Parameters

Parameter	Description	Possible Values	Default Value
vlan_num	Number identifying the VLAN		
module	The module number		
port	Number of the port on the module. You can also specify a range of ports separated by a dash, for example, 10/5-6 for both ETH LAN ports 5-6 on the front panel.		

User Level

read-write

Context

general

Example

To set the VLAN ID for port 10/3 to 1:

```
G450-001(super)# set port vlan 1 10/3
Port 10/3 added to VLAN 1
```

Related Commands

clear port static-vlan, clear vlan, icc-vlan, interface vlan, set port static-vlan, set port vlan-binding-mode, set trunk, set vlan, show cam vlan, show port vlan-binding-mode, show trunk, show vlan

set port vlan-binding-mode

Use the **set port vlan-binding-mode** command to define which VLANs will be bound to the specified port.

Syntax

set port vlan-binding-mode *module/port_list value*

Parameters

Parameter	Description	Possible Values	Default Value
module	The module number		
port_list	The port to bind to VLANs. You can also specify a range of ports separated by a dash, for example, 10/5-6 for both ETH LAN ports 5-6 on the front panel.		
value	The type of VLAN binding	**static** - the port supports only the VLANs that are manually configured for this port **bind-to-configured** - the port supports all the VLANs configured on the device	

User Level

read-write

Context

general

Example

To specify that ports 10/5 to port 10/6 will only support the VLANs manually configured for those ports:

```
G450-001# set port vlan-binding-mode 10/5-6 static
Set Port vlan binding method:10/5
Set Port vlan binding method:10/6
```

Related Commands

clear port static-vlan, clear vlan, icc-vlan, interface vlan, set port static-vlan, set port vlan, set trunk, set vlan, show cam vlan, show port vlan-binding-mode, show trunk, show vlan

set trunk

Use the **set trunk** command to configure the VLAN tagging mode of a port.

Syntax

set trunk *module/port* {off|dot1q}

Parameters

Parameter	Description	Possible Values	Default Value
module	Number of the module		
port	Number of the port on the module. You can also specify a range of ports separated by a dash, for example, 10/5-6 for both ETH LAN ports 5-6 on the front panel.		
off	Keyword that specifies to force the port to become a non-tagging port and persuade the neighboring port to become a non-tagging port. The port becomes a non-tagging port even if the neighbor port does not agree to become a non-tagging port.		
dot1q	Keyword that specifies IEEE 802.1q tagging on a Fast Ethernet or Gigabit Ethernet port		

User Level

read-write

Context

general

Example

To configure 802.1q VLAN tagging for port 6/5 in the G450:

```
G450-001(super)# set trunk 6/5 dot1q
Dot1Q VLAN tagging set on port 6/5.
```

Related Commands

clear port static-vlan, clear vlan, icc-vlan, interface vlan, set port static-vlan, set port vlan, set port vlan-binding-mode, set vlan, show cam vlan, show port vlan-binding-mode, show trunk, show vlan

set vlan

Use the **set vlan** command to create or modify a VLAN.

Syntax

set vlan *vlan_id* [name *vlan_name*]

Parameters

Parameter	Description	Possible Values	Default Value
vlan_id	The VLAN number	**1-4090**	
name	Keyword that allows naming or renaming the VLAN		
vlan_name	The VLAN name	string from 1-32 characters	

User Level

read-write

Context

general

Example

To create VLAN number 3, named “gregory”:

```
G450-001# set vlan 3 name gregory
VLAN id 3, vlan-name gregory created.
```

Note:

If you wish to define a name which includes spaces, you must enclose the entire name in quotation marks, for example “new york”.

Related Commands

clear port static-vlan, clear vlan, icc-vlan, interface vlan, set port static-vlan, set port vlan, set port vlan-binding-mode, set trunk, show cam vlan, show port vlan-binding-mode, show trunk, show vlan

show cam vlan

Use the **show cam vlan** command to display all MAC entries in the CAM table for a specific VLAN.

Syntax

show cam vlan *vlan_number*

Parameters

Parameter	Description	Possible Values	Default Value
vlan_number	VLAN for which to display the CAM table		

User Level

read-only

Context

general

Example

To display all MAC entries in the CAM table for VLAN 54:

```
G450-001(super)# show cam vlan 54
Total Matching CAM Entries Displayed = 3
Dest MAC/Route Dest VLAN Destination Ports
------------------- ---- -----------------
00:01:02:dd:2f:9f   54   6/13
00:02:2d:47:00:6f   54   10/2
00:02:4b:5b:28:40   54   6/13
```

Related Commands

clear port static-vlan, clear vlan, icc-vlan, interface vlan, set port static-vlan, set port vlan, set port vlan-binding-mode, set trunk, set vlan, show port vlan-binding-mode, show trunk, show vlan

show port vlan-binding-mode

Use the **show port-vlan-binding** command to display port VLAN binding mode information. If no module number is specified, information for all ports on all modules is displayed. If no port number is specified, information for all ports on the specified module is displayed.

Syntax

show port vlan-binding-mode [*module*[/*port*]]

Parameters

Parameter	Description	Possible Values	Default Value
module	The number of the module		
port	The number of the port on the module. You can also specify a range of ports, for example, 10/5-6 for both ETH LAN ports 5-6 on the front panel.		

User Level

read-only

Context

general

Example

To display VLAN binding information for all ports:

```
G450-001(super)# show port vlan-binding-mode
port 10/5 is statically bound
port 10/6 is statically bound
```

Related Commands

clear port static-vlan, clear vlan, icc-vlan, interface vlan, set port static-vlan, set port vlan, set port vlan-binding-mode, set trunk, set vlan, show cam vlan, show port vlan-binding-mode, show trunk, show vlan

show trunk

Use the **show trunk** command to display VLAN tagging information for the media gateway. If no port is specified, information for all ports is displayed.

Syntax

show trunk [*module*[/*port*]]

Parameters

Parameter	Description	Possible Values	Default Value
module	Number of the module		
port	Number of the port on the module. You can also specify a range of ports separated by a dash, for example, 10/5-6 for both ETH LAN ports 5-6 on the front panel.		

User Level

read-only

Context

general

Example

To display binding information for port 10/5 to port 10/6:

```
G450-001(super)# show trunk 10/5-6
Port   Mode  Binding mode     Native vlan    Vlans allowed on trunk
------ ----- ---------------  -----------    ----------------------
10/5   off   statically bound  1              1

Port   Mode  Binding mode     Native vlan    Vlans allowed on trunk
------ ----- ---------------  -----------    ----------------------
10/6   off   statically bound  1              1
```

Output fields:

Field	Description
Port	Module and port numbers
Mode	VLAN tagging status of the port. Possible values: • **dot1q** — the port uses dot1Q tagging mode • **off** — the port uses clear tagging mode
Binding mode	Binding mode of the port. Possible values: • **statically bound** • **bound-to-configured**
Native vlan	Number of the Port VLAN ID. This is the VLAN to which received untagged traffic is assigned.

Related Commands

clear port static-vlan, clear vlan, icc-vlan, interface vlan, set port static-vlan, set port vlan, set port vlan-binding-mode, set trunk, set vlan, show cam vlan, show port vlan-binding-mode, show vlan

show vlan

Use the **show vlan** command to display the VLANs configured in the media gateway. If no VLAN is specified, information for all VLANs is displayed.

Syntax

show vlan [*vlan_id* | name *vlan_name*]

Parameters

Parameter	Description	Possible Values	Default Value
vlan_id	VLAN number to display	**1-4090**	
name	Keyword indicating to specify the VLAN by name		
vlan_name	VLAN name to display		

User Level

read-only

Context

general

Example

To display information for all VLANs:

```
G450-001(super)# show vlan

VLAN ID Vlan-name
------- --------------------------------
1       v1
5       V5
10      V10
15      V15
20      V20
25      V25
```

To display information for VLAN 1:

```
G450-001(super)# show vlan 1

VLAN ID Vlan-name
------- --------------------------------
1       V1
Switch Ports currently bound to this vlan:
In module 10: 5
Switch Ports statically bound to this vlan:
None
```

Related Commands

clear port static-vlan, clear vlan, icc-vlan, interface vlan, set port static-vlan, set port vlan, set port vlan-binding-mode, set trunk, set vlan, show cam vlan, show port vlan-binding-mode, show trunk

VoIP

campon-busyout voip-dsp

Use the **campon-busyout voip-dsp** command to put the entire VoIP engine or individual DSP childboard in busyout (not available) state for maintenance or firmware upgrade.

Syntax

campon-busyout voip-dsp [*dsp-id*[*/core-id*]]

Parameters

Parameter	Description	Possible Values	Default Value
dsp-id	Keyword indicating the slot number of the VoIP DSP childboard	**1-4**	
core-id	Keyword indicating the core ID	**1-4**	

User Level

read-write

Context

general

Example

To camp on busyout the entire VoIP engine:

```
G450-001(super)# campon-busyout voip-dsp
```

To camp on busyout DSP childboard #3:

```
G450-001(super)# campon-busyout voip-dsp 3
```

To camp on busyout DSP childboard #3, Core 2:

```
G450-001(super)# campon-busyout voip-dsp 3/2
```

Related Commands

busyout voip-dsp, release voip-dsp, reset voip-dsp, show voip-dsp, show voip-parameters, test voip-dsp

reset voip-dsp

Use the **reset voip-dsp** command to reset a VoIP DSP childboard on the motherboard.

Syntax

reset voip-dsp *dsp-id*

Parameters

Parameter	Description	Possible Values	Default Value
dsp-id	The slot number of the VoIP DSP childboard	**1-4**	

User Level

read-write

Context

general

Example

To reset the VoIP childboard in slot 2:

```
G450-001(super)# reset voip-dsp 2
```

Related Commands

busyout voip-dsp, campon-busyout voip-dsp, release voip-dsp, show voip-dsp, show voip-parameters, test voip-dsp

show voip-dsp

Use the **show voip-dsp** command to display information about the DSP and DSP cores parameters, status and occupancy.

Syntax

show voip-dsp [*dsp-id*]

Parameters

Parameter	Description	Possible Values	Default Value
dsp-id	Keyword indicating the slot number of the VoIP DSP childboard	**1-4**	

User Level

read-only

Context

general

Examples

To display DSP parameters of DSP 1 use:

```
G450-001(super)# show voip-dsp 1

DSP #1 PARAMETERS
----------------------------------------------------------
Slot              : 1
Board type        : 8122
Hw  Vintage       :  3
FW Vintage        : 235

DSP #1 CURRENT STATE
----------------------------------------------------------
In Use  :     10 of  80 channels, 37 of 300 points (0.0% used)
State   :     InUse
Admin State:  Release

Core#  Channels        Admin state   State      Error
       In Use                                  Msg
----   -------         -----------    -----      ------------------
1      4 of 20           Release      InUse      No Status Messages
2      1 of 20           Camp-on      InUse      No Status Messages
3      5 of 20           Release      InUse      No Status Messages
4      0 of 20           Busyout      Idle       No Status Messages
```

Related Commands

busyout voip-dsp, campon-busyout voip-dsp, release voip-dsp, reset voip-dsp, show voip-parameters, test voip-dsp

show voip-parameters

Use the **show voip-parameters** command to display information about the VoIP engine.

Syntax

show voip-parameters

User Level

read-only

Context

general

Examples

To display VoIP information:

```
G450-001(super)# show voip-parameters

VOIP ENGINE PARAMETERS
------------------------------------------------------------
IP (PMI)                    : 149.49.78.140
DSP Firmware Version        : N/A
Fault Status                : No Fault Messages
Additional Status           : No Status Messages

CURRENT STATE
------------------------------------------------------------
In Use     : 20 of  100 channels, 240 of 1200 points (0.0% used)

VoIP -DSPs PARAMETERS
VoIP   Child   CODE  SUFFIX     HW      FW          Chan      Admin     Oper     Fault
Slot   Board                 VINTAGE  VINTAGE       InUse     State     State    Status
----   -----   ----  ------  -------  --------      -------   -----     -----    ------
1      VOIP    8122    A       3       235          20/80     Release    InUse  No Error
2      VOIP    7119    A       5       215          0/20      Busyout    Idle   No Error
3      -- Not Installed --
4      SYNC
```

Related Commands - VoIP

busyout voip-dsp, campon-busyout voip-dsp, release voip-dsp, reset voip-dsp, show voip-dsp, test voip-dsp

Related Commands - QoS

set qos bearer, set qos control, set qos signal, show qos-rtcp

VoIP testing

busyout voip-dsp

Use the **busyout voip-dsp** command to put the VoIP entity in busyout (not available) state. This is recommended before starting a Bit Transfer Rate test.

Note:

Status changes made during the Bit Transfer Rate test create SNMP traps.

Syntax

busyout voip-dsp [*dsp-id*[*/core-id*]]

Parameters

Parameter	Description	Possible Values	Default Value
dsp-id	The slot number of the VoIP DSP childboard	**1-4**	
core-id	The core ID	**1-4**	

User Level

read-write

Context

general

Example

To busyout DSP childboard #3:

```
G450-001(super)# busyout voip-dsp 3
```

To busyout DSP childboard # 1, Core 2:

```
G450-001(super)# busyout  voip-dsp 1/2
```

Related Commands

campon-busyout voip-dsp, release voip-dsp, reset voip-dsp, show voip-dsp, show voip-parameters, test voip-dsp

release voip-dsp

Use the **release voip-dsp** command to release the VoIP entity from a busyout (not available) state. This command also ends a running Bit Transfer Rate test.

Note:

Status changes that occur during the Bit Transfer Rate test create SNMP traps.

Syntax

release voip-dsp [*dsp-id*[*/core-id*]]

Parameters

Parameter	Description	Possible Values	Default Value
dsp-id	The slot number of the VoIP DSP childboard	**1-4**	
core-id	The core ID	**1-4**	

User Level

read-write

Context

general

Example

To release the entire VoIP engine:

```
G450-001(super)# release voip-dsp
```

To release DSP childboard #2:

```
G450-001(super)# release voip-dsp 2
```

To release core #4 in DSP childboard #1:

```
G450-001(super)# release voip-dsp 1/4
```

Related Commands

busyout voip-dsp, campon-busyout voip-dsp, reset voip-dsp, show mm, show voip-dsp, show voip-parameters, test voip-dsp

show voip-parameters

Use the **show voip-parameters** command to display information about the current VoIP engine.

Syntax

show voip-parameters

User Level

read-only

Context

general

Examples

To display VoIP information:

```
G450-001(super)# show voip-parameters

VOIP ENGINE PARAMETERS
------------------------------------------------------------
IP (PMI)                   : 149.49.78.140
DSP Firmware Version       : N/A
Fault Status               : No Fault Messages
Additional Status          : No Status Messages

CURRENT STATE
------------------------------------------------------------
In Use     : 20 of  100 channels, 240of 1200 points (0.0% used)

VoIP -DSPs PARAMETERS
VoIP   Child   CODE  SUFFIX     HW      FW          Chan      Admin     Oper     Fault
Slot   Board                  VINTAGE  VINTAGE       InUse     State     State    Status
----   -----   ----  ------  -------  --------      -------   -----     -----    ------
1      VOIP    8122    A       3       235          20/80     Release    InUse  No Error
2      VOIP    7119    A       5       215          0/20      Busyout    Idle   No Error
3      -- Not Installed --
4      SYNC
```

Related Commands - VoIP

busyout voip-dsp, campon-busyout voip-dsp, release voip-dsp, reset voip-dsp, show voip-dsp, test voip-dsp

Related Commands - QoS

set qos bearer, set qos control, set qos signal, show ip qos-list

test voip-dsp

Use the **test voip-dsp** command to start a BTR test on the VoIP engine or a VoIP subsystem. Also refer to busyout voip-dsp on page 1247, and release voip-dsp on page 1248.

Note:

If you do not run the busyout voip-dsp command before the **test voip-dsp** command, only non-disruptive tests will run.

Note:

Status changes during the test create SNMP traps.

Syntax

test voip-dsp [*dsp-id*[*/core-id*]]

Parameters

Parameter	Description	Possible Values	Default Value
dsp-id	The slot number of the VoIP DSP childboard	**1-4**	
core-id	The core ID	**1-4**	

User Level

read-write

Context

general

Example:

To start a BTR test on all DSPs at once:

```
G450-001(super)# test voip-dsp

DSP      Core                    Result                Error Code
----     -----                   ------------          -----------------
1          1                       PASS
1          2                       FAIL                Error Code #1
1          3                       FAIL                Error Code #3
1          4                       PASS
2          1                       PASS
3          -                       Not Present
4          -                       Not a VoIP-DSP childboard
```

```
Error Codes
1       Loopback test 1 failed
2       Loopback test 2 failed
3       Loopback test 3 failed
4       Loopback test 4 failed
5       Loopback test 5 failed
6       Ping test failed
7       Core not responding
```

To launch a BTR test on core 2 in DSP 1:

```
G450-001(super)# test voip-dsp 1/2
DSP CORE TEST RESULTS
DSP   Core                    Result              Error Code
----  -----                   -------             ------------
1     2                        FAIL               Error Code #1
```

Related Commands

busyout voip-dsp, campon-busyout voip-dsp, release voip-dsp, reset voip-dsp, show voip-dsp, show voip-parameters

VPN

clear crypto isakmp

Use the **clear crypto isakmp** command to flush a specific ISAKMP SA or all the ISAKMP SAs.

Tip:

Use the command **show crypto isakmp sa** to display the connection IDs.

Tip:

It is recommended to use the command **clear crypto sa** before running **clear crypto isakmp**.

Syntax

clear crypto isakmp [*C-id*]

Parameters

Parameter	Description	Possible Values	Default Value
C-id	The connection ID. **Note:** If you do not enter a connection ID, the entire database is flushed.	**0-32, 766**	

User Level

read-write

Context

general

Example

To clear connection 1:

```
G450-001(super)# clear crypto isakmp 1
```

To clear the entire database:

```
G450-001(super)# clear crypto isakmp
```

Related Commands

clear crypto sa, clear crypto sa counters, show crypto ipsec sa, show crypto ipsec transform-set, show crypto isakmp peer, show crypto isakmp peer-group, show crypto isakmp policy, show crypto isakmp sa, show crypto map, show ip active-lists, show ip crypto-list

clear crypto sa

Use the **clear crypto sa** command to clear all or specific IPSec SAs (Security Association structures).

Syntax

clear crypto sa [all | **list** ***crypto_list_id*** | **peer** ***peer_ip_address*** | **spi** ***peer_ip_address*** **esp** ***spi number*****]**

Parameters

Parameter	Description	Possible Values	Default Value
all	Keyword specifying that all IPSec SAs should be cleared		
list	Keyword specifying that all crypto IPSec SAs associated with *crypto_list_id* should be cleared		
peer	Keyword specifying that all crypto IPSec SAs associated with crypto peer having the address *peer_ip_address* should be cleared		
spi	Keyword specifying that all crypto IPSec SAs associated with *peer_ip_address* and *spi* should be cleared. SPI is the ID of a specific SA, and can be learned by running show crypto ipsec sa.		

User Level

read-write

Context

general

Examples

To clear all IPSec SAs:

```
G450-001(super)# clear crypto sa all
```

To clear IPSec SA with peer IP address 1.0.0.2 and SPI number 70045:

```
G450-001(super)# clear crypto sa spi 1.0.0.2 esp 70045
```

Related Commands

clear crypto isakmp, clear crypto sa counters, show crypto ipsec sa, show crypto ipsec transform-set, show crypto isakmp peer, show crypto isakmp peer-group, show crypto isakmp policy, show crypto isakmp sa, show crypto map, show ip active-lists, show ip crypto-list

clear crypto sa counters

Use the **clear crypto sa counters** command to clear the crypto SA counters.

Syntax

clear crypto sa counters

User Level

read-write

Context

general

Example

To clear crypto SA counters:

```
G450-001(super)# clear crypto sa counters
```

Related Commands

clear crypto isakmp, clear crypto sa, show crypto ipsec sa, show crypto ipsec transform-set, show crypto isakmp peer, show crypto isakmp peer-group, show crypto isakmp policy, show crypto isakmp sa, show crypto map, show ip active-lists, show ip crypto-list

crypto ipsec df-bit

Use the **crypto ipsec df-bit** command to set the Don't-Fragment bit to one of the following modes:

- **clear** — the DF bit of the encapsulated packet is never set, and PMTUD is not maintained for the IPSec tunnel. Packets traversing an IPSec tunnel are pre-fragmented according to the MTU of the SA, regardless of their DF bit. In case packets are fragmented, the DF bit is copied to every fragment of the original packet.
- **copy** — the DF bit of the encapsulated packet is copied from the original packet, and Path MTU Discovery (PMTUD) is maintained for the IPSec tunnel.

Use the **no** form of the command to restore the Don't-Fragment bit to the default value: `copy`.

Syntax

[no] crypto ipsec df-bit {clear | copy}

Parameters

Parameter	Description	Possible Values	Default Value
clear	Keyword indicating to clear the Don't-Fragment bit		
copy	Keyword indicating to copy the Don't-Fragment bit		

User Level

read-write

Context

interface:Serial (DS1 PPP L2, DS1 PPP L2-L3, DS1 FR-SUB L2, DS1 FR-SUB L2-L3, USP PPP L2, USP PPP L2-L3), FastEthernet (L2, L2-L3, PPP L2, PPP L2-L3), VLAN (L2, L2-L3), Dialer (L2, L2-L3)

Example

To set the Don't-Fragment bit to the state of clear:

```
G450-001(if:Serial 4/1)# crypto ipsec df-bit clear
```

Related Commands

crypto ipsec minimal-pmtu, ip crypto-group

crypto ipsec minimal-pmtu

Use the **crypto ipsec minimal-pmtu** command to set the minimal PMTU value which can be applied to an SA when the G450 participates in Path MTU Discovery (PMTUD) for the tunnel pertaining to that SA. Use the **no** form of the command to restore the minimal PMTU to the default value: 300.

Syntax

[no] crypto ipsec minimal-pmtu *bytes*

Parameters

Parameter	Description	Possible Values	Default Value
bytes	The length of the minimum PMTU	**68-1400**	**300**

User Level

read-write

Context

interface:Serial (DS1 PPP L2, DS1 PPP L2-L3, DS1 FR-SUB L2, DS1 FR-SUB L2-L3, USP PPP L2, USP PPP L2-L3), FastEthernet (L2, L2-L3, PPP L2, PPP L2-L3), VLAN (L2, L2-L3), Dialer (L2, L2-L3)

Example

To set the minimal PMTU value to 128:

```
G450-001(if:Serial 4/1)# crypto ipsec minimal-pmtu 128
```

Related Commands

crypto ipsec df-bit, ip crypto-group

crypto ipsec nat-transparency udp-encapsulation

NAT Traversal is enabled in the device by default. Use the **crypto ipsec nat-transparency udp-encapsulation** command to re-enable NAT Traversal if it was disabled. Use the **no** form of the command to completely disable NAT Traversal in the device.

Syntax

[no] crypto nat-transparency udp-encapsulation

User Level

read-write

Context

general

Example

To re-enable NAT Traversal:

```
G450-001(super)# no crypto ipsec nat-transparency udp-encapsulation
```

Related Commands

crypto isakmp nat keepalive, ip crypto-group

crypto ipsec transform-set

Use the **crypto ipsec transform-set** command to enter the IKE phase 2 (IPSec) transform-set context and create or edit IPSec parameters for the VPN tunnel. Use the **no** form of the command to delete IKE phase 2 (IPSec) parameters for the VPN tunnel.

Syntax

[no] crypto ipsec transform-set ***name***
{esp-des | esp-3des | esp-aes | esp-aes-192 | esp-aes-256 | esp-null} [{esp-md5-hmac | esp-sha-hmac}] [comp-lzs]

Note:

If you want to enable authentication only, you must enter the **esp-null** parameter.

Parameters

Parameter	Description	Possible Values	Default Value
name	The transform-set name	**1-32 characters, no spaces**	
esp-des	Keyword specifying the following encryption type: Encapsulation Security Protocol and Data Encryption Standard		
esp-3des	Keyword specifying the following encryption type: Encapsulation Security Protocol and Triple Data Encryption Standard		
esp-aes	Keyword specifying the following encryption type: Encapsulation Security Protocol and Advanced Encryption Standard using a 128-bit key		
esp-aes-192	Keyword specifying the following encryption type: Encapsulation Security Protocol and Advanced Encryption Standard using a 192-bit key		
esp-aes-256	Keyword specifying the following encryption type: Encapsulation Security Protocol and Advanced Encryption Standard using a 256-bit key		

Parameter	Description	Possible Values	Default Value
esp-null	Keyword specifying the following encryption type: Encapsulation Security Protocol without encryption. **Note:** This option is intended for lab testing.		
esp-md5-hmac	Keyword specifying the following authentication type: Encapsulation Security Protocol, md5 hashing and keyed-hash mac		
esp-sha-hmac	Keyword specifying the following authentication type: Encapsulation Security Protocol, secure hash algorithm and keyed-hash mac		
comp-lzs	Keyword specifying IP compression with the LZS algorithm		

User Level

read-write

Context

general

Examples

To configure an IPSec transform set with encryption and authentication:

```
G450-001(super)# crypto ipsec transform-set ts2 esp-des esp-md5-hmac
G450-001(config-transform:ts2)#
```

To configure an IPSec transform set with encryption, authentication and IP compression:

```
G450-001(super)# crypto ipsec transform-set ts6 esp-des esp-md5-hmac comp-lzs
G450-001(config-transform:ts6)#
```

To configure an IPSec transform set with authentication only:

```
G450-001(super)# crypto ipsec transform-set ts3 esp-null esp-md5-hmac
G450-001(config-transform:ts3)#
```

To enter the crypto IPSec transform-set context:

```
G450-001(super)# crypto ipsec transform-set ts1
G450-001(config-transform:ts1)#
```

Related Commands

crypto map, crypto isakmp peer, crypto isakmp peer-group, crypto isakmp policy, ip crypto-group, ip crypto-list, mode, set pfs, set security-association lifetime, show crypto ipsec transform-set

mode

Use the **mode** command to set the IPSec encapsulation mode. Use the **no** form of the command to return the value to the default encapsulation mode, which is tunnel mode.

Note:

Transport mode cannot be used unless the remote VPN peer supports Transport mode and is configured to use it.

Syntax

[no] mode {tunnel | transport}

Parameters

Parameter	Description	Possible Values	Default Value
tunnel	Keyword specifying the IPSec VPN tunnel mode. This is the default setting.		
transport	Keyword specifying the IPSec VPN transport mode. **Note:** Specify this mode only for a GRE tunnel.		

User Level

read-write

Context

crypto ipsec transform-set

Example

To set the IPSec encapsulation mode to tunnel:

```
G450-001(config-transform:ts1)# mode tunnel
```

Related Commands

crypto ipsec transform-set, set pfs, set security-association lifetime, show crypto ipsec transform-set

set pfs

Use the **set pfs** command to specify whether each IKE phase 2 negotiation will employ Perfect Forward Secrecy (PFS), and if yes, which Diffie-Hellman group to employ. PFS ensures that even if someone were to discover the long-term secret(s), the attacker would not be able to recover the session keys, both past and present. In addition, the discovery of a session key compromises neither the long-term secrets nor the other session keys.

Use the **no** form of the command to disable PFS for IKE phase 2 (default setting).

Syntax

[no] set pfs [group1 | group2 | group5 | group14]

Note:

Using **set pfs** with no parameters sets the PFS group to 1.

Parameters

Parameter	Description	Possible Values	Default Value
group1	Keyword specifying that IKE employ the 768-bit Diffie-Hellman prime modulus group		
group2	Keyword specifying that IKE employ the 1,024-bit Diffie-Hellman prime modulus group		
group5	Keyword specifying that IKE employ the 1536-bit Diffie-Hellman prime modulus group		
group14	Keyword specifying that IKE employ the 2048-bit Diffie-Hellman prime modulus group		

User Level

read-write

Context

crypto ipsec transform-set

Example

To specify that IKE employs the 768-bit Diffie-Hellman prime modulus group:

```
G450-001(config-transform:ts1)# set pfs group1
```

Related Commands

crypto ipsec transform-set, mode, set security-association lifetime, show crypto ipsec transform-set

set security-association lifetime

Use the **set security-association lifetime** command to set the IKE phase 2 (IPSec) SA (security-association) lifetime. Use the **no** form of the command to disable the SA lifetime.

Syntax

[no] set security-association lifetime { **seconds** ***seconds*** | **kilobytes** {***kilobytes*** | disable} }

Parameters

Parameter	Description	Possible Values	Default Value
seconds	Keyword indicating to specify the lifetime in seconds		
seconds	The lifetime, in seconds	**120-86,400**	
kilobytes	Keyword indicating to specify the lifetime by the amount of traffic that should pass through the IPSec tunnel before the security association should time out		
kilobytes	The amount of traffic, in kilobytes	**2,560-536,870,912**	
disable	Keyword specifying unlimited lifetime		

User Level

read-write

Context

crypto ipsec transform-set

Example

To set the IKE phase 2 SA lifetime to 300 seconds

```
G450-001(config-transform:ts1)# set security-association lifetime seconds 300
```

Related Commands

crypto ipsec transform-set, mode, set pfs, show crypto ipsec transform-set

crypto isakmp invalid-spi-recovery

Use the **crypto isakmp invalid-spi-recovery** command to enable invalid SPI recovery (default setting). Use the **no** form of the command to disable invalid SPI recovery.

Syntax

[no] crypto isakmp invalid-spi-recovery

User Level

read-write

Context

general

Example

To enable invalid SPI recovery:

```
G450-001(super)# no crypto isakmp invalid-spi-recovery
```

Related Commands

ip crypto-group

crypto isakmp nat keepalive

NAT Traversal keepalive is enabled in the device by default. Use the **crypto isakmp nat keepalive** command to re-enable NAT Traversal keepalive if it was disabled, and configure the keepalive interval. The purpose of this command is to keep the NAT devices tables updated. Use the **no** form of the command to disable NAT Traversal keepalives.



Tip:

Set the NAT Traversal keepalive interval to be less than the NAT translation aging time on the NAT device.

Syntax

[no] crypto isakmp nat keepalive [*seconds*]

Parameters

Parameter	Description	Possible Values	Default Value
seconds	The number of seconds between NAT Traversal keepalive messages	**5-3600**	

User Level

read-write

Context

general

Example

To enable NAT Traversal keepalive for an interval of 60 seconds:

```
G450-001(super)# crypto isakmp nat keepalive 60
```

Related Commands

crypto ipsec nat-transparency udp-encapsulation, ip crypto-group

crypto isakmp peer

Use the **crypto isakmp peer** command to enter the crypto ISAKMP peer context and create or edit an ISAKMP peer. Use the **no** form of the command to delete a remote VPN peer.

Note:

You cannot delete an ISAKMP peer that is referenced by a crypto map; you must first delete the peer from the crypto map by entering crypto map context using the **crypto map** command, and then delete the peer using the **no set peer** command.

Syntax

[no] crypto isakmp peer {address *peer-address* | fqdn *fqdn-str*}

Parameters

Parameter	Description	Possible Values	Default Value
peer-address	The IP address of the ISAKMP peer		
fqdn	The Fully Qualified Domain Name of the ISAKMP peer	A string of up to 110 characters.	

User Level

read-write

Context

general

Examples

To enter the crypto ISAKMP peer context for the ISAKMP peer at IP address 149.49.70.1:

```
G450-001(super)# crypto isakmp peer address 149.49.70.1
G450-001(config-peer:149.49.70.1)#
```

To enter the crypto ISAKMP peer context for the ISAKMP peer at FQDN vpn.lnd.ny.avaya.com:

```
G450-001(super)# crypto isakmp peer fqdn vpn.lnd.ny.avaya.com
G450-001(config-peer:vpn.lnd.ny.avaya.com)#
```

Related Commands

continuous-channel, crypto ipsec transform-set, crypto map, crypto isakmp peer-group, crypto isakmp policy, description (ISAKMP peer), initiate mode, ip crypto-group, ip crypto-list, isakmp-policy, keepalive (VPN), keepalive-track, pre-shared-key, self-identity, show crypto isakmp peer, suggest-key

continuous-channel

Use the **continuous-channel** command in a crypto ISAKMP peer context, to enable continuous-channel IKE, which keeps the IKE phase1 session always up and running, even if there is no traffic. Use the **no** form of this command to disable continuous-channel IKE (default setting).

Use the **continuous-channel** command in a crypto map context, to enable continuous-channel IPSec, which keeps an IPSec tunnel continuously up, even if there is no traffic. Use the **no** form of this command to disable continuous-channel IPSec (default setting).

Syntax

[no] continuous-channel

User Level

read-write

Context

crypto isakmp peer, crypto map

Example

To enable continuous-channel IKE:

```
G450-001(config-peer:149.49.70.1)# continuous-channel
```

To enable continuous-channel IPSec:

```
G450-001(config-crypto:10)# continuous-channel
```

Related Commands - VPN - crypto isakmp peer

description (ISAKMP peer), crypto isakmp peer, initiate mode, isakmp-policy, keepalive (VPN), keepalive-track, pre-shared-key, self-identity, show crypto isakmp peer, suggest-key

Related Commands - VPN - crypto map

crypto map, description (crypto map), set transform-set, set dscp, set peer (crypto map), set peer-group, show crypto map

description (ISAKMP peer)

Use the **description** command to enter a description for the ISAKMP peer. Use the **no** form of the command to clear a description for the ISAKMP peer.

Syntax

[no] description *desc*

Parameters

Parameter	Description	Possible Values	Default Value
desc	The description of the ISAKMP peer. **Note:** If you wish to include spaces in the description, you must enclose the string in quotation marks (“”).	string of 1-80 characters	

User Level

read-write

Context

crypto isakmp peer

Example

```
To specify the ISAKMP peer description as “New York office”:
G450-001(config-peer:135.64.102.109)# description "New York office"
```

Related Commands

continuous-channel, crypto isakmp peer, initiate mode, isakmp-policy, keepalive (VPN), keepalive-track, pre-shared-key, self-identity, show crypto isakmp peer, suggest-key

initiate mode

Use the **initiate mode** command to specify which IKE Phase-1 mode to use when communicating with the peer. Use the **no** form of this command to restore the default setting, which is **main** mode.

Note:

Aggressive mode is one of the prerequisites for working with dynamic IP addresses.

Syntax

[no] initiate mode {main | aggressive | none}

Parameters

Parameter	Description	Possible Values	Default Value
main	Keyword specifying that the device operate in IKE main mode		
aggressive	Keyword specifying that the device operate in IKE aggressive mode. Specify this option when local IP is dynamic.		
none	Keyword specifying that the device act as an IKE Phase-1 responder. Specify this option only when communicating with a dynamically addressed remote peer.		

User Level

read-write

Context

crypto isakmp peer

Example

To initiate aggressive mode:

```
G450-001(config-peer:149.49.70.1)# initiate mode aggressive
```

Related Commands

continuous-channel, description (ISAKMP peer), crypto isakmp peer, isakmp-policy, keepalive (VPN), keepalive-track, pre-shared-key, self-identity, show crypto isakmp peer, suggest-key

isakmp-policy

Use the **isakmp-policy** command to set the ISAKMP policy for the ISAKMP peer. Use the **no** form of the command to delete the ISAKMP policy for the ISAKMP peer.

Note:

You cannot delete an ISAKMP policy that is referenced by an ISAKMP peer that is, in turn, referenced by an active crypto map.

Syntax

[no] isakmp-policy ***id***

Parameters

Parameter	Description	Possible Values	Default Value
id	The ID of the ISAKMP policy	**1-20**	

User Level

read-write

Context

crypto isakmp peer

Example

To set ISAKMP policy for peer 149.49.70.1:

```
G450-001(config-peer:149.49.70.1)# isakmp-policy 20
```

Related Commands

description (ISAKMP peer), continuous-channel, crypto isakmp peer, initiate mode, keepalive (VPN), keepalive-track, pre-shared-key, self-identity, show crypto isakmp peer, suggest-key

keepalive (VPN)

Use the **keepalive** command in crypto isakmp peer interface context to enable DPD (Dead Peer Detection) keepalives that check whether the remote peer is up. Use the **no** form of this command to disable DPD keepalives (default setting).

Syntax

[no] keepalive [*seconds* [retry *retry-seconds*] [on-demand | periodic]]

Parameters

Parameter	Description	Possible Values	Default Value
seconds	The number of seconds between DPD keepalive probes	**10-3600**	
retry-seconds	The number of seconds between retries if keepalive fails	**2-60**	

Parameter	Description	Possible Values	Default Value
on-demand	Keyword indicating to send DPD probes only when data traffic is sent to the remote peer		
periodic	Keyword indicating to send DPD probes periodically, regardless of whether data traffic is being sent to the remote peer		

User Level

read-write

Context

crypto isakmp peer

Example

To enable DPD keepalives, setting the rate to 10 seconds and retries to 2:

```
G450-001(config-peer:149.49.70.1)# keepalive 10 retry 2
```

Related Commands

description (ISAKMP peer), continuous-channel, crypto isakmp peer, initiate mode, isakmp-policy, keepalive-track, pre-shared-key, self-identity, show crypto isakmp peer, suggest-key

keepalive-track

Use the **keepalive-track** command to bind an object tracker to a remote VPN peer or to an interface, to check whether the remote peer or the interface is up. Use the **no** form of this command to disable this mechanism (default setting).

Note:

When configuring VPN, you can use the **keepalive-track** command instead of the **keepalive** command when the remote peer does not support DPD, or when you want to monitor servers behind the VPN remote peer.

Note:

You cannot configure both **keepalive-track** and **ip address dhcp** (DHCP Client) on the WAN FastEthernet interface.

Syntax

keepalive-track ***track-id***

no keepalive-track

Parameters

Parameter	Description	Possible Values	Default Value
track-id	The ID of the object tracker	**1-100**	

User Level

read-write

Context

interface:Serial (DS1 PPP L2, DS1 PPP L2-L3, DS1 FR-SUB L2, DS1 FR-SUB L2-L3, USP PPP L2, USP PPP L2-L3) FastEthernet (L2, L2-L3, PPP L2, PPP L2-L3), Loopback (L2, L2-L3), Dialer (L2, L2-L3)
crypto isakmp peer

Example

To register a remote VPN peer with object tracker 5:

```
G450-001(config-peer:149.49.70.1)# keepalive-track 5
```

To register the FastEthernet interface with object tracker 2:

```
G450-001(config-if:FastEthernet 10/2)# keepalive-track 2
```

Related Commands - VPN

description (ISAKMP peer), continuous-channel, crypto isakmp peer, initiate mode, isakmp-policy, keepalive (VPN), pre-shared-key, self-identity, show crypto isakmp peer, suggest-key

pre-shared-key

Use the **pre-shared-key** command to configure the IKE pre-shared key. Use the **no** form of the command to delete the IKE pre-shared key.

Tip:

You can use the command suggest-key to generate a key.

Syntax

[no] pre-shared-key *psk-str* [hexadecimal]

Parameters

Parameter	Description	Possible Values	Default Value
psk-str	The pre-shared key string	**1-127** alphanumerical characters **1-64** bytes in hexadecimal notation	**32**
hexadecimal	Keyword indicating that the pre-shared key string is being specified in hexadecimal notation		

User Level

read-write

Context

crypto isakmp peer

Example

To configure the IKE pre-shared key as `GNpi1odGNBrB5z4GJLzI`:

```
G450-001(config-peer:149.49.70.1)# pre-shared-key GNpi1odGNBrB5z4GJLzI
```

To configure the IKE pre-shared key as 61623 hexadecimal:

```
G450-001(config-peer:149.49.70.1)# pre-shared-key 616263 hexadecimal
```

Related Commands

description (ISAKMP peer), continuous-channel, crypto isakmp peer, initiate mode, isakmp-policy, keepalive (VPN), keepalive-track, self-identity, show crypto isakmp peer, suggest-key

self-identity

Use the **self-identity** command to set the identity of the current device. Use the **no** form of this command to return the value to the default value which is the address of the device.

Syntax

[no] self-identity {address | fqdn *fqdn-str*}

Note:

Specify the self-identity in FQDN format when using aggressive mode.

Note:

If the remote ISAKMP peer is an Avaya Security Gateway (VSU / SG), you must specify the self-identity FQDN using upper-case letters only.

Parameters

Parameter	Description	Possible Values	Default Value
address	Keyword indicating to set self-identity to the address of the current device. This is the default setting		
fqdn-str	Sets self-identity to the Fully Qualified Domain Name of the current device		

User Level

read-write

Context

crypto isakmp peer

Example

To set self-identity to the address of the current device:

```
G450-001(config-peer:149.49.70.1)# self-identity address
```

Related Commands

description (ISAKMP peer), continuous-channel, crypto isakmp peer, initiate mode, isakmp-policy, keepalive (VPN), keepalive-track, pre-shared-key, show crypto isakmp peer, suggest-key

suggest-key

Use the **suggest-key** utility command to generate a random string which you can use as a pre-shared key for IKE. You must use the same key on both peers.

Syntax

suggest-key [*key-length*] [key-type {alphanumeric | hexadecimal}]

Parameters

Parameter	Description	Possible Values	Default Value
key-length	The length of the key to be generated	**8-127** alphanumerical characters, or **8-64** bytes in hexadecimal notation	**32** characters
key-type	Keyword indicating the type of key to be generated	**alphanumeric** or **hexadecimal**	**alphanumeric**

User Level

read-write

Context

crypto isakmp peer

Example

To generate a cryptographic-grade random string:

```
G450-001(config-peer:149.49.70.1)# suggest-key
The suggest key: GNpi1odGNBrB5z4GJLz156jDmRWAGFES
```

To generate a random string of 8 alphanumeric characters:

```
G450-001(config-peer:149.49.70.1)# suggest-key 8 alphanumeric
The suggest key: iEvKoQ1e
```

Related Commands

continuous-channel, description (ISAKMP peer), initiate mode, isakmp-policy, keepalive (VPN), keepalive-track, pre-shared-key, self-identity, show controllers remote

crypto isakmp peer-group

Use the **crypto isakmp peer-group** command to enter the crypto ISAKMP peer-group context and create or edit an ISAKMP peer group. Use the **no** form of the command to delete a peer-group.

Note:

A peer-group must contain at least one peer in order for it to be *ready*. Use the **set peer** command to add a peer to the peer-group.

Note:

You cannot delete an ISAKMP peer-group that is referenced by a crypto map; you must first delete the peer-group from the crypto map by entering crypto map context using the **crypto map** command, and then delete the peer using the **no set peer-group** command.

Syntax

[no] crypto isakmp peer-group *peer-group-name*

Parameters

Parameter	Description	Possible Values	Default Value
peer-group-name	The name of the ISAKMP peer group	A string no longer than 110 characters	

User Level

read-write

Context

general

Example

To enter the crypto ISAKMP peer-group context for the peer-group vpn.avaya.com:

```
G450-001(super)# crypto isakmp peer-group vpn.avaya.com
G450-001(config-peer-grp:vpn.avaya.com)#
```

Related Commands

crypto ipsec transform-set, crypto map, crypto isakmp peer, crypto isakmp policy, description (ISAKMP peer group), ip crypto-group, ip crypto-list, set peer (peer group), show crypto isakmp peer-group

description (ISAKMP peer group)

Use the **description** command to enter a description for the ISAKMP peer group. Use the **no** form of the command to clear a description for the ISAKMP peer group.

Syntax

[no] description *desc*

Parameters

Parameter	Description	Possible Values	Default Value
desc	The description of the ISAKMP peer group. **Note:** If you wish to include spaces in the description, you must enclose the string in quotation marks (“”).	string of 1-80 characters	

User Level

read-write

Context

crypto isakmp peer-group

Example

To specify the ISAKMP peer group description as “Avaya peer group”:

```
G450-001(config-peer-grp:vpn.avaya.com)# description "Avaya peer group"
```

Related Commands

crypto isakmp peer-group, set peer (peer group), show crypto isakmp peer-group

set peer (peer group)

Use the **set peer** command to add a peer to the peer-group. Use the **no** form of the command to remove a peer from the peer-group.

Syntax

[no] set peer {*ip-address* | *hostname*} [index *index*]

Parameters

Parameter	Description	Possible Values	Default Value
ip-address	The remote peer IP address		

Parameter	Description	Possible Values	Default Value
hostname	The remote peer hostname		
index	A number specifying the relative position of the peer within the peer-group. If this optional parameter is not used, the current peer is added at the end of the peer-group list, and is assigned an index following the last peer's index.	**1-5**	

User Level

read-write

Context

crypto isakmp peer-group

Examples

To add the peer at IP address 149.49.52.135 to the first position of the peer group:

```
G450-001(config-peer-grp:vpn.avaya.com)# set peer 149.49.52.135 1
```

Related Commands

crypto isakmp peer-group, description (ISAKMP peer group), show crypto isakmp peer-group

crypto isakmp policy

Use the **crypto isakmp policy** command to enter the crypto ISAKMP policy context and create or edit IKE Phase 1 parameters.

Syntax

crypto isakmp policy ***id***

Parameters

Parameter	Description	Possible Values	Default Value
id	The identity of the ISAKMP policy	**1-20**	

User Level

read-write

Context

general

Example

To enter the crypto ISAKMP policy context and create or edit IKE Phase 1 parameters for the ISAKMP policy 1:

```
G450-001(super)# crypto isakmp policy 1
G450-001(config-isakmp:1)#
```

Related Commands

authentication, crypto ipsec transform-set, crypto map, crypto isakmp peer, crypto isakmp peer-group, crypto isakmp policy, description (ISAKMP policy), encryption, group, hash, ip crypto-list, ip crypto-group, lifetime, show crypto isakmp policy

authentication

Use the **authentication** command to set the authentication of ISAKMP policy to pre-shared secret.

Syntax

authentication { pre-share }

Parameters

Parameter	Description	Possible Values	Default Value
pre-share	Keyword specifying the method of authentication of the ISAKMP policy. This is the default setting.		

User Level

read-write

Context

crypto isakmp policy

Example

To set the authentication of ISAKMP policy to pre-shared secret:

```
G450-001(config-isakmp:1)# authentication pre-share
```

Related Commands

crypto isakmp policy, description (ISAKMP policy), encryption, group, hash, lifetime, show crypto isakmp policy

description (ISAKMP policy)

Use the **description** command to enter a description for the ISAKMP policy. Use the **no** form of the command to clear a description for the ISAKMP policy.

Syntax

[no] description *desc*

Parameters

Parameter	Description	Possible Values	Default Value
desc	The description of the ISAKMP policy. **Note:** If you wish to include spaces in the description, you must enclose the string in quotation marks (“”).	string of 1-80 characters	

User Level

read-write

Context

crypto isakmp policy

Example

To specify the ISAKMP policy description as “isakmp policy 1”:

```
G450-001(config-isakmp:1)# description "isakmp policy 1"
```

Related Commands

authentication, crypto isakmp policy, encryption, group, hash, lifetime, show crypto isakmp policy

encryption

Use the **encryption** command to set the encryption algorithm for an ISAKMP policy. Use the **no** form of this command to clear the encryption algorithm.

Syntax

[no] encryption *encryption*

Parameters

Parameter	Description	Possible Values	Default Value
encryption	The encryption algorithm to be used: • **des** — Data Encryption Standard - 56 bits • **3des** — Triple DES - 168 bits • **aes** — Advanced Encryption Standard - 128 bits • **aes-192** — Advanced Encryption Standard - 192 bits • **aes-256** — Advanced Encryption Standard - 256 bits	**des, 3des, aes, aes-192, aes-256**	**des**

User Level

read-write

Context

crypto isakmp policy

Example

To set the encryption algorithm for an ISAKMP policy as Triple DES:

```
G450-001(config-isakmp:1)# encryption 3des
```

Related Commands

authentication, crypto isakmp policy, description (ISAKMP policy), group, hash, lifetime, show crypto isakmp policy

group

Use the **group** command to set the Diffie-Hellman group for an ISAKMP policy. Use the **no** form of the command to set the Diffie-Hellman group to the default group 1.

Syntax

[no] group *group*

Parameters

Parameter	Description	Possible Values	Default Value
group	The Diffie-Hellman group for the ISAKMP policy	**1**, **2**, **5**, **14**	**1**

User Level

read-write

Context

crypto isakmp policy

Example

To set the Diffie-Hellman group for an ISAKMP policy to 1:

```
G450-001(config-isakmp:1)# group 1
```

Related Commands

authentication, crypto isakmp policy, description (ISAKMP policy), encryption, hash, lifetime, show crypto isakmp policy

hash

Use the **hash** command to set the hash method for an ISAKMP policy. Use the **no** form of the command to return the hash method to the default (`sha`).

Syntax

[no] hash *hash-method*

Parameters

Parameter	Description	Possible Values	Default Value
hash-method	The hash method for the ISAKMP policy: **sha** – Secure Hash Algorithm **md5** – Message Digest algorithm 5		**sha**

User Level

read-write

Context

crypto isakmp policy

Example

To set the hash method to Message Digest algorithm 5:

```
G450-001(config-isakmp:1)# hash md5
```

Related Commands

authentication, crypto isakmp policy, description (ISAKMP policy), encryption, group, lifetime, show crypto isakmp policy

---

lifetime

Use the **lifetime** command to set the lifetime of the ISAKMP SA in seconds. Use the **no** form of the command to return the lifetime to the default value.

Note:

You cannot change the lifetime settings of an ISAKMP policy referenced by an ISAKMP peer that is linked to a crypto map.

Syntax

[no] lifetime *seconds*

Parameters

Parameter	Description	Possible Values	Default Value
seconds	The number of seconds defining the lifetime of the ISAKMP SA	**60-86,400** (1 minute to 24 hours)	**86,400**

User Level

read-write

Context

crypto isakmp policy

Example

To set the lifetime of the ISAKMP SA to 100 seconds:

```
G450-001(config-isakmp:1)# lifetime 100
```

Related Commands

authentication, crypto isakmp policy, description (ISAKMP policy), encryption, group, hash, show crypto isakmp policy

crypto isakmp suggest-key

Use the **crypto isakmp suggest-key** command to generate a random string which you can use as a pre-shared key for IKE. You must use the same key on both peers.

Syntax

crypto isakmp suggest-key [*key-length*] [key-type {alphanumeric | hexadecimal}]

Parameters

Parameter	Description	Possible Values	Default Value
key-length	The length of the key to be generated	**8-127** alphanumerical characters **8-64** bytes in hexadecimal notation	**32** characters
key-type	Keyword indicating the type of key to be generated	**alphanumeric** or **hexadecimal**	**alphanumeric**

User Level

read-write

Context

general

Example

To generate a random string of any length:

```
G450-001# crypto isakmp suggest-key
The suggest key: GNpi1odGNBrB5z4GJLz156jDmRWAGFES
```

To generate a random string of 8 characters:

```
G450-001# crypto isakmp suggest-key 8
The suggest key: iEvKoQ1e
```

Related Commands

continuous-channel, crypto isakmp peer, description (ISAKMP peer), initiate mode, isakmp-policy, keepalive (VPN), keepalive-track, pre-shared-key, self-identity, show crypto isakmp peer, suggest-key

crypto map

Use the **crypto map** command to enter crypto map context and create or edit a crypto map. Use the **no** form of the command to delete a specific crypto map.

Note:

You cannot delete a crypto map that is being used by an active crypto-list.

Syntax

[no] crypto map *id*

Parameters

Parameter	Description	Possible Values	Default Value
id	The crypto map ID	**1-50**	

User Level

read-write

Context

general

Example

To enter the crypto map context and create or edit crypto map 10:

```
G450-001(super)# crypto map 10
G450-001(config-crypto:10)#
```

Related Commands

continuous-channel, crypto ipsec transform-set, crypto isakmp peer, crypto isakmp peer-group, crypto isakmp policy, description (crypto map), ip crypto-list, ip crypto-group, set transform-set, set dscp, set peer (crypto map), set peer-group, show crypto map

continuous-channel

Use the **continuous-channel** command in a crypto ISAKMP peer context, to enable continuous-channel IKE, which keeps the IKE phase1 session always up and running, even if there is no traffic. Use the **no** form of this command to disable continuous-channel IKE (default setting).

Use the **continuous-channel** command in a crypto map context, to enable continuous-channel IPSec, which keeps an IPSec tunnel continuously up, even if there is no traffic. Use the **no** form of this command to disable continuous-channel IPSec (default setting).

Syntax

[no] continuous-channel

User Level

read-write

Context

crypto isakmp peer, crypto map

Example

To enable continuous-channel IKE:

```
G450-001(config-peer:149.49.70.1)# continuous-channel
```

To enable continuous-channel IPSec:

```
G450-001(config-crypto:10)# continuous-channel
```

Related Commands - VPN - crypto isakmp peer

description (ISAKMP peer), crypto isakmp peer, initiate mode, isakmp-policy, keepalive (VPN), keepalive-track, pre-shared-key, self-identity, show crypto isakmp peer, suggest-key

Related Commands - VPN - crypto map

crypto map, description (crypto map), set transform-set, set dscp, set peer (crypto map), set peer-group, show crypto map

---

description (crypto map)

Use the **description** command to enter a description for the crypto map. Use the **no** form of the command to clear a description for the crypto map.

Syntax

[no] description *desc*

Parameters

Parameter	Description	Possible Values	Default Value
desc	The description of the crypto map. **Note:** If you wish to include spaces in the description, you must enclose the string in quotation marks (“”).	string of 1-80 characters	

User Level

read-write

Context

crypto map

Example

To specify the crypto map description as “crypto map 1”:

```
G450-001(config-crypto:10)# description "crypto map 1"
```

Related Commands

continuous-channel, crypto map, set transform-set, set dscp, set peer (crypto map), set peer-group, show crypto map

set dscp

Use the **set dscp** command to set the DSCP value in the tunneled packet. Use the **no** form of this command to take the DSCP value from the original header (default setting).

Syntax

[no] set dscp *dscp-value*

Parameters

Parameter	Description	Possible Values	Default Value
dscp-value	The static DSCP value in the DS field of the tunneled packet. The default setting is **no set dscp**, which specifies that the DSCP is copied from the DS field of the original packet.	**0-63**	

User Level

read-write

Context

crypto map

Examples

To set the DSCP value in the tunneled packet to 10:

```
G450-001(config-crypto:1)# set dscp 10
```

To specify that the DSCP is copied from the DS field of the original packet:

```
G450-001(config-crypto:1)# no set dscp
```

Related Commands

continuous-channel, description (crypto map), set peer (crypto map), set peer-group, set transform-set

---

set peer (crypto map)

Use the **set peer** command to attach a peer to a crypto map. Use the **no** form of the command to remove the peer from the crypto map.

Note:

You can only change the peer of a crypto map when the map is inactive.

Note:

The **set peer** and **set peer-group** commands are mutually exclusive. You can attach to a given crypto map either a peer or a peer-group, not both.

Syntax

set peer {***ip-address*** | ***hostname***}

no set peer

Parameters

Parameter	Description	Possible Values	Default Value
ip-address	The remote peer IP address		
hostname	The remote peer hostname		

User Level

read-write

Context

crypto map

Examples

To attach the peer at IP address 149.49.52.135 to crypto map 1:

```
G450-001(config-crypto:1)# set peer 149.49.52.135
```

Related Commands

continuous-channel, crypto map, description (crypto map), set transform-set, set dscp, set peer-group, show crypto map

---

set peer-group

Use the **set peer-group** command to attach a peer-group to a crypto map. Use the **no** form of the command to remove the peer-group from the crypto map.

Note:

You can only change the peer-group of a crypto map when the map is inactive.

Note:

The **set peer** and **set peer-group** commands are mutually exclusive. You must attach to a given crypto map either a peer or a peer-group, not both.

Syntax

set peer-group *peer-group-name*

no set peer-group

Parameters

Parameter	Description	Possible Values	Default Value
peer-group-name	The name of the peer-group		

User Level

read-write

Context

crypto map

Examples

To attach the peer group vpn.avaya.com to crypto map 1:

```
G450-001(config-crypto:1)# set peer-group vpn.avaya.com
```

Related Commands

continuous-channel, crypto map, description (crypto map), set transform-set, set dscp, set peer (crypto map), show crypto map

set transform-set

A crypto map object points to a single transform-set object, which contains the parameters required for IKE Phase 2 negotiation.

Use the **set transform-set** command to configure the transform-set. Use the **no** form of the command to remove the transform-set from the crypto map.

Note:

You cannot remove a transform-set from a crypto map that is being used by an active crypto-list. You must first de-activate the crypto-list, using the **no** form of the **ip crypto-group** command. See ip crypto-group on page 1290.

Syntax

[no] set transform-set *name*

Parameters

Parameter	Description	Possible Values	Default Value
name	The name of the transfer set	1-32 characters	

User Level

read-write

Context

crypto map

Example

To configure transform-set ts1:

```
G450-001(config-crypto:10)# set transform-set ts1
```

Related Commands

continuous-channel, crypto map, description (crypto map), set dscp, set peer (crypto map), set peer-group, show crypto map

ip crypto-group

Use the **ip crypto-group** command to activate a crypto-list in the context of the interface on which the crypto-list is activated. The command applies to the following interfaces:

- Serial
- FastEthernet
- Dialer

Use the **no** form of the command to deactivate a crypto-list.

Note:

The **ip crypto-group** command applies also to the VLAN interface, but this option is not recommended.

Note:

Most IPSec VPN parameters cannot be modified if they are linked to an active crypto-list. To modify a parameter linked to an active crypto-list, you must first deactivate the list using the **no ip crypto-group** command in the context of the interface on which the crypto-list is activated.

Syntax

[no] ip crypto-group *crypto-list-id*

Parameters

Parameter	Description	Possible Values	Default Value
crypto_list_id	The crypto-list number	**901-999**	

User Level

read-write

Context

interface:Serial (DS1 FR-SUB L2, DS1 FR-SUB L2-L3, DS1 PPP L2, DS1 PPP L2-L3, USP PPP L2, USP PPP L2-L3), FastEthernet (L2, L2-L3, PPP L2, PPP L2-L3, PPP L3), Dialer (L2, L2-L3), VLAN (L2, L2-L3)

Example

To activate crypto-list 901:

```
G450-001(if:Serial 4/1)# ip crypto-group 901
```

Related Commands

crypto ipsec df-bit, crypto ipsec minimal-pmtu

---

ip crypto-list

Use the **ip crypto-list** command to enter crypto-list context and create or edit a crypto-list. Use the **no** form of the command to delete a crypto-list.

Note:

You cannot delete an active crypto-list. You must first deactivate the list, using the **no** form of the **ip crypto-group** command.

Syntax

[no] ip crypto-list *index*

Parameters

Parameter	Description	Possible Values	Default Value
index	The crypto-list number	**901-999**	

User Level

read-write

Context

general

Example

To enter the crypto-list 901 context:

```
G450-001(super)# ip crypto-list 901
G450-001(Crypto 901)#
```

Related Commands

crypto ipsec transform-set, crypto map, crypto isakmp peer, crypto isakmp peer-group, crypto isakmp policy, description (ip rule), destination-ip, ip-rule (VPN), ip crypto-group, local-address, protect crypto map, source-ip, show ip active-lists, show ip crypto-list

ip-rule (VPN)

Use the **ip-rule** command to enter ip-rule context and create or modify a specific rule. Use the **no** form of the command to delete a specific rule.

Syntax

[no] ip-rule {*index* | default}

Parameters

Parameter	Description	Possible Values	Default Value
index	Number of the ip-rule	**1-1000**	
default	Keyword specifying ip-rule number 10,000 (last rule in the ordered list of rules)		

User Level

read-write

Context

ip crypto-list

Example

Create or modify rule 22 and enter its context:

```
G450-001(Crypto 901)# ip-rule 21
G450-001(Crypto 901/ip rule 21)#
```

Related Commands

description (ip rule), destination-ip, ip crypto-list, local-address, protect crypto map, source-ip, show ip crypto-list

description (ip rule)

Use the **description** command to enter a description for the ip-rule in the ip crypto-list. Use the **no** form of the command to clear a description for the ip-rule.

Syntax

[no] description *desc*

Parameters

Parameter	Description	Possible Values	Default Value
desc	The description of the ip-rule. **Note:** If you wish to include spaces in the description, you must enclose the string in quotation marks (“”).	string of 1-80 characters	

User Level

read-write

Context

ip crypto-list ip-rule

Example

To specify the ip-rule description as “vpn tunnel to uk headquarters”:

```
G450-001(Crypto 901/ip rule 20)# description "vpn tunnel to uk headquarters"
```

Related Commands

destination-ip, ip crypto-list, ip-rule (VPN), local-address, protect crypto map, source-ip, show ip crypto-list

destination-ip

Use the **destination-ip** command to specify the destination IP address of packets to which the current rule applies.

Use the **no** form of the command to set the destination IP address to any.

Syntax

destination-ip {host *ip*}|any|{*ip wildcard*}

no destination-ip

Parameters

Parameter	Description	Possible Values	Default Value
host	Keyword that specifies the current rule applies to a single host IP address		
ip	The destination IP address of the rule		
any	Keyword that specifies the current rule applies to any address		
ip wildcard	The range of IP addresses of the rule. The zero bits in the wildcard correspond to bits in the IP address that remain fixed. The one bits in the wildcard correspond to bits in the IP address that can vary. **Note:** This is the opposite of how bits are used in a netmask.		

User Level

read-write

Context

ip capture-list/ip-rule, ip access-control-list/ip-rule, ip pbr-list/ip-rule, ip qos-list/ip-rule, ip crypto-list ip-rule

Example

To specify that rule 22 applies to all packets having destination IP address 135.64.104.102:

```
G450-001(Crypto 901/ip rule 22)# destination-ip host 135.64.104.102
```

Related Commands - Packet sniffing

dscp (policy-based routing, packet sniffing, VPN), icmp, ip-protocol, show ip capture-list, source-ip, tcp destination-port, tcp source-port, udp destination-port, udp source-port

Related Commands - Policy-based routing

dscp (policy-based routing, packet sniffing, VPN), next-hop (policy-based routing), show ip next-hop-list, show isdn bri link

Related Commands - Policy

composite-operation, dscp (policy), show dscp-table, icmp, show composite-operation, show isdn bri link, source-ip, tcp destination-port, tcp established, tcp source-port, udp destination-port, udp source-port

Related Commands - VPN

description (ip rule), ip crypto-list, ip-rule (VPN), local-address, protect crypto map, source-ip, show ip crypto-list

protect crypto map

Use the **protect crypto map** command to protect traffic that matches this rule, by applying the IPSec processing configured by the specific crypto map.

Use the **no protect** command to specify that traffic matching this IP rule should not be protected. Traffic that matches this rule bypasses IPSec processing, and continues unprotected.

Note:

You cannot enable or disable crypto map protection when the crypto-list is active. You must first deactivate the list using the **no ip crypto-group** command in the context of the interface on which the crypto-list is activated.

Syntax

protect crypto map *crypto-map-id*

no protect

Parameters

Parameter	Description	Possible Values	Default Value
crypto-map-id	The ID of the crypto map	**1-50**	

User Level

read-write

Context

ip crypto-list/ip-rule

Examples

To protect traffic by applying the IPSec processing configured by crypto map 5:

```
G450-001(crypto 901/ip rule 21)# protect crypto map 5
```

Related Commands

description (ip rule), destination-ip, ip crypto-list, ip-rule (VPN), local-address, source-ip, show ip crypto-list

source-ip

Use the **source-ip** command to indicate that the current rule applies to packets from the specified source IP address.

Use the **no** form of the command to indicate that the current rule applies to packets from any IP address.

Syntax

source-ip {host *ip_address* | any | *ip_address wildcard*}

no source-ip

Parameters

Parameter	Description	Possible Values	Default Value
host	Keyword that indicates a specific host IP address		
ip_address	The IP address of packets to which the rule is applied		
any	Keyword that indicates any IP address		
ip_address wildcard	The range of IP addresses of the rule. The zero bits in the wildcard correspond to bits in the IP address that remain fixed. The one bits in the wildcard correspond to bits in the IP address that can vary. **Note:** This is the opposite of how bits are used in a netmask.		

User Level

read-write

Context

ip pbr-list ip-rule, ip qos-list ip-rule, ip capture-list ip-rule, ip access-control-list ip-rule, ip crypto-list ip-rule

Example

To specify that rule 22 of QoS policy list 460 applies to any packet coming from IP address 135.64.104.102:

```
G450-001(QoS 460/rule 22)# source-ip host 135.64.104.102
```

Related Commands - Policy-based routing

destination-ip, dscp (policy-based routing, packet sniffing, VPN), icmp, ip-protocol, show ip capture-list, tcp destination-port, tcp source-port, udp destination-port, udp source-port

Related Commands - Policy

composite-operation, destination-ip, dscp (policy), icmp, show composite-operation, show dscp-table, show isdn bri link, tcp destination-port, tcp established, tcp source-port, udp destination-port, udp source-port

Related Commands - VPN

description (ip rule), destination-ip, ip crypto-list, ip-rule (VPN), local-address, protect crypto map, show ip crypto-list

---

local-address

Use the **local-address** command to set the local IP address for the IPSec tunnels derived from the crypto-list. Use the **no** form of the command to delete the local IP address.

Note:

You must configure a local address before activating a list.

Note:

You cannot change or delete the local address of an active list.

Syntax

[no] local-address {*ip-interface-address* | *ip-interface-name-id*}

Parameters

Parameter	Description	Possible Values	Default Value
ip-interface-address	The IP address of an IP interface of the device		
ip-interface-name-id	The name of an IP interface of the device		

User Level

read-write

Context

ip crypto-list

Example

To set the local IP address for the IPSec tunnels to 192.168.49.1:

```
G450-001(crypto 901)# local-address 192.168.49.1
```

To set the local IP address for the IPSec tunnels to that of the FastEthernet 10/2.0:

```
G450-001(crypto 901)# local-address FastEthernet 10/2.0
```

Related Commands

description (ip rule), destination-ip, ip crypto-list, ip-rule (VPN), protect crypto map, source-ip, show ip crypto-list

---

show crypto ipsec sa

Use the **`show crypto ipsec sa`** command to display the IPSec SA database and related runtime, statistical, and configuration information. If no crypto-list, crypto-list rule, or peer IP address are specified, then all SAs are displayed, sorted first by interface and then by crypto-list rule index.

Note:

The IPSec SA statistics counters are reset when any of the following occurs:

- The **`clear crypto sa counters`** command is used.
- `avipsMonitorRstCntrs` is set in the MIB (equivalent to the above).
- The **`clear crypto sa all`** command is used.
- The crypto-list is activated on an interface for the first time.
- A failing-over to a different peer occurs.
- A new local-address is learned (due to DHCP, PPPoE, user configuration).

Note:

The IP Payload Compression (IPPCP) numbers refer to data as it is presented to the compression/decompression engine, which is before outbound protection and after inbound de-protection. Hence, the numbers do not take into account encapsulation and encryption overheads.

Syntax

show crypto ipsec sa [list *crypto-list-id* [rule *rule-id*] | address] [detail]

Parameters

Parameter	Description	Possible Values	Default Value
crypto-list-id	The crypto-list whose SA configuration should be displayed		
rule-id	The ip-rule in the crypto-list whose SA configuration should be displayed		
address	Keyword specifying to display SA configuration by peer IP address.		
detail	Keyword specifying to display detailed output		

User Level

read-only

Context

general

Example

To display the IPSec SA database and related information:

(In this example, active SAs exist for the rule.)

```
G450-001(super)# show crypto ipsec sa
Interface: FastEthernet 10/2
 Crypto list id: 901, Local address: 149.49.77.202
  Rule: 10, Crypto map: 1
  Local address:   149.49.77.202, Remote address: 135.64.102.109
  Local identity:  149.49.77.0/255.255.255.0
  Remote identity: 135.64.102.0/255.255.255.0
  path mtu 1500, media mtu 1500
  Current outbound spi: 0xfdc7d80c
  Inbound packets                Outbound packets
  -------------------------      ----------------------------------
  Total              6412359     Total                         3643507
    Total OK         6412359       Total OK                    3643507
      Decrypt        6412359         Encrypt                   3643507
      Verify         6412359         Digest                    3643507
```

```
    Decaps        6412359          Encaps                    3643507
   Total discards        0        Total discards                  0
    SA Type      SPI        Transform     PFS Secs left KB left Mode
   ------------ ---------- ------------  --- --------- ------- ----
   Inbound ESP  0x1698      esp-des       No  3501     4607999 Tunnel
                           esp-md5-hmac
   Outbound ESP 0xfdc7d80c  esp-des       No  3501     4607999 Tunnel
                           esp-md5-hmac
  ------------------------------------------------------------------
  Rule: 20, Crypto map: 1
  ...
```

To display the IPSec SA database and related information in detail:

(In this example, IP Payload Compression (IPPCP) is used.)

```
G450-001(super)# show crypto ipsec sa detail
Inbound pkts errors (global):
     Invalid spi                1
     Invalid interface          0

Interface: FastEthernet 10/2
 Crypto list id: 901, Local address: FastEthernet 10/2.0
  Rule: 10, Crypto map: 1
  Local address:   134.1.157.2
  Remote address: 134.1.155.1
  Local identity:  8.0.0.0/255.0.0.0
  Remote identity: 149.49.43.0/255.255.255.0
  path mtu 1500, media mtu 1500
  Current outbound spi: 0x0
  Inbound packets                Outbound packets
  -------------------------      ----------------------------------
  Total                   0      Total                          1075
    Total OK              0        Total OK                     1044
      Decrypt             0          Encrypt                    1044
      Verify              0          Digest                     1044
      Decaps              0          Encaps                     1044
      Decompompressed     0          Compressed                    0
      Incompressible      0          Incompressible                0
                                       Comp bypass                 0
                                       Comp abort                  0
    Total discards        0        Total discards                31
       Invalid len        0          No sa                       31
       Replay failed      0          Seq rollover                 0
       Sa expired         0          Sa expired                   0
       Auth failed        0
       Bad padding        0
       Invalid identity   0
       Unprotected        0
       Other discards     0          Other discards               0
  Overall decompression ratio 1.00  Overall compression ratio   1.00
  Decompression ratio         1.00  Compression ratio           1.00
```

```
    Uncomp bytes                  0     Uncomp bytes                  0
    Comp bytes                    0     Comp bytes                    0
    Incomp bytes                  0     Incomp bytes                  0
=========================================================================
```

Output fields

Name	Description
Inbound pkts errors (global) *	The global inbound packets' error statistics, as follows: • **Invalid spi *** — The number of packets received with an invalid SPI (that does not resolve to any known SA • **Invalid interface *** — The number of packets received with an SPI which is valid on a different interface than the one on which it was received
Interface	The interface for which the following SA information is being displayed. **Note:** If the crypto-list activated on the interface is also activated on other interfaces, these interfaces are also listed here. **Note:** Interfaces in the 'down' state are designated as such.
Crypto list id	The ID of the crypto-list that contains the SAs being displayed
Local address	The local address configured for the crypto list, used for the local tunnel endpoint of all traffic protected by SAs pertaining to the crypto-list. The local address is either an interface name or an IP address, depending on configuration.
Rule	The ID of the crypto-list rule that contains the SAs being displayed
Crypto Map	The ID of the crypto-map that the rule points to, including its user-defined description
Local address	The IP address of the local tunnel endpoint of traffic protected by this SA. **Note:** If NAT Traversal is used, the UDP encapsulation port number is appended.
Remote address	The IP address and, optionally, hostname of the remote peer. A hostname is displayed if the peer was configured by its FQDN. **Note:** If NAT Traversal is used, the UDP encapsulation port number is appended.

* This parameter appears when the `detail` keyword is specified.

This parameter appears when IP Payload Compression (IPPCP) is used.

& The SA table is displayed only when active SAs exist for the rule.

Name	Description
Local identity	The local subnet protected by this SA, as it was configured in the crypto-list rule. The subnet is expressed as <address>/<wildcard>.
Remote identity	The remote subnet protected by this SA, as it was configured in the crypto-list rule. The subnet is expressed as <address>/<wildcard>.
Path mtu	The path MTU kept for this SA, as received from the network by path MTU discovery error messages. This does not include the IPSec encapsulation overhead.
Media mtu	The media MTU kept for this SA, as learned from the underlying interface. This does not include the IPSec encapsulation overhead.
Current outbound spi	The value of the currently active outbound SPI, expressed in hexadecimal encoding. If none exists, `0x0` is displayed.
	* This parameter appears when the `detail` keyword is specified. # This parameter appears when IP Payload Compression (IPPCP) is used. & The SA table is displayed only when active SAs exist for the rule.

Name	Description
Inbound packets	The inbound packets statistics for the crypto-list rule: • **Total** — the total number of inbound packets received • **Total OK** — the total number of inbound packets received and not discarded • **Decrypt** — the total number of packets successfully decrypted • **Verify** — the total number of packets successfully verified by HMAC • **Decaps** — the total number of packets successfully decapsulated from the IPSec tunnel header • **Decompressed** # — the total number of packets successfully decompressed by the IP Payload Compression (IPPCP) process • **Incompressible** # — the total number of uncompressed packets successfully received, when IPPCP is enabled • **Total Discards** — the total number of packets discarded due to some error. This number is an aggregate of the more specific numbers below. • **Invalid len *** — the number of packets discarded after being received through this tunnel, because the length is not aligned to the cipher block • **Replay failed *** — the number of packets discarded after being received through this tunnel, because of anti-replay verification failure • **Sa expired *** — the number of packets discarded after being received through this tunnel, because the SA KB lifetime is smaller then the external IP packet total length • **Auth failed *** — the number of packets discarded after being received through this tunnel, because of HMAC verification failure
	* This parameter appears when the `detail` keyword is specified. # This parameter appears when IP Payload Compression (IPPCP) is used. & The SA table is displayed only when active SAs exist for the rule.

Name	Description
Inbound packets (Cont)	• **Bad padding *** — the number of packets discarded after being received through this tunnel, because of bad ESP trailer format received failure • **Invalid identity *** — the number of packets discarded after being received through this tunnel, because of invalid identity. That is, the inner (original) IP header address does not match the IP subnet configured in the containing crypto-list rule. • **Unprotected *** — the number of packets discarded after being received in the clear (unprotected), although they were expected to arrive protected by this tunnel (that is, unprotected packets with source and destination IP matching the IP subnet configured in the containing crypto-list rule) • **Other discards *** — the number of packets dropped due to other reasons which were not covered by the above counters • **Overall decompression ratio** # — a measure of the total compression efficiency at the remote peer. This is the ratio between the number of octets resulting after decompression and the number of octets received before decompression – for all packets, including incompressible packets. • **Decompression ratio** #* — a measure of the efficiency of the compression engine at the remote peer. This is the ratio between the number of octets resulting after decompression and the number of octets received before decompression, for compressible packets only. • **Uncomp bytes** #* — the total number of bytes after decompression, including incompressible packets. • **Comp bytes** #* — the total number of bytes received compressed • **Incomp bytes** #* — the total number of incompressible bytes received, that is, that were received uncompressed
Outbound packets	The outbound packets statistics for the crypto-list rule: • **Total** — the total number of outbound packets sent • **Total OK** — the total number of outbound packets sent and not discarded • **Encrypt** — the total number of packets successfully encrypted. • **Digest** — the total number of packets successfully attached with an HMAC • **Encaps** — the total number of packets successfully encapsulated with an IPSec tunnel header
	* This parameter appears when the `detail` keyword is specified. # This parameter appears when IP Payload Compression (IPPCP) is used. & The SA table is displayed only when active SAs exist for the rule.

Name	Description
Outbound packets (Cont)	• **Compressed** # — the total number of packets successfully compressed • **Incompressible** # — the total number of incompressible packets when IPPCP is enabled • **Comp bypass** #* — the number of incompressible packets due to the packet being too short to compress • **Comp abort** #* — the number of incompressible packets due to the compression result being longer than the original packet • **Total Discards** — the total number of packets discarded due to some error • **No sa *** — the number of packets dropped before being transmitted through this tunnel due to no IPSec SA existed when the packet arrived • **Seq rollover *** — the number of packets dropped before being transmitted through this tunnel, due to sequence number rollover: the sequence number of the IPSec SA reached its capacity • **Sa expired *** — the number of packets dropped before being transmitted through this tunnel due to SA expired: SA KB lifetime is smaller then the external IP packet total length • **Other discards *** — the number of packets dropped due to other reasons not covered by any of the above counters • **Overall compression ratio** # — a measure of the total compression efficiency. This is the ratio between the number of octets before compression and the number of octets resulting after compression — for all packets, including incompressible packets. • **Compression ratio** #* — a measure of the compression engine's efficiency. This is the ratio between the number of octets before compression and the number of octets resulting after compression, for compressible packets only. • **Uncomp bytes** #* — the number of bytes that were presented to the compression engine, including incompressible packets • **Comp bytes** #* — the number of compressed bytes that resulted from the compression engine (compressible packets only) • **Incomp bytes** #* — the number of bytes from incompressible packets
SA Type &	The type of the SA: ESP Inbound or ESP Outbound
SPI &	The SPI of the SA in hexadecimal encoding

* This parameter appears when the `detail` keyword is specified.

This parameter appears when IP Payload Compression (IPPCP) is used.

& The SA table is displayed only when active SAs exist for the rule.

Name	Description
Transform	Lists all the transforms being used by the SA. Each transform is listed in a separate row.
PFS &	Displays information about Perfect Forward Secrecy (PFS) usage, when the SA is negotiated by IKE Phase-2. Possible values are: • **No** – PFS is not used • **#<N>** – PFS is used with Diffie-Hellman group N
Secs left &	The number of seconds left for this SA's expiration
KB left &	The number of kilobytes left for this SA's expiration
Mode &	The encapsulation mode: `tunnel` or `transport`
	* This parameter appears when the `detail` keyword is specified. # This parameter appears when IP Payload Compression (IPPCP) is used. & The SA table is displayed only when active SAs exist for the rule.

Related Commands

clear crypto isakmp, clear crypto sa, clear crypto sa counters, crypto ipsec transform-set, show crypto ipsec transform-set, show crypto isakmp peer, show crypto isakmp peer-group, show crypto isakmp policy, show crypto isakmp sa, show crypto map, show ip active-lists, show ip crypto-list

show crypto ipsec transform-set

Use the **`show crypto ipsec transform-set`** command to display the configuration for the specified transform-set or all transform-sets.

Syntax

`show crypto ipsec transform-set [`*`transform-set-name`*`]`

Parameters

Parameter	Description	Possible Values	Default Value
`transform-set-name`	The name of the transform set you wish to display. If you do not enter a value, all transform-sets are displayed.		

User Level

read-only

Context

general

Example

To display the configuration for all transform-sets:

```
G450-001(super)# show crypto ipsec transform-set
Showing 10 rows
Name                 ESP Enc ESP Hash PCP PFS Life Sec   Life KB    Mode
-------------------- ------- -------- --- --- ---------- ---------- ------
ts1                  aes     sha-hmac No  No        3600    4608000 Tunnel
ts18                 aes-192 md5-hmac No  No        3600    4608000 Tunnel
ts2                  des     sha-hmac No  No        3600    4608000 Tunnel
ts3                  des     md5-hmac No  No        3600    4608000 Tunnel
ts4                  aes-256 sha-hmac No  No        3600    4608000 Tunnel
ts5                  3des    md5-hmac No  No        3600    4608000 Tunnel
ts6                  aes-192 sha-hmac No  No        3600    4608000 Tunnel
ts7                  3des    sha-hmac No  No        3600    4608000 Tunnel
tsDef                3des    sha-hmac No  #2        3600    4608000 Tunnel
tsVoip               des     sha-hmac No  No        3600    4608000 Tunnel
```

Output fields

Name	Description
Name	the name of the transform-set
ESP Enc	the type of encryption required for ESP traffic
ESP Hash	the type of HMAC (Hash Message Authentication Code) required for ESP traffic
PCP	whether IP Payload Compression is required
PFS	whether Perfect Forward Secrecy is required when negotiating the SA, and if so, which Diffie-Hellman group to use
Life sec	the required lifetime of the SA, in seconds
Life KB	the required lifetime of the SA, in kilobytes
Mode	the required encapsulation mode — `tunnel` or `transport`

Related Commands

clear crypto isakmp, clear crypto sa, clear crypto sa counters, crypto ipsec transform-set, show crypto ipsec sa, show crypto isakmp peer, show crypto isakmp peer-group, show crypto isakmp policy, show crypto isakmp sa, show crypto map, show ip active-lists, show ip crypto-list

show crypto isakmp peer

Use the **`show crypto isakmp peer`** command to display crypto ISAKMP peer configuration.

Syntax

`show crypto isakmp peer`

User Level

read-only

Context

general

Example

To display the crypto ISAKMP peer configuration:

```
G450-001(super)# show crypto isakmp peer
Description      Peer identity     Self identity     Auth Plc Md DPD   Track Cnt
                                                                K-alv Id
---------------- ----------------- ----------------   ---- --- -- ----- ----- --
San Jose office  111.110.110.112   IPv4 Address       psk  2   MM none        No
New Jersey       vpn.nj.avaya.com  vpn.ca.avaya.com  psk  5   AM on-de  5    No
New York office  vpn.ny.avaya.com  vpn.ca.avaya.com  psk  5   AM priod  10   Yes
                 vpn.wip.com       IPv4 Address       ?    ?   MM on-de       No
```

Output fields

Name	Description
Auth	Pre-shared-key usage: • **psk** — pre-shared-key • **?** — no pre-shared-key
Plc	The ISAKMP policy. • **?** — no ISAKMP policy

1 of 2

Name	Description
Md	The IKE mode of operation: • **MM** — Main Mode • **AM** — Aggressive Mode
DPD K-alv	The keepalive state: • **none** — no keepAlive • **on-de** — on demand • **priod** — periodic
Track Id	The ID of the object tracker which is bound to the peer status
Cnt	Indicates whether or not continuous channel is enabled
	2 of 2

Related Commands

clear crypto isakmp, clear crypto sa, clear crypto sa counters, crypto isakmp peer, show crypto ipsec sa, show crypto ipsec transform-set, show crypto isakmp peer-group, show crypto isakmp policy, show crypto isakmp sa, show crypto map, show ip active-lists, show ip crypto-list

show crypto isakmp peer-group

Use the **`show crypto isakmp peer-group`** command to display crypto ISAKMP peer-group configuration.

Syntax

```
show crypto isakmp peer group
```

User Level

read-only

Context

general

Example

To display crypto ISAKMP peer-group configuration:

```
G450-001(super)# show crypto isakmp peer-group
Peer-group      Peer identity     Self identity     Auth Plc Md DPD   Track Cnt
                                                                K-alv Id
--------------- ----------------- ----------------   ---- --- -- ----- ----- --
San-Jose-group   111.110.110.112   IPv4 Address       psk  2  MM none        No
                vpn.nj.avaya.com  vpn.ca.avaya.com   psk  5  AM on-de 5     No
New-York-group   vpn.ny.avaya.com  vpn.ca.avaya.com   psk  5  AM priod 10
Yes
                 vpn.wip.com       IPv4 Address       ?    ? MM on-de       No
```

For an explanation of the output fields, see the explanation of the output fields of the show crypto isakmp peer command.

Related Commands

clear crypto isakmp, clear crypto sa, clear crypto sa counters, crypto isakmp peer-group, show crypto ipsec sa, show crypto ipsec transform-set, show crypto isakmp peer, show crypto isakmp policy, show crypto isakmp sa, show crypto map, show ip active-lists, show ip crypto-list

show crypto isakmp policy

Use the **show crypto isakmp policy** command to display ISAKMP policy configuration.

Syntax

show crypto isakmp policy

User Level

read-only

Context

general

Example

To display the ISAKMP policy configuration:

```
G450-001(super)# show crypto isakmp policy

Id Description     Encr    Hash    Authentication DH group Life sec
-- --------------- ------- ------- -------------- -------- ----------
1 Tel-Aviv-Ike     3des    md5     Preshared key        2      86400
2 Haifa-Ike        des     md5     Preshared key        1        600
```

Output fields

Name	Description
Id	The ID of the ISAKMP policy list whose parameters are being listed
Description	The description of the ISAKMP policy list
Encr	The encryption algorithm used (`des`, `3des`, `aes`, `aes-192`, or `aes-256`)
Hash	The hashing algorithm used (`md5` or `sha`)
Authentication	The authentication type
DH group	The Diffie-Hellman group
Life sec	The lifetime of the ISAKMP SA

Related Commands

clear crypto isakmp, clear crypto sa, clear crypto sa counters, crypto isakmp policy, show crypto ipsec sa, show crypto ipsec transform-set, show crypto isakmp peer, show crypto isakmp peer-group, show crypto isakmp sa, show crypto map, show ip active-lists, show ip crypto-list

show crypto isakmp sa

Use the **`show crypto isakmp sa`** command to display the ISAKMP SA database status.

Syntax

`show crypto isakmp sa`

User Level

read-only

Context

general

Example

To display the ISAKMP SA database status:

```
G450-001(super)# show crypto isakmp sa
Showing 6 rows:
C-id Local           Remote            State     Encr    Hash  Aut  DH TTL      DPD Nat-T
---- --------------- ---------------   -------   ----    ----  ---- -- -------- --- ----
1    123.123.123.123 133.133.133.133   Ready      des     md5   psk  1   29600   Yes  No
vpn.nj.avaya.com
2    222.123.123.123 111.133.133.133   AM Neg
5    1.1.1.1         2.2.2.2           MM Neg
10   1.1.1.1         3.3.3.3           No-Srvc   aes256 sha   psk  2   80000   Yes Yes
17   123.1.2.1       135.34.3.2        Delete    3des   sha   psk  2      20    No  No
25   1.1.1.1         4.4.4.4           Backoff
```

Output fields

Name	Description
C-id	Connection ID (set using the crypto map command)
Local	IP address of local peer
Remote	IP address of remote peer
State	The state of the ISAKMP SA • **Ready** — ready to pass ISAKMP information • **MM Neg** — Main Mode Negotiation • **AM Neg** — Aggressive Mode Negotiation • **No-Srvc** — in Deactivate process • **Delete** — in Delete process • **Backoff** — in Back-off period, after remote peer presumed dead
Encr	The encryption algorithm used (`des`, `3des`, `aes`, `aes-192`, or `aes-256`)
Hash	The hashing algorithm used (`md5` or `sha`)
Aut	The authentication type
DH	The Diffie-Hellman group
TTL	Time left for SA (set using the lifetime command in crypto isakmp policy context)
DPD	Whether Dead Peer Detection is enabled
Nat-T	Whether NAT-traversal is enabled

Related Commands

clear crypto isakmp, clear crypto sa, clear crypto sa counters, show crypto ipsec sa, show crypto ipsec transform-set, show crypto isakmp peer, show crypto isakmp peer-group, show crypto isakmp policy, show crypto map, show ip active-lists, show ip crypto-list

show crypto map

Use the **show crypto map** command to display all or specific crypto map configurations.

Syntax

show crypto map [*id*]

Parameters

Parameter	Description	Possible Values	Default Value
id	The ID of the crypto map for which to display configuration information. If you do not enter a value then all crypto map configurations are displayed.		

User Level

read-only

Context

general

Example

To display all crypto map configurations:

```
G450-001(super)# show crypto map
ID   Description         Remote Peer / Group  Transform-set         DSCP C-cnl
---- ------------------- -------------------- --------------------- ---- -----
5    Tel Aviv VPN        1.0.0.2              Tel-Aviv-Transform    copy Yes
7    UK VPN              vpn.lnd.uk.avaya.com UK-Transform          copy Yes
8    NY VPN group        ny-vpn-group         NY-Transform          copy Yes
10   Haifa VPN           2.1.1.2              Haifa-Transform       10   No
15                       ?                    ?                     copy No
```

Output fields

Name	Description
ID	Crypto map ID (set using the crypto map command)
Description	Crypto map description
Remote peer / Group	IP address or name of remote peer, or name of Peer Group
Transform-set	The name of the transform-set
DSCP	The DSCP configuration
C-cnl	Whether continuous channel is enabled (`Yes`) or disabled (`No`)

Related Commands

clear crypto isakmp, clear crypto sa, clear crypto sa counters, crypto map, show crypto ipsec sa, show crypto ipsec transform-set, show crypto isakmp peer, show crypto isakmp peer-group, show crypto isakmp policy, show crypto isakmp sa, show ip active-lists, show ip crypto-list

show ip active-lists

Use the **`show ip active-lists`** command to display information about a specific policy list or all lists.

Syntax

`show ip active-lists [`*`list_index`*`|`*`list_type`*`]`

Parameters

Parameter	Description	Possible Values	Default Value
`list_index`	The index of the policy list to view	**300-499**	
`list_type`	The type of list: ACL, Crypto, PBR, QoS		

User Level

read-only

Context

general

Example

To display information about all lists:

```
G450-001(super)# show ip active-lists

Interface Name                    Dir. Type     Idx List Name
--------------------------------- ---- -------- --- ----------------
FastEthernet 10/2                 In   ACL      300 Default ACL List
FastEthernet 10/2                 In   QoS      400 Default QoS List
FastEthernet 10/2                 Out  ACL      300 Default ACL List
FastEthernet 10/2                 Out  QoS      400 Default QoS List
FastEthernet 10/2                 ---- Crypto   901 list #901
Vlan 1                            In   ACL      300 Default ACL List
Vlan 1                            In   QoS      400 Default QoS List
Vlan 1                            Out  ACL      300 Default ACL List
Vlan 1                            Out  QoS      400 Default QoS List
```

Output fields

Name	Description
Interface Name	The name of the interface on which the list is operating
Dir.	The direction of traffic on which the list is operating. Options are: • **In** — the list is operating on incoming traffic • **Out** — the list is operating on outgoing traffic
Type	The type of list. Options are: • **ACL** — Access Control List. Controls which packets are authorized to pass through the interface. • **QoS** — QoS List. Can change the value of the QoS field in a packet. • **PBR** — Policy-Based Routing List. Determines the routing of packets that match the rules defined in the list. • **Crypto** — IPSec Crypto List. Provides encryption rules for VPN traffic that needs protection.
Idx	The ID of the list. List IDs must be within the following range: • **ACL** — 300-399 • **QoS** — 400-499 • **PBR** — 800-899 • **Crypto** — 900-999
List Name	The name of the list, as determined by the name command

Related Commands - Policy-based routing

ip next-hop-list, ip pbr-group, ip pbr-list, show ip active-pbr-lists, show ip pbr-list

Related Commands - VPN

clear crypto isakmp, clear crypto sa, clear crypto sa counters, ip crypto-list, show crypto ipsec sa, show crypto ipsec transform-set, show crypto isakmp peer, show crypto isakmp peer-group, show crypto isakmp policy, show crypto isakmp sa, show crypto map, show ip crypto-list

show ip crypto-list

Use the **`show ip crypto-list`** command to display all or specific crypto-list configurations.

Syntax

`show ip crypto-list [{`*`list-number`*` | {active-list | all} [detail] }]`

Parameters

Parameter	Description	Possible Values	Default Value
`list-number`	The ID of the crypto-list for which to display configuration information		
`active-list`	Keyword specifying to show all active crypto-lists		
`all`	Keyword specifying to show all crypto-lists		
`detail`	Keyword specifying to display detailed configuration information		

User Level

read-only

Context

general, interface:Dialer (L2, L2-L3)

Examples

To display the configuration of a specific crypto-list:

```
G450-001(super)# show ip crypto-list 901

Index Description                    Status     Owner
----- ------------------------------ ---------  ------
901   VPN_via_leased_Line            valid      other

Local address: 210.210.210.210

Rules:

  Index Protocol     IP               Wildcard        Action  Crypto map
  ----- -------- --- ---------------- --------------- ------- ---------
  10     Any     Src  100.1.0.0       0.0.255.255     protect 1
                 Dst  10.1.1.0        0.0.0.255
  20     Any     Src  100.1.0.0       0.0.255.255     protect 1
                 Dst  10.1.11.0       0.0.0.255
  30     Any     Src  100.1.0.0       0.0.255.255     protect 2
                 Dst  10.2.1.0        0.0.0.255
  40     Any     Src  100.1.0.0       0.0.255.255     protect 2
                 Dst  10.2.11.0       0.0.0.255
  50     Any     Src  100.1.0.0       0.0.255.255     protect 3
                 Dst  10.3.1.0        0.0.0.255
  60     Any     Src  100.1.0.0       0.0.255.255     protect 3
                 Dst  10.3.11.0       0.0.0.255
  70     Any     Src  100.1.0.0       0.0.255.255     protect 22
                 Dst  100.2.0.0       0.0.255.255
  80     Any     Src  100.1.0.0       0.0.255.255     protect 23
                 Dst  100.3.0.0       0.0.255.255
  90     Any     Src  100.1.1.0       0.0.0.255       protect 24
                 Dst  100.4.0.0       0.0.255.255
  100    Any     Src  100.1.11.0      0.0.0.255       protect 24
                 Dst  100.4.0.0       0.0.255.255
  Deflt  Any     Src  Any                             bypass  -
                 Dst  Any

Applicable crypto maps:

  Id  Description         Remote peer/group   Transform-set   DSCP C-cnl
  --  ------------------  ------------------  --------------- ---- ----
   1  VoIP_2_HQ           101.101.101.110     ts1             copy No
   2  VoIP_2_Reg_1        102.102.102.151     ts2             copy No
   3  VoIP_2_Reg_2        reg2voip.vpn.com    ts3             copy No
  22  VoIP_2_B2           165.100.10.220      ts7             copy No
  23  VoIP_2_B3           152.152.152.230     ts17            copy No
```

To display all crypto-lists:

```
G450-001(super)# show ip crypto-list

Index Description                    Status     Owner
----- ------------------------------ ---------  -----
900   Default Crypto List            valid      other
901   VPN_via-lease_Line             valid      other
```

Output fields

Name	Description
Index	The index of the crypto-list
Description	The user-defined description of the crypto-list
Status	Whether the crypto-list is valid or invalid. A crypto-list is valid if and only if all the crypto maps it points to exist and are valid. A crypto map is valid if and only if it is fully configured with all the obligatory parameters, and points to a valid ISAKMP peer.
Owner	This field exists for legacy purposes, and is not currently relevant
Local Address	The configured local address for the crypto-list. Can be either an IP address or an interface name.
Rules	The table of ip-rules, as follows:
Index	The index number of the ip-rule. `Deflt` indicates the default ip-rule.
Protocol	This field is reserved for future use
IP	The source or destination IP address of the rule. For each rule, the source IP is displayed first and the destination IP is displayed in the next line.
Wildcard	The source or destination wildcard of the rule. For each rule, the source wildcard is displayed first and the destination wildcard is displayed in the next line.
Action	Whether to protect traffic that matches the source and destination addresses, or bypass protection
Crypto map	The ID of the crypto map specifying how to protect traffic
Applicable crypto maps	The table of crypto maps pointed to by this crypto-list, as follows:
ID	Crypto map ID

1 of 2

Name	Description
Description	Crypto map description
Remote peer / Group	IP address or name of remote peer, or name of Peer Group
Transform-set	The name of the transform-set to which this crypto map points
DSCP	The tunnel DSCP configuration, which can be either `copy` or a decimal number in the range [0-63]
C-cnl	Whether IPSec continuous channel is enabled (`Yes`) or disabled (`No`)

2 of 2

Related Commands

clear crypto isakmp, clear crypto sa, clear crypto sa counters, ip crypto-list, ip-rule (VPN), show crypto ipsec sa, show crypto ipsec transform-set, show crypto isakmp peer, show crypto isakmp peer-group, show crypto isakmp policy, show crypto isakmp sa, show crypto map, show ip active-lists

VRRP

ip vrrp

Use the **ip vrrp** command to create a virtual router on the current interface. Use the **no** form of this command to delete a virtual router.

Syntax

[no] ip vrrp ***vr_id*** | [address ***ip-addr*** | auth-key ***string*** | override addr owner | preempt | primary ***primary-addr*** | priority ***pri-value*** | timer ***value***

Parameters

Parameter	Description	Possible Values	Default Value
vr_id	The virtual router ID	**1–255**	
ip-addr	The IP address to be associated with the virtual router on the VLAN		
string	The authentication password	maximum eight character string	
primary-addr	The primary IP address of the virtual router on the VLAN		
pri-value	The priority value	**1–254**	
value	The advertisement timer value	**1–255**	

User Level

read-write

Context

interface:FastEthernet (L2, L2-L3), VLAN (L2, L2-L3)

Example

To create virtual router #1 on the Vlan 2 interface:

```
G450-001(if:Vlan 2)# ip vrrp 1
```

Related Commands

ip vrrp address, ip vrrp auth-key, ip vrrp override addr owner, ip vrrp preempt, ip vrrp primary, ip vrrp priority, ip vrrp timer, router vrrp, show ip vrrp

ip vrrp address

Use the **ip vrrp address** command to assign an IP address to the virtual router. Use the **no** form of this command to remove an IP address from a virtual router.

Syntax

[no] ip vrrp *vr_id* address *ip_address*

Parameters

Parameter	Description	Possible Values	Default Value
vr_id	The virtual router ID number	**1-255**	
ip_address	The IP address to assign to the virtual router		

User Level

read-write

Context

interface:FastEthernet (L2-L3, L2), VLAN (L2-L3, L2)

Example

To assign address 10.0.1.2 to virtual router 1:

```
G450-001(if:Vlan 2)# ip vrrp 1 address 10.0.1.2
```

Related Commands

ip vrrp, ip vrrp auth-key, ip vrrp override addr owner, ip vrrp preempt, ip vrrp primary, ip vrrp priority, ip vrrp timer, router vrrp, show ip vrrp

ip vrrp auth-key

Use the **ip vrrp auth-key** command to set the virtual router simple password authentication for the virtual router ID. Use the **no** form of this command to disable simple password authentication for the virtual router instance.

Syntax

[no] ip vrrp *vr_id* auth-key *key_string*

Parameters

Parameter	Description	Possible Values	Default Value
vr_id	The virtual router ID	**1-255**	
key_string	The password string		

User Level

read-write

Context

interface:FastEthernet (L2-L3, L2), VLAN (L2-L3, L2)

Example

To specify the password authentication for virtual router 1 as “sec01”:

```
G450-001(if:Vlan 2)# ip vrrp 1 auth-key sec01
```

Related Commands

ip vrrp, ip vrrp address, ip vrrp override addr owner, ip vrrp preempt, ip vrrp primary, ip vrrp priority, ip vrrp timer, router vrrp, show ip vrrp

---

ip vrrp override addr owner

Use the **ip vrrp override addr owner** command to accept packets addressed to the IP address associated with the virtual router, such as ICMP, SNMP, and Telnet (if it is not the IP address owner and it is the master). Use the **no** form of this command to discard these packets.

Syntax

[no] ip vrrp *vr_id* override addr owner

Parameters

Parameter	Description	Possible Values	Default Value
vr_id	The virtual router ID	**1-255**	

User Level

read-write

Context

interface:FastEthernet (L2-L3, L2), VLAN (L2-L3, L2)

Example

To specify that virtual router 1 accepts ICMP, SNMP, and Telnet packets:

```
G450-001(if:Vlan 2)# ip vrrp 1 override addr owner
```

Related Commands

ip vrrp, ip vrrp address, ip vrrp auth-key, ip vrrp preempt, ip vrrp primary, ip vrrp priority, ip vrrp timer, router vrrp, show ip vrrp

ip vrrp preempt

Use the **ip vrrp preempt** command to configure the router to preempt a lower priority master for the virtual router ID. Use the **no** form of this command to disable preemption for the virtual router instance. By default, preemption is enabled.

Syntax

[no] ip vrrp *vr_id* preempt

Parameters

Parameter	Description	Possible Values	Default Value
vr_id	The virtual router ID	**1-255**	

User Level

read-write

Context

interface:FastEthernet (L2-L3, L2), VLAN (L2-L3, L2)

Example

To specify that virtual router 1 preempts a lower priority master:

```
G450-001(if:Vlan 2)# ip vrrp 1 preempt
```

Related Commands

ip vrrp, ip vrrp address, ip vrrp auth-key, ip vrrp override addr owner, ip vrrp primary, ip vrrp priority, ip vrrp timer, router vrrp, show ip vrrp

ip vrrp primary

Use the **ip vrrp primary** command to set the primary address that is used as the source address of VRRP packets for the virtual router ID. Use the **no** form of this command to restore the default primary address for the virtual router instance. By default, the primary address is selected automatically by the device.

Syntax

[no] ip vrrp *vr_id* primary *ip_address*

Parameters

Parameter	Description	Possible Values	Default Value
vr_id	The virtual router ID	**1-255**	
ip_address	The primary IP address of the virtual router. This address should be one of the router addresses on the fabric.		

User Level

read-write

Context

interface:FastEthernet (L2-L3, L2), VLAN (L2-L3, L2)

Example

To specify the source IP address for virtual router 1 as 192.168.66.23:

```
G450-001(if:Vlan 2)# ip vrrp 1 primary 192.168.66.23
```

Related Commands

ip vrrp, ip vrrp address, ip vrrp auth-key, ip vrrp override addr owner, ip vrrp preempt, ip vrrp priority, ip vrrp timer, router vrrp, show ip vrrp

ip vrrp priority

Use the **ip vrrp priority** command to set the virtual router priority value used when selecting a master router. Use the **no** form of this command to restore the default value.

Syntax

[no] ip vrrp *vr_id* priority *pri_value*

Parameters

Parameter	Description	Possible Values	Default Value
vr_id	The virtual router ID	**1-255**	
pri_value	The priority value	**1-254**	

User Level

read-write

Context

interface:FastEthernet (L2-L3, L2), VLAN (L2-L3, L2)

Example

To specify the priority of virtual router 1 as 10:

```
G450-001(if:Vlan 2)# ip vrrp 1 priority 10
```

Related Commands

ip vrrp, ip vrrp address, ip vrrp auth-key, ip vrrp override addr owner, ip vrrp preempt, ip vrrp primary, ip vrrp timer, router vrrp, show ip vrrp

ip vrrp timer

Use the **ip vrrp timer** command to set the virtual router advertisement timer value for the virtual router ID. Use the **no** form of this command to restore the default value.

Syntax

[no] ip vrrp *vr_id* timer *value*

Parameters

Parameter	Description	Possible Values	Default Value
vr_id	The virtual router ID	**1-255**	
value	The advertisement transmit time in seconds	**1-255**	

User Level

read-write

Context

interface:FastEthernet (L2-L3, L2), VLAN (L2-L3, L2)

Example

To set the virtual router advertisement timer value for virtual router 3 to 2 seconds:

```
G450-001(if:Vlan 2)# ip vrrp 3 timer 2
```

Related Commands

ip vrrp, ip vrrp address, ip vrrp auth-key, ip vrrp override addr owner, ip vrrp preempt, ip vrrp primary, ip vrrp priority, router vrrp, show ip vrrp

---

router vrrp

Use the **router vrrp** command to enable VRRP routing globally. Use the **no** form of this command to disable VRRP routing.

Note:
You cannot activate both VRRP and SRRP protocols at the same time.

Syntax

[no] router vrrp

User Level

read-write

Context

general

Related Commands

ip vrrp, ip vrrp address, ip vrrp auth-key, ip vrrp override addr owner, ip vrrp preempt, ip vrrp primary, ip vrrp priority, ip vrrp timer, show ip vrrp

show ip vrrp

Use the **show ip vrrp** command to display VRRP information for a given VLAN. If no VLAN is specified, information for all VLANs is displayed.

Syntax

show ip vrrp [*vlan* [router-id *vr_id*]] [detail]

Parameters

Parameter	Description	Possible Values	Default Value
vlan	Filter by the specified VLAN	**1-4095**	
router_id	Keyword specifying to filter by virtual router ID		
vr_id	The virtual router ID	**1-255**	
detail	Keyword specifying to provide detailed information		

User Level

read-only

Context

general

Example

To show VRRP information for all VLANs:

```
G450-001(super)# show ip vrrp
VRRP is globally enabled
VLAN  VRID  IP Address      Pri   Timer     State     Since
----- ----- -------------  ----  -------  ---------  -----------
1     1     192.168.66.23  255     1       MASTER     00:00:00
1     2     192.168.66.24  100     1       BACKUP     00:00:00
```

To show detailed VRRP information for all VLANs:

```
G450-001(super)# show ip vrrp detail
VRRP is globally enabled
Virtual Router on VLAN:             1
Router-id:                          1
State:                              MASTER
Priority:                           255
Advertisement Interval:             1
Last State Change:                  00:00:00
Override Address Ownership Rule: No
Authentication Type:                None
Authentication Key:       ""
Master IP Address                   192.168.66.23
Has 1 IP addresses
IP addresses:
192.168.66.23
Primary IP Address:                 192.168.66.23
Primary IP Address was chosen by default
Preemption Mode:          enabled
# of times Master:                                  2
# of received Advertisements:                      0
# of transmitted Advertisements:                   20
# of received Advertisements with Security Violations: 0
Virtual Router on VLAN:       1
Router-id:                2
State:                    BACKUP
Priority:                 100
Advertisement Interval:   1
Last State Change:        00:00:00
Override Address Ownership Rule: No
Authentication Type:      None
Authentication Key:       ""
Master IP Address         0.0.0.0
Has 1 IP addresses
IP addresses:
192.168.66.24
Primary IP Address:       192.168.66.23
Primary IP Address was chosen by default
Preemption Mode:          enabled
# of times Master:                                  1
# of received Advertisements:                      0
# of transmitted Advertisements:                   13
# of received Advertisements with Security Violations: 0
```

Related Commands

ip vrrp, ip vrrp address, ip vrrp auth-key, ip vrrp override addr owner, ip vrrp preempt, ip vrrp primary, ip vrrp priority, ip vrrp timer, router vrrp

WAN configuration, verifying

show controllers

Use the **show controllers** command to display status information about a controller interface.

Syntax

show controllers *module/port*

Parameters

Parameter	Description	Possible Values	Default Value
module	The module number		
port	The port number		

User Level

read-write

Context

general

Example

To display controller status information:

```
G450-001(super)# show controllers
T1 5/1 is down.
Cablelength is long gain26 0db.
Transmitter is sending remote alarm.
Receiver has loss of signal.
Framing is SF, Line Code is AMI, Clock Source is Line.
Data in current interval (802 seconds elapsed):
0 Line Code Violations, 0 Path Code Violations
0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 802 Unavail Secs
Total Data (last 4 15 minute intervals):
10 Line Code Violations, 0 Path Code Violations
0 Slip Secs, 0 Fr Loss Secs, 1 Line Err Secs, 0 Degraded Mins
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 3600 Unavail Secs
```

Related Commands - E1/T1 interfaces

cablelength long, cablelength short, channel-group, clock source, controller, ds-mode, framing, interface serial, ip address, linecode (E1), linecode (T1), remote

Related Commands - Verifying WAN configuration

show frame-relay fragment, show frame-relay lmi, show frame-relay pvc, show frame-relay traffic, show interfaces, show ip interface, show map-class frame-relay

show frame-relay fragment

Use the **show frame-relay fragment** command to display frame-relay fragmentation statistics and configuration on all PVCs, all PVCs associated with an interface, or a specific PVC.

Note:

When statistics for multiple PVCs are shown, they are sorted first by interface type and number, and then by DLCI.

Syntax

show frame-relay fragment [interface *interface_name*|*dlci_number*]

Parameters

Parameter	Description	Possible Values	Default Value
interface_name	Type and identifier of the interface, enclosed in quotes		
dlci_number	The PVC identifier	**16-1007**	

User Level

read-only

Context

general

Example

To show details on configuration and statistics for fragmentation on all PVCs associated with interface Serial 4/1:

```
G450-001(super)# show frame-relay fragment interface "Serial 4/1"
```

Related Commands

clear frame-relay counters, frame-relay class-dlci, interface serial, map-class frame-relay, fragment, show frame-relay pvc brief, show interfaces

show frame-relay lmi

Use the **show frame-relay lmi** command to display LMI statistics for a particular interface or for all interfaces. The output displayed differs depending on the type of interface.

Syntax

show frame-relay lmi [interface *interface_name*]

Parameters

Parameter	Description	Possible Values	Default Value
interface_ name	The name of the interface		

User Level

read-only

Context

general

Example

To display LMI statistics for all interfaces:

```
G450-001(super)# show frame-relay lmi
LMI Statistics for interface Serial 1 (Frame Relay DTE)
LMI TYPE = ANSI Annex D  Invalid Unnumbered info     0,    Invalid Prot Disc
0  Invalid dummy Call Ref        0,     Invalid Msg Type             0  Invalid
Status Message         0,     Invalid Lock Shift            0  Invalid
Information ID         0,     Invalid Report IE Len         0  Invalid Report
Request        0,    Invalid Keep IE Len         0  Num Status Enq. Sent
0,     Num Status msgs Rcvd         0  Num Update Status Rcvd        0,     Num
Status Timeouts           0
LMI Statistics for interface Serial 2 (Frame Relay DTE)
LMI TYPE = Auto Detect Mode  Invalid Unnumbered info        0,     Invalid Prot
Disc           0  Invalid dummy Call Ref        0,    Invalid Msg Type
0  Invalid Status Message        0,     Invalid Lock Shift           0  Invalid
Information ID         0,     Invalid Report IE Len         0  Invalid Report
Request        0,    Invalid Keep IE Len         0  Num Status Enq. Sent
```

```
0,     Num Status msgs Rcvd          0  Num Update Status Rcvd         0,     Num
Status Timeouts            0
```

Output Fields

Item	Description
LMI Statistics	Signaling or LMI specification: ANSI, or ITU-T
Invalid Unnumbered info	Number of received LMI messages with invalid unnumbered information field
Invalid Prot Disc	Number of received LMI messages with invalid protocol discriminator
Invalid dummy Call Ref	Number of received LMI messages with invalid dummy call references
Invalid Msg Type	Number of received LMI messages with invalid message type
Invalid Status Message	Number of received LMI messages with invalid status message
Invalid Lock Shift	Number of received LMI messages with invalid lock shift type
Invalid Information ID	Number of received LMI messages with invalid information identifier
Invalid Report IE Len	Number of received LMI messages with invalid Report IE Length
Invalid Report Request	Number of received LMI messages with invalid Report Request
Invalid Keep IE Len	Number of received LMI messages with invalid Keep IE Length
Num Status Enq. Sent	Number of LMI status inquiry messages sent
Num Status Msgs Rcvd	Number of LMI status messages received
Num Update Status Rcvd	Number of LMI asynchronous update status messages received
Num Status Timeouts	Number of times the status message was not received within the keepalive time value
Num Status Enq. Rcvd	Number of LMI status enquiry messages received
Num Status Msgs Sent	Number of LMI status messages sent
Num Status Enq. Timeouts	Number of times the status enquiry message was not received within the T392 DCE timer value
Num Update Status Sent	Number of LMI asynchronous update status messages sent

Related Commands

show controllers, show frame-relay fragment, show frame-relay pvc, show frame-relay traffic, show interfaces, show ip interface, show map-class frame-relay

show frame-relay map

Use the **show frame-relay map** command to display a summary table of Frame Relay sub-interfaces and DLCIs associated with the sub-interfaces.

Syntax

show frame-relay map

User Level

read-only

Context

general

Example

To display information about the Frame Relay sub-interfaces:

```
G450-001(super)# show frame-relay map

Showing 2 frame-relay map entries
Interface   State  Interface Type DLCI DLCI Type DLCI State
----------- ------ -------------- ---- --------- ------
Serial 1.1  down   point-to-point   17 broadcast deleted
Serial 1.1  down   point-to-point   18 broadcast deleted
```

Related Commands

clear frame-relay counters, frame-relay class-dlci, interface serial, map-class frame-relay, show frame-relay pvc brief, show interfaces

show frame-relay pvc

Use the **show frame-relay pvc** command to display detailed PVC information. The information can be shown for all PVCs known to the device, for all PVCs learned on an interface, or for a specific PVC (DLCI). Note that in this case, all PVCs with the same DLCI are displayed. When statistics for multiple PVCs are shown, they are sorted first by interface type and number, and then by DLCI.

Syntax

show frame-relay pvc [interface *interface_name* | *dlci_number*]

Parameters

Parameter	Description	Possible Values	Default Value
interface_name	Type and identifier of the interface, enclosed in quotes		
dlci_number	The PVC identifier	**16-1007**	

User Level

read-only

Context

general

Example

To show details on configuration and statistics for all PVCs associated with interface “Serial 1.1":

```
G450-001(super)# show frame-relay pvc interface "Serial 1.1"
Showing 1 PVCPVC Statistics for interface Serial 1 (Frame Relay DTE) DLCI =
17, USAGE = LOCAL ,
PVC STATUS = DELETED ,
INTERFACE = Serial 1.1
input pkts          0,
output pkts         0,
dropped pkts        0
in bytes            0,
out bytes           0
in FECN pkts        0
in BECN pkts        0
in DE pkts          0,
```

```
out DE pkts          0
pvc create time 00:05:17,
last time pvc status changed 00:05:07  traffic-shaping configured by map-class
foobar
cir             70000,
bc               7000,
be                  0  interval          100,
current bc       7000,
current be          0  pkts                0,
delayed pkts        0,
dropped pkts        0  bytes               0,
delayed byts        0,
dropped byts        0  de pre mark is on,
threshold is 20% of bc  end-to-end fragmentation is on,
fragment size is 88PVC Statistics for interface Serial 2 (Frame Relay DTE)
```

Related Commands

show controllers, show frame-relay fragment, show frame-relay lmi, show frame-relay traffic, show interfaces, show ip interface, show map-class frame-relay

show frame-relay traffic

Use the **show frame-relay traffic** command to display frame-relay protocol statistics, including ARP requests and replies sent and received over Frame Relay interfaces.

Syntax

show frame-relay traffic

User Level

read-only

Context

general

Example

To display frame-relay statistics:

```
G450-001(super)# show frame-relay traffic
Frame Relay statistics:
ARP requests sent       0,    ARP replies sent       0
ARP requests recvd      0,    ARP replies recvd      0
```

Related Commands

show controllers, show frame-relay fragment, show frame-relay lmi, show frame-relay pvc, show interfaces, show ip interface, show map-class frame-relay

show interfaces

Use the **show interfaces** command to display interface configuration and statistics for a particular interface or all interfaces. The Frame Relay sub-interface only includes the following counters:

- packets & bytes in
- packets & bytes out
- input errors
- output drops

Syntax

show interfaces [*interface_type interface_identifier*]

Parameters

Parameter	Description	Possible Values	Default Value
interface_type	The type of interface	**Dialer, FastEthernet, Serial, Vlan, Loopback, Console, Tunnel, USB**	
interface_identifier	The interface number. The format varies depending on the value of interface_type: For FastEthernet: **module/port** For Serial: **module/port:channel-group** For Vlan: **Vlan id** For LoopBack: **Loopback number** For Tunnel: **Tunnel number**	For FastEthernet: **10/2 or 10/4** For Serial(USP): **3/1, 4/1, 8/1** For Serial (DS1): module/port: **3/1, 4/1, 8/1** channel-group: E1: **0-30** T1: **0-23** For VLAN: **1-4090** For Loopback: **1-99** For Tunnel: **1-50** For Dialer: **1**	

User Level

read-write

Context

general

Example

To show information about all the interfaces:

```
G450-001(super)# show interfaces
Vlan 1 is up, line protocol is up
Physical address is 00.04.0d.29.c5.11.
Internet address is 172.16.1.139, mask is 255.255.255.240
Primary management interface
MTU 1500 bytes. Bandwidth 100000 kbit.
Reliability 255/255 txLoad 1/255 rxLoad 1/255
Encapsulation ARPA, ICC-VLAN
Link status trap disabled
Full-duplex, 100Mb/s
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:30, Last output 00:00:30
Last clearing of 'show interface' counters never.
5 minute input rate 144 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 input drops, 0 output drops, 0 unknown protocols
3425 packets input, 323518 bytes
3425 broadcasts received, 0 giants
0 input errors, 0 CRC
32 packets output, 896 bytes
0 output errors, 0 collisions

FastEthernet 10/2 is up, line protocol is down
Physical address is 00.04.0d.29.c5.10.
MTU 1500 bytes. Bandwidth 10000 kbit.
Reliability 1/255 txLoad 255/255 rxLoad 255/255
Encapsulation ARPA
Link status trap disabled
Half-duplex, 10Mb/s, 10BaseTX
ARP type: ARPA, ARP Timeout 04:00:00
Dynamic CAC BBL: 1500 kbps
Dynamic CAC activation priority: 50
Dynamic CAC interface status: active
Last input never, Last output never
Last clearing of 'show interface' counters never.
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 input drops, 0 output drops, 0 unknown protocols
0 packets input, 0 bytes
0 broadcasts received, 0 giants
```

```
0 input errors, 0 CRC
0 packets output, 0 bytes
0 output errors, 0 collisions

Tunnel 1 is up, line protocol is up
Internet address is 177.0.0.17, mask is 255.0.0.0
MTU 468 bytes. Bandwidth 9 kbit
Reliability 255/255 txLoad 1/255 rxLoad 1/255
Encapsulation GRE
Link status trap enabled
Keepalive set (10 sec), retries 3
Tunnel source 17.0.0.17, destination 12.0.0.3
Tunnel protocol/transport GRE/IP, key 777
Checksumming of packets enabled
Tunnel DSCP 63, Tunnel TTL 255
Path MTU Discovery, ager 10 mins, MTU 976, expires 00:09:33
Last input never, Last output never
Last clearing of 'show interface' counters never.
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 input drops, 0 output drops, 0 unknown protocols
0 packets input, 0 bytes
0 broadcasts received, 0 giants
0 input errors, 0 CRC
0 packets output, 0 bytes
0 output errors, 0 collisions

Console asynchronous mode is terminal
Terminal baud rate is 9600
```

Related Commands - Frame relay encapsulation

clear frame-relay counters, frame-relay class-dlci, interface serial, map-class frame-relay, fragment, show frame-relay pvc brief

Related Commands - PPP encapsulation

interface dialer, interface fastethernet, interface serial

Related Commands - Verifying WAN configuration

show controllers, show frame-relay fragment, show frame-relay lmi, show frame-relay pvc, show frame-relay traffic, show interfaces, show ip interface, show map-class frame-relay

show map-class frame-relay

Use the **show map-class frame-relay** command to display the map-class Frame Relay table.

Syntax

show map-class frame-relay

User Level

read-only

Context

general

Example

To display the map class Frame Relay table:

```
G450-001(super)# show map-class frame-relay
Showing 3 frame-relay map-class entries
       Map Class Name           CIR       BC        BE      Fragment
----------------------------- --------- --------- --------- --------
default                         56000      7000         0      OFF
orna1                           56000      7000         0      OFF
stam                            56000      7000         0      OFF
```

Related Commands - Frame relay encapsulation

clear frame-relay counters, interface serial, encapsulation, frame-relay class-dlci, frame-relay interface-dlci, frame-relay lmi-n391dte, frame-relay lmi-n392dte, frame-relay lmi-n393dte, frame-relay lmi-type, frame-relay priority-dlci-group, frame-relay traffic-shaping, ip address, map-class frame-relay, bc out, be out, cir out, fragment, show frame-relay map, show frame-relay pvc brief, show interfaces, show traffic-shape, GRE tunneling, show traffic-shape-statistics

Related Commands - Traffic shaping

frame-relay traffic-shaping, map-class frame-relay, bc out, be out, cir out, fragment, show traffic-shape, show traffic-shape-queue, show traffic-shape-statistics, traffic-shape rate

Related Commands - Verifying WAN configuration

show controllers, show frame-relay fragment, show frame-relay lmi, show frame-relay pvc, show frame-relay traffic, show interfaces, show ip interface

WAN Ethernet port configuration

interface FastEthernet

Use the **interface FastEthernet** command to enter Interface FastEthernet configuration mode. Use the **no** form of this command to delete an IP interface.

If the specified interface does not exist, the system creates it and enters its configuration mode.

Syntax

[no] interface FastEthernet [*module/port*[.*ip_interface*]]

Parameters

Parameter	Description	Possible Values	Default Value
module	The module number of the interface	**10**	
port	The port number of the interface	**3**	
ip_interface	The IP sub-interface number within this interface. A number of IP interfaces may be bound to a Layer 3 interface.	**0-1024**	

User Level

read-write

Context

general

Example

To create a FastEthernet interface and enter its context:

```
G450-001(super)# interface FastEthernet 10/2
```

To create a Level 3 sub-interface on the FastEthernet interface:

```
G450-001(super)# interface FastEthernet 10/2.1
```

Related Commands

description (interface), interface console, interface loopback, interface serial, interface tunnel, interface USB-modem, interface vlan, ip address, ip admin-state, ip broadcast-address, ip crypto-group, load-interval, show ip interface brief

autoneg

Use the **autoneg** command to set the port speed and duplex to auto-negotiation mode for the external Fast Ethernet port. Use the **no** form of this command to disable auto-negotiation mode.

Syntax

[no] autoneg

User Level

read-write

Context

interface:FastEthernet (L2, L2-L3)

Related Commands

interface FastEthernet, duplex, keepalive-track, speed (interface), traffic-shape rate

duplex

Use the **duplex** command to control the duplex setting for the current interface.

Note:
This command functions only in **no autoneg** mode.

Syntax

duplex {full|half}

Parameters

Parameter	Description	Possible Values	Default Value
full	Keyword indicating that the interface is set to full duplex		
half	Keyword indicating that the interface is set to half duplex		

User Level

read-only

Context

interface:FastEthernet (L2, L2-L3)

Example

To specify full duplex for the FastEthernet interface:

```
G450-001(super-if:FastEthernet 1.1)# duplex full
```

Related Commands

interface FastEthernet, autoneg, keepalive-track, speed (interface), traffic-shape rate

keepalive-track

Use the **keepalive-track** command to bind an object tracker to a remote VPN peer or to an interface, to check whether the remote peer or the interface is up. Use the **no** form of this command to disable this mechanism (default setting).

Note:

When configuring VPN, you can use the **keepalive-track** command instead of the **keepalive** command when the remote peer does not support DPD, or when you want to monitor servers behind the VPN remote peer.

Note:

You cannot configure both **keepalive-track** and **ip address dhcp** (DHCP Client) on the WAN FastEthernet interface.

Syntax

keepalive-track ***track-id***

no keepalive-track

Parameters

Parameter	Description	Possible Values	Default Value
track-id	The ID of the object tracker	**1-100**	

User Level

read-write

Context

interface:Serial (DS1 PPP L2, DS1 PPP L2-L3, DS1 FR-SUB L2, DS1 FR-SUB L2-L3, USP PPP L2, USP PPP L2-L3) FastEthernet (L2, L2-L3, PPP L2, PPP L2-L3), Loopback (L2, L2-L3), Dialer (L2, L2-L3)
crypto isakmp peer

Example

To register a remote VPN peer with object tracker 5:

```
G450-001(config-peer:149.49.70.1)# keepalive-track 5
```

To register the FastEthernet interface with object tracker 2:

```
G450-001(config-if:FastEthernet 10/2)# keepalive-track 2
```

Related Commands - WAN Ethernet port configuration

interface FastEthernet, autoneg, duplex, speed (interface), traffic-shape rate

Related Commands - VPN

description (ISAKMP peer), continuous-channel, crypto isakmp peer, initiate mode, isakmp-policy, keepalive (VPN), pre-shared-key, self-identity, show crypto isakmp peer, suggest-key

---

speed (interface)

Use the **speed** command to control the speed setting for the interface.

Note:
This command functions only in **no autoneg** mode.

Syntax

speed speed_rate

Parameters

Parameter	Description	Possible Values	Default Value
speed_rate	The interface speed	**10MB**, **100MB**	

User Level

read-write

Context

interface:FastEthernet (L2, L2-L3, PPP L2, PPP L2-L3)

Example

To set the interface speed to 100MB:

```
G450-001(if:FastEthernet 10/2)# speed 100MB
```

Related Commands

interface FastEthernet, autoneg, duplex, keepalive-track, traffic-shape rate

traffic-shape rate

Use the **traffic-shape rate** command to configure traffic shaping for outbound traffic on the current interface.

Syntax

traffic-shape rate ***bit_rate***

Parameters

Parameter	Description	Possible Values	Default Value
bit_rate	The bit-rate that traffic is shaped to, in bits per second	**64000-10240000**	

User Level

read-write

Context

interface:FastEthernet(L2, L2-L3)

Example

To set the traffic-shaping rate to 128000:

```
G450-001(if:FastEthernet 10/2)# traffic-shape rate 128000
```

Related Commands - WAN Ethernet port configuration

interface FastEthernet, autoneg, duplex, keepalive-track, speed (interface),

Related Commands - Traffic shaping

frame-relay traffic-shaping, map-class frame-relay, bc out, be out, cir out, fragment, show map-class frame-relay, show traffic-shape, show traffic-shape-queue, show traffic-shape-statistics

WFVQ (Weighted Fair VoIP Queueing)

fair-queue-limit

Use the **fair-queue-limit** command to specify the maximum number of packets that can be queued in the weighted fair queue. The allowable upper limit depends on the bandwidth configured for the interface.

Note:

The command **fair-queue-limit** is not applicable to an interface on which Frame Relay Traffic Shaping is enabled. Instead, this command is now applicable in map-class frame-relay context, to control the specific DLCI queueing parameters.

Syntax

[no] fair-queue-limit *size*

Parameters

Parameter	Description	Possible Values	Default Value
size	The maximum number of packets that can be queued in the weighted fair queue		

User Level

admin

Context

interface:Dialer (L2, L2-L3), Serial (DS1 PPP L2, DS1 PPP L2-L3, USP PPP L2, USP PPP L2-L3), FastEthernet (L2, L2-L3, PPP L2, PPP L2-L3) - when traffic shaping is configured, Serial (DS1 FR L2, USP FR L2) - when Frame Relay Traffic Shaping is not configured, map-class frame-relay

Example

To specify the maximum number of packets queued in the weighted fair queue as 500:

```
G450-001(super-if:FastEthernet 10/2)# fair-queue-limit 500
```

Related Commands - WFVQ

fair-voip-queue, priority-queue, show queue, show queueing, voip-queue

---

fair-voip-queue

Use the **fair-voip-queue** command to enable Weighted Fair VoIP Queueing (WFVQ) on the current interface. WFVQ provides more fair service for data packets, and improves response time for interactive data applications (such as Telnet). WFVQ is the default queueing mode for all Serial interfaces and all FastEthernet interfaces for which traffic-shaping is enabled. To disable WFVQ, you must enable another queueing mode, using either the **voip-queue** or the **priority-queue** command in interface context.

Note:

The commands **fair-voip-queue** and **voip-queue** are mutually exclusive, and cannot both appear in a configuration script.

Note:

The command **fair-voip-queue** is not applicable for an interface on which Frame-Relay Traffic-Shaping is enabled.

Syntax

fair-voip-queue

User Level

admin

Context

interface:Dialer (L2, L2-L3), Serial (DS1 PPP L2, DS1 PPP L2-L3, USP PPP L2, USP PPP L2-L3), FastEthernet (L2, L2-L3, PPP L2, PPP L2-L3) - when traffic shaping is configured, Serial (DS1 FR L2, USP FR L2) - when Frame Relay Traffic Shaping is not configured

Example

To enable Weighted Fair VoIP Queueing:

```
G450-001(super-if:FastEthernet 10/2)# fair-voip-queue
```

Related Commands - WFVQ

fair-queue-limit, priority-queue, show queue, show queueing, voip-queue

---

priority-queue

Use the **priority-queue** command to enable priority queueing mode in a serial or FastEthernet interface. By default, priority queueing is off, and WFVQ is enabled on all Serial interfaces and all FastEthernet interfaces for which traffic-shaping is enabled. If you disable priority queueing by using the **no** form of the **priority-queue** command, WFVQ is re-enabled.

Syntax

[no] priority-queue

User Level

read-write

Context

interface:Serial (DS1 PPP L2-L3, DS1 PPP L2, USP PPP L2, USP PPP L2-L3), FastEthernet (L2, L2-L3) - when Frame Relay Traffic Shaping is configured, Serial (DS1 FR L2, USP FR L2) - when Frame Relay Traffic Shaping is not configured, Dialer (L2, L2-L3)

Example

To enable priority queueing:

```
G450-001(if:Serial 3/1:1)# priority-queue
```

Related Commands - Priority queueing

queue-limit, show queueing, voip-queue, voip-queue-delay

Related Commands - WFVQ

fair-queue-limit, fair-voip-queue, show queue, show queueing, voip-queue

---

show queue

Use the **show queue** command to display information about the real-time status of output queues for the current interface.

Note:

This command is only applicable in fair-voip-queue mode.

Syntax

show queue ***type identifier***

Parameters

Parameter	Description	Possible Values	Default Value
type	The type of interface	**Fast Ethernet** **Serial**	
identifier	The identifier depends on the interface type: For Fast Ethernet: ***module/port*** For Serial: ***module/port:channel-group***	 channel-group: E1: **0-30** T1: **0-23**	

User Level

read-only

Context

interface:Serial (DS1 PPP L2-L3, DS1 PPP L2, DS1 FR L2, USP FR L2, USP PPP L2, USP PPP L2-L3), FastEthernet (L2, L2-L3) - when traffic shaping is configured, Dialer (L2, L2-L3)

Examples

To display output queues real-time status information for FastEthernet port 10/2:

```
G450-001(super)# show queue FastEthernet 10/2
```

To display output queues real-time status information for Serial port 3/1:2:

```
G450-001(super)# show queue Serial 3/1:2
```

Related Commands - WFVQ

fair-queue-limit, fair-voip-queue, priority-queue, show queueing, voip-queue

show queueing

Use the **show queueing** command to display the priority queueing and WFVQ configuration, for a specific interface type or interface, or for all interfaces.

Syntax

show queueing [*interface_type if_number*]

Parameters

Parameter	Description	Possible Values	Default Value
interface_type	The type of interface	**Serial, Fast-Ethernet**	
if_number	The port number of this interface in the form: ***port***[:***channel_group***]	port: **1, 2** channel_group: E1: **0-30** T1: **0-23**	

User Level

read

Context

general

Note:

This command is also used for the FastEthernet interface when traffic shaping has been configured.

Example

To display the priority queue size in packets:

```
G450-001(super)# show queueing
Current priority queue configuration:

Interface Name  VOIP   Est. Delay    Q.1(High)    Q.2   Q.3   Q.4(Low)    DE Buf
                       [ms]
Serial 3/1      OFF    OFF           524          524   524   524         -
Serial 4/1:1    OFF    OFF           507          507   507   507         507
Current voip fair queue configuration:

 Interface Name  Total         Flow discard  Dynamic    Max voip      Priority
                 discard       threshold     Queue      delay (ms)    queues
                 threshold
 Serial 3/1:1    256           64            16         20            1
```

Output fields

Field	Description
VOIP	Indicates if VoIP queueing is enabled. VoIP queueing is enabled using the **`voip-queue`** command.
Est. Delay [ms]	If VoIP queueing is enabled, displays the maximum queue delay for which to estimate the high priority queue size necessary to meet the queueing delay for a specific VoIP codec. By default, this is estimated for the G.729 codec and is 20 ms. Can be configured through the **`voip-queue-delay`** command. If VoIP queueing is not enabled, the Est. Delay column displays **OFF**.
Q.1	The size, in packets, of the highest priority queue
Q.2	The size, in packets, of the second highest priority queue
Q.3	The size, in packets, of the second lowest priority queue
Q.4	The size, in packets, of the lowest priority queue
Total discard threshold	The total buffer credits limit for WFQ. Configurable through **`fair-queue-limit`** command.
Flow discard threshold	Per subqueue buffer credits. Not configurable.
Dynamic queues	The total number of subqueues. Not configurable.

1 of 2

Field	Description
Max voip delay [ms]	Maximum delay for VoIP bearer
Priority queues	The number of priority queues in the system. Not configurable. From the user's point of view control and bearer queues are the same queue.

2 of 2

Related Commands - Priority queueing

priority-queue, queue-limit, voip-queue, voip-queue-delay

Related Commands - WFVQ

fair-queue-limit, fair-voip-queue, priority-queue, show queue, voip-queue

voip-queue

Use the **voip-queue** command to select custom queueing for VoIP traffic. By default, VoIP queueing is off, and Weighted Fair VoIP Queueing (WFVQ) is enabled on all Serial interfaces and all FastEthernet interfaces for which traffic-shaping is enabled. If you disable custom queueing by using the **no** form of the **voip-queue** command, WFVQ is re-enabled.

Syntax

[no] voip-queue

User Level

read-write

Context

interface:Serial (DS1 PPP L2-L3, DS1 PPP L2, DS1 FR L2, USP FR L2, USP PPP L2, USP PPP L2-L3), FastEthernet (L2, L2-L3) - when traffic shaping is configured, Dialer (L2, L2-L3)

Example

To enable VoIP queueing:

```
G450-001(if:Serial 3/1:1)# voip-queue
```

Related Commands - Priority queueing

priority-queue, queue-limit, show queueing, voip-queue-delay

Related Commands - WFVQ

fair-queue-limit, fair-voip-queue, priority-queue, show queue, show queueing

Alphabetical Index of Commands

A

Abbreviating commands 160
add nfas-interface 1049
add port 1072
analog-test 161
area 660
arp 194
arp timeout 195
async mode interactive 607
async mode terminal 607
async modem-init-string 608, 617
async reset-modem (Console port) 609
async reset-modem (USB port) 618
authentication 1277
autoneg 1341

B

backup config usb 221, 1194
backup delay 223
backup interface 224
bandwidth 650, 1218
banner login 359
banner post-login 360
bc out 462, 1183
be out 463, 1184
bootfile 325
bri 960
busyout voip-dsp 1247

C

cablelength long 385
cablelength short 386
campon-busyout voip-dsp 1243
cancel 161
capture buffer-mode 670
capture buffer-size 671
capture filter-group 672
capture interface 673
capture ipsec 674
capture max-frame-size 675
capture start 675
capture stop 676
capture-service 677
channel-group 387
cir out 464, 1185
class-identifier 343
clear arp-cache 196
clear attendant 978
clear bri 978
clear cam 227
clear capture-buffer 678
clear controller counters 383
clear counters (CNA test plugs) 240
clear counters (interface) 273
clear crypto isakmp 1251
clear crypto sa 1252
clear crypto sa counters 1254
clear dial-pattern 979
clear ds1 980
clear dynamic-trap-manager 380
clear extension 980
clear fac 981
clear fragment 444
clear frame-relay counters 448
clear incoming-routing 982
clear ip dhcp server statistics 321
clear ip dhcp-client statistics 306
clear ip dhcp-server binding 320
clear ip domain statistics 366
clear ip route 919
clear ip rtp header-compression 537
clear ip tcp header-compression 538, 1223
clear ip tftp-server statistics 515, 1176
clear ip traffic 274
clear logging file 579
clear logging server 580
clear mgc list 596
clear port mirror 836
clear port static-vlan 1229
clear profile 162
clear radius authentication server 879
clear rmon statistics 907
clear screen 360
clear sig-group 983
clear slot-config 984
clear ssh-client known-hosts 1152
clear station 985
clear survivable-config 986
clear sync interface 1157
clear tac 1075
clear tcp syn-cookies counters 1162
clear trunk-group 986
clear utilization cpu 284
clear vlan 1230
client-identifier 326

clock source 388
cna testplug 239
cna-testplug-service 247
composite-operation 685, 720, 755, 762, 766
continuous-channel 1264, 1284
controller 384
control-port 241
cookie 683, 717, 760, 804
copy announcement-file ftp 182
copy announcement-file scp 183
copy announcement-file usb 184
copy auth-file ftp 200
copy auth-file scp 201
copy auth-file tftp 202
copy auth-file usb 203
copy capture-file ftp 679
copy capture-file scp 680
copy capture-file tftp 681
copy capture-file usb 682
copy cdr-file ftp 229
copy cdr-file scp 230
copy cdr-file tftp 231
copy cdr-file usb 232
copy dhcp-binding ftp 301
copy dhcp-binding scp 302
copy dhcp-binding tftp 303
copy dhcp-binding usb 304
copy ftp announcement-file 185
copy ftp auth-file 204
copy ftp EW_archive 428
copy ftp license-file 553
copy ftp module 429
copy ftp phone-image 516
copy ftp phone-script 517
copy ftp startup-config 251
copy ftp SW_imageA 430
copy ftp SW_imageB 431
copy license-file ftp 554
copy license-file scp 555
copy license-file tftp 556
copy license-file usb 556
copy phone-script ftp 518
copy phone-script scp 519
copy phone-script tftp 520
copy phone-script usb 521
copy running-config ftp 252
copy running-config scp 253
copy running-config startup-config 254
copy running-config tftp 255
copy scp announcement-file 186
copy scp auth-file 205
copy scp license-file 557
copy scp phone-script 522
copy scp startup-config 256
copy startup-config ftp 257
copy startup-config scp 258
copy startup-config tftp 259
copy startup-config usb 260
copy syslog-file ftp 1165
copy syslog-file scp 1166
copy syslog-file tftp 1167
copy syslog-file usb 1167
copy tftp auth-file 206
copy tftp EW_archive 432
copy tftp license-file 558
copy tftp module 433
copy tftp phone-image 523
copy tftp phone-script 524
copy tftp startup-config 261
copy tftp SW_imageA 434
copy tftp SW_imageB 435
copy usb announcement-file 187
copy usb auth-file 207
copy usb EW_archive 436
copy usb license-file 559
copy usb module 437
copy usb phone-image 525
copy usb phone-script 526
copy usb startup-config 262
copy usb SW_image 438
cos 756
crypto ipsec df-bit 1254
crypto ipsec minimal-pmtu 1255
crypto ipsec nat-transparency udp-encapsulation . . 1256
crypto ipsec transform-set 1257
crypto isakmp invalid-spi-recovery 1262
crypto isakmp nat keepalive 1262
crypto isakmp peer 1263
crypto isakmp peer-group 1273
crypto isakmp policy 1276
crypto isakmp suggest-key 1282
crypto key generate 1152
crypto map 1283

D

default-metric (interface route metric value) 915
default-metric (OSPF) 661, 915
default-metric (RIP) 901, 916
default-router 327
description (crypto map) 1285
description (DNS resolver) 369
description (interface) 506
description (ip rule) 1292
description (ISAKMP peer group) 1274
description (ISAKMP peer) 1265
description (ISAKMP policy) 1278
description (object tracking) 647
destination-ip 686, 721, 767, 807, 1293
dialer modem-interface 351

dialer order 352
dialer persistent 353
dialer persistent delay 353
dialer persistent initial delay 354
dialer persistent max-attempts 355
dialer persistent re-enable 356
dialer string 356
dialer wait-for-ipcp 357
dial-pattern 987
dir 439, 1195
disconnect ssh 1153
distribution-list 901
dns-server 327
domain-name 328
DoS-classification 625
ds1 998
dscp (object tracking) 631
dscp (policy) 723, 757, 769
dscp (policy-based routing, packet sniffing, VPN) 688, 809
dscp-table 761
ds-mode 395
duplex 1341
dynamic-cac 379

E

encapsulation 451, 846
encapsulation pppoe 855
encryption 1279
end-ip-addr 329
erase announcement-file 188
erase auth-file 208
erase phone-image 527
erase phone-script 527
erase startup-config 262
erase usb 1197
exit 234

F

fail-retries 632
fair-queue-limit 1345
fair-voip-queue 1346
fdl 389
fingerprint 241
fragment 465, 689, 724, 770, 810, 1186
fragment chain 445
fragment size 446
fragment timeout 447
frame-relay class-dlci 452
frame-relay interface-dlci 453
frame-relay lmi-n391dte 454
frame-relay lmi-n392dte 455
frame-relay lmi-n393dte 456
frame-relay lmi-type 457
frame-relay priority-dlci-group 458
frame-relay traffic-shaping 459, 1181
framing 390
frequency 633

G

group 1280

H

hash 1280
hostname 361, 1154

I

icc-vlan 490, 1232
icmp 690, 725, 771, 805
icmp in-echo-limit 627
idle-character 1219
ignore dcd 1220
incoming-routing 1017
initiate mode 1266
interface console 498, 606
interface dialer 350, 499
interface FastEthernet 854, 1340
interface fastethernet 500
interface loopback 501
interface serial 396, 449, 502, 845, 1179, 1217
interface tunnel 477, 503
interface USB-modem 504
interface usb-modem 616
interface vlan 505, 1231
interface-keepalive bypass-logic 634
invert txclock 1221
ip access-control-list 716
ip access-group 746
ip address 397, 460, 507, 848
ip address dhcp 306
ip address negotiated 358, 856
ip admin-state 508
ip bootp-dhcp network 299
ip bootp-dhcp relay 300
ip bootp-dhcp server 300
ip broadcast-address 509
ip capture-list 683
ip crypto-group 1290
ip crypto-list 1291
ip default-gateway 281, 920
ip dhcp activate pool 321
ip dhcp client client-id 307
ip dhcp client hostname 308
ip dhcp client lease 309
ip dhcp client request 310

ip dhcp client route track 311
ip dhcp ping packets 322
ip dhcp ping timeout 323
ip dhcp pool 324
ip dhcp-server 347
ip directed-broadcast 225
ip distribution access-default-action 889
ip distribution access-list 890
ip distribution access-list-cookie 891
ip distribution access-list-copy 892
ip distribution access-list-name 892
ip distribution access-list-owner 893
ip domain list 366
ip domain lookup 367
ip domain name-server-list 368
ip domain retry 370
ip domain timeout 371
ip http 489
ip icmp-errors 491
ip license-server 552
ip max-arp-entries 197
ip netbios-rebroadcast 225
ip netmask-format 921
ip next-hop-list 798
ip ospf authentication 651
ip ospf authentication-key 652
ip ospf cost 653
ip ospf dead-interval 654
ip ospf hello-interval 655
ip ospf message-digest-key 656
ip ospf network point-to-multipoint 657
ip ospf priority 657
ip ospf router-id 658
ip pbr-group 802
ip pbr-list 803
ip peer address 609, 619
ip policy-list-copy 747, 752
ip proxy-arp 873
ip qos-group 753
ip qos-list 754
ip redirects 922
ip rip authentication key 894
ip rip authentication mode 895
ip rip default-route-mode 896
ip rip poison-reverse 897
ip rip rip-version 897
ip rip send-receive-mode 898
ip rip split-horizon 899
ip route 922
ip routing 924
ip rtp compression-connections 539
ip rtp header-compression 540
ip rtp max-period 541
ip rtp max-time 542
ip rtp non-tcp-mode 543
ip rtp port-range 544
ip simulate 748, 795
ip snmp 1102
ip ssh 1155
ip tcp compression-connections 545, 1224
ip tcp header-compression 1225
ip telnet 1172
ip telnet-client 1173
ip telnet-services 1174
ip tftp-server 1177
ip tftp-server file-system size 528, 1177
ip unnumbered 535
ip vrrp 1319
ip vrrp address 1320
ip vrrp auth-key 1321
ip vrrp override addr owner 1322
ip vrrp preempt 1323
ip vrrp primary 1324
ip vrrp priority 1325
ip vrrp timer 1325
ip-fragments-in 718
ip-option-in 719
ip-protocol 692, 727, 772, 811
ip-rule (policy, policy-based routing, packet sniffing) 684, 719, ...765, 806
ip-rule (VPN) 1292
isakmp-policy 1267

K

keepalive (GRE tunnel) 478
keepalive (PPP) 849
keepalive (VPN) 1268
keepalive-icmp 492
keepalive-icmp failure-retries 493
keepalive-icmp interval 494
keepalive-icmp source-address 495
keepalive-icmp success-retries 496
keepalive-icmp timeout 497
keepalive-track 1269, 1342
key config-key password-encryption 594

L

launch 163
lease 330
lifetime 1281
line 362
linecode (E1) 391
linecode (T1) 392
load-interval 509
local-address 1297
login authentication inactivity-period 1203
login authentication local-craft-password 210
login authentication lockout 209, 1204

login authentication min-password-digit-chars 1205
login authentication min-password-length 1206
login authentication min-password-lower-chars . . . 1207
login authentication min-password-special-chars . . 1208
login authentication min-password-upper-chars . . . 1209
login authentication password-expire 1210
login authentication response-time 211
login authentication services-login 212
loopback 393

M

map-class frame-relay 461, 1181
mode 1259
mtu 857

N

name . . . 331, 334, 344, 704, 741, 758, 763, 787, 826
name-server 369
network (OSPF) 661
network (RIP) 902
next-hop (object tracking) 634
next-hop (policy-based routing) 813
next-hop-interface 799
next-hop-ip 801
next-server 332
nrzi-encoding 1221
nslookup 372
nvram initialize 263

O

object 648
option 333
owner 705, 742, 788, 827

P

passive-interface 662
password 1212
ping 269
pmi 714
ppp authentication 213, 610, 620
ppp chap hostname 858
ppp chap password 859
ppp chap refuse 860
ppp chap-secret 611, 621
ppp ipcp dns request 373, 860
ppp pap refuse 861
ppp pap sent-username 862
ppp timeout authentication 612, 622
ppp timeout ncp 850
ppp timeout retry 851
pppoe-client persistent delay 863
pppoe-client persistent max-attempts 864
pppoe-client service-name 865
pppoe-client wait-for-ipcp 866
pre-classification 789
pre-shared-key 1270
priority-queue 867, 1347
profile 164
protect crypto map 1295

Q

queue-limit 868

R

redistribute (OSPF) 663, 917
redistribute (RIP) 903, 918
release dhcp 312
release voip-dsp 1248
remote 394
remove nfas-interface 1050
remove port 1075
rename announcement-file 189
renew dhcp 313
reset 235
reset voip-dsp 1244
restore usb 887, 1197
retstatus 236
rmon alarm 907
rmon event 909
rmon history 910
router ospf 659
router rip 900
router vrrp 1326
rtp-echo-port 242
rtp-stat clear 937
rtp-stat event-threshold 938
rtp-stat fault 940
rtp-stat min-stat-win 941
rtp-stat qos-trap 942
rtp-stat qos-trap-rate-limit 943
rtp-stat threshold 944
rtp-stat-service 944
rtp-test-port 243
rtr 629
rtr-schedule 639

S

safe-removal usb 1198
sat 956
scheduler 244
self-identity 1271

server-name . . . 336
session . . . 597
set associated-signaling . . . 1051
set attendant . . . 1023
set balance . . . 175
set bearer-capability . . . 961, 1000
set bit-rate . . . 1001
set boot bank . . . 441
set busy-disconnect . . . 1076
set cbc . . . 1077
set cbc-parameter . . . 1079
set cbc-service-feature . . . 1080
set channel-numbering . . . 1002
set channel-preference . . . 1081
set codeset-display . . . 1082
set codeset-national . . . 1083
set connect . . . 1003
set contact-closure admin . . . 270
set contact-closure pulse-duration . . . 271
set cor . . . 1056
set country-protocol . . . 962, 1004
set crosstalk-destination . . . 165
set crosstalk-port . . . 166
set crosstalk-responder . . . 167
set date . . . 279
set date-format . . . 1024
set delete-digits . . . 989, 1018
set deny . . . 990
set destination . . . 168
set dial . . . 1084
set digit-handling . . . 1084
set digits . . . 1086
set digit-treatment . . . 1087
set directory-number-a . . . 964
set directory-number-b . . . 965
set dscp . . . 1286
set echo-cancellation analog . . . 401
set echo-cancellation config analog . . . 402
set echo-cancellation config voip . . . 405
set echo-cancellation voip . . . 407
set endpoint-init . . . 966
set etr . . . 425
set expansion-module . . . 1059
set fac . . . 1025
set icc-monitoring . . . 598
set incoming-destination . . . 1088
set incoming-dialtone . . . 1089
set insert-digits (dial-pattern) . . . 990
set insert-digits (incoming-routing) . . . 1019
set interface . . . 967, 1005
set interface-companding . . . 968, 1007
set ip-codec-set . . . 1026
set japan-disconnect . . . 1090
set layer1-stable . . . 969
set length . . . 1020
set lldp re-init-delay . . . 566
set lldp system-control . . . 567
set lldp tx-delay . . . 567
set lldp tx-hold-multiplier . . . 568
set lldp tx-interval . . . 569
set logging file . . . 581
set logging server . . . 583
set logging server access-level . . . 584
set logging server condition . . . 585
set logging server enable | disable . . . 586
set logging server facility . . . 587
set logging session . . . 588
set logout . . . 236
set long-timer . . . 1008
set match-pattern . . . 1021
set max-ip-registrations . . . 1027
set max-length . . . 991
set mediaserver . . . 598
set mgc list . . . 599
set min-length . . . 992
set mss-notification rate . . . 627
set name . . . 970, 1009, 1059, 1091
set numbering-format . . . 1092
set password . . . 1061
set peer (crypto map) . . . 1287
set peer (peer group) . . . 1275
set peer-group . . . 1288
set pfs . . . 1260
set pim-lockout . . . 1027
set port . . . 169, 1062
set port auto-negotiation-flowcontrol-advertisement . 410
set port classification . . . 834
set port duplex . . . 411
set port edge admin state . . . 412, 1135
set port enable | disable . . . 413
set port flowcontrol . . . 414
set port level . . . 416
set port lldp . . . 570
set port lldp tlv . . . 571
set port mirror . . . 837
set port name . . . 417
set port negotiation . . . 418
set port point-to-point admin status . . . 419, 1136
set port redundancy . . . 839
set port redundancy enable|disable . . . 841
set port redundancy-intervals . . . 842
set port spantree . . . 1137
set port spantree cost . . . 1138
set port spantree force-protocol-migration . . . 1139
set port spantree priority . . . 1140
set port speed . . . 420
set port static-vlan . . . 1233
set port trap . . . 1123
set port vlan . . . 1234
set port vlan-binding-mode . . . 1235

set primary-dchannel . . . 1052
set protocol-version . . . 1010
set qos bearer . . . 874
set qos control . . . 875
set qos rsvp . . . 932
set qos rtcp . . . 934
set qos signal . . . 876
set radius authentication . . . 880
set radius authentication retry-number . . . 881
set radius authentication retry-time . . . 882
set radius authentication secret . . . 882
set radius authentication server . . . 883
set radius authentication udp-port . . . 884
set receive-gain . . . 176
set reset-times . . . 600
set responder . . . 170
set responder-type . . . 171
set security-association lifetime . . . 1261
set send-name . . . 1093
set send-number . . . 1095
set side . . . 971, 1012
set signaling-mode . . . 1013
set slot-config . . . 1028
set sls . . . 958
set snmp community . . . 1103
set snmp retries . . . 1104
set snmp timeout . . . 1105
set snmp trap enable | disable auth . . . 1125
set snmp trap enable | disable frame-relay . . . 1125
set spantree default-path-cost . . . 1141
set spantree enable | disable . . . 1142
set spantree forward-delay . . . 1143
set spantree hello-time . . . 1143
set spantree max-age . . . 1144
set spantree priority . . . 1145
set spantree tx-hold-count . . . 1146
set spantree version . . . 1147
set spid-a . . . 973
set spid-b . . . 974
set supervision . . . 1096
set swhook-flash . . . 1063
set sync interface . . . 1158
set sync source . . . 1159
set sync switching . . . 1160
set system contact . . . 1170
set system location . . . 1171
set system name . . . 1171
set tac . . . 1097
set tei-assignment . . . 975
set terminal recovery password . . . 886
set tgnum . . . 993
set time . . . 280
set transform-set . . . 1289
set transmit-gain . . . 177
set trunk . . . 1236
set trunk-destination . . . 1064
set trunk-group-chan-select . . . 1053
set trunk-hunt . . . 1098
set type . . . 172
set type (dial-pattern) . . . 994
set type (station) . . . 1065
set utilization cpu . . . 284
set vlan . . . 1237
set web aux-files-url . . . 219
show (bri) . . . 976
show (dial-pattern) . . . 997
show (ds1) . . . 1014
show (incoming-routing) . . . 1022
show (profile) . . . 173
show (sig-group) . . . 1054
show (station) . . . 1067
show (trunk-group) . . . 1099
show announcements files . . . 190
show application-memory . . . 529, 1178
show attendant . . . 1030
show auth-file info . . . 214
show backup status . . . 222, 1199
show banner login . . . 363
show banner post-login . . . 363
show boot bank . . . 442
show bri . . . 1030
show cam . . . 227
show cam mac . . . 228
show cam vlan . . . 1238
show capture . . . 706
show capture-buffer hex . . . 707
show cna testplug . . . 247
show composite-operation . . . 728, 743, 759, 774, 790
show contact-closure . . . 272
show controllers . . . 398, 1329
show controllers remote . . . 399
show copy status . . . 264
show correction . . . 178
show crypto ipsec sa . . . 1298
show crypto ipsec transform-set . . . 1306
show crypto isakmp peer . . . 1308
show crypto isakmp peer-group . . . 1309
show crypto isakmp policy . . . 1310
show crypto isakmp sa . . . 1311
show crypto map . . . 1313
show csu loopbacks . . . 277
show csu status . . . 278
show date-format . . . 1032
show dev log file . . . 590
show dial-pattern . . . 1032
show download . . . 285
show download announcement-file status . . . 191
show download auth-file status . . . 215
show download license-file status . . . 560
show download phone-image-file status . . . 530

show download phone-script-file status 531
show download software status 442
show download status 265
show ds1 1034
show dscp-table 764, 775, 791
show ds-mode 400
show dynamic-cac 380
show echo-cancellation 408
show erase status 266
show etr 426
show extension 1035
show fac 1037
show faults 286
show fragment 447
show frame-relay fragment 1330
show frame-relay lmi 1331
show frame-relay map 466, 1333
show frame-relay pvc 1334
show frame-relay pvc brief 467
show frame-relay traffic 1335
show icc-monitoring 601
show icc-vlan 490
show image version 443
show incoming-routing 1038
show interfaces 467, 486, 851, 1336
show ip access-control-list 750
show ip active-lists 831, 1314
show ip active-pbr-lists 833
show ip arp 198
show ip capture-list 708
show ip crypto-list 1316
show ip dhcp-client 314
show ip dhcp-client statistics 318
show ip dhcp-pool 337
show ip dhcp-server bindings 347
show ip dhcp-server statistics 348
show ip distribution access-lists 905
show ip domain 373
show ip domain statistics 375
show ip icmp 492
show ip interface 510
show ip interface brief 513
show ip next-hop-list 814
show ip ospf 665
show ip ospf database 666
show ip ospf interface 667
show ip ospf neighbor 668
show ip pbr-list 833
show ip protocols 669, 905
show ip qos-list 796
show ip reverse-arp 199
show ip route 925
show ip route best-match 926
show ip route static 927
show ip route summary 928
show ip route track-table 929
show ip rtp header-compression 546
show ip rtp header-compression brief 548
show ip ssh 1156
show ip tcp header-compression 549, 1226
show ip tcp header-compression brief 551, 1227
show ip telnet 1174
show ip tftp-server files 532
show ip tftp-server statistics 533
show ip traffic 275
show ip vrrp 1327
show ip-codec-set 1039
show ip-rule 693, 729, 744, 776, 792, 815, 828
show isdn bri link 563
show isdn link summary 564
show isdn pri link 565
show keepalive-icmp 497
show last-pim-update 1040
show license status 561
show list 745, 794, 830
show lldp 573
show lldp config 575
show logging file condition 590
show logging file content 591
show logging server condition 592
show logging session condition 593
show login authentication 216, 1213
show logout 237
show map-class frame-relay 470, 1187, 1339
show max-ip-registrations 1040
show mediaserver 602
show mg list_config 287
show mgc 288, 603
show mgc list 604
show mm 289
show module 290
show mss-notification rate 628
show next-hop 802
show pim-lockout 1041
show platform fans 427, 710
show platform mainboard 712
show platform power 711
show pmi 715
show port 843
show port auto-negotiation-flowcontrol-advertisement 421
show port classification 835
show port edge state 422, 1148
show port flowcontrol 423
show port lldp config 576
show port lldp vlan-name config 578
show port mirror 838
show port point-to-point status 1149
show port redundancy 843
show port trap 1126
show port vlan-binding-mode 1239

show ppp authentication 613, 623
show profile 179
show protocol 377
show qos-rtcp 877, 933, 935
show queue 1348
show queueing 869, 1349
show radius authentication 885
show recovery 291, 605
show restart-log 292
show restore status 888, 1200
show result 180
show result (profile) 174
show rmon alarm 911
show rmon event 912
show rmon history 913
show rmon statistics 914
show rtp-stat config 947
show rtp-stat detailed 948
show rtp-stat sessions 949
show rtp-stat summary 952
show rtp-stat thresholds 953
show rtp-stat traceroute 954
show rtr configuration 640
show rtr operational-state 642
show running-config 266
show sig-group 1041
show slot-config 1042
show sls 959
show snmp 1106, 1127
show snmp engineID 1107
show snmp group 1108
show snmp retries 1109
show snmp timeout 1110
show snmp user 1111
show snmp usertogroup 1112
show snmp view 1113
show spantree 1149
show startup-config 267
show station 1043
show sync timing 1161
show system 293
show tcp syn-cookies 1163
show temp 294
show timeout 295
show track 643
show traffic-shape 471, 1188
show traffic-shape-queue 473, 1190
show traffic-shape-statistics 475, 1191
show trunk 1240
show trunk-group 1045
show upload 296
show upload announcement-file status 192
show upload auth-file status 217
show upload cdr-file status 233
show upload dhcp-binding-file status 305
show upload license-file status 562
show upload phone-script-file status 534
show upload status 268
show upload syslog-file status 1168
show usb 1201
show username 1214
show utilization 297
show vlan 1241
show voip-dsp 1244
show voip-parameters 878, 1246, 1249
show voltages 297
show web aux-files-url 220
shutdown (CNA test plugs) 245
shutdown (interface) 514, 614
shutdown (USB modem) 624
sig-group 1047
sls 957
snmp trap link-status 1128
snmp-server community 1114
snmp-server dynamic-trap-manager 381
snmp-server enable notifications 1129
snmp-server engineID 1115
snmp-server group 1117
snmp-server host 1130
snmp-server informs 1133
snmp-server remote-user 1119
snmp-server user 1120
snmp-server view 1122
source-address 636
source-ip 695, 731, 778, 816, 1296
speed (interface) 1343
speed (PPP) 615
start-ip-addr 341
station 1055
subnet-mask 342
success-retries 637
suggest-key 1272

T

tcp destination-port 696, 732, 779, 818
tcp established 734
tcp source-port 698, 735, 781, 820
tcp syn-cookies 1164
tech 238
telnet 1175
terminal length 364
terminal width 365
test led 298
test voip-dsp 1250
test-rate-limit 246
threshold count 649
timeout absolute 615, 624
timers basic 904
timers spf 664

traceroute 929
track 645
traffic-shape rate 1193, 1344
transmitter-delay 1222
tree 238
trunk-group 1068
tunnel checksum 479
tunnel destination 479
tunnel dscp 480
tunnel key 481
tunnel mode 482
tunnel path-mtu-discovery 483
tunnel source 484
tunnel ttl 485
type 630

U

udp destination-port 700, 737, 783, 822
udp source-port 702, 739, 785, 824
username 218, 1215
Using auto-complete 160
Using Help 160

V

value 335, 345
vendor-specific-option 343
voip-queue 871, 1351
voip-queue-delay 872

W

wait-interval 638

Z

zeroize 283

Topical Index of Commands

A

Analog testing
- analog-test . . . 161
  - cancel . . . 161
  - clear profile . . . 162
  - launch . . . 163
  - profile . . . 164
    - set crosstalk-destination . . . 165
    - set crosstalk-port . . . 166
    - set crosstalk-responder . . . 167
    - set destination . . . 168
    - set port . . . 169
    - set responder . . . 170
    - set responder-type . . . 171
    - set type . . . 172
    - show (profile) . . . 173
    - show result (profile) . . . 174
  - set balance . . . 175
  - set receive-gain . . . 176
  - set transmit-gain . . . 177
  - show correction . . . 178
  - show profile . . . 179
  - show result . . . 180

Announcement files
- copy announcement-file ftp . . . 182
- copy announcement-file scp . . . 183
- copy announcement-file usb . . . 184
- copy ftp announcement-file . . . 185
- copy scp announcement-file . . . 186
- copy usb announcement-file . . . 187
- erase announcement-file . . . 188
- rename announcement-file . . . 189
- show announcements files . . . 190
- show download announcement-file status . . . 191
- show upload announcement-file status . . . 192

ARP table
- arp . . . 194
- arp timeout . . . 195
- clear arp-cache . . . 196
- ip max-arp-entries . . . 197
- show ip arp . . . 198
- show ip reverse-arp . . . 199

ASG authentication
- copy auth-file ftp . . . 200
- copy auth-file scp . . . 201
- copy auth-file tftp . . . 202
- copy auth-file usb . . . 203
- copy ftp auth-file . . . 204
- copy scp auth-file . . . 205
- copy tftp auth-file . . . 206
- copy usb auth-file . . . 207
- erase auth-file . . . 208
- login authentication local-craft-password . . . 210
- login authentication lockout . . . 209, 1204
- login authentication response-time . . . 211
- login authentication services-login . . . 212
- ppp authentication . . . 213, 610, 620
- show auth-file info . . . 214
- show download auth-file status . . . 215
- show login authentication . . . 216, 1213
- show upload auth-file status . . . 217
- username . . . 218, 1215

autoneg . . . 156

Auxiliary files
- set web aux-files-url . . . 219
- show web aux-files-url . . . 220

B

Backing up the gateway to a USB device
- backup config usb . . . 221, 1194
- show backup status . . . 222, 1199

Backup interfaces
- backup delay . . . 223
- backup interface . . . 224

BOOTP relay, *see* DHCP and BOOTP relay

BRI links, *see* Link status

Broadcast relay
- ip directed-broadcast . . . 225
- ip netbios-rebroadcast . . . 225

C

CAC, *see* Dynamic CAC

Call admission control, *see* Dynamic CAC

CAM table
- clear cam . . . 227
- show cam . . . 227
- show cam mac . . . 228

CDR file
- copy cdr-file ftp . . . 229
- copy cdr-file scp . . . 230
- copy cdr-file tftp . . . 231
- copy cdr-file usb . . . 232
- show upload cdr-file status . . . 233

Chatter, *see* CNA test plugs

CLI sessions

exit . . . 234
reset . . . 235
retstatus . . . 236
set logout . . . 236
show logout . . . 237
tech . . . 238
tree . . . 238
CNA test plugs
cna testplug . . . 239
clear counters . . . 240
control-port . . . 241
fingerprint . . . 241
rtp-echo-port . . . 242
rtp-test-port . . . 243
scheduler . . . 244
shutdown . . . 245
test-rate-limit . . . 246
cna-testplug-service . . . 247
show cna testplug . . . 247
Commands
add nfas-interface . . . 131
add port . . . 133
area . . . 93
arp . . . 47
arp timeout . . . 47
async mode interactive . . . 88
async mode terminal . . . 88
async modem-init-string . . . 88
async reset-modem . . . 88
async-limit-string . . . 89
async-reset-modem . . . 89
authentication . . . 151
backup config usb . . . 50, 143
backup delay . . . 51
backup interface . . . 51
bandwidth . . . 93, 145
banner login . . . 66
banner post-login . . . 66
bc out . . . 75, 142
be out . . . 75, 142
bootfile . . . 63
bri . . . 123
busyout voip-dsp . . . 148
cable length long . . . 69
cable length short . . . 69
campon-busyout voip-dsp . . . 147
capture buffer-mode . . . 94
capture buffer-size . . . 94
capture filter-group . . . 94
capture interface . . . 95
capture ipsec . . . 95
capture max-frame-size . . . 95
capture start . . . 95
capture stop . . . 95
capture-service . . . 95
channel-group . . . 69
cir out . . . 75, 142
class-identifier . . . 64
clear arp-cache . . . 47
clear attendant . . . 124, 126
clear bri . . . 124, 126
clear cam . . . 52
clear capture-buffer . . . 95
clear controller counters . . . 69
clear counter . . . 53
clear counters . . . 57
clear crypto isakmp . . . 148
clear crypto sa . . . 148
clear crypto sa counters . . . 148
clear dial-pattern . . . 125, 127
clear ds1 . . . 125, 127
clear dynamic-trap-manager . . . 68
clear extension . . . 125, 127
clear fac . . . 125, 127
clear fragment . . . 74
clear frame-relay counters . . . 74
clear incoming-routing . . . 125, 127
clear ip dhcp-client statistics . . . 61, 62
clear ip dhcp-server binding . . . 62
clear ip dhcp-server statistics . . . 62
clear ip domain statistics . . . 66
clear ip route . . . 120
clear ip rtp header-compression . . . 82
clear ip tcp header-compression . . . 82, 145
clear ip tftp-server statistics . . . 80, 142
clear ip traffic . . . 57
clear logging file . . . 86
clear mgc list . . . 87
clear port mirror . . . 111
clear port static-vlan . . . 146
clear radius authentication server . . . 116
clear rmon statistics . . . 119
clear screen . . . 66
clear sig-group . . . 125, 127
clear slot-config . . . 125, 127
clear ssh-client known-hosts . . . 139
clear station . . . 125, 127
clear survivable-config . . . 125, 127
clear sync interface . . . 139
clear tac . . . 133
clear tcp syn-cookies counters . . . 140
clear trunk-group . . . 125, 127
clear utilization cpu . . . 58
clear vlan . . . 146
client-identifiers . . . 63
clock source . . . 69
cna-testplug . . . 53
cna-testplug-service . . . 54
composite-operation . . . 96, 100, 104, 105
continuous-channel . . . 149, 151

controller . . . 69
control-port . . . 53
cookie . . . 96, 99, 104, 109
copy announcement-file ftp . . . 46
copy announcement-file scp . . . 46
copy announcement-file usb . . . 46
copy auth-file ftp . . . 48
copy auth-file scp . . . 48
copy auth-file tftp . . . 48
copy auth-file usb . . . 48
copy capture-file ftp . . . 95
copy capture-file scp . . . 95
copy capture-file tftp . . . 95
copy capture-file usb . . . 95
copy cdr-file ftp . . . 52
copy cdr-file scp . . . 52
copy cdr-file tftp . . . 52
copy cdr-file usb . . . 52
copy dhcp-binding ftp . . . 60
copy dhcp-binding scp . . . 60
copy dhcp-binding tftp . . . 60
copy dhcp-binding usb . . . 60
copy ftp announcement-file . . . 47
copy ftp auth-file . . . 48
copy ftp EW_archives . . . 72
copy ftp license-file . . . 84
copy ftp module . . . 72
copy ftp phone-image . . . 80
copy ftp phone-script . . . 80
copy ftp startup-config . . . 54
copy ftp SW_imageA . . . 72
copy ftp SW_imageB . . . 72
copy license-file ftp . . . 84
copy license-file scp . . . 84
copy license-file tftp . . . 84
copy license-file usb . . . 84
copy phone-script ftp . . . 80
copy phone-script scp . . . 81
copy phone-script tftp . . . 81
copy phone-script usb . . . 81
copy running-config ftp . . . 54
copy running-config scp . . . 54
copy running-config startup-config . . . 55
copy running-config tftp . . . 55
copy scp announcement-file . . . 47
copy scp auth-file . . . 48
copy scp license-file . . . 84
copy scp phone-script . . . 81
copy scp startup-config . . . 55
copy startup-config ftp . . . 55
copy startup-config scp . . . 55
copy startup-config tftp . . . 55
copy startup-config usb . . . 55
copy syslog-file ftp . . . 140
copy syslog-file tftp . . . 140
copy syslog-file usb . . . 140
copy tftp auth-file . . . 48
copy tftp EW_archives . . . 73
copy tftp license-file . . . 84
copy tftp module . . . 73
copy tftp phone-image . . . 81
copy tftp phone-script . . . 81
copy tftp startup-config . . . 55
copy tftp SW_imageA . . . 73
copy tftp SW_imageB . . . 73
copy usb announcement-file . . . 47
copy usb auth-file . . . 48
copy usb EW_archive . . . 73
copy usb license-file . . . 84
copy usb module . . . 73
copy usb phone-image . . . 81
copy usb phone-script . . . 81
copy usb startup-config . . . 55
copy usb SW_image . . . 73
cos . . . 104
crypto ipsec df-bit . . . 152
crypto ipsec minimal-pmtu . . . 152
crypto isakmp invalid-spi-recovery . . . 149
crypto isakmp nat keepalive . . . 149
crypto isakmp peer . . . 149
crypto isakmp peer-group . . . 150
crypto isakmp policy . . . 150
crypto isakmp suggest-key . . . 151
crypto ispec nat-transparency udp-encapsulation 148
crypto ispec transform-set . . . 148
crypto key generate . . . 139
crypto map . . . 151
default-metric . . . 93, 118, 119, 120
default-routers . . . 63
description . . . 67, 80, 92, 149, 150, 151, 152
destination . . . 105
destination-ip . . . 96, 100, 109, 152
dialer modem-interface . . . 65
dialer order . . . 65
dialer persistent . . . 65
dialer persistent delay . . . 65
dialer persistent initial delay . . . 65
dialer persistent max-attempts . . . 65
dialer persistent re-enable . . . 65
dialer string . . . 65
dialer wait-for-ipcp . . . 65
dial-pattern . . . 125, 127
dir . . . 73, 143
disconnect ssh . . . 139
distribution-list . . . 118
dns-server . . . 63
domain-name . . . 63
dos-classification . . . 90
ds1 . . . 128
dscp . . . 91, 96, 100, 104, 105, 109
dscp-table . . . 104
dynamic-cac . . . 68

encapsulation 74, 112
encapsulation pppoe 113
encryption 151
end-ip-addr 63
erase announcement-file 47
erase auth-file 48
erase phone-image 81
erase phone-script 81
erase startup-config 55
erase usb 143
exit 53
fail-retries 91
fair-queue-limit 156
fair-voip-queue 156
FastEthernet 113
fdl 69
fingerprint 54
fragment 75, 96, 100, 105, 109, 142
fragment chain 74
fragment size 74
fragment timeout 74
frame-relay class-dlcl 74
frame-relay interface-dlcl 74
frame-relay lmi-n391dte 75
frame-relay lmi-n392dte 75
frame-relay lmi-n393dte 75
frame-relay lmi-type 75
frame-relay priority-dlcl-group 75
frame-relay traffic-shaping 75, 142
framing 69
frequency 91
group 151
hash 151
hostname 66, 139
icmp 96, 100, 106, 109
icmp in-echo-limit 90
idle-character 145
ignore dcd 145
incoming-routing 129
initiate mode 149
interface console 79, 88
interface dialer 65, 79
interface FastEthernet 61, 79, 156
interface loopback 79
interface serial 69, 74, 79, 112, 142, 145
interface tunnel 76, 79
interface usb 79
interface usb-modem 89
interface vlan 77, 79, 146
interface-keepalive bypass-logic 91
invert txclock 145
ip access-control-list 99
ip access-group 98
ip address 69, 75, 80, 88, 90, 112, 113
ip address dhcp 61
ip address negotiated 65, 113
ip admin-state 80
ip bootp-dhcp network 60
ip bootp-dhcp relay 60
ip bootp-dhcp server 60
ip broadcast-address 80
ip capture-list 95
ip crypto-group 152
ip crypto-list 152
ip default-gateway 58, 120
ip dhcp activate pool 62
ip dhcp client client-id 61
ip dhcp client hostname 61
ip dhcp client lease 61
ip dhcp client request 61
ip dhcp client route track 61
ip dhcp ping packets 62
ip dhcp ping timeout 62
ip dhcp pools 62
ip dhcp-server 64
ip directed-broadcast 51
ip distribution access-default-action 118
ip distribution access-list 118
ip distribution access-list-cookie 118
ip distribution access-list-copy 118
ip distribution access-list-name 118
ip distribution access-list-owner 118
ip domain list 67
ip domain lookup 67
ip domain name-server-list 67
ip domain retry 67
ip domain timeout 67
ip icmp-errors 78
ip license-server 83
ip max-arp-entries 47
ip netbios-rebroadcast 51
ip netmask-format 120
ip next-hop-list 108
ip ospf authentication 93
ip ospf authentication-key 93
ip ospf cost 93
ip ospf dead-interval 93
ip ospf hello-interval 93
ip ospf message-digest-key 93
ip ospf network point-to-multipoint 93
ip ospf priority 93
ip ospf router-id 93
ip pbr-group 108
ip pbr-list 109
ip peer address 89, 90
ip policy-list-copy 102, 103
ip proxy-arp 115
ip qos-group 103
ip qos-list 103
ip redirects 120

ip rip authentications key . . . 117
ip rip authentications mode . . . 118
ip rip default-route-mode . . . 118
ip rip poison-reverse . . . 118
ip rip rip-version . . . 118
ip rip send-receive-mode . . . 118
ip rip split-horizon . . . 118
ip route . . . 120
ip routing . . . 121
ip rtp compression-connections . . . 82
ip rtp header-compression . . . 82
ip rtp max-period . . . 82
ip rtp max-time . . . 82
ip rtp non-tcp-mode . . . 83
ip rtp port-range . . . 83
ip set system contact . . . 141
ip simulate . . . 99, 103
ip snmp . . . 135
ip ssh . . . 139
ip tcp compression-connections . . . 83, 146
ip tcp header-compression . . . 146
ip telnet . . . 141
ip telnet-client . . . 141
ip telnet-services . . . 141
ip tftp-server . . . 142
ip tftp-server file-system size . . . 81, 142
ip unnumbered . . . 82
ip vrrp . . . 154
ip vrrp address . . . 154
ip vrrp auth-key . . . 154
ip vrrp override addr owner . . . 154
ip vrrp preempt . . . 154
ip vrrp primary . . . 154
ip vrrp priority . . . 154
ip vrrp timer . . . 155
ipcopy syslog-file scp . . . 140
ipds-mode . . . 69
ip-fragments-in . . . 99
ip-option-in . . . 99
ip-protocol . . . 96, 100, 106, 109
ip-rule . . . 96, 100, 105, 109, 152
isakmp-policy . . . 150
iss-vlan . . . 77, 146
keepalive . . . 76, 112, 150
keepalive-icmp . . . 78
keepalive-icmp failure-retries . . . 78
keepalive-icmp interval . . . 78
keepalive-icmp source-address . . . 78
keepalive-icmp success-retries . . . 78
keepalive-icmp timeout . . . 78
keepalive-track . . . 113, 150
key config-key password-encryption . . . 87
lease . . . 63
lifetime . . . 151
line . . . 66
linecode . . . 69
load-interval . . . 80
local-address . . . 153
login authentication inactivity-period . . . 144
login authentication local-craft-password . . . 49
login authentication lockout . . . 48, 144
login authentication min-password-digit-chars . . . 144
login authentication min-password-length . . . 144
login authentication min-password-lower-chars . . . 144
login authentication min-password-special-chars . . . 144
login authentication min-password-upper-chars . . . 144
login authentication password-expire . . . 144
login authentication response-time . . . 49
login authentication services-logins . . . 49
loopback . . . 69
map-class frame-relay . . . 75, 142
mode . . . 149
mtu . . . 113
name . . . 63, 64, 97, 102, 104, 105, 107, 110
name-server . . . 67
network . . . 94
next-hop . . . 92
next-hop (policy-based routing) . . . 109
next-hop-interface . . . 108
next-hop-ip . . . 109
next-server . . . 63
nslookup . . . 67
nvram initialize . . . 55
nzri-encoding . . . 145
object . . . 92
option . . . 63
owner . . . 97, 102, 107, 110
passive-interfaces . . . 94
password . . . 144
ping . . . 56
pmi . . . 98
PPP authentication . . . 90
ppp authentication . . . 49, 89
ppp chap hostname . . . 113
ppp chap password . . . 113
ppp chap refuse . . . 113
PPP chap-secret . . . 90
ppp chap-secret . . . 89
ppp ipcp dns request . . . 67, 114
ppp pap refuse . . . 114
ppp pap sent username . . . 114
ppp timeout authentication . . . 89, 90
ppp timeout ncp . . . 112
ppp timeout retry . . . 113
pppoe-client persistent delay . . . 114
pppoe-client persistent max-attempts . . . 114
pppoe-client service-name . . . 114
pppoe-client wait-for-ipcp . . . 114
pre-classification . . . 107
pre-shared-key . . . 150

priority-queue . . . 115, 157
protect crypto-map . . . 153
queue-limit . . . 115
redistribute . . . 94, 119, 120
release dhcp . . . 61
release voip-dsp . . . 148
remote . . . 69
remove nfas-interface . . . 131
remove port . . . 133
rename announcement-file . . . 47
renew dhcp . . . 61
reset . . . 53
reset voip-dsp . . . 147
restore usb . . . 117, 143
retstatus . . . 53
rmon alarm . . . 119
rmon event . . . 119
rmon history . . . 119
router ospf . . . 93, 120
router rip . . . 118, 120
router vrrp . . . 155
rtp-echo-port . . . 54
rtp-stat clear . . . 122
rtp-stat event-threshold . . . 122
rtp-stat fault . . . 122
rtp-stat min-stat-win . . . 122
rtp-stat qos-trap . . . 122
rtp-stat qos-trap-rate-limit . . . 122
rtp-stat service . . . 122
rtp-stat thresholds . . . 122
rtp-test-port . . . 54
rtr . . . 91
rtr-schedule . . . 92
safe-removal usb . . . 143
sat . . . 123
scheduler . . . 54
self-identity . . . 150
server-name . . . 63
session . . . 87
set associated-signaling . . . 131
set attendant . . . 130
set bearer-capability . . . 123, 128
set bit-rate . . . 128
set boot bank . . . 73
set busy-disconnect . . . 133
set cbc . . . 133
set cbc-parameter . . . 133
set cbc-service-feature . . . 133
set channel-numbering . . . 128
set channel-preference . . . 133
set codeset-display . . . 133
set codeset-national . . . 133
set connect . . . 128
set contact-closure admin . . . 56
set contact-closure pulse-duration . . . 56
set cor . . . 132
set country-protocol . . . 123, 128
set date . . . 57
set date-format . . . 130
set delete-digits . . . 125, 127, 129
set deny . . . 125, 127
set dial . . . 134
set digit-handling . . . 134
set digits . . . 134
set digit-treatment . . . 134
set directory-number-a . . . 123
set directory-number-b . . . 123
set dscp . . . 151
set echo-cancellation analog . . . 70
set echo-cancellation config analog . . . 70
set echo-cancellation config voip . . . 70
set echo-cancellation voip . . . 70
set endpoint-init . . . 124, 126
set etr . . . 72
set expansion-module . . . 132
set fac . . . 130
set icc-monitoring . . . 87
set incoming-destination . . . 134
set incoming-dialtone . . . 134
set insert-digits (dial-pattern) . . . 128
set insert-digits (incoming-routing) . . . 129
set interface . . . 124, 126, 128
set interface-companding . . . 124, 126, 128
set ip-codec-set . . . 130
set japan-disconnect . . . 134
set layer1-stable . . . 124, 126
set length . . . 129
set lldp re-init-delay . . . 85
set lldp system-control . . . 85
set lldp tx-delay . . . 85
set lldp tx-hold-multiplier . . . 85
set lldp tx-interval . . . 85
set logging file . . . 86
set logging server . . . 86
set logging server access level . . . 86
set logging server condition . . . 86
set logging server facility . . . 86
set logging session . . . 86
set logout . . . 53
set long-timer . . . 128
set match-pattern . . . 129
set max-ip-registrations . . . 130
set max-length . . . 128
set mediaserver . . . 87
set mgc list . . . 87
set min-length . . . 128
set mss-notification rate . . . 91
set name . . . 124, 126, 129, 132, 134
set numbering-format . . . 134
set password . . . 132

set peer . . . 150, 152
set peer-group . . . 152
set pfs . . . 149
set pim-lockout . . . 130
set port . . . 132
set port auto-negotiation-flowcontrol-advertisement 71
set port classification . . . 111
set port duplex . . . 71
set port edge admin state . . . 71, 138
set port flowcontrol . . . 71
set port level . . . 71
set port lldp . . . 85
set port lldp tlv . . . 85
set port mirror . . . 111
set port name . . . 71
set port negotiation . . . 71
set port point-to-point admin status . . . 71, 138
set port redundancy . . . 111
set port redundancy on|off . . . 111
set port redundancy-intervals . . . 112
set port spantree . . . 138
set port spantree cost . . . 138
set port spantree force-protocol-migration . . . 138
set port spantree priority . . . 138
set port speed . . . 71
set port static-vlan . . . 146
set port trap . . . 137
set port vlan . . . 146
set port vlan-binding-mode . . . 146
set primary-dchannel . . . 131
set protocol-version . . . 129
set qos bearer . . . 116
set qos control . . . 116
set qos rsvp . . . 121
set qos rtcp . . . 121
set qos signal . . . 116
set radius authentication . . . 116
set radius authentication retry-number . . . 116
set radius authentication retry-time . . . 116
set radius authentication secret . . . 116
set radius authentication server . . . 116
set radius authentication udp-port . . . 116
set reset-times . . . 88
set security-association lifetime . . . 149
set send-name . . . 134
set send-number . . . 135
set side . . . 124, 126, 129
set signaling-mode . . . 129
set slot-config . . . 130
set sls . . . 123
set snmp community . . . 135
set snmp retries . . . 135
set snmp timeout . . . 135
set snmp trap . . . 137
set spantree default-path-cost . . . 138
set spantree enable/disable . . . 138
set spantree forward-delay . . . 138
set spantree hello-time . . . 138
set spantree max-age . . . 138
set spantree priority . . . 138
set spantree tx-hold-count . . . 138
set spantree version . . . 138
set spid-a . . . 124, 126
set spid-b . . . 124, 126
set supervision . . . 135
set swhook-flash . . . 132
set sync interface . . . 139
set sync source . . . 139
set sync switching . . . 139
set system location . . . 141
set system name . . . 141
set tac . . . 135
set tei-assignment . . . 124, 126
set terminal recovery password . . . 117
set tgnum . . . 128
set time . . . 57
set transform-set . . . 152
set trunk . . . 146
set trunk-destination . . . 132
set trunk-group-chan-select . . . 132
set trunk-hunt . . . 135
set type (dial-pattern) . . . 128
set type (station) . . . 132
set utilization cpu . . . 58
set vlan . . . 146
set web aux-files-url . . . 50
show
ip tcp header-compression . . . 146
ip tcp header-compression brief . . . 146
show (bri) . . . 124, 126
show (dial-pattern) . . . 128
show (ds1) . . . 129
show (incoming-routing) . . . 129
show (sig-group) . . . 132
show (station) . . . 132
show (trunk-group) . . . 135
show announcement-file . . . 47
show application-memory . . . 81, 142
show attendant . . . 130
show auth-file info . . . 49
show auth-file status . . . 49
show backup status . . . 50, 143
show banner login . . . 66
show banner post-login . . . 66
show boot bank . . . 73
show bri . . . 130
show cam . . . 52
show cam mac . . . 52
show cam vlan . . . 147
show capture . . . 97

show capture-buffer hex . . . 97
show cna testplug . . . 54
show composite-operation . . . 101, 102, 104, 106, 107
show contact-closure . . . 56
show controllers . . . 69, 155
show controllers remote . . . 70
show copy status . . . 55
show crypto ipsec sa . . . 153
show crypto ipsec transform-set . . . 153
show crypto isakmp peer . . . 153
show crypto isakmp peer-group . . . 153
show crypto isakmp policy . . . 153
show crypto isakmp sa . . . 153
show crypto map . . . 153
show csu loopbacks . . . 57
show csu status . . . 57
show date-format . . . 130
show dev log file . . . 86
show dial-pattern . . . 130
show download . . . 58
show download announcement-file status . . . 47
show download license-file status . . . 84
show download phone-image-file status . . . 81
show download phone-script-file status . . . 81
show download software status . . . 73
show download status . . . 55, 56
show ds1 . . . 130
show dscp-table . . . 105, 106, 107
show ds-mode . . . 70
show dynamic-cac . . . 68
show echo-cancellation . . . 70
show erase status . . . 55
show etr . . . 72
show extension . . . 130
show fac . . . 130
show faults . . . 58
show fragment . . . 74
show frame-relay fragment . . . 155
show frame-relay lmi . . . 155
show frame-relay map . . . 75, 155
show frame-relay pvc . . . 155
show frame-relay pvc brief . . . 75
show frame-relay traffic . . . 155
show icc-monitoring . . . 88
show icc-vlan . . . 77
show image version . . . 73
show incoming-routing . . . 131
show interfaces . . . 76, 77, 113, 155
show ip access-control-list . . . 99, 102
show ip active-lists . . . 110, 154
show ip active-pbr-lists . . . 110
show ip arp . . . 48
show ip capture-list . . . 97
show ip crypto-lists . . . 154
show ip dhcp-client . . . 61, 62
show ip dhcp-client statistics . . . 61
show ip dhcp-pool . . . 63
show ip dhcp-server bindings . . . 64
show ip dhcp-server statistics . . . 64
show ip distribution access-lists . . . 119
show ip domain . . . 67
show ip domain statistics . . . 67
show ip icmp . . . 78
show ip interface . . . 80
show ip interface brief . . . 80
show ip ospf . . . 94
show ip ospf database . . . 94
show ip ospf interface . . . 94
show ip ospf neighbor . . . 94
show ip ospf protocols . . . 94
show ip pbr-list . . . 110
show ip protocols . . . 119
show ip qos-list . . . 103
show ip reverse-arp . . . 48
show ip route . . . 121
show ip route best-match . . . 121
show ip route static . . . 121
show ip route summary . . . 121
show ip rtp header-compression . . . 83
show ip rtp header-compression brief . . . 83
show ip ssh . . . 139
show ip tcp header-compression . . . 83
show ip tcp header-compression brief . . . 83
show ip telnet . . . 141
show ip tftp-server files . . . 81
show ip tftp-server statistics . . . 81
show ip track-table . . . 121
show ip traffic . . . 57
show ip vrrp . . . 155
show ip-codec-set . . . 131
show ip-next-hop-list . . . 110
show ip-qos-list . . . 108
show ip-rule . . . 96, 101, 102, 106, 107, 110
show isdn bri link . . . 85
show isdn link summary . . . 85
show isdn pri link . . . 85
show keepalive-icmp . . . 78
show last-pim-update . . . 131
show license status . . . 84
show list . . . 102, 108, 110
show lldp . . . 85
show lldp config . . . 85
show logging file condition . . . 86
show logging file content . . . 87
show logging server condition . . . 87
show logging session condition . . . 87
show login authentication . . . 49, 144
show logout . . . 53
show map-class frame-relay . . . 76, 143, 155
show max-ip-registrations . . . 131

show mediaserver 88
show mg list_config 58
show mgc 59, 88
show mgc list 88
show module 59
show mss-notification rate 91
show next-hop 109
show pim-lockout 131
show platform fans 72, 97
show platform power 97
show platform supervisor 97
show pmi 98
show point-to-point status 138
show port 112
show port auto-negotiation-flowcontrol-advertisement 71
show port classification 111
show port edge state 138
show port edge status 71
show port flowcontrol 71
show port lldp config 86
show port lldp vlan-name config 86
show port mirror 111
show port redundancy 112
show port trap 137
show port vlan-binding-mode 147
show ppp authentication 89, 90
show protocols 67
show qos rtcp 116, 121
show qos-rtcp 121
show queue 157
show queueing 115, 157
show radius authentication 116
show recovery 59, 88
show restart-log 59
show restore status 117, 144
show rmon alarm 119
show rmon event 119
show rmon history 119
show rmon statistics 119
show rtp-stat config 122
show rtp-stat detailed 122
show rtp-stat sessions 122
show rtp-stat summary 122
show rtp-stat thresholds 122
show rtp-stat traceroute 122
show rtr configuration 92
show rtr operational-state 92
show running-config 55
show sig-group 131
show slot-config 131
show sls 123
show snmp 135, 137
show snmp engineID 135
show snmp group 136
show snmp retries 136
show snmp timeout 136
show snmp user 136
show snmp usertogroup 136
show snmp view 136
show spantree 138
show startup-config 56
show station 131
show sync timing 139
show system 59
show tcp syn-cookies 140
show temp 59
show timeout 59
show track 92
show traffic-shape 76, 143
show traffic-shape-queue 76, 143
show traffic-shape-statistics 76, 143
show trunk 147
show trunk-group 131
show upload 59
show upload announcement-file status 47
show upload auth-file status 49
show upload cdr-file status 52
show upload dhcp-binding-file status 60
show upload license-file status 84
show upload phone-script-file status 81
show upload syslog-file status 140
show usb 144
show username 144
show utilization 59
show vlan 147
show voip-dsp 147
show voip-parameters 147, 148
show voltages 59
shutdown 54, 80, 89, 90, 114
sig-group 131
sls 123
snmp trap link-status 137
snmp-server community 136
snmp-server dynamic-trap-manager 68
snmp-server enable notification 137
snmp-server engineID 136
snmp-server group 136
snmp-server host 137
snmp-server informs 137
snmp-server remote-user 136
snmp-server user 136
snmp-server view 136
source-address 92
source-ip 96, 101, 106, 110, 153
speed 89
start-ip-addr 64
station 132
subnet-mask 64
success-retries 92
suggest-key 150

tcp destination-port 96, 101, 106, 110
tcp established 101
tcp source-port 96, 101, 106, 110
tcp syn-cookies 140
tech 53
telnet 141
terminal length 66
terminal width 66
test led 59
test voip-dsp 148
test-rate-limit 54
threshold count 92
timeout absolute 89, 90
timers basic 119
timers spf 94
traceroute 121
track 92
traffic-shape rate 143
transmitter-delay 145
tree 53
trunk-group 132
tunnel checksum 76
tunnel destination 76
tunnel dscp 76
tunnel key 76
tunnel mode 77
tunnel path-mtu-discovery 77
tunnel source 77
tunnel ttl 77
type 91
udp destination-port 96, 101, 107, 110
udp source-port 97, 101, 107, 110
username 49, 144
value 63, 64
vendor-specific-option 64
voip-queue 115, 157
voip-queue-delay 115
wait-interval 92
zeroize 58

Configuration files
copy ftp startup-config 251
copy running-config ftp 252
copy running-config scp 253
copy running-config startup-config 254
copy running-config tftp 255
copy scp startup-config 256
copy startup-config ftp 257
copy startup-config scp 258
copy startup-config tftp 259
copy startup-config usb 260
copy tftp startup-config 261
copy usb startup-config 262
erase startup-config 262
nvram initialize 263
show copy status 264
show download status 265
show erase status 266
show running-config 266
show startup-config 267
show upload status 268

Connectivity
ping 269

Contact closure
set contact-closure admin 270
set contact-closure pulse-duration 271
show contact-closure 272

Contents Address Memory, *see* CAM table
Converged Network Analyzer, *see* CNA test plugs

Counters
clear counters 273
clear ip traffic 274
show ip traffic 275

CSU loopbacks
show csu loopbacks 277
show csu status 278

D

Date and time setting
set date 279
set time 280

Default gateway
ip default-gateway 281, 920

Default settings
zeroize 283

Device status
clear utilization cpu 284
set utilization cpu 284
show faults 286
show mg list_config 287
show mgc 288, 603
show mm 289
show module 290
show recovery 291, 605
show restart-log 292
show system 293
show temp 294
show timeout 295
show upload 285, 296
show utilization 297
show voltages 297
test led 298

DHCP and BOOTP relay
ip bootp-dhcp network 299
ip bootp-dhcp relay 300
ip bootp-dhcp server 300

DHCP binding file
copy dhcp-binding ftp 301
copy dhcp-binding scp 302
copy dhcp-binding tftp 303

copy dhcp-binding usb . . . 304
show upload dhcp-binding-file status . . . 305
DHCP client
clear ip dhcp-client statistics . . . 306
ip address dhcp . . . 306
ip dhcp client client-id . . . 307
ip dhcp client hostname . . . 308
ip dhcp client lease . . . 309
ip dhcp client request . . . 310
ip dhcp client route track . . . 311
release dhcp . . . 312
renew dhcp . . . 313
show ip dhcp-client . . . 314
show ip dhcp-client statistics . . . 318
DHCP server
clear ip dhcp-server binding . . . 320
clear ip dhcp-server statistics . . . 321
ip dhcp activate pool . . . 321
ip dhcp ping packets . . . 322
ip dhcp ping timeout . . . 323
ip dhcp pool . . . 324
bootfile . . . 325
client-identifier . . . 326
default-router . . . 327
dns-server . . . 327
domain-name . . . 328
end-ip-addr . . . 329
lease . . . 330
name 331, 334, 344, 704, 741, 758, 763, 787, 826
next-server . . . 332
option . . . 333
name331, 334, 344, 704, 741, 758, 763, 787, 826
value . . . 335, 345
server-name . . . 336
show ip dhcp-pool . . . 337
start-ip-addr . . . 341
subnet-mask . . . 342
vendor-specific-option . . . 343
class-identifier . . . 343
name331, 334, 344, 704, 741, 758, 763, 787, 826
value . . . 335, 345
ip dhcp-server . . . 347
show ip dhcp-server bindings . . . 347
show ip dhcp-server statistics . . . 348
Dial backup, *see* Dialer interface
Dialer interface
interface dialer . . . 350, 499
dialer modem-interface . . . 351
dialer order . . . 352
dialer persistent . . . 353
dialer persistent delay . . . 353
dialer persistent initial delay . . . 354
dialer persistent max-attempts . . . 355
dialer persistent re-enable . . . 356
dialer string . . . 356
dialer wait-for-ipcp . . . 357
ip address negotiated . . . 358, 856
Directed broadcast forwarding, *see* Broadcast relay
Display
banner login . . . 359
banner post-login . . . 360
clear screen . . . 360
hostname . . . 361, 1154
line . . . 362
show banner login . . . 363
show banner post-login . . . 363
terminal length . . . 364
terminal width . . . 365
DNS resolver
clear ip domain statistics . . . 366
ip domain list . . . 366
ip domain lookup . . . 367
ip domain name-server-list . . . 368
description (DNS resolver) . . . 369
name-server . . . 369
ip domain retry . . . 370
ip domain timeout . . . 371
nslookup . . . 372
ppp ipcp dns request . . . 373, 860
show ip domain . . . 373
show ip domain statistics . . . 375
show protocol . . . 377
duplex . . . 156
Dynamic CAC
dynamic-cac . . . 379
show dynamic-cac . . . 380
Dynamic trap manager
clear dynamic-trap-manager . . . 380
snmp-server dynamic-trap-manager . . . 381

E

E1/T1 interfaces
clear controller counters . . . 383
controller . . . 384
cablelength long . . . 385
cablelength short . . . 386
channel-group . . . 387
clock source . . . 388
fdl . . . 389
framing . . . 390
linecode (E1) . . . 391
linecode (T1) . . . 392
remote . . . 394
ds-mode . . . 395
interface serial . . . 396, 449, 502, 845, 1217
ip address . . . 397, 460, 507, 848
show controllers . . . 398, 1329
show controllers remote . . . 399
show ds-mode . . . 400

Echo control
set echo-cancellation analog . . . 401
set echo-cancellation config analog . . . 402
set echo-cancellation config voip . . . 405
set echo-cancellation voip . . . 407
show echo-cancellation . . . 408
Emergency transfer relay, *see* ETR
Ethernet port configuration
set port auto-negotiation-flowcontrol-advertisement 410
set port duplex . . . 411
set port enable | disable . . . 413
set port flowcontrol . . . 414
set port level . . . 416
set port name . . . 417
set port negotiation . . . 418
set port point-to-point admin status . . . 419, 1136
set port speed . . . 420
show port auto-negotiation-flowcontrol-advertisement 421
show port edge state . . . 412, 422, 1148
show port flowcontrol . . . 423
ETR
set etr . . . 425
show etr . . . 426

F

Fan
show platform fans . . . 427, 710
FIPS
show system . . . 293
zeroize . . . 283
Firmware management
copy ftp EW_archive . . . 428
copy ftp module . . . 429
copy ftp SW_imageA . . . 430
copy ftp SW_imageB . . . 431
copy tftp EW_archive . . . 432
copy tftp module . . . 433
copy tftp SW_imageA . . . 434
copy tftp SW_imageB . . . 435
copy usb EW_archive . . . 436
copy usb module . . . 437
copy usb SW_image . . . 438
dir . . . 439, 1195
set boot bank . . . 441
show boot bank . . . 442
show download software status . . . 442
show image version . . . 443
Firmware, *see* Firmware management
Fragmentation
clear fragment . . . 444
fragment chain . . . 445
fragment size . . . 446
fragment timeout . . . 447
show fragment . . . 447
Frame relay encapsulation
clear frame-relay counters . . . 448
interface serial . . . 396, 449, 502, 845, 1179, 1217
encapsulation . . . 451, 846
frame-relay class-dlci . . . 452
frame-relay interface-dlci . . . 453
frame-relay lmi-n391dte . . . 454
frame-relay lmi-n392dte . . . 455
frame-relay lmi-n393dte . . . 456
frame-relay lmi-type . . . 457
frame-relay priority-dlci-group . . . 458
frame-relay traffic-shaping . . . 459, 1181
ip address . . . 397, 460, 507, 848
map-class frame-relay . . . 461, 1181
bc out . . . 462, 1183
be out . . . 463, 1184
cir out . . . 464, 1185
fragment . . . 465, 1186
show frame-relay map . . . 466, 1333
show frame-relay pvc brief . . . 467
show interfaces . . . 467, 486, 851, 1336
show map-class frame-relay . . . 470
show traffic-shape . . . 471
show traffic-shape-queue . . . 473
show traffic-shape-statistics . . . 475

G

GRE tunneling
interface tunnel . . . 477, 503
keepalive (GRE tunnel) . . . 478
tunnel checksum . . . 479
tunnel destination . . . 479
tunnel dscp . . . 480
tunnel key . . . 481
tunnel mode . . . 482
tunnel path-mtu-discovery . . . 483
tunnel source . . . 484
tunnel ttl . . . 485
show interfaces . . . 467, 486, 851, 1336
Guide
latest version, downloading . . . 35

H

Header compression, *see* IPHC header compression, Van Jacobson header compression
HTTP server
ip http . . . 489

I

ICC configuration
icc-vlan . . . 490, 1232
show icc-vlan . . . 490

ICMP errors
ip icmp-errors . . . 491
show ip icmp . . . 492
ICMP keepalive
keepalive-icmp . . . 492
keepalive-icmp failure-retries . . . 493
keepalive-icmp interval . . . 494
keepalive-icmp source-address . . . 495
keepalive-icmp success-retries . . . 496
keepalive-icmp timeout . . . 497
show keepalive-icmp . . . 497
interface FastEthernet . . . 78
ip http . . . 77
IP interface configuration
description (interface) . . . 506
interface Console . . . 606
interface console . . . 498
interface dialer . . . 350, 499
interface FastEthernet . . . 500, 854, 1340
interface loopback . . . 501
interface serial . . . 396, 449, 502, 845, 1179, 1217
interface tunnel . . . 477, 503
interface USB-modem . . . 504, 616
interface vlan . . . 505, 1231
ip address . . . 397, 460, 507, 848
ip admin-state . . . 508
ip broadcast-address . . . 509
load-interval . . . 509
show ip interface . . . 510
show ip interface brief . . . 513
shutdown . . . 514, 614
IP phone upgrades
clear ip tftp-server statistics . . . 515, 1176
copy ftp phone-image . . . 516
copy ftp phone-script . . . 517
copy phone-script ftp . . . 518
copy phone-script scp . . . 519
copy phone-script tftp . . . 520
copy phone-script usb . . . 521
copy scp phone-script . . . 522
copy tftp phone-image . . . 523
copy tftp phone-script . . . 524
copy usb phone-image . . . 525
copy usb phone-script . . . 526
erase phone-image . . . 527
erase phone-script . . . 527
ip tftp-server file-system size . . . 528, 1177
show application-memory . . . 529, 1178
show download phone-image-file status . . . 530
show download phone-script-file status . . . 531
show ip tftp-server files . . . 532
show ip tftp-server statistics . . . 533
show upload phone-script-file status . . . 534
IP unnumbered
ip unnumbered . . . 535
IPHC header compression
clear ip rtp header-compression . . . 537
clear ip tcp header-compression . . . 538, 1223
ip rtp compression-connections . . . 539
ip rtp header-compression . . . 540
ip rtp max-period . . . 541
ip rtp max-time . . . 542
ip rtp non-tcp-mode . . . 543
ip rtp port-range . . . 544
ip tcp compression-connections . . . 545, 1224
show ip rtp header-compression . . . 546
show ip rtp header-compression brief . . . 548
show ip tcp header-compression . . . 549, 1226
show ip tcp header-compression brief . . . 551, 1227

K

Keepalive, *see* ICMP keepalive
keepalive-track . . . 156
keepalive-track, *see* VPN, WAN Ethernet port configuration

L

License file of CM
ip license-server . . . 552
License file of gateway
copy ftp license-file . . . 553
copy license-file ftp . . . 554
copy license-file scp . . . 555
copy license-file tftp . . . 556
copy license-file usb . . . 556
copy scp license-file . . . 557
copy tftp license-file . . . 558
copy usb license-file . . . 559
show download license-file status . . . 560
show license status . . . 561
show upload license-file status . . . 562
Link status
show isdn bri link . . . 563
show isdn link summary . . . 564
show isdn pri link . . . 565
LLDP
set lldp re-init-delay . . . 566
set lldp system-control . . . 567
set lldp tx-delay . . . 567
set lldp tx-hold-multiplier . . . 568
set lldp tx-interval . . . 569
set port lldp . . . 570
set port lldp tlv . . . 571
show lldp . . . 573
show lldp config . . . 575
show port lldp config . . . 576
show port lldp vlan-name config . . . 578
Log file, *see* Logging
Logging

clear logging file . . . 579
clear logging server . . . 580
set logging file . . . 581
set logging server . . . 583
set logging server access-level . . . 584
set logging server condition . . . 585
set logging server enable|disable . . . 586
set logging server facility . . . 587
set logging session . . . 588
show dev log file . . . 590
show logging file condition . . . 590
show logging file content . . . 591
show logging server condition . . . 592
show logging session condition . . . 593
Loopbacks, *see* CSU loopbacks

M

Master key configuration
key config-key password-encryption . . . 594
Media Gateway Controller, *see* MGC configuration
MGC configuration
clear mgc list . . . 596
session . . . 597
set icc-monitoring . . . 598
set mediaserver . . . 598
set mgc list . . . 599
set reset-times . . . 600
show icc-monitoring . . . 601
show mediaserver . . . 602
show mgc . . . 288, 603
show mgc list . . . 604
show recovery . . . 291, 605
Modem configuration
interface Console . . . 606
async mode interactive . . . 607
async mode terminal . . . 607
async modem-init-string . . . 608, 617
async reset-modem . . . 609
ip peer address . . . 609, 619
ppp authentication . . . 213, 610, 620
ppp chap-secret . . . 611, 621
ppp timeout authentication . . . 612, 622
show ppp authentication . . . 613, 623
shutdown (interface) . . . 514, 614
speed (PPP) . . . 615
timeout absolute . . . 615, 624
interface console . . . 498
interface USB-modem . . . 504, 616
async modem-init-string . . . 608, 617
async reset-modem . . . 618
ip peer address . . . 609, 619
ppp authentication . . . 213, 610, 620
ppp chap-secret . . . 611, 621
ppp timeout authentication . . . 612, 622
show ppp authentication . . . 613, 623
shutdown (USB modem) . . . 624
speed (PPP) . . . 615
timeout absolute . . . 615, 624
Modem dial backup, *see* Dialer interface
MSS notifications
DoS-classification . . . 625
icmp in-echo-limit . . . 627
set mss-notification rate . . . 627
show mss-notification rate . . . 628

N

NetBIOS rebroadcast, *see* Broadcast relay
NVRAM, *see* Configuration files

O

Object tracking
rtr . . . 629
type . . . 630
dscp (object tracking) . . . 631
fail-retries . . . 632
frequency . . . 633
interface-keepalive bypass-logic . . . 634
next-hop (object tracking) . . . 634
source-address . . . 636
success-retries . . . 637
wait-interval . . . 638
rtr-schedule . . . 639
show rtr configuration . . . 640
show rtr operational-state . . . 642
show track . . . 643
track . . . 645
description (object tracking) . . . 647
object . . . 648
threshold count . . . 649
Open Shortest Path First, *see* OSPF
OSPF
bandwidth . . . 650, 1218
ip ospf authentication . . . 651
ip ospf authentication-key . . . 652
ip ospf cost . . . 653
ip ospf dead-interval . . . 654
ip ospf hello-interval . . . 655
ip ospf message-digest-key . . . 656
ip ospf network point-to-multipoint . . . 657
ip ospf priority . . . 657
ip ospf router-id . . . 658
router ospf . . . 659
area . . . 660
default-metric (OSPF) . . . 661, 915
network (OSPF) . . . 661
passive-interface . . . 662
redistribute . . . 663, 917

timers spf 664
show ip ospf 665
show ip ospf database 666
show ip ospf interface 667
show ip ospf neighbor 668
show ip protocols 669, 905

P

Packet sniffing
capture buffer-mode 670
capture buffer-size 671
capture filter-group 672
capture interface 673
capture max-frame-size 675
capture start 675
capture stop 676
capture-service 677
clear capture-buffer 678
copy capture-file ftp 679
copy capture-file scp 680
copy capture-file tftp 681
copy capture-file usb 682
ip capture-list 683
cookie 683, 717, 760, 804
ip-rule 684, 719, 765, 806
composite-operation . 685, 720, 755, 762, 766
destination-ip 686, 721, 767, 807, 1293
dscp 688, 809
fragment 689, 724, 770, 810
icmp 690, 725, 771, 805
ip-protocol 692, 727, 772, 811
show ip-rule 693, 729, 744, 776, 792, 815, 828
source-ip 695, 731, 778, 816, 1296
tcp destination-port 696, 732, 779, 818
tcp source-port 698, 735, 781, 820
udp destination-port . . . 700, 737, 783, 822
udp source-port 702, 739, 785, 824
name 331, 334, 344, 704, 741, 758, 763, 787, 826
owner 705, 742, 788, 827
show capture 706
show capture-buffer hex 707
show ip capture-list 708
Platform information
show platform fans 427, 710
show platform power 711
PMI
pmi 714
show pmi 715
Policy - access control lists
ip access-control-list 716
cookie 683, 717, 760, 804
ip-fragments-in 718
ip-option-in 719
ip-rule 684, 719, 765, 806
composite-operation . 685, 720, 755, 762, 766
destination-ip 686, 721, 767, 807, 1293
dscp 723, 757, 769
fragment 689, 724, 770, 810
icmp 690, 725, 771, 805
ip-protocol 692, 727, 772, 811
show composite-operation 728, 743, 759, 774, 790
show ip-rule 693, 729, 744, 776, 792, 815, 828
source-ip 695, 731, 778, 816, 1296
tcp destination-port 696, 732, 779, 818
tcp established 734
tcp source-port 698, 735, 781, 820
udp destination-port 700, 737, 783, 822
udp source-port 702, 739, 785, 824
name 331, 334, 344, 704, 741, 758, 763, 787, 826
owner 705, 742, 788, 827
show composite-operation 728, 743, 759, 774, 790
show ip-rule . . 693, 729, 744, 776, 792, 815, 828
show list 745, 794, 830
ip access-group 746
ip policy-list-copy 747, 752
ip simulate 748, 795
show ip access-control-list 750
Policy - QoS lists
ip policy-list-copy 747, 752
ip qos-group 753
ip qos-list 754
composite-operation . . . 685, 720, 755, 762, 766
cos 756
dscp 723, 757, 769
name 331, 334, 344, 704, 741, 758, 763, 787, 826
show composite-operation 728, 743, 759, 774, 790
cookie 683, 717, 760, 804
dscp-table 761
composite-operation . 685, 720, 755, 762, 766
name 331, 334, 344, 704, 741, 758, 763, 787, 826
show dscp-table 764, 775, 791
ip-rule 684, 719, 765, 806
composite-operation . 685, 720, 755, 762, 766
destination-ip 686, 721, 767, 807, 1293
dscp 723, 757, 769
fragment 689, 724, 770, 810
icmp 690, 725, 771, 805
ip-protocol 692, 727, 772, 811
show composite-operation 728, 743, 759, 774, 790
show dscp-table 764, 775, 791
show ip-rule 693, 729, 744, 776, 792, 815, 828
source-ip 695, 731, 778, 816, 1296
tcp destination-port 696, 732, 779, 818
tcp source-port 698, 735, 781, 820
udp destination-port 700, 737, 783, 822
udp source-port 702, 739, 785, 824
name 331, 334, 344, 704, 741, 758, 763, 787, 826
owner 705, 742, 788, 827
pre-classification 789

show composite-operation 728, 743, 759, 774, 790
show dscp-table 764, 775, 791
show ip-rule . . 693, 729, 744, 776, 792, 815, 828
show list 745, 794, 830
ip simulate 748, 795
show ip qos-list 796
Policy-based routing
ip next-hop-list 798
next-hop-interface 799
next-hop-ip 801
show next-hop. 802
ip pbr-group 802
ip pbr-list 803
cookie 683, 717, 760, 804
icmp 690, 725, 771, 805
ip-rule. 684, 719, 765, 806
destination-ip. . . . 686, 721, 767, 807, 1293
dscp 688, 809
fragment 689, 724, 770, 810
ip-protocol 692, 727, 772, 811
next-hop (policy-based routing) 813
show ip next-hop-list 814
show ip-rule 693, 729, 744, 776, 792, 815, 828
source-ip. 695, 731, 778, 816, 1296
tcp destination-port 696, 732, 779, 818
tcp source-port 698, 735, 781, 820
udp destination-port . . . 700, 737, 783, 822
udp source-port 702, 739, 785, 824
name 331, 334, 344, 704, 741, 758, 763, 787, 826
owner. 705, 742, 788, 827
show ip-rule . . 693, 729, 744, 776, 792, 815, 828
show list 745, 794, 830
show ip active-lists 831, 1314
show ip active-pbr-lists 833
show ip pbr-list 833
Port classification
set port classification 834
show port classification 835
Port mirroring
clear port mirror 836
set port mirror 837
show port mirror 838
Port redundancy
set port redundancy. 841
set port redundancy on|off. 839
set port redundancy-intervals 842
show port redundancy 843
Port status
show port 843
PPP encapsulation
interface serial . . . 396, 449, 502, 845, 1179, 1217
encapsulation 451, 846
ip address. 397, 460, 507, 848
keepalive (PPP) 849
ppp timeout ncp 850
ppp timeout retry 851
show interfaces 467, 486, 851, 1336
PPP over Ethernet, *see* PPPoE
PPPoE
interface FastEthernet 500, 854, 1340
encapsulation pppoe 855
ip address negotiated. 358, 856
mtu 857
ppp chap hostname 858
ppp chap password 859
ppp chap refuse 860
ppp ipcp dns request 373, 860
ppp pap refuse. 861
ppp pap sent-username 862
pppoe-client persistent delay 863
pppoe-client persistent max-attempts 864
pppoe-client service-name 865
pppoe-client wait-for-ipcp 866
PRI links, *see* Link status
Primary management interface, *see* PMI
Priority queueing
priority-queue 867, 1347
queue-limit 868
show queueing 869, 1349
voip-queue 871, 1351
voip-queue-delay 872
Proxy ARP
ip proxy-arp 873

Q

QoS
set qos bearer. 874
set qos control 875
set qos signal 876
show qos-rtcp 877
show voip-parameters 878, 1246, 1249
QoS, *see* RTP, RTCP, RSVP, WFVQ

R

RADIUS authentication
clear radius authentication server. 879
set radius authentication 880
set radius authentication retry-number 881
set radius authentication retry-time 882
set radius authentication secret. 882
set radius authentication server 883
set radius authentication udp-port 884
show radius authentication 885
Recovery password
set terminal recovery password. 886
Redundancy, *see* Port redundancy
Restoring gateway configuration
restore usb 887, 1197

show restore status 888, 1200
RIP
ip distribution access-default-action 889
ip distribution access-list 890
ip distribution access-list-cookie 891
ip distribution access-list-copy 892
ip distribution access-list-name 892
ip distribution access-list-owner 893
ip rip authentication key 894
ip rip authentication mode 895
ip rip default-route-mode 896
ip rip poison-reverse 897
ip rip rip-version 897
ip rip send-receive-mode 898
ip rip split-horizon 899
router rip 900
default-metric (RIP) 901, 916
distribution-list 901
network (RIP) 902
redistribute 903, 918
timers basic 904
show ip distribution access-lists 905
show ip protocols 669, 905
RMON monitoring
rmon alarm 907
rmon event 909
rmon history 910
show rmon alarm 911
show rmon event 912
show rmon history 913
show rmon statistics 914
Route redistribution
default-metric (interface route metric value) 915
default-metric (OSPF) 661, 915
default-metric (RIP) 901, 916
redistribute (OSPF) 663, 917
redistribute (RIP) 903, 918
Routing information protocol, *see* RIP
Routing table configuration
clear ip route 919
ip default-gateway 281, 920
ip netmask-format 921
ip redirects 922
ip route 922
ip routing 924
show ip route 925
show ip route best-match 926
show ip route static 927
show ip route summary 928
show ip route track-table 929
traceroute 929
RSVP
set qos rsvp 932
show qos-rtcp 877, 933, 935
RTCP
set qos rtcp 934
show qos-rtcp 877, 933, 935
RTP header compression, *see* IPHC header compression
RTP MIB, *see* RTP statistics
RTP statistics
rtp-stat clear 937
rtp-stat event-threshold 938
rtp-stat fault 940
rtp-stat min-stat-win 941
rtp-stat qos-trap 942
rtp-stat qos-trap-rate-limit 943
rtp-stat threshold 944
rtp-stat-service 944
show rtp-stat config 947
show rtp-stat detailed 948
show rtp-stat sessions 949
show rtp-stat summary 952
show rtp-stat thresholds 953
show rtp-stat traceroute 954
RTR, *see* Object tracking

S

SAA, *see* Object tracking
SAT
sat 956
Session logs, *see* Logging
set logging server enable/disable 86
SLS survivability
set sls 958
show sls 959
sls 957
bri 960
set bearer-capability 961, 1000
set country-protocol 962, 1004
set directory-number-a 964
set directory-number-b 965
set endpoint-init 966
set interface 967, 1005
set interface-companding 968, 1007
set layer1-stable 969
set name 970, 1009, 1059, 1091
set side 971, 1012
set spid-a 973
set spid-b 974
set tei-assignment 975
show 976
clear attendant 978
clear bri 978
clear dial-pattern 979
clear ds1 980
clear extension 980
clear fac 981
clear incoming-routing 982
clear sig-group 983

clear slot-config . . . 984
clear station . . . 985
clear survivable-config . . . 986
clear trunk-group . . . 986
dial-pattern . . . 987
  set delete-digits . . . 989
  set deny . . . 990
  set insert-digits . . . 990
  set max-length . . . 991
  set min-length . . . 992
  set tgnum . . . 993
  set type . . . 994
  show . . . 997
ds1 . . . 998
  set bearer-capability . . . 961, 1000
  set bit-rate . . . 1001
  set channel-numbering . . . 1002
  set connect . . . 1003
  set country-protocol . . . 962, 1004
  set interface . . . 967, 1005
  set interface-companding . . . 968, 1007
  set long-timer . . . 1008
  set name . . . 970, 1009, 1059, 1091
  set protocol-version . . . 1010
  set side . . . 971, 1012
  set signaling-mode . . . 1013
  show . . . 1014
incoming-routing . . . 1017
  set delete-digits . . . 1018
  set insert-digits . . . 1019
  set length . . . 1020
  set match-pattern . . . 1021
  show . . . 1022
set attendant . . . 1023
set date-format . . . 1024
set fac . . . 1025
set ip-codec-set . . . 1026
set max-ip-registrations . . . 1027
set pim-lockout . . . 1027
set slot-config . . . 1028
show attendant . . . 1030
show bri . . . 1030
show date-format . . . 1032
show dial-pattern . . . 1032
show ds1 . . . 1034
show extension . . . 1035
show fac . . . 1037
show incoming-routing . . . 1038
show ip-codec-set . . . 1039
show last-pim-update . . . 1040
show max-ip-registrations . . . 1040
show pim-lockout . . . 1041
show sig-group . . . 1041
show slot-config . . . 1042
show station . . . 1043
show trunk-group . . . 1045
sig-group . . . 1047
  add nfas-interface . . . 1049
  remove nfas-interface . . . 1050
  set associated-signaling . . . 1051
  set primary-dchannel . . . 1052
  set trunk-group-chan-select . . . 1053
  show . . . 1054
station . . . 1055
  set cor . . . 1056
  set expansion-module . . . 1059
  set name . . . 970, 1009, 1059, 1091
  set password . . . 1061
  set port . . . 1062
  set swhook-flash . . . 1063
  set trunk-destination . . . 1064
  set type . . . 1065
  show . . . 1067
trunk-group . . . 1068
  add port . . . 1072
  clear tac . . . 1075
  remove port . . . 1075
  set cbc . . . 1076, 1077
  set cbc-parameter . . . 1079
  set cbc-service-feature . . . 1080
  set channel-preference . . . 1081
  set codeset-display . . . 1082
  set codeset-national . . . 1083
  set dial . . . 1084
  set digit-handling . . . 1084
  set digits . . . 1086
  set digit-treatment . . . 1087
  set incoming-destination . . . 1088
  set incoming-dialtone . . . 1089
  set japan-disconnect . . . 1090
  set name . . . 970, 1009, 1059, 1091
  set numbering-format . . . 1092
  set send-name . . . 1093
  set send-number . . . 1095
  set supervision . . . 1096
  set tac . . . 1097
  set trunk-hunt . . . 1098
  show . . . 1099
SNMP access configuration
  ip snmp . . . 1102
  set snmp community . . . 1103
  set snmp retries . . . 1104
  set snmp timeout . . . 1105
  show snmp . . . 1106, 1127
  show snmp engineID . . . 1107
  show snmp group . . . 1108
  show snmp retries . . . 1109
  show snmp timeout . . . 1110
  show snmp user . . . 1111
  show snmp usertogroup . . . 1112

show snmp view 1113
snmp-server community 1114
snmp-server engineID 1115
snmp-server group 1117
snmp-server remote-user 1119
snmp-server user 1120
snmp-server view 1122
SNMP trap configuration
set port trap 1123
set snmp trap enable|disable auth 1125
set snmp trap enable|disable frame-relay 1125
show port trap 1126
show snmp 1106, 1127
snmp trap link-status 1128
snmp-server enable notifications 1129
snmp-server host 1130
snmp-server informs 1133
Software management, *see* Firmware management
Spanning tree
set port edge admin state 412, 1135
set port point-to-point admin status 419, 1136
set port spantree 1137
set port spantree cost 1138
set port spantree force-protocol-migration . . . 1139
set port spantree priority 1140
set spantree default-path-cost 1141
set spantree enable/disable 1142
set spantree forward-delay 1143
set spantree hello-time 1143
set spantree max-age 1144
set spantree priority 1145
set spantree tx-hold-count 1146
set spantree version 1147
show port edge state 422, 1148
show port point-to-point status 1149
show spantree 1149
speed 156
SSH protocol
clear ssh-client known-hosts 1152
crypto key generate 1152
disconnect ssh 1153
hostname 361, 1154
ip ssh 1155
show ip ssh 1156
Standard Local Survivability, *see* SLS survivability
Status of the device, *see* Device status
Switch Ethernet ports, *see* Ethernet port configuration
Synchronization
clear sync interface 1157
set sync interface 1158
set sync source 1159
set sync switching 1160
show sync timing 1161
SYN-cookies
clear tcp syn-cookies counters 1162
show tcp syn-cookies 1163
tcp syn-cookies 1164
Syslog files
copy syslog-file ftp 1165
copy syslog-file scp 1166
copy syslog-file tftp 1167
copy syslog-file usb 1167
show upload syslog-file status 1168
Syslog, *see* Logging
System Access Terminal, *see* SAT
System identification
set system contact 1170
set system location 1171
set system name 1171

T

TCP header compression, *see* IPHC header compression, Van Jacobson header compression
Telnet access
ip telnet 1172
ip telnet-client 1173
ip telnet-services 1174
telnet 1175
Terminal display, *see* Display
TFTP server
clear ip tftp-server statistics 515, 1176
IP phone upgrades, *see* IP phone upgrades
ip tftp-server 1177
ip tftp-server file-system size 528, 1177
show application-memory 529, 1178
Traffic shaping
interface serial 449, 1179
map-class frame-relay 1181
bc out 1183
be out 1184
cir out 1185
fragment 1186
show map-class frame-relay 1187
show traffic-shape 471, 1188
show traffic-shape-queue 473, 1190
show traffic-shape-statistics 475, 1191
traffic-shape rate 1193
traffic-shape rate 156

U

Upgrading firmware, *see* Firmware management
USB mass storage device
backup config usb 221, 1194
dir 439, 1195
erase usb 1197
restore usb 887, 1197
safe-removal usb 1198
show backup status 222, 1199

show restore status 888, 1200
show usb 1201
User accounts
login authentication inactivity-period 1203
login authentication lockout 209, 1204
login authentication min-password-digit-chars . 1205
login authentication min-password-length. . . . 1206
login authentication min-password-lower-chars . 1207
login authentication min-password-special-chars 1208
login authentication min-password-upper-chars . 1209
login authentication password-expire 1210
password 1212
show login authentication 216, 1213
show username 1214
username 218, 1215
USP configuration
interface serial . . . 396, 449, 502, 845, 1179, 1217
bandwidth 650, 1218
idle-character 1219
ignore dcd 1220
invert txclock 1221
nrzi-encoding 1221
transmitter-delay 1222

V

Van Jacobson header compression
clear ip tcp header-compression 538, 1223
ip tcp compression-connections 545, 1224
ip tcp header-compression 1225
show ip tcp header-compression. 549, 1226
show ip tcp header-compression brief . . . 551, 1227
Virtual Private Networks, *see* VPN
VLAN configuration
clear port static-vlan 1229
clear vlan 1230
interface vlan 505, 1231
icc-vlan 490, 1232
set port static-vlan 1233
set port vlan 1234
set port vlan-binding-mode 1235
set trunk 1236
set vlan 1237
show cam vlan 1238
show port vlan-binding-mode 1239
show trunk 1240
show vlan 1241
VoIP
campon-busyout voip-dsp 1243
reset voip-dsp 1244
show voip-dsp 1244
show voip-parameters 1246, 1249
VoIP QoS, *see* QoS
VoIP testing
busyout voip-dsp 1247
release voip-dsp. 1248
show voip-parameters 878, 1246, 1249
test voip-dsp 1250
VPN
clear crypto isakmp 1251
clear crypto sa 1252
clear crypto sa counters 1254
crypto ipsec df-bit 1254
crypto ipsec minimal-pmtu 1255
crypto ipsec nat-transparency udp-encapsulation 1256
crypto ipsec transform-set 1257
mode 1259
set pfs 1260
set security-association lifetime 1261
crypto isakmp invalid-spi-recovery 1262
crypto isakmp nat keepalive 1262
crypto isakmp peer 1263
continuous-channel 1264, 1284
description (ISAKMP peer) 1265
initiate mode 1266
isakmp-policy 1267
keepalive (VPN) 1268
keepalive-track 1269, 1342
pre-shared-key 1270
self-identity 1271
suggest-key 1272
crypto isakmp peer-group 1273
description (ISAKMP peer group) 1274
set peer (peer group) 1275
crypto isakmp policy 1276
authentication 1277
description (ISAKMP policy) 1278
encryption 1279
group 1280
hash. 1280
lifetime 1281
crypto isakmp suggest-key 1282
crypto map 1283
continuous-channel 1264, 1284
description (crypto map) 1285
set dscp 1286
set peer (crypto map) 1287
set peer-group 1288
set transform-set 1289
ip crypto-group 1290
ip crypto-list 1291
ip-rule 1292
description (ip rule) 1292
destination-ip 686, 721, 767, 807, 1293
protect crypto map 1295
source-ip 695, 731, 778, 816, 1296
local-address 1297
show crypto ipsec sa 1298
show crypto ipsec transform-set 1306
show crypto isakmp peer. 1308

show crypto isakmp peer-group 1309
show crypto isakmp policy. 1310
show crypto isakmp sa 1311
show crypto map 1313
show ip active-lists 831, 1314
show ip crypto-list. 1316
VPN license, *see* License files
VRRP
ip vrrp 1319
ip vrrp address 1320
ip vrrp auth-key. 1321
ip vrrp override addr owner 1322
ip vrrp preempt 1323
ip vrrp primary 1324
ip vrrp priority. 1325
ip vrrp timer 1325
router vrrp 1326
show ip vrrp 1327

W

WAN configuration, verifying
show controllers 398, 1329
show frame-relay fragment 1330
show frame-relay lmi 1331
show frame-relay map 466, 1333
show frame-relay pvc 1334
show frame-relay traffic 1335
show interfaces. 467, 486, 851, 1336
show map-class frame-relay. 470, 1187, 1339
WAN Ethernet port configuration
interface FastEthernet 500, 854, 1340
autoneg. 1341
duplex 1341
keepalive-track 1269, 1342
speed (interface) 1343
traffic-shape rate 1193, 1344
WAN interfaces, *see* E1/T1 interfaces, USP interfaces, PPP encapsulation, PPPoE, Frame relay encapsulation, Verifying WAN configuration
Weighted Fair VoIP Queueing, *see* WFVQ
WFVQ
fair-queue-limit 1345
fair-voip-queue 1346
priority-queue. 867, 1347
show queue 1348
show queueing 869, 1349
voip-queue 871, 1351