

Avaya G250 and Avaya G350

CLI Reference

03-300437
Issue 2.1
August 2006

© 2006 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 21

Overview 21
Audience 21
Using this book 21
Conventions 22
Downloading this book and updates from the Web 22
Downloading this book 23
Related resources 23
Technical assistance 24
Within the US 24
International 24
Trademarks 24
Sending us comments 25

Chapter 1: User Levels and Contexts 27

User Levels 27
Contexts 28
Interface contexts 28
Entering an Interface 29
Command line prompts 29
Available contexts 30

Chapter 2: CLI Commands 33

About the CLI 33
Logging in to the CLI 33
Using the CLI 34
Using Help 34
Using auto-complete 34
Abbreviating commands 34
Alphabetical listing of CLI commands 35
add port 35
area 36
arp 37
arp timeout 38
async mode interactive 39
async mode terminal 39
async modem-init-string 40
async modem-type 41
async reset-modem (Console port) 42
async reset-modem (USB port) 42
authentication 43
autoneg 44
backup delay 44
backup interface 45
bandwidth 46
banner login 47

banner post-login . . . 47
bc out . . . 48
be out . . . 49
bootfile . . . 50
busyout voip-dsp . . . 51
cablelength long . . . 51
cablelength short . . . 52
capture buffer-mode . . . 53
capture buffer-size . . . 54
capture filter-group . . . 55
capture interface . . . 55
capture max-frame-size . . . 56
capture start . . . 57
capture stop . . . 58
capture-service . . . 59
channel-group . . . 60
cir out . . . 61
class-identifier . . . 62
clear arp-cache . . . 62
clear cam . . . 64
clear capture-buffer . . . 64
clear controller counters . . . 65
clear counters (interface) . . . 65
clear counters (CNA test plugs) . . . 66
clear crypto isakmp . . . 67
clear crypto sa . . . 68
clear crypto sa counters . . . 69
clear dial-pattern . . . 69
clear dot1x config . . . 70
clear extension . . . 71
clear fac . . . 72
clear fragment . . . 73
clear frame-relay counters . . . 73
clear ip dhcp-client statistics . . . 74
clear ip dhcp-server binding . . . 75
clear ip dhcp server statistics . . . 76
clear ip domain statistics . . . 77
clear ip route . . . 77
clear ip rtp header-compression . . . 78
clear ip tcp header-compression . . . 79
clear ip tftp-server statistics . . . 80
clear ip traffic . . . 81
clear logging file . . . 81
clear logging server . . . 82
clear mgc list . . . 83
clear port mirror . . . 84
clear port static-vlan . . . 85

clear radius authentication server . . . 86
clear screen . . . 87
clear snmp trap . . . 87
clear ssh-client known-hosts . . . 88
clear survivable-config . . . 89
clear sync interface . . . 89
clear tac . . . 90
clear tcp syn-cookies counters . . . 91
clear trunk-group . . . 91
clear utilization cpu . . . 92
clear vlan . . . 93
client-identifier . . . 94
clock source . . . 95
cna-testplug . . . 96
cna-testplug-service . . . 97
composite-operation . . . 98
continuous-channel . . . 99
control-port . . . 100
controller . . . 100
cookie . . . 101
copy announcement-file scp . . . 102
copy capture-file ftp . . . 103
copy capture-file scp . . . 104
copy capture-file tftp . . . 105
copy dhcp-binding ftp . . . 106
copy dhcp-binding scp . . . 107
copy dhcp-binding tftp . . . 108
copy ftp EW_archive . . . 109
copy ftp license-file . . . 110
copy ftp module . . . 111
copy ftp phone-image . . . 112
copy ftp phone-script . . . 113
copy ftp startup-config . . . 114
copy ftp SW_imageA . . . 115
copy ftp SW_imageB . . . 116
copy phone-script ftp . . . 117
copy phone-script scp . . . 118
copy phone-script tftp . . . 119
copy running-config ftp . . . 120
copy running-config scp . . . 121
copy running-config startup-config . . . 122
copy running-config tftp . . . 122
copy scp announcement-file . . . 123
copy scp license-file . . . 125
copy scp phone-script . . . 126
copy scp startup-config . . . 127
copy startup-config ftp . . . 128

copy startup-config scp . . . 129
copy startup-config tftp . . . 130
copy tftp EW_archive . . . 131
copy tftp license-file . . . 132
copy tftp module . . . 133
copy tftp phone-image . . . 134
copy tftp phone-script . . . 135
copy tftp startup-config . . . 136
copy tftp SW_imageA . . . 137
copy tftp SW_imageB . . . 138
cos . . . 139
crypto ipsec df-bit . . . 140
crypto ipsec minimal-pmtu . . . 141
crypto ipsec nat-transparency udp-encapsulation . . . 141
crypto ipsec transform-set . . . 142
crypto isakmp invalid-spi-recovery . . . 144
crypto isakmp nat keepalive . . . 144
crypto isakmp peer . . . 145
crypto isakmp peer-group . . . 146
crypto isakmp policy . . . 148
crypto isakmp suggest-key . . . 149
crypto key generate . . . 150
crypto map . . . 151
default-metric (OSPF) . . . 152
default-metric (RIP) . . . 152
default-metric (interface route metric value) . . . 153
default-router . . . 154
description (interface) . . . 155
description (DNS resolver) . . . 156
description (crypto map) . . . 156
description (ISAKMP policy) . . . 157
description (ISAKMP peer) . . . 158
description (ISAKMP peer group) . . . 159
description (ip rule) . . . 160
description (object tracking) . . . 161
destination-ip . . . 162
dialer modem-interface . . . 163
dialer order . . . 164
dialer persistent . . . 165
dialer persistent delay . . . 165
dialer persistent initial delay . . . 166
dialer persistent max-attempts . . . 167
dialer persistent re-enable . . . 168
dialer string . . . 168
dialer wait-for-ipcp . . . 169
dir . . . 170
disable link encryption . . . 171

disable media encryption . . . 172
disconnect ssh . . . 172
distribution-list . . . 173
dns-server . . . 174
domain-name . . . 175
dscp (object tracking) . . . 175
dscp (policy) . . . 176
dscp (policy-based routing, packet sniffing, VPN) . . . 177
dscp-table . . . 179
ds-mode . . . 180
DoS-classification . . . 181
duplex . . . 182
dynamic-cac . . . 183
encapsulation . . . 184
encapsulation pppoe . . . 185
encryption . . . 186
end-ip-addr . . . 187
enhanced security . . . 188
erase announcement-file . . . 189
erase phone-image . . . 189
erase phone-script . . . 190
erase startup-config . . . 190
exit . . . 191
fail-retries . . . 192
fair-queue-limit . . . 192
fair-voip-queue . . . 193
fan speed level low . . . 194
fdl . . . 195
fragment . . . 196
fragment chain . . . 197
fragment size . . . 198
fragment timeout . . . 199
frame-relay class-dlci . . . 200
frame-relay interface-dlci . . . 201
frame-relay lmi-n391dte . . . 202
frame-relay lmi-n392dte . . . 203
frame-relay lmi-n393dte . . . 204
frame-relay lmi-type . . . 205
frame-relay priority-dlci-group . . . 206
frame-relay traffic-shaping . . . 207
framing . . . 207
frequency . . . 208
group . . . 209
hash . . . 210
hostname . . . 211
icc-vlan . . . 212
icmp . . . 213

icmp in-echo-limit . . . 214
idle-character . . . 215
ignore dcd . . . 216
initiate mode . . . 216
interface Console . . . 217
interface dialer . . . 218
interface FastEthernet . . . 219
interface Loopback . . . 220
interface serial . . . 221
interface tunnel . . . 222
interface USB-Modem . . . 223
interface vlan . . . 224
interface-keepalive bypass-logic . . . 225
invert txclock . . . 226
ip access-control-list . . . 226
ip access-group . . . 227
ip address . . . 228
ip address dhcp . . . 229
ip address negotiated . . . 230
ip admin-state . . . 231
ip bootp-dhcp network . . . 232
ip bootp-dhcp relay . . . 233
ip bootp-dhcp server . . . 233
ip broadcast-address . . . 234
ip capture-list . . . 235
ip crypto-group . . . 236
ip crypto-list . . . 237
ip default-gateway . . . 238
ip dhcp activate pool . . . 239
ip dhcp client client-id . . . 240
ip dhcp client hostname . . . 241
ip dhcp client lease . . . 242
ip dhcp client request . . . 243
ip dhcp client route track . . . 244
ip dhcp pool . . . 245
ip dhcp ping packets . . . 246
ip dhcp ping timeout . . . 246
ip dhcp-server . . . 247
ip directed-broadcast . . . 248
ip distribution access-default-action . . . 248
ip distribution access-list . . . 249
ip distribution access-list-cookie . . . 251
ip distribution access-list-copy . . . 251
ip distribution access-list-name . . . 252
ip distribution access-list-owner . . . 253
ip domain list . . . 254
ip domain lookup . . . 255

ip domain name-server-list . . . 255
ip domain retry . . . 256
ip domain timeout . . . 257
ip http . . . 258
ip icmp . . . 258
ip icmp redirect . . . 259
ip icmp-errors . . . 259
ip max-arp-entries . . . 260
ip netbios-rebroadcast . . . 261
ip netmask-format . . . 262
ip next-hop-list . . . 263
ip ospf authentication . . . 264
ip ospf authentication-key . . . 265
ip ospf cost . . . 266
ip ospf dead-interval . . . 267
ip ospf hello-interval . . . 268
ip ospf message-digest-key . . . 269
ip ospf network point-to-multipoint . . . 270
ip ospf priority . . . 270
ip ospf router-id . . . 271
ip pbr-group . . . 272
ip pbr-list . . . 273
ip peer address . . . 274
ip policy-list-copy . . . 275
ip proxy-arp . . . 276
ip qos-group . . . 276
ip qos-list . . . 277
ip redirects . . . 278
ip rip authentication key . . . 278
ip rip authentication mode . . . 279
ip rip default-route-mode . . . 280
ip rip poison-reverse . . . 281
ip rip rip-version . . . 282
ip rip send-receive-mode . . . 283
ip rip split-horizon . . . 284
ip route . . . 285
ip routing . . . 287
ip rtp compression-connections . . . 287
ip rtp header-compression . . . 288
ip rtp max-period . . . 290
ip rtp max-time . . . 291
ip rtp non-tcp-mode . . . 292
ip rtp port-range . . . 293
ip simulate . . . 294
ip snmp-server . . . 295
ip ssh . . . 296
ip tcp compression-connections . . . 297

ip tcp header-compression . . . 297
ip telnet . . . 299
ip telnet-client . . . 300
ip tftp-server . . . 300
ip tftp-server file-system size . . . 301
ip unnumbered . . . 302
ip vrrp . . . 303
ip vrrp address . . . 304
ip vrrp auth-key . . . 305
ip vrrp override addr owner . . . 306
ip vrrp preempt . . . 306
ip vrrp primary . . . 307
ip vrrp priority . . . 308
ip vrrp timer . . . 309
ip-fragments-in . . . 310
ip-option-in . . . 311
ip-protocol . . . 312
ip-rule (policy, policy-based routing, packet sniffing) . . . 313
ip-rule (VPN) . . . 314
isakmp-policy . . . 315
keepalive-icmp . . . 316
keepalive-icmp failure-retries . . . 317
keepalive-icmp interval . . . 318
keepalive-icmp source-address . . . 318
keepalive-icmp success-retries . . . 319
keepalive-icmp timeout . . . 320
keepalive-track . . . 321
keepalive (GRE tunnel) . . . 322
keepalive (PPP) . . . 323
keepalive (VPN) . . . 324
lease . . . 325
lifetime . . . 325
line . . . 326
linecode (E1) . . . 327
linecode (T1) . . . 328
load-interval . . . 329
local-address . . . 330
loopback diag . . . 331
loopback local . . . 331
loopback remote . . . 332
map-class frame-relay . . . 333
mode . . . 334
mtu . . . 335
name . . . 336
name-server . . . 337
network (RIP) . . . 338
network (OSPF) . . . 339

next-hop (policy-based routing) . . . 340
next-hop (object tracking) . . . 341
next-hop-interface . . . 342
next-hop-ip . . . 343
next-server . . . 344
nrzi-encoding . . . 345
nslookup . . . 345
nvram initialize . . . 346
object . . . 347
option . . . 348
owner . . . 349
passive-interface . . . 350
ping . . . 351
pmi . . . 352
ppp authentication . . . 352
ppp chap hostname . . . 353
ppp chap password . . . 354
ppp chap refuse . . . 355
ppp chap-secret . . . 356
ppp ipcp dns request . . . 357
ppp pap refuse . . . 357
ppp pap-sent username . . . 358
ppp timeout ncp . . . 359
ppp timeout retry . . . 360
pppoe-client persistent delay . . . 360
pppoe-client persistent max-attempts . . . 361
pppoe-client service-name . . . 362
pppoe-client wait-for-ipcp . . . 363
pre-classification . . . 364
pre-shared-key . . . 365
priority-queue . . . 366
protect crypto map . . . 367
queue-limit . . . 368
redistribute (RIP) . . . 369
redistribute (OSPF) . . . 370
release dhcp . . . 371
release voip-dsp . . . 372
remote . . . 372
remove port . . . 373
rename announcement-file . . . 374
renew dhcp . . . 375
reset . . . 376
retstatus . . . 377
rmon alarm . . . 378
rmon event . . . 379
rmon history . . . 380
router ospf . . . 381

router rip . . . 382
router vrrp . . . 382
rtp-echo-port . . . 383
rtp-stat clear . . . 383
rtp-stat event-threshold . . . 384
rtp-stat fault . . . 386
rtp-stat min-stat-win . . . 387
rtp-stat qos-trap . . . 388
rtp-stat qos-trap-rate-limit . . . 389
rtp-stat service . . . 390
rtp-stat threshold . . . 390
rtp-test-port . . . 393
rtr . . . 394
rtr-schedule . . . 395
sat . . . 395
save config . . . 396
scheduler . . . 397
self-identity . . . 398
server-name . . . 399
session . . . 400
set boot bank . . . 401
set contact-closure admin . . . 402
set contact-closure pulse-duration . . . 403
set cor . . . 404
set date-format . . . 405
set dial . . . 405
set dial-pattern . . . 406
set digits . . . 408
set digit-treatment . . . 409
set dot1x m tlv . . . 410
set dot1x max-req . . . 411
set dot1x max-supp-per-port . . . 412
set dot1x port-mode . . . 413
set dot1x quiet-period . . . 414
set dot1x re-authperiod . . . 415
set dot1x server-timeout . . . 416
set dot1x supp-timeout . . . 417
set dot1x system-auth-control disable . . . 418
set dot1x system-auth-control enable . . . 418
set dot1x tx-period . . . 419
set dscp . . . 420
set expansion-module . . . 421
set etr . . . 422
set fac . . . 423
set icc-monitoring . . . 424
set ip-codec-set . . . 425
set lldp re-init-delay . . . 426

set lldp system-control . . . 426
set lldp tx-delay . . . 427
set lldp tx-hold-multiplier . . . 428
set lldp tx-interval . . . 429
set logging file . . . 430
set logging server . . . 431
set logging server access-level . . . 432
set logging server condition . . . 433
set logging server enable/disable . . . 435
set logging server facility . . . 436
set logging session . . . 437
set logout . . . 439
set max-ip-registrations . . . 440
set mediaserver . . . 441
set mgc list . . . 442
set mss-notification rate . . . 443
set password . . . 444
set peer (crypto map) . . . 445
set peer (peer group) . . . 446
set peer-group . . . 447
set pfs . . . 448
set pim-lockout . . . 449
set port . . . 449
set port auto-negotiation-flowcontrol-advertisement . . . 451
set port classification . . . 452
set port disable . . . 453
set port dot1x initialize . . . 454
set port dot1x port-control . . . 455
set port dot1x port-mode . . . 456
set port dot1x re-authenticate . . . 457
set port dot1x re-authentication . . . 458
set port duplex . . . 459
set port edge admin state . . . 460
set port enable . . . 461
set port flowcontrol . . . 462
set port level . . . 464
set port lldp . . . 465
set port lldp tlv . . . 466
set port mirror . . . 468
set port name . . . 469
set port negotiation . . . 470
set port point-to-point admin status . . . 471
set port powerinline . . . 472
set port powerinline priority . . . 474
set port powerinline type . . . 475
set port redundancy . . . 476
set port redundancy on|off . . . 477

set port redundancy-intervals . . . 478
set port spantree . . . 479
set port spantree cost . . . 480
set port spantree force-protocol-migration . . . 481
set port spantree priority . . . 482
set port speed . . . 483
set port static-vlan . . . 484
set port trap . . . 485
set port vlan . . . 486
set port vlan-binding-mode . . . 488
set powerinline trap disable . . . 489
set powerinline trap enable . . . 490
set qos bearer . . . 490
set qos control . . . 492
set qos rsvp . . . 493
set qos rtcp . . . 494
set qos signal . . . 495
set radius authentication . . . 496
set radius authentication retry-number . . . 497
set radius authentication retry-time . . . 498
set radius authentication secret . . . 498
set radius authentication server . . . 499
set radius authentication udp-port . . . 500
set reset-times . . . 501
set security-association lifetime . . . 502
set snmp community . . . 503
set snmp retries . . . 504
set snmp timeout . . . 505
set snmp trap . . . 506
set spantree default-path-cost . . . 508
set spantree enable/disable . . . 509
set spantree forward-delay . . . 510
set spantree hello-time . . . 511
set spantree max-age . . . 512
set spantree priority . . . 513
set spantree tx-hold-count . . . 514
set spantree version . . . 515
set supervision . . . 516
set survivable-call-engine . . . 517
set swhook-flash . . . 518
set sync interface . . . 519
set sync source . . . 520
set sync switching . . . 521
set system contact . . . 522
set system location . . . 523
set system name . . . 524
set tac . . . 525

set terminal recovery password . . . 526
set transform-set . . . 526
set trunk . . . 527
set trunk-destination . . . 529
set type . . . 530
set utilization cpu . . . 531
set vlan . . . 532
set web aux-files-url . . . 533
show . . . 534
show announcements files . . . 536
show application-memory . . . 537
show banner login . . . 538
show banner post-login . . . 539
show boot bank . . . 539
show cam . . . 540
show cam mac . . . 541
show cam vlan . . . 542
show capture . . . 543
show capture-buffer hex . . . 544
show cna testplug . . . 545
show composite-operation . . . 548
show contact-closure . . . 549
show controllers . . . 550
show controllers remote . . . 551
show copy status . . . 552
show crypto ipsec sa . . . 553
show crypto ipsec transform-set . . . 561
show crypto isakmp peer . . . 563
show crypto isakmp peer-group . . . 564
show crypto isakmp policy . . . 565
show crypto isakmp sa . . . 566
show crypto map . . . 568
show csu loopbacks . . . 569
show csu status . . . 570
show date-format . . . 572
show dev log file . . . 572
show dial-pattern . . . 573
show dot1x . . . 574
show download announcement-file status . . . 575
show download license-file status . . . 576
show download phone-image-file status . . . 577
show download phone-script-file status . . . 578
show download software status . . . 579
show download status . . . 580
show dscp-table . . . 581
show ds-mode . . . 582
show dynamic-cac . . . 582

show erase status . . . 583
show etr . . . 584
show extension . . . 584
show fac . . . 586
show faults . . . 587
show flows . . . 588
show fragment . . . 589
show frame-relay fragment . . . 589
show frame-relay lmi . . . 590
show frame-relay map . . . 593
show frame-relay pvc . . . 593
show frame-relay pvc brief . . . 595
show frame-relay traffic . . . 596
show icc-monitoring . . . 596
show icc-vlan . . . 597
show image version . . . 597
show interfaces . . . 598
show ip access-control-list . . . 601
show ip active-lists . . . 604
show ip active-pbr-lists . . . 606
show ip arp . . . 607
show ip capture-list . . . 608
show ip-codec-set . . . 609
show ip crypto-list . . . 610
show ip dhcp-client . . . 613
show ip dhcp-client statistics . . . 616
show ip dhcp-pool . . . 618
show ip dhcp-server bindings . . . 623
show ip dhcp-server statistics . . . 624
show ip distribution access-lists . . . 625
show ip domain . . . 626
show ip domain statistics . . . 628
show ip icmp . . . 630
show ip interface . . . 630
show ip interface brief . . . 633
show ip next-hop-list . . . 635
show ip ospf . . . 636
show ip ospf database . . . 636
show ip ospf interface . . . 638
show ip ospf neighbor . . . 639
show ip pbr-list . . . 640
show ip protocols . . . 641
show ip qos-list . . . 642
show ip reverse-arp . . . 643
show ip route . . . 644
show ip route best-match . . . 646
show ip route static . . . 647

show ip route summary . . . 648
show ip route track-table . . . 648
show ip rtp header-compression . . . 649
show ip rtp header-compression brief . . . 651
show ip-rule . . . 653
show ip ssh . . . 654
show ip tcp header-compression . . . 656
show ip tcp header-compression brief . . . 657
show ip tftp-server files . . . 659
show ip tftp-server statistics . . . 660
show ip traffic . . . 661
show ip vrrp . . . 663
show isdn bri link . . . 665
show isdn link summary . . . 666
show isdn pri link . . . 666
show keepalive-icmp . . . 667
show last-pim-update . . . 668
show license status . . . 669
show list . . . 669
show lldp . . . 670
show lldp config . . . 672
show logging file condition . . . 673
show logging file content . . . 674
show logging server condition . . . 675
show logging session condition . . . 677
show logout . . . 677
show map-class frame-relay . . . 678
show max-ip-registrations . . . 679
show mediaserver . . . 679
show mg list_config . . . 680
show mgc . . . 681
show mgc list . . . 682
show mm . . . 683
show module . . . 685
show mss-notification rate . . . 686
show next-hop . . . 686
show pim-lockout . . . 687
show pmi . . . 688
show port . . . 688
show port auto-negotiation-flowcontrol-advertisement . . . 690
show port classification . . . 691
show port dot1x . . . 692
show port dot1x statistics . . . 693
show port dot1x supp-mac . . . 695
show port edge state . . . 696
show port flowcontrol . . . 697
show port lldp config . . . 699

show port lldp vlan-name config . . . 701
show port mirror . . . 702
show port point-to-point status . . . 703
show port redundancy . . . 704
show port trap . . . 705
show port vlan-binding-mode . . . 706
show powerinline . . . 707
show ppp authentication . . . 708
show protocol . . . 708
show qos-rtcp . . . 710
show queue . . . 712
show queueing . . . 713
show radius authentication . . . 714
show recovery . . . 715
show restart-log . . . 716
show rmon alarm . . . 717
show rmon event . . . 718
show rmon history . . . 719
show rmon statistics . . . 720
show rtp-stat config . . . 721
show rtp-stat detailed . . . 722
show rtp-stat sessions . . . 723
show rtp-stat summary . . . 725
show rtp-stat thresholds . . . 726
show rtp-stat traceroute . . . 727
show rtr configuration . . . 729
show rtr operational-state . . . 731
show running-config . . . 733
show self-test-status . . . 734
show snmp . . . 735
show snmp engineID . . . 736
show snmp group . . . 737
show snmp retries . . . 738
show snmp timeout . . . 739
show snmp user . . . 740
show snmp user summary . . . 741
show snmp usertogroup . . . 741
show snmp view . . . 743
show spantree . . . 744
show startup-config . . . 746
show status . . . 747
show survivable-call-engine . . . 748
show sync timing . . . 749
show system . . . 749
show tcp syn-cookies . . . 750
show temp . . . 753
show timeout . . . 753

show track . . . 754
show traffic-shape . . . 756
show traffic-shape queue . . . 757
show traffic-shape statistics . . . 759
show trunk . . . 761
show trunk-group . . . 762
show upload announcement-file status . . . 764
show upload dhcp-binding-file status . . . 765
show upload phone-script-file status . . . 766
show upload status . . . 767
show username . . . 768
show utilization . . . 768
show vlan . . . 769
show voip-parameters . . . 771
show voltages . . . 772
show web aux-files-url . . . 773
shutdown (CNA test plugs) . . . 773
shutdown (interface) . . . 774
shutdown (USB modem) . . . 775
snmp trap link-status . . . 776
snmp-server community . . . 777
snmp-server dynamic-trap-manager . . . 778
snmp-server enable notifications . . . 779
snmp-server engineID . . . 780
snmp-server group . . . 781
snmp-server host . . . 783
snmp-server informs . . . 786
snmp-server remote-user . . . 787
snmp-server user . . . 789
snmp-server view . . . 791
source-address . . . 792
source-ip . . . 793
speed (PPP) . . . 794
speed (interface) . . . 795
start-ip-addr . . . 796
station . . . 797
subnet-mask . . . 798
success-retries . . . 799
suggest-key . . . 800
survivable-call-engine . . . 801
tcp destination-port . . . 802
tcp established . . . 803
tcp source-port . . . 804
tcp syn-cookies . . . 806
tech . . . 807
telnet . . . 807
terminal length . . . 808

terminal width . . . 809
test led . . . 810
test voip-dsp . . . 810
test-rate-limit . . . 811
threshold count . . . 812
timeout absolute . . . 813
timers basic . . . 814
timers spf . . . 815
traceroute . . . 816
track . . . 818
traffic-shape rate . . . 820
transmitter-delay . . . 821
tree . . . 821
trunk-group . . . 822
tunnel checksum . . . 824
tunnel destination . . . 825
tunnel dscp . . . 826
tunnel key . . . 827
tunnel mode . . . 828
tunnel path-mtu-discovery . . . 828
tunnel source . . . 830
tunnel ttl . . . 831
type . . . 832
udp destination-port . . . 833
udp source-port . . . 835
username . . . 837
value . . . 838
vendor-specific-option . . . 839
voip-queue . . . 840
voip-queue-delay . . . 841
wait-interval . . . 842
zeroize . . . 843

Topical Index of Commands . . . 845

About this Book

Overview

The *Avaya G250 and Avaya G350 CLI Reference* describes the commands used to configure and manage the Avaya G250 and Avaya G350 Media Gateways after they are already installed. For instructions on using these commands to configure and manage the Avaya G250 and Avaya G350 Media Gateways, refer to *Administration for the Avaya G250 and Avaya G350 Media Gateways*, 03-300436.

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 G250/G350 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.

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 G250 and Avaya G350 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

To download the latest version of this book:

1. Access the Avaya web site at http://www.avaya.com/support.
2. On the left side of the page, click **Product Documentation**.

   The system displays the Welcome to Product Documentation page.
3. On the right side of the page, type **03-300437**, and then click **Search**.

   The system displays the Product Documentation Search Results page.
4. Scroll down to find the latest issue number, and then click the book title that is to the right of the latest issue number.
5. On the next page, scroll down and click one of the following options:
   - **PDF Format** to download the book in regular PDF format
   - **ZIP Format** to download the book as a zipped PDF file

Related resources

For more information on the Avaya G250 and Avaya G350 Media Gateways and related features, see the following books:

Title	Number
Overview for the Avaya G250 and Avaya G350 Media Gateways	03-300345
Quick Start for Hardware Installation for the Avaya G250 Media Gateway	03-300433
Quick Start for Hardware Installation for the Avaya G350 Media Gateway	03-300148
Installing and Upgrading the Avaya G250 Media Gateway	03-300434
Installing and Upgrading the Avaya G350 Media Gateway	03-300394
Administration for the Avaya G250 and Avaya G350 Media Gateways	03-300436
Maintenance for the Avaya G250 and Avaya G350 Media Gateways	03-300438

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 G250 and Avaya G350 CLI Reference*, 03-300437.

Chapter 1: User Levels and Contexts

The G250/G350 Command Line Interface (CLI) consists of commands that are divided into logical contexts. These contexts enable you to view and configure the Avaya G250/G350 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 G250/G350 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.

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
- Interface Dialer
- Interface Fast Ethernet
- 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 the **`interface`** command description.

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	G250/G350 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 <list#>	QoS policy list	**(QoS 401)#**
rule <rule#>	QoS policy list entry	**(QoS 401/rule 4)#**
composite-operation <cot#>	QoS policy list match action	**(QoS 401/CompOp 2)#**
dscp-table <table#>	QoS policy list DSCP to CoS map	**(QoS 401/dscp 63)#**
ip Access-Control-List <list#>	Security Access list	**(ACL 301)#**
ip-rule <rule#>	Security ACL list entry	**(ACL 301/ip rule 4)#**
composite-operation <cot#>	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 <name>	Create a QoS template	**(map-class)#**
rtr	Enter RTR configuration mode	**(rtr icmp 1)#**

2 of 3

Table 1: List of CLI Contexts (continued)

Context	Description	CLI prompt
track	Configure an object tracker	**(track rtr 1)#**
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)#**
survivable-call-engine	Configure Standard Local Survivability (SLS) on the G250 Media Gateway	**(survivable-call-engine)**
survivable-call-engine/ station	Configure SLS stations	**(sls-station-<extension>)**
survivable-call-engine/ station	Configure SLS trunks	**(sls-trunk-group-<tgnum>)**

3 of 3

Chapter 2: CLI Commands

About the CLI

The Avaya G250/G350 Media Gateway CLI is accessible directly via the serial console port, remotely via telnet, 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 28.

This chapter lists all the CLI commands for the Avaya G250/G350 Media Gateway. All commands are supported for both the G250 and the Avaya G250 and Avaya G350 Media Gateways except where otherwise noted.

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 27.

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, the system displays a list of commands matching those letters.

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
```

Alphabetical listing of CLI commands

add port

Use the **add port** command to administer the virtual integrated port appropriate for G250 Standard Local Survivability (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.

Note:

This command is not supported on the G350.

Syntax

add port *module-port*

Parameters

Parameter	Description	Possible Values	Default Value
module-port	The virtual integrated port assignment for this ***group-type***	See below	

Assign a port from this list:

G250 model	Analog loop-start trunks (***group-type*** parameter is **loop-start**)	Analog DID trunks (***group-type*** parameter is **did**)
G250-Analog	V301, V302, V303, V304	V305, V306
G250-BRI	V301	V302, V303
G250-DCP	V301, V302, V303, V304	V305, V306
G250-DS1	V301	V302, V303

User level

read-write

Context

survivable-call-engine/trunk-group

Example

```
G250-100 (sls-trunk-group-<tgnum>)# add port v304
```

Related commands

set dial, set tac, clear tac, remove port, set digit-treatment, set digits, set supervision, show, trunk-group

---

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	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:

```
G350-001(router:ospf)# area 192.168.49.1
```

To configure a stub area for this OSPF interface with IP address 176.1.13.12:

```
G350-001(router:ospf)# area 176.1.13.12 stub
```

To remove the area with IP address 192.168.49.1:

```
G350-001(router:ospf)# no area 192.168.49.1
```

Related commands

default-metric (OSPF), network (OSPF), passive-interface, redistribute (OSPF), timers spf

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:

```
G350-001(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:

```
G350-001(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:

```
G350-001(super)# arp timeout 3600
```

To restore the default value for ARP timeout:

```
G350-001(super)# no arp timeout
```

Related commands

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

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

Related commands

async mode terminal, async modem-type, 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

Related commands

async mode interactive, async modem-type, 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

Example

To set the modem initialization string to 'AT&FE0Q0V0X0&D2N0S37=6':

```
G350-001(super-if:Console)# async modem-init-string
AT&FE0Q0V0X0&D2N0S37=6
```

Related commands

async mode interactive, async mode terminal, async modem-type, 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 modem-type

Use the **async modem-type** command to set the type of modem being used. This command also sets the default modem parameter values such as default initialization string and escape sequence for the specified type of modem. Use the **no** form of the command to return modem type to its default value of **MultiTech-ZBA**.

Note:

If modem-type is specified as **none**, the system connects the PPP stack to the console port.

Syntax

async modem-type {multitech-zba | multitech-isdn}

no async {multitech-zba | multitech-isdn}

Parameters

Parameter	Description	Possible Values	Default Value
multitech-zba	Set the modem type to be **MultiTech-ZBA**		
multitech-isdn	Set the modem type to be **MultiTech-ISDN**		

User level

admin

Context

Interface: Console

Example

To set the modem type to MultiTech-ZBA:

```
G350-001(super-if:Console)# async modem-type multitech-zba
```

Related commands

async mode interactive, async mode terminal, ip address, ppp authentication, shutdown (interface), 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, async modem-type, ip address, ppp authentication, shutdown (interface), speed (PPP), 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

Related commands

ip address, ppp authentication, shutdown (USB modem), speed (PPP), timeout absolute

authentication

Use the **authentication** command to set the authentication of ISAKMP policy pre-shared secret.

Syntax

authentication { pre-share }

Parameters

Parameter	Description	Possible Values	Default Value
pre-share	The authentication of the ISAKMP policy pre-shared secret. This is the default setting.		

User level

read-write

Context

crypto isakmp policy

Example

```
G350-001(config-isakmp:1)# authentication pre-share
```

Related commands

crypto isakmp policy, description (ISAKMP policy), encryption, group, hash, lifetime, show crypto isakmp policy

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

duplex, shutdown (interface), speed (interface), traffic-shape rate

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:

```
G350-001(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**	
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)

Example

To specify that Serial interface 2/1:1 is a backup interface for the current interface:

```
G350-001(if:Serial 2/1:2)# backup interface Serial 2/1:1
```

Related commands

backup delay

---

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), Fast Ethernet (L2, L2-L3), VLAN (L2, L2-L3), Loopback (L2, L2-L3), Tunnel (L2, L2-L3)

Example

To manually set the bandwidth for the VLAN interface to 100 KB/s:

```
G350-001(if:Vlan 1)# bandwidth 100
```

Related commands

idle-character, ignore dcd, interface serial, invert txclock, nrzi-encoding, transmitter-delay

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 displays before the user is prompted for the login name. To enter text for the login banner, refer to the command line on page 326.

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:

```
G350-001(super)# banner login
G350-001(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 displays 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 326.

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:

```
G350-001(super)# banner post-login
G350-001(super-post-login)#
```

Related commands

banner login, clear screen, hostname, line, show banner login, show banner post-login, terminal length, terminal width

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:

```
G350-001(map-class)# bc out 64000
```

Related commands

be out, cir out

---

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:

```
G350-001(map-class)# be out 64000
```

Related commands

bc out, cir out

---

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 the file “booter” as the bootfile:

```
G350-001(DHCP 5)# bootfile "booter"
```

To clear the bootfile definition:

```
G350-001(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

busyout voip-dsp

Use the **busyout voip-dsp** command to put the VoIP engine in busyout (not available) state for a Bit Transfer Rate test.

Note:

Status changes made during the test create SNMP traps.

Syntax

busyout voip-dsp

User level

read-write

Context

general

Related commands

release voip-dsp, show voip-parameters, test voip-dsp

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:

```
G350-001(controller:5/1)# cablelength long gain36 -7.5db
```

Related commands

cablelength short, channel-group, clock source, controller, ds-mode, framing, interface serial, ip address, linecode (E1), linecode (T1), remote, show controllers

---

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:

```
G350-001(controller:5/1)# cablelength short 399ft
```

Related commands

cablelength long, channel-group, clock source, controller, ds-mode, framing, interface serial, ip address, linecode (E1), linecode (T1), remote, show controllers

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	Linear buffer that is used until it is filled up		
cyclic	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

```
G350-001(super)# capture buffer-mode cyclic
```

Related commands

capture buffer-size, capture filter-group, capture interface, 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	**256-10000 (Kbytes)**	**1000**

User level

read-write

Context

general

Example

```
G350-001(super)# capture buffer-size 2000
```

Related commands

capture buffer-mode, 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 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

```
G350-001(super)# capture filter-group 501
```

Related commands

capture buffer-mode, capture buffer-size, 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 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

```
G350-001(super)# capture interface FastEthernet 10/2
```

Related commands

capture buffer-mode, capture buffer-size, capture filter-group, 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

```
G350-001(super)# capture max-frame-size 68
```

Related commands

capture buffer-mode, capture buffer-size, capture filter-group, capture interface, 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:

```
G350-001(super)# capture start
Starting the packet sniffing process
```

If the packet sniffing service has not been enabled by the administrator:

```
G350-001(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 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:

```
G350-001(super)# capture stop
110 packets captured.
```

If the packet sniffing service has not been enabled by the administrator:

```
G350-001(super)# capture stop
The Packet sniffing process is not running.
```

Related commands

capture buffer-mode, capture buffer-size, capture filter-group, capture interface, capture 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:

```
G350-001(super)# capture-service
Packet sniffing service enabled
```

To disable packet sniffing:

```
G350-001(super)# no capture-service
Packet sniffing service disabled
```

Related commands

capture buffer-mode, capture buffer-size, capture filter-group, capture interface, capture max-frame-size, capture start, capture stop, clear capture-buffer, ip capture-list, name, show capture, show capture-buffer hex

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.

Note:

The G250 only supports one channel group per interface.

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:

```
G350-001(controller:5/1)# channel-group 2 timeslots 5-6,8 speed 56
```

Related commands

cablelength long, cablelength short, clock source, controller, ds-mode, framing, interface serial, ip address, linecode (E1), linecode (T1), remote, show controllers

---

cir out

Use the **cir out** command to configure the Committed Information Rate 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:

```
G350-001(map-class)# cir out 64000
```

Related commands

bc out, be out

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

User level

read-write

Context

dhcp pool vendor specific

Example

To set an identifier string for vendor-specific option 1:

```
G350-001(DHCP 5/vendor specific 1)# class-identifier "ccp.avaya.com"
```

Related commands

value

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	**1-3071**	
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:

```
G350-001(super)# clear arp-cache

Flushing all arp entries
Flushed 22 ARP entries.
```

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

```
G350-001(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:

```
G350-001(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:

```
G350-001(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

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:

```
G350-001(super)# clear cam
CAM table cleared.
```

Related commands

show cam, show cam mac

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

```
G350-001(super)# clear capture-buffer
```

Related commands

capture buffer-mode, capture buffer-size, capture filter-group, capture interface, capture max-frame-size, capture start, capture stop, capture-service, ip capture-list, name, show capture, show capture-buffer hex

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, port 1:

```
G350-001(super)# clear controller counters 3/1
```

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** For Serial(USP): **2/1** For Serial (DS1): module/port: **2/1** channel-group: E1: **0-30** T1: **0-23** For VLAN: **1-3071** For Loopback: **1-99**	

User level

read-write

Context

general

Example

To clear counters on interface “Vlan 1”:

```
G350-001(super)# clear counters Vlan 1
```

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:

```
G350-003(cna-testplug 1)# clear counters
```

Related commands

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

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 C-id 1:

```
G350-001(super)# clear crypto isakmp 1
```

To clear the entire database:

```
G350-001(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

```
G350-001(super)# clear crypto sa all
G350-001(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

```
G350-001(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

clear dial-pattern

Use the **clear dial-pattern** command to delete a single dialed string pattern entry in the SLS data set on the G250.

Note:

This command is not supported on the G350.

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

survivable-call-engine

Example

```
G250-001(super-survivable-call-engine)# clear dial-pattern 49139
Dial Pattern 49139 was removed.
```

Related commands

clear survivable-config, clear extension, clear trunk-group, save config, set date-format, set dial-pattern, set ip-codec-set, set max-ip-registrations, set survivable-call-engine, show date-format, show dial-pattern, show extension, , show ip-codec-set, show last-pim-update, show max-ip-registrations, show survivable-call-engine, show trunk-group, survivable-call-engine

clear dot1x config

Use the **clear dot1x config** command to disable 802.1x on all ports and return values to the default settings.

Syntax

clear dot1x config

User level

admin

Example

```
G350-001(super)# clear dot1x config
```

Related commands

set dot1x m tlv, set dot1x max-req, set dot1x max-supp-per-port, set dot1x port-mode, set dot1x quiet-period, set dot1x re-authperiod, set dot1x server-timeout, set dot1x supp-timeout, set dot1x system-auth-control disable, set dot1x system-auth-control enable, set dot1x tx-period, set port dot1x initialize, set port dot1x port-control, set port dot1x port-mode, set port dot1x re-authenticate, set port dot1x re-authentication, show dot1x, show port dot1x, show port dot1x statistics, show port dot1x supp-mac

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:

This command is not supported on the G350.

Syntax

clear extension *extnum*

Parameters

Parameter	Description	Possible Values	Default Value
extnum	Specifies the extension number to delete	1-7 digit number	

User level

read-write

Context

survivable-call-engine

Example

```
G250-001(super-survivable-call-engine)# clear extension 1234
Extension 1234 was removed.
```

Related commands

station, trunk-group, show extension, clear trunk-group, show trunk-group, set max-ip-registrations, show max-ip-registrations, set pim-lockout, show pim-lockout, show, set fac, show fac, clear fac, set date-format, show date-format, set ip-codec-set, copy running-config startup-config, clear survivable-config, show last-pim-update, survivable-call-engine

---

clear fac

Use the **clear fac** command to delete an administered Feature Access Code (FAC) for Standard Local Survivabiltiy (SLS) on the G250.

Note:

This command is not supported on the G350.

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

survivable-call-engine

Example

```
G250-001(super-survivable-call-engine)# clear fac hold
Done!
```

Related commands

station, trunk-group, clear extension, show extension, clear trunk-group, show trunk-group, set max-ip-registrations, show max-ip-registrations, set pim-lockout, show pim-lockout, show, set fac, show fac, set date-format, show date-format, set ip-codec-set, copy running-config startup-config, clear survivable-config, show last-pim-update, survivable-call-engine

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

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:

```
G350-001(super)# clear frame-relay counters
```

To clear a specific Frame Relay interface's counters:

```
G350-001(super)# clear frame-relay counters interface "Serial 4/1.100"
```

Related commands

clear frame-relay counters, frame-relay class-dlci, interface serial, map-class frame-relay, show frame-relay map, show frame-relay pvc brief, show interfaces

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: Fast Ethernet

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

```
G350-001(config-if:FastEthernet 10/2)# clear ip dhcp-client statistics
```

Related commands

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, show ip dhcp-client statistics

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:

```
G350-001(super)# clear ip dhcp-server bindings 1.1.1.1
```

To clear all DHCP server IP address allocations:

```
G350-001(super)# clear ip dhcp-server bindings 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:

```
G350-001(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

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

```
G350-001(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

clear ip route

Use the **clear ip route** command to delete all the dynamic routing entries from the routing table.

Syntax

clear ip route * | {*ip_addr* [*ip_mask*]}

Parameters

Parameter	Description	Possible Values	Default Value
*	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:

```
G350-001(super)# clear ip route *
```

To clear a range of entries:

```
G350-001(super)# clear ip route 192.168.49.1 255.255.255.0
```

Related commands

ip default-gateway, ip route, show ip route, show ip route best-match, show ip route static, show ip route summary ,show ip route track-table, traceroute

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:

```
G350-001(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:

```
G350-001(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

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:

```
G350-001# 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

clear ip traffic

Use the **clear ip traffic** command to clear the IP counters.

Syntax

clear ip traffic

User level

read-only

Context

general

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:

```
G350-001(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:

```
G350-001(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

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:

```
G350-001(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

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 5/1 by port 5/3:

```
G350-001(super)# clear port mirror 5/1 5/3
```

Related commands

set port mirror, show port mirror

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 number or range of port numbers		
vlan_id	The VLAN ID to remove		

User level

read-write

Context

general

Example

To remove VLAN 5 from port 6/10:

```
G350-001(super)# clear port static-vlan 6/10 5
```

VLAN 5 is unbound from port 6/10

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 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:

```
G350-001(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

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

clear snmp trap

Use the **clear snmp trap** command to clear an entry from the SNMP trap receiver table.

Syntax

clear snmp trap {*rcvr_addr*|all}

Parameters

Parameter	Description	Possible Values	Default Value
rcvr_addr	The IP address of the trap receiver (the SNMP management station) to remove		
all	Keyword used to clear all entries in the SNMP trap receiver table		

User level

read-write

Context

general

Example

To remove the SNMP trap server with IP address 192.122.173.82 from the table:

```
G350-001(super)# clear snmp trap 192.122.173.82
SNMP trap receiver deleted.
```

Related commands - SNMP access configuration

ip snmp-server, set snmp community, set snmp retries, set snmp timeout, show port trap, show snmp, show snmp engineID, show snmp group, show snmp retries, show snmp timeout, show snmp user, show snmp user summary, 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, show snmp, snmp trap link-status, snmp-server enable notifications, snmp-server host, snmp-server informs

---

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

```
G350-001(super)# clear ssh-client known-hosts
```

Related commands

crypto key generate, disconnect ssh, ip ssh, show ip ssh

clear survivable-config

Use the **clear survivable-config** command to set the SLS parameters in the G250 to their default values.

Note:

This command is not supported on the G350.

Syntax

clear survivable-config

User level

read-write

Context

survivable-call-engine

Example

```
G250-001(super-survivable-call-engine)# clear survivable-config
Survivable-call-engine configuration is cleared
```

Related commands

station, trunk-group, clear extension, show extension, clear trunk-group, show trunk-group, set max-ip-registrations, show max-ip-registrations, set pim-lockout, show pim-lockout, show, set fac, show fac, clear fac, set date-format, show date-format, set ip-codec-set, copy running-config startup-config, show last-pim-update, survivable-call-engine

clear sync interface

Use the **clear sync interface** command to disassociate a previously specified interface 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:

```
G350-001(super)# clear sync interface primary
```

Related commands

set sync interface, set sync source, set sync switching, show sync timing

clear tac

Use the **clear tac** command to remove a trunk access code (TAC) assignment from a trunk group in Standard Local Survivability (SLS). The set tac command establishes the TAC assignment to the trunk group.

Note:

This command is not supported on the G350.

Syntax

clear tac

User level

read-write

Context

survivable-call-engine/trunk-group

Example

```
G250-100 (sls-trunk-group-<tgnum>)# clear tac
```

Related commands

set dial, set tac, add port, remove port, set digit-treatment, set digits, set supervision, show

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

```
G350-001(super)# clear tcp syn-cookies counters
```

Related commands

show tcp syn-cookies, tcp syn-cookies

clear trunk-group

Use the **clear trunk-group** command to delete a trunk group entry from the Standard Local Survivability (SLS) data set.

Note:

The trunk group must have already been administered with the trunk-group command before this command will work. This command is not supported on the G350.

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

survivable-call-engine

Example

```
G250-001(super-survivable-call-engine)# clear trunk-group 13
Trunk group 13 was removed.
```

Related commands

station, trunk-group, clear extension, show extension, show trunk-group, set max-ip-registrations, show max-ip-registrations, set pim-lockout, show pim-lockout, show, set fac, show fac, clear fac, set date-format, show date-format, set ip-codec-set, copy running-config startup-config, clear survivable-config, show last-pim-update, survivable-call-engine, trunk-group

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:

```
G350-001(super)# clear utilization cpu 10
```

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:

```
G350-001(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

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`:

```
G350-001(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

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:

```
G350-001(controller:5/1)# clock source external
```

Related commands

cablelength long, cablelength short, channel-group, controller, ds-mode, framing, interface serial, ip address, linecode (E1), linecode (T1), remote, show controllers

cna-testplug

The G250/G350 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:

```
G350-003# cna-testplug 1
G350-003(cna-testplug 1)#
```

Related commands

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

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:

```
G350-003# cna-testplug-service
The Converged Network Analyzer test plug is enabled.
```

Related commands

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

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:

```
G350-001(QoS 440)# composite-operation 13
G350-001(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

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

Examples

```
G350-001(config-peer:149.49.70.1)# continuous-channel
G350-001(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

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 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:

```
G350-001(cna-testplug 1)# control-port 12843
```

Related commands

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

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		
port_number	The port to configure		

User level

read-write

Context

general

Example

To enter configuration mode for a T1 controller on port 5/1:

```
G350-001(super)# controller t1 5/1
```

Related commands

cablelength long, cablelength short, channel-group, clock source, ds-mode, framing, interface serial, ip address, linecode (E1), linecode (T1), remote, show controllers

---

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:

```
G350-001(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

---

copy announcement-file scp

Use the **copy announcement-file scp** command to upload an announcement file from the G250/G350 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 G250/G350 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 “announcement1.wav” from the announcements directory to a remote SCP server with IP address 192.168.49.10:

```
G350-001(super)# copy announcement-file scp announcement1.wav 192.168.49.10
```

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”:

```
G350-001(super)# copy announcement-file scp local_announcement2.wav
192.168.49.10 c:\remote_announcement2.wav
```

To upload the file “local announcement2.wav” to a remote SCP server with IP address 192.168.49.10, store it in c:\, and name it “remote announcement2.wav”.

```
G350-001(super)# copy announcement-file scp “local announcement2.wav”
192.168.49.10 “c:\remote announcement2.wav”
```

Related commands

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

---

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 the g350.cap file on the FTP server at IP address 135.64.10.33:

```
G350-001(super)# copy capture-file ftp g350.cap 135.64.10.33
```

Related commands

composite-operation, cookie, copy capture-file scp, copy capture-file tftp, 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 the g350.cap file on the FTP server at IP address 135.64.10.33:

```
G350-001(super)# copy capture-file scp g350.cap 135.64.10.33
```

Related commands

composite-operation, cookie, copy capture-file ftp, copy capture-file tftp, 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 the g350.cap file on the TFTP server at IP address 135.64.10.33:

```
G350-001(super)# copy capture-file tftp g350.cap 135.64.10.33
```

Related commands

composite-operation, cookie, copy capture-file ftp, copy capture-file scp, ip-rule (policy, policy-based routing, packet sniffing), owner, show ip capture-list, show upload status

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 with file name dhcp_binding.txt to the host with IP address 192.168.49.10:

```
G350-001(super)# copy dhcp-binding ftp dhcp_binding.txt 192.168.49.10
```

Related commands

copy dhcp-binding scp, copy dhcp-binding tftp

copy dhcp-binding scp

Use the **copy dhcp-binding scp** command to copy the dhcp bindings file to a remote server using FTP.

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 with file name dhcp_binding.txt to the host with IP address 192.168.49.10:

```
G350-001(super)# copy dhcp-binding scp dhcp_binding.txt 192.168.49.10
```

Related commands

copy dhcp-binding ftp, copy dhcp-binding tftp

---

copy dhcp-binding tftp

Use the **copy dhcp-binding tftp** command to copy 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:

```
G350-001(super)# copy dhcp-binding tftp dhcp_binding.txt 192.168.49.10
```

Related commands

copy dhcp-binding ftp, copy dhcp-binding scp

copy ftp EW_archive

Use the **copy ftp EW_archive** command to download Avaya G350 Manager software from an FTP server. The FTP command prompts for the username and password after the command is entered.

Note:

This command is not supported by the G250.

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 the g350.img file from the FTP server at IP address 135.64.10.33, using login dan:

```
G350-001(super)# copy ftp EW_archive g350.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, dir, set boot bank, show boot bank, show download software status, show image version

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 `g350.lic` from the FTP site at IP address 198.87.134.153:

```
G350-001(super)# copy ftp license-file g350.lic 198.87.134.153
```

Related commands

copy scp license-file, copy tftp license-file, show download license-file status, show license status

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.

Note:

This command is not supported by the G250.

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 site at IP address 135.64.10.33 using login dan:

```
G350-001(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, dir, set boot bank, show boot bank, show download software status, show image version

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.

Note:

The G250/G350 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

```
G350-001# 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, 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 G250/G350 TFTP directory.

Note:

The G250/G350 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

```
G350-001# 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 ftp phone-image, 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 ip tftp-server files, show download phone-script-file status, show upload phone-script-file status

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, g350.img, from the FTP server at IP address 135.64.10.33 using login dan:

```
G350-001(super)# copy ftp startup-config g350.img 135.64.10.33
Username: dan
Password:

G350-001(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 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, g350.img, from the FTP site at IP address 135.64.10.33 using login dan:

```
G350-001(super)# copy ftp SW_imageA g350.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, 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, g350.img, from the FTP site at IP address 135.64.10.33 using login dan:

```
G350-001(super)# copy ftp SW_imageB g350.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, dir, set boot bank, show boot bank, show download software status, show image version

copy phone-script ftp

Use the **copy phone-script ftp** command to upload a phone script file from the local G250/G350 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

```
G350-001# 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 phone-script scp, copy phone-script tftp

copy phone-script scp

Use the **copy phone-script scp** command to upload a phone script file from the local G250/G350 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

```
G350-001# 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 phone-script ftp, copy phone-script tftp

copy phone-script tftp

Use the **copy phone-script tftp** command to upload a phone script file from the local G250/G350 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

```
G350-001(super)# copy phone-scriptA tftp 46xxupgrade.txt 192.168.49.10
```

Related commands

copy phone-script ftp, copy phone-script scp

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 the g350.cfg file on the ftp server at IP address 135.64.10.33 using login dan:

```
G350-001(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

```
G350-001(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.

Note:

Station passwords are NVRAM to prevent them from being uploaded or downloaded through unsecure protocols. This command is not supported on the G350.

Syntax

copy running-config startup-config

User level

read-write

Context

general

Example

```
G350-001(super)# copy running-config startup-config
```

Related commands

station, trunk-group, clear extension, show extension, clear trunk-group, show trunk-group, set max-ip-registrations, show max-ip-registrations, set pim-lockout, show pim-lockout, show, set fac, show fac, clear fac, set date-format, show date-format, set ip-codec-set, clear survivable-config, show last-pim-update, survivable-call-engine

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 the g350.cfg file on the TFTP server at IP address 135.64.10.33:

```
G350-001(super)# copy running-config tftp g350.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 announcement-file

Use the **copy scp announcement-file** command to download an announcement file from the Voice Announcements Manager to the G250/G350 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 the file “announcement_file1.wav” from the Voice Announcements Manager on host 192.168.49.10:

```
G350-001(super)# copy scp announcement-file c:\temp\announcement_file1.wav
192.168.49.10
```

To download the file “announcement_file1.wav” from the Voice Announcements Manager on host 192.168.49.10, and change the name to “local_announcement_file2”:

```
G350-001(super)# copy scp announcement-file c:\temp\announcement_file2.wav
192.168.49.10 local_announcement_file2
```

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

```
G350-001(super)# copy scp announcement-file c:\temp\announcement_file2.wav
192.168.49.10 “local announcement file2”
```

Related commands

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

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 `g350.lic` from the SCP site at IP address 198.87.134.153:

```
G350-001(super)# copy scp license-file g350.lic 198.87.134.153
```

Related commands

copy ftp license-file, copy tftp license-file, show download license-file status, show license status

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 G250/G350 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

```
G350-001# 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 ftp phone-image, copy ftp phone-script, copy tftp phone-image, copy tftp phone-script, 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 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

```
G350-001(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 the g350.cfg file on the FTP server at IP address 135.64.10.33:

```
G350-001(super)# copy startup-config ftp g350.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 the router1.cfg file on the SCP server at IP address 192.168.49.10:

```
G350-001(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 the g350.cfg file on the TFTP server at IP address 135.64.10.33:

```
G350-001(super)# copy startup-config tftp g350.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 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 require an additional TFTP server.

Note:

This command is not supported by the G250.

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 of mgr.cfg, from the TFTP server located at IP address 192.168.49.10:

```
G350-001(super)# copy tftp EW_archive c:\G350\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, dir, set boot bank, show boot bank, show download software status, show image version

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 `g350.lic` from the TFTP site at IP address 198.87.134.153:

```
G350-001(super)# copy tftp license-file g350.lic 198.87.134.153
```

Related commands

copy ftp license-file, copy scp license-file, show download license-file status, show license status

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, an additional TFTP server is not required.

Note:

Perform the **nvram initialize** command prior to the **copy tftp module** command.

Note:

This command is not supported by the G250.

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:

```
G350-001(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, dir, set boot bank, show boot bank, show download software status, show image version

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 G250/G350 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

```
G350-001(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, 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 G250/G350 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

```
G350-001(super)# copy tftp phone-scriptA file1.txt 135.64.100.205
Confirmation - do you want to continue (Y/N)? y
```

Related commands

copy ftp phone-image, copy ftp phone-script, copy scp phone-script, copy tftp phone-image, 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 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:

```
G350-001(super)# copy tftp startup-config c:\G350\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 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, an additional TFTP server is not required.

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:

```
G350-001(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, 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, an additional TFTP server is not required.

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:

```
G350-001(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, dir, set boot bank, show boot bank, show download software status, show image version

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:

```
G350-001(QoS 440/CompOp 12)# cos 3
```

Related commands

dscp (policy-based routing, packet sniffing, VPN), name, show composite-operation

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	Clear the Don't-Fragment bit		
copy	Copy the Don't-Fragment bit		

User level

read-write

Context

interface

Example

```
G350-001(if:Serial 5/1)# 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 G250/G350 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

Example

```
G350-001(if:Serial 5/1)# 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

```
G350-001(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	Encryption type: Encapsulation Security Protocol and Data Encryption Standard		
esp-3des	Encryption type: Encapsulation Security Protocol and Triple Data Encryption Standard		
esp-aes	Encryption type: Encapsulation Security Protocol and Advanced Encryption Standard using a 128-bit key		
esp-aes-192	Encryption type: Encapsulation Security Protocol and Advanced Encryption Standard using a 192-bit key		

Parameter	Description	Possible Values	Default Value
esp-aes-256	Encryption type: Encapsulation Security Protocol and Advanced Encryption Standard using a 256-bit key		
esp-null	Encryption type: Encapsulation Security Protocol without encryption. **Note**: This option is intended for lab testing.		
esp-md5-hmac	Authentication type: Encapsulation Security Protocol, md5 hashing and keyed-hash mac		
esp-sha-hmac	Authentication type: Encapsulation Security Protocol, secure hash algorithm and keyed-hash mac		
comp-lzs	IP compression with the LZS algorithm.		

User level

read-write

Context

general

Examples

Example 1: To configure an IPSec transform set with encryption and authentication:

```
G350-001(super)# crypto ipsec transform-set ts2 esp-des esp-md5-hmac
G350-001(config-transform:ts2)#
```

Example 2: To configure an IPSec transform set with encryption, authentication and IP compression:

```
G350-001(super)# crypto ipsec transform-set ts6 esp-des esp-md5-hmac
comp-lzs
G350-001(config-transform:ts6)#
```

Example 3: To configure an IPSec transform set with authentication only:

```
G350-001(super)# crypto ipsec transform-set ts3 esp-null esp-md5-hmac
G350-001(config-transform:ts3)#
```

Example 4: To enter the crypto IPSec transform-set context:

```
G350-001(super)# crypto ipsec transform-set ts1
G350-001(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

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

```
G350-001(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

```
G350-001(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

```
G350-001(super)# crypto isakmp peer address 149.49.70.1
G350-001(config-peer:149.49.70.1)#
```

```
G350-001(super)# crypto isakmp peer fqdn vpn.lnd.ny.avaya.com
G350-001(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

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 of up to 110 characters.	

User level

read-write

Context

general

Example

```
G350-001(super)# crypto isakmp peer-group vpn.avaya.com
G350-001(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

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

```
G350-001(super)# crypto isakmp policy 1
G350-001(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

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	The type of key to be generated.	**alphanumeric** or **hexadecimal**	**alphanumeric**

User level

read-write

Context

general

Examples

```
G350-001# crypto isakmp suggest-key
The suggest key: GNpi1odGNBrB5z4GJLz156jDmRWAGFES
```

```
G350-001# 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 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	The number of bits in the key	**512-2048**	1024

User level

admin

Context

general

Example

```
G350-001(super)# crypto key generate
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

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

Examples

```
G350-001(super)# crypto map 10
G350-001(config-crypto:10)#


G350-001(super)# no crypto map 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

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:

```
G350-001(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:

```
G350-001(router:rip)# default-metric 5
```

Related commands

default-metric (RIP), distribution-list, network (RIP), redistribute (RIP), timers basic

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), Fast Ethernet (L3, L2-L3), VLAN (L2-L3, L3), Tunnel (L2-L3, L3)

Example

To set the default metric to 10:

```
G350-001(if:FastEthernet 10/2)# default-metric 10
```

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:

```
G350-001(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

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

Example

To specify the for the VLAN 3 interface as “Marketing VLAN”:

```
G350-001(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

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

```
G350-001(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,

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

```
G350-001(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

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

```
G350-001(config-isakmp:1)# description "isakmp policy 1"
```

Related commands

authentication, crypto isakmp policy, encryption, group, hash, lifetime, show crypto isakmp policy

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

```
G350-001(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

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

```
G350-001(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

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

```
G350-001(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

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 enter a description for a simple object tracker tracking a single RTR:

```
G350-001(config-track rtr 1)# description "track rtr-2"
```

To enter a description for a Track List object tracker tracking several objects:

```
G350-001(config track list 10)# description "track list rtr-4 and
rtr-5"
G350-001(config track list 12)# description "track list rtr-4 and
list-10"
```

Related commands

object, threshold count, track, show track

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 specify that the current rule will apply to all packets that do *not* have this destination IP address.

Syntax

[no] destination-ip {host *ip*}|any|{*ip wildcard*}

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	A network 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 that 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:

```
G350-001(QoS 460/rule 22)# destination-ip host 135.64.104.102
```

To specify that rule 17 applies to packets whose destination IP address is in the range of 176.13.0.0 through 176.13.255.255:

```
G350-001(QoS 460/rule 17)# 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

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 disable the 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

Example

```
G350-001(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.		
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

Example

```
G350-001(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

dialer persistent

User level

read-write

Context

interface dialer

Example

```
G350-001(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

dialer persistent delay ***sec***

Parameters

Parameter	Description	Possible Values	Default Value
sec	Redial interval	**1-1000**	**20**

User level

read-write

Context

interface dialer

Example

```
G350-001(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 G250/G350 is reset 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

Example

```
G350-001(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

Example

```
G350-001(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

Example

```
G350-001(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

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

Example

```
G350-001(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

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

Example

```
G350-001(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

---

dir

Use the **dir** command to show the files that have been downloaded to the media gateway using the Avaya G250 and Avaya G350 CLI Reference Download interface and the SNMP MIB.

Syntax

dir [*module_number*]

Parameters

Parameter	Description	Possible Values	Default Value
module_number	Displays downloaded files for the specified module only.		

User level

read-only

Context

general

Example

To display a list of downloaded files:

```
G350-001(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 G350-A           24.6.0    SW RT Image  Flash Bank A   Software Image Bank A
10 G350-B           24.8.0    SW Component Flash Bank B   Software Image Bank B
```

```
10 G350              2.2.4     SW Web Image Nv-Ram         EmWeb application
10 G350-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
```

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, set boot bank, show boot bank, show download software status, show image version

disable link encryption

Use the **disable link encryption** command to disable H.248 signalling encryption.

Syntax

disable link encryption

User level

admin

Context

general

Example

To disable H.248 signalling encryption:

```
G350-001(super)# disable link encryption
```

disable media encryption

Use the **disable media encryption** command to disable Avaya media encryption (SRTP, AEA, RTP/AES).

Syntax

disable media encryption

User level

admin

Context

general

Example

To disable Avaya media encryption:

```
G350-001(super)# disable media encryption
```

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

distribution-list

Use the **distribution-list** command to apply a distribution policy rule for incoming or outgoing routing information in route updates. Use the **no** form of this command to deactivate the rule.

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 policy rule 10 to incoming router updates on the VLAN 1 interface:

```
G350-001(router:rip)# distribution-list 10 in "Vlan 1"
```

To apply distribution policy rule 20 to outgoing router updates on the Serial 2/1:1 interface:

```
G350-001(router:rip)# distribution-list 20 out "Serial 2/1:1":
```

To apply distribution policy rule 40 to outgoing router updates from OSPF:

```
G350-001(router:rip)# distribution-list 40 out ospf
```

Related commands

default-metric (RIP), network (RIP), redistribute (RIP), timers basic

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:

```
G350-001(DHCP 5)# dns-server 164.35.2.4
```

To set 164.35.2.4 and 135.64.102.3 as DNS IP addresses:

```
G350-001(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”:

```
G350-001(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

dscp (object tracking)

Use the **dscp** command to set the DSCP value for the packets of the RTR probes. Use the **no** form of this command to restore the value to the default value of 48.

Syntax

[no] dscp *dscp*

Parameters

Parameter	Description	Possible Values	Default Value
dscp	The dscp value	**0-63**	**48**

User level

read-write

Context

rtr type

Example

To set the DSCP value for RTR 1:

```
G350-001(config-rtr icmp 1)# dscp 42
```

Related commands

fail-retries, frequency, next-hop (object tracking), rtr, source-address, success-retries, type, wait-interval

dscp (policy)

Use the **dscp** command to specify the DSCP value that is set by the current policy operation. Use the **no** form of the command to specify that the current operation set the DSCP value to the default.

Syntax

dscp {*dscp_value* | no-change}

no dscp

Parameters

Parameter	Description	Possible Values	Default Value
dscp_value	The DSCP value	**0-63**	
no-change	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:

```
G350-001(QoS 440/CompOp 17)# 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

---

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 **no** form of the command to specify that the current operation set the DSCP value to the default.

Note:

In crypto-lists, this command is only applicable for rules whose action is **no protect**.

Syntax

dscp {*dscp_value* | any}

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.

Example

To specify that ip-rule 10 in crypto-list 901 match a DSCP value of 43:

```
G350-001(Crypto 901/ip rule 10)# dscp 43
```

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

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:

```
G350-001(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

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 E1 mode:

```
G350-001(super)# ds-mode t1
```

To change ds-mode, copy the running configuration to the start-up configuration file, and reset the device.

Related commands

cablelength long, cablelength short, channel-group, clock source, controller, framing, interface serial, ip address, linecode (E1), linecode (T1), remote, show controllers, show ds-mode

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	The default DoS classification for an ACL rule		
fraggle	User-defined DoS classification label usually used to report reception of Fraggle packets		
smurf	User-defined DoS classification label usually used to report reception of Smurf packets		
ip-spoofing	User-defined DoS classification label usually used to report reception of IP-spoofing packets		
other-attack-100	User-defined DoS classification label for any packet criteria		
other-attack-101	User-defined DoS classification label for any packet criteria		
other-attack-102	User-defined DoS classification label for any packet criteria		
other-attack-103	User-defined DoS classification label for any packet criteria		
other-attack-104	User-defined DoS classification label for any packet criteria		
other-attack-105	User-defined DoS classification label for any packet criteria		

User level

read-write

Context

ip access-control-list/ip-rule

Example

```
G350-001(config)# DoS-classification other-attack-101
```

Related commands

set security-association lifetime, show rtp-stat config

---

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:

```
G350-001(super-if:FastEthernet 1.1)# duplex full
```

Related commands

autoneg, shutdown (interface), speed (interface), traffic-shape rate

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 G250/G350 reports the BBL of the interface with the highest activation priority.

Syntax

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

Related commands

show dynamic-cac

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:

```
G350-001(if:Serial 2/1:1)# 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

---

encapsulation pppoe

Use the **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:

1. 'ip address' is configured on the interface
2. The interface is part of a backup scheme
3. Dynamic CAC is configured on the interface

Syntax

encapsulation pppoe

no encapsulation

Parameters

Parameter	Description	Possible Values	Default Value
pppoe	Keyword indicating that the encapsulation be set to PPP Power Over Ethernet.		

User level

read-write

Context

Interface: Fast Ethernet

Example

To create a PPPoE interface:

```
G350-001(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, show ppp authentication

---

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**

User level

read-write

Context

crypto isakmp policy

Example

```
G350-001(config-isakmp:1)# encryption 3des
```

Related commands

authentication, crypto isakmp policy, description (ISAKMP policy), group, hash, lifetime, show crypto isakmp policy

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

```
G350-001(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

enhanced security

Use the **enhanced security** command to activate enhanced-security mode which:

- Disables the following management protocols on the internal emb-vlan interface: TELNET, FTP, TFTP, SNMP
- Inhibits output data traffic during powerup/error states
- Inhibits modification of the active IPSEC transform-set parameters
- In the G250 only: the G250 switches from performing symmetric encryption with a hardware accelerator, to software-based encryption

Note:

This command can only be executed on FIPS-ready hardware.

Syntax

enhanced security

User level

Read-write

Context

general

Example

```
G350-001(super)# enhanced security
```

Related commands

show self-test-status, show system, zeroize

erase announcement-file

Use the **erase announcement-file** command to erase an announcement file in the G250/G350 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

```
G350-001# erase announcement-file local_announcement1.wav
```

Related commands

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

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

```
G350-001# 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, 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

```
G350-001(super)# erase phone-scriptA
Beginning erase operation .... Done!
```

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 346.

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

---

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:

```
G350-001(ACL 330/ip rule 22)# exit
G350-001(ACL 330)# exit
G350-001(super)#
```

Related commands

reset, set logout, show logout

fail-retries

Use the **fail-retries** command to specify how many consecutive unanswered probes change the status of an RTR operation device from up to down. Use the **no** form of this command to restore the value to the default.

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 type

Example

To set the fail-retries value for RTR 1:

```
G350-001(config-rtr icmp 1)# fail-retries 4
```

Related commands

dscp-table, frequency, next-hop (object tracking), rtr, source-address, success-retries, type, wait-interval

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-classs frame-relay context, to control the specific DLCI queueing parameters.

Syntax

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: 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

Example

```
G350-001(super-if:FastEthernet 10/2)# fair-queue-limit 500
```

Related commands - WFVQ

fair-voip-queue, voip-queue, voip-queue-delay

---

fair-voip-queue

Use the **fair-voip-queue** command to enable Weighted Fair VoIP Queuing (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 queuing mode for all Serial interfaces and all Fast Ethernet interfaces for which traffic-shaping is enabled. To disable WFVQ, you must enable another queuing 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: 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

Example

```
G350-001(super-if:FastEthernet 10/2)# fair-voip-queue
```

Related commands - WFVQ

fair-queue-limit, voip-queue, voip-queue-delay

---

fan speed level low

Use the **fan speed level low** command to enable the low cooling fan speed. Use the **no fan speed level low** form of this command to disable the low cooling fan speed.

The fan speed will rise automatically if the working temperature of the branch gateway exceeds a pre-determined limit.

Note:

This command only applies to the following hardware versions:

- G250 HW Vintage 00; Hardware Suffix E, or higher
- G350 HW Vintage 00; Hardware Suffix D, or higher

Syntax

[no] fan speed level low

User level

read-write

Context

general

Example

```
G350-001# fan speed level low
G350-001# no fan speed level low
```

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**	

User level

read-write

Context

Interface: Controller (T1)

Example

To set the FDL type to ansi:

```
G350-001(controller:5/1)# fdl ansi
```

fragment

Use the **fragment** command to apply the 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

```
G350-001(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

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:

```
G350-001(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 undergoing 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:

```
G350-001(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:

```
G350-001(super)# fragment timeout 30
```

Related commands

clear fragment, fragment chain, fragment size, show fragment

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”:

```
G350-001(super-if:Serial 2/1:1)#frame-relay class-dlci 17 myVoIpClass
```

Related commands

clear frame-relay counters, interface serial, map-class frame-relay, show frame-relay map, show frame-relay pvc brief, show interfaces

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 will create and associate 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.

```
G350-001(super-if:Serial 2/1:1)# frame-relay interface-dlci 17
```

Related commands

encapsulation, 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

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_interval*

Parameters

Parameter	Description	Possible Values	Default Value
polling_interval	Interval in seconds	**1-255**	**6**

User level

read-write

Context

Interface: Serial (DS1 FR L2, USP FR L2)

Example

To set the number of seconds between status enquiry messages to 17 seconds:

```
G350-001(if:Serial 2/1:1)# frame-relay lmi-n391dte 17
```

Related commands

encapsulation, 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

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:

```
G350-001(if:Serial 2/1:1)# frame-relay lmi-n392dte 5
```

Related commands

encapsulation, 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

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 203. 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:

```
G350-001(if:Serial 2/1:1)# frame-relay lmi-n393dte 5
```

Related commands

encapsulation, 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

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:

```
G350-001(if:Serial 2/1:1)# frame-relay lmi-type q933a
```

Related commands

encapsulation, 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

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:

```
G350-001(if:Serial 2/1:1.1)# frame-relay priority-dlci-group 17 18 19
```

Related commands

encapsulation, 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

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:

```
G350-001(if:Serial 2/1:1)# frame-relay traffic-shaping
```

Related commands

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, ip address

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:

```
G350-001(controller:5/1)# framing esf
```

Related commands

cablelength long, cablelength short, channel-group, clock source, controller, ds-mode, interface serial, ip address, linecode (E1), linecode (T1), remote, show controllers

frequency

Use the **frequency** command to specify how often to send RTR probes. Use the **no** form of this command to restore the frequency value to the default.

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	Specifies to set the frequency of RTR probes in units of seconds		
milliseconds	Specifies to set the frequency of RTR probes in units of milliseconds		

User level

read-write

Context

rtr type

Example

To set the frequency value for RTR 1

```
G350-001(config-rtr icmp 1)# frequency 20 seconds
```

Related commands

dscp-table, fail-retries, next-hop (object tracking), rtr, source-address, success-retries, type, wait-interval

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

```
G350-001(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

```
G350-001(config-isakmp:1)# hash md5
```

Related commands

authentication, crypto isakmp policy, description (ISAKMP policy), encryption, group, lifetime, show crypto isakmp policy

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	**G250 or G350**

User level

read-write

Context

general

Example

To set the CLI prompt to “GTW-HQ”:

```
G350-001(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
G350-001(super)#
```

Related commands

banner login, banner post-login, clear screen, line, show banner login, show banner post-login, terminal length, terminal width

---

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:

```
G350-001(super)# interface vlan 2
G350-001(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

icmp

Use the **icmp** command to specify that the current rule applies to a specific type of ICMP packet. Use the **no** form of this command to specify that the rule applies to all packets *except* those of the specified ICMP type.

Note:

The icmp command also sets the IP protocol to ICMP.

Syntax

[no] icmp {*name* | {*icmp_type icmp_code*}}

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

Example

To specify that rule 33 applies to any ICMP packet type except type 1 code 2:

```
G350-001(ACL 333/ip rule 33)# no icmp 1 2
```

To specify that rule 27 applies to ICMP error-reply packets:

```
G350-001(ACL 333/ip rule 27)# icmp Echo-Reply
```

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

---

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 the limit to its default value.

Syntax

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:

```
G350-001(super)# icmp in-echo-limit 500
```

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:

```
G350-001(if:Serial 2/1)# 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:

```
G350-001(if:Serial 2/1:1)# ignore dcd
```

Related commands

bandwidth, idle-character, interface serial, invert txclock, nrzi-encoding, transmitter-delay

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	Specifies that the device operate in IKE main mode		
aggressive	Specifies that the device operate in IKE aggressive mode. Specify this option when local IP is dynamic.		
none	Specifies 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

```
G350-001(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

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:

```
G350-001(super)# interface Console
G350-001(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 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

Example

```
G350-001(super)# interface dialer 1
G350-001(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 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	**2**	
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:

```
G350-001(super)# interface FastEthernet 10/2
```

To create a Level 3 sub-interface on the FastEthernet interface:

```
G350-001(super)# interface FastEthernet 10/2.1
```

To remove the Level 3 sub-interface:

```
G350-001(super)# no 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 Interface Loopback 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:

```
G350-001(super)# interface Loopback 1
```

To create a Layer 3 sub-interface:

```
G350-001(super)# interface Loopback 1.1
```

To delete the Layer 3 sub-interface:

```
G350-001(super)# no interface Loopback 1.0
```

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
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:

```
G350-001(super)# interface Serial 2/1:2.17 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 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:

```
G350-001(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 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 interface context:

```
G350-001(super)# interface USB-Modem
G350-001(super-if:USB-Modem)#
```

Related commands - IP interface configuration

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 interface brief

Related commands - Modem configuration

async modem-init-string, interface Console, ppp chap-secret

---

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	**1-3071**	
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:

```
G350-001(super)# interface Vlan 2
```

To create a sub interface 1 on VLAN 2:

```
G350-001(if:Vlan 2)# interface Vlan 2.1
```

To delete sub interface 1 of VLAN 2:

```
G350-001(super)# no 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

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 type

Related commands

dscp-table, fail-retries, frequency, next-hop (object tracking), rtr, source-address, success-retries, type, wait-interval

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:

```
G350-001(if:Serial 2/1:1)# invert txclock
```

Related commands

bandwidth, idle-character, ignore dcd, interface serial, nrzi-encoding, transmitter-delay

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.

Syntax

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:

```
G350-001(super)# ip access-control-list 320
G350-001(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

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), Tunnel (L2, L2-L3), VLAN (L2, L2-L3)

Example

To enable access control list 310 for outbound packets on the FastEthernet interface:

```
G350-001(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 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: 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), Console, USB, Loopback (L2-L3, L3), Tunnel (L2-L3, L3), Dialer

Example

To assign the IP address 192.168.22.33 with mask 255.255.255.0 to the Fast Ethernet interface:

```
G350-001(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 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 Fast Ethernet interface.
You cannot configure both **ip address dhcp** and **keepalive-icmp** (extended keepalive) on the WAN Fast Ethernet interface.
You cannot configure both **ip address dhcp** and **ip address negotiated** (PPP/IPCP address negotiation) on the WAN Fast Ethernet 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: Fast Ethernet

Example

```
G350-001(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 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 Fast Ethernet interface.

Syntax

[no] ip address negotiated

User level

read-write

Context

Interface: Dialer, FastEthernet (PPPoE only)

Example

```
G350-001(config-if:FastEthernet 10/2)# ip address negotiated
```

Related commands

ppp ipcp dns request

---

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)

Example

```
G350-001(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 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-L3, L2), VLAN (L2-L3, L2)

Example

To select the network 192.168.169.0 as the network from which an address should be allocated for BOOTP/DHCP requests:

```
G350-001(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:

```
G350-001(super)# ip bootp-dhcp relay
```

To disable relaying of BOOTP and DHCP requests:

```
G350-001(super)# no 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-L3, L2), VLAN (L2-L3, L2)

Example

To add station 192.168.37.46 as a BOOTP/DHCP server to handle BOOTP/DHCP requests:

```
G350-001(if:Vlan 1.2)# ip bootp-dhcp server 192.168.37.46
```

Related commands

ip bootp-dhcp network, ip bootp-dhcp relay

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), VLAN (L2-L3, L3)

Example

To set the broadcast address for the VLAN 1 interface to 192.168.255.255:

```
G350-001(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

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

```
G350-001(super)# ip capture-list 501
G350-001(super-Cap 501)#
```

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, name, show capture, show capture-buffer hex

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

Examples

```
G350-001(if:Serial 5/1)# no ip crypto-group
G350-001(if:Serial 5/1)# 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

```
G350-001(super)# ip crypto-list 901
G350-001(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 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 that 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:

```
G350-001(super)# ip default-gateway 132.55.4.45 4 high track 20
```

To set the default gateway to be the Serial interface:

```
G350-001(super)# ip default-gateway Serial 5/1:1.1 permanent
```

To remove the default gateway:

```
G350-001(super)# no ip default-gateway
```

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

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:

```
G350-001(super)# ip dhcp activate pool 5
```

To deactivate DHCP pool 5:

```
G350-001(super)# no 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 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: Fast Ethernet

Example

```
G350-001(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 G250 or G350'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: Fast Ethernet

Example

```
G350-001(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: Fast Ethernet

Examples

```
G350-001(config-if:FastEthernet 10/2)#ip dhcp client lease 1 4 15
G350-001(config-if:FastEthernet 10/2)#ip dhcp client lease 1 2
G350-001(config-if:FastEthernet 10/2)#ip dhcp client lease 1
```

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 request 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
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: Fast Ethernet

Example

```
G350-001(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.

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: Fast Ethernet (not running ARPA)

Example

```
G350-001(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

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:

```
G350-001(super)# ip dhcp pool 5
G350-001(DHCP 5)#
```

To delete pool 5:

```
G350-001(super)# no ip dhcp pool 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

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 not to send ping packets to an IP address before assigning the IP address to a requesting client:

```
G350-001(DHCP 5)# no 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:

```
G350-001(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-server

By default, DHCP server is inactive. Use the **dhcp-server** command to activate the DHCP server on the G350. 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:

```
G350-001(super)# ip dhcp-server
```

To disable DHCP server:

```
G350-001(super)# no 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

---

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), VLAN (L2-L3, L3)

Related commands

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

---

ip distribution access-default-action

Use the **ip distribution access-default-action** command to set the default action for a specific RIP distribution policy list.

Syntax

ip distribution access-default-action *list_number default_action*

Parameters

Parameter	Description	Possible Values	Default Value
list_number	The distribution list number	**1-99**	
default_action	The default action	**default-action-deny, default-action-permit**	

User level

read-write

Context

general

Example

To specify the default action for distribution policy list 1 is to deny packets:

```
G350-001(super)# ip distribution access-default-action 1
default-action-deny
```

ip distribution access-list

Use the **ip distribution access-list** command to create a distribution Policy rule. Use the **no** form of this command to delete a distribution list rule. Apply the distribution rule using the **distribution-list** command.

Syntax

ip distribution access-list *policy_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
policy_list_number	The policy 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:

```
G350-001(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:

```
G350-001(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:

```
G350-001(super)# ip distribution access-list 20 4 permit any
```

To remove RIP distribution access list number 2:

```
G350-001(super)# no ip distribution access-list 2 25
```

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:

```
G350-001(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:

```
G350-001(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”:

```
G350-001(super)# ip distribution access-list-name 5 evening
```

To name distribution access-list #22 as “Daily Job”:

```
G350-001(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:

```
G350-001(super)# ip distribution access-list-owner 78 "Jane Wiley"
```

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

Examples

```
G350-001(super)# ip domain list 2 support.avaya.com
G350-001(super)# no ip domain list 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

```
G350-001(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

```
G350-001(super)# ip domain name-server-list 1
G350-001(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

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

```
G350-001(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

```
G350-001(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

ip http

Use the **ip http** command to enable the HTTP server. Use the **no** form of the command to disable the HTTP server.

Note:

This command is not supported by the G250.

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

ip icmp

Use the **ip icmp** command to enable ICMP services. Use the **no** form of the command to disable ICMP services.

Syntax

ip icmp [echo]

no ip icmp

Parameters

Parameter	Description	Possible Values	Default Value
echo	Enables ICMP only for echo packets and destination unreachable packets		

User level

read-write

Context

general

ip icmp redirect

Use the **ip icmp redirect** command to enable the ICMP redirect service. If the ICMP service is down, the command fails and returns an error message. Use the **no** form of the command to disable the ICMP redirect service.

Syntax

[no] ip icmp redirect

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

show ip icmp

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:

```
G350-001(super)# ip max-arp-entries 8000
```

To restore the maximum number of ARP cache entries to the default value:

```
G350-001(super)# no ip max-arp-entries
```

Related commands

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

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 L3, USP PPP L2-L3), FastEthernet (L2-L3, L3), VLAN (L2-L3, L3)

Example

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

```
G350-001(if:FastEthernet 10/2)# ip netbios-rebroadcast both
```

Related commands

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

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:

```
G350-001(super)# ip netmask-format bitcount
```

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

```
G350-001(super)# ip next-hop-list 2
G350-001(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

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), VLAN (L2-L3, L3), Loopback (L2-L3, L3), Tunnel (L3, L2-L3)

Example

To set the OSPF authentication for the FastEthernet interface as “message-digest”:

```
G350-001(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), VLAN (L2-L3, L3), Loopback (L2-L3, L3), Tunnel (L3, L2-L3)

Example

To set the authentication password for the VLAN 1 interface as “my_pass”:

```
G350-001(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), VLAN (L2-L3, L3), Loopback (L2-L3, L3), Tunnel (L3, L2-L3)

Example

To set the cost metric for the VLAN 1 interface to 10:

```
G350-001(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), VLAN (L2-L3, L3), Loopback (L2-L3, L3), Tunnel (L3, L2-L3)

Example

To specify an interval of 15 seconds to wait before declaring a neighbor dead:

```
G350-001(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), VLAN (L2-L3, L3), Loopback (L2-L3, L3), Tunnel (L3, L2-L3)

Example

To specify an interval of five seconds between hello packets:

```
G350-001(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		**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), VLAN (L2-L3, L3), Loopback (L2-L3, L3), Tunnel (L3, L2-L3)

Example

To specify the message-digest key to be 3 with password mypwd:

```
G350-001(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), VLAN (L2-L3, L3), Loopback (L2-L3, L3), Tunnel (L3, L2-L3)

Example

To specify a network type of point-to-multipoint for the VLAN 1 interface:

```
G350-001(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), VLAN (L2-L3, L3), Loopback (L2-L3, L3), Tunnel (L3, L2-L3)

Example

To set the interface OSPF priority to 17:

```
G350-001(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:

```
G350-001(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

---

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

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), VLAN (L2, L2-L3), Loopback (L2, L2-L3), Tunnel (L2, L2-L3)

Example

```
G350-001(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

```
G350-001(super)# ip pbr-list 802
G350-001(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

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

Example

To configure the USB interface to offer requesting calling hosts the IP address 192.168.49.2:

```
G350-001(super-if:USB-Modem)# ip peer address 192.168.49.2
```

Related commands

async mode interactive, async mode terminal, async modem-type, ip address, ppp authentication, shutdown (interface), speed (PPP), timeout absolute

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:

```
G350-001(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 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 disable proxy ARP on an interface:

```
G350-001(if:Vlan 1)# no ip proxy-arp
```

Related commands

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

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

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), VLAN (L2, L2-L3), Loopback (L2, L2-L3), Tunnel (L2, L2-L3)

Example

To apply QoS list 440 to all incoming packets on the Vlan 1 interface:

```
G350-001(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:

```
G350-012# ip qos-list 440
G350-012(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

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), VLAN (L2-L3, L3)

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), VLAN (L2-L3, L3), Loopback (L2-L3, L3), Tunnel (L2-L3, L3)

Example

To set the authentication string on the VLAN 1 interface to “hush-hush”:

```
G350-001(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), VLAN (L2-L3, L3), Loopback (L2-L3, L3), Tunnel (L2-L3, L3)

Example

To specify that RIP packets use simple authentication mode:

```
G350-001(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), VLAN (L2-L3, L3), Loopback (L2-L3, L3), Tunnel (L2-L3, L3)

Example

To specify that the RIP protocol sends, but does not receive, default route updates on the VLAN 1 interface:

```
G350-001(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), VLAN (L2-L3, L3), Loopback (L2-L3, L3), Tunnel (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), VLAN (L2-L3, L3), Loopback (L2-L3, L3), Tunnel (L2-L3, L3)

Example

To specify that RIP version 2 packets should be running on the Serial 2/1:1 interface:

```
G350-001(if:Serial 2/1:1)# 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), VLAN (L2-L3, L3), Loopback (L2-L3, L3), Tunnel (L2-L3, L3)

Example

To set the RIP protocol to receive and transmit update on the Serial interface:

```
G350-001(if:Serial 2/1:1)# 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), VLAN (L2-L3, L3), Loopback (L2-L3, L3), Tunnel (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

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

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 Fast Ethernet interface on which DHCP address negotiation is configured, you must specify the interface type as the Fast Ethernet 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**

Parameter	Description	Possible Values	Default Value
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:

```
G350-001(super)# ip route 132.55.0.0 255.255.0.0 132.55.4.45 3 high
track 6
```

To remove the static route defined for IP address 134.66.0.0:

```
G350-001(super)# no ip route 134.66.0.0 255.255.0.0
```

To create a static discard route on IP address 134.66.0.0:

```
G350-001(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:

```
G350-001# ip route 1.1.1.0 255.255.255.0 FastEthernet 10/2
```

Related commands

clear ip route, ip default-gateway, 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

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-L3, DS1 PPP L2, DS1 FR-SUB L2-L3, DS1 FR-SUB L2, USP PPP L2, USP PPP L2-L3)

Example

To allow 48 RTP connections on the Serial interface:

```
G350-001(if:Serial 2/1:1.1) 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-L3, DS1 PPP L2, DS1 FR-SUB L2-L3, DS1 FR-SUB L2, USP PPP L2, USP PPP L2-L3)

Example

To enable RTP and TCP header compression on a serial interface:

```
G350-001(config-if:Serial 2/1:1.1) 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-L3, DS1 PPP L2, DS1 FR-SUB L2-L3, DS1 FR-SUB L2, USP PPP L2, USP PPP L2-L3)

Example

To allow a maximum of 512 compressed headers to be sent before a full header must be sent:

```
G350-001(config-if:Serial 2/1:1.1)# 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-L3, DS1 PPP L2, DS1 FR-SUB L2-L3, DS1 FR-SUB L2, USP PPP L2, USP PPP L2-L3)

Example

To allow no more than 15 seconds to pass between the sending of full headers:

```
G350-001(if:Serial 2/1:1.1)# 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

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-L3, DS1 PPP L2, DS1 FR-SUB L2-L3, DS1 FR-SUB L2, USP PPP L2, USP PPP L2-L3)

Example

To set the Serial interface to perform IPHC RFC header compression:

```
G350-001(if:Serial 2/1:1.1)# 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

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-L3, DS1 PPP L2, DS1 FR-SUB L2-L3, DS1 FR-SUB L2, USP PPP L2, USP PPP L2-L3)

Example

To specify that ports in the range 49,152 through 65535 are RTP ports:

```
G350-001(if:Serial 2/1:1.1)# 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 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**	
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), Tunnel (L2, L2-L3), VLAN (L2, L2-L3)

Example

To simulate the effects of applying access control list 330 to a packet entering the media gateway through the Fast Ethernet interface, from IP address 192.67.85.12 to IP address 192.67.54.25:

```
G350-001(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

ip snmp-server

Use the **ip snmp-server** command to enable the SNMP agent for the G350. Use the **no** form of the command to disable the SNMP agent for the G350. Disabling the SNMP agent also blocks SNMP traps. However, users can change SNMP configuration settings even when the agent is disabled.

Syntax

ip snmp-server [volatile]

no ip snmp-server

Parameters

Parameter	Description	Possible Values	Default Value
volatile	Specifies that the SNMP agent is only enabled temporarily, until the system is reset		

User level

admin

Context

general

Example

```
G350-001(ACL 330)(super)# ip snmp-server volatile
```

Related commands - SNMP access configuration

set snmp community, set snmp retries, set snmp timeout, show port trap, show snmp, show snmp engineID, show snmp group, show snmp retries, show snmp timeout, show snmp user, show snmp user summary, 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

clear snmp trap, set port trap, set snmp 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

---

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 G250/G350 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 G250/G350 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

Related commands

clear ssh-client known-hosts, crypto key generate, disconnect ssh, show ip ssh

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-L3, DS1 PPP L2, DS1 FR-SUB L2-L3, DS1 FR-SUB L2, USP PPP L2, USP PPP L2-L3)

Example

```
G350-001(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-L3, DS1 PPP L2, DS1 FR-SUB L2-L3, DS1 FR-SUB L2, USP PPP L2, USP PPP L2-L3)

Example

To enable TCP header compression on a Serial interface:

```
G350-001(if:Serial 2/1:1.1) 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

ip telnet

Use the **ip telnet** command to enable the Telnet server. 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 708).

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

genera

Related commands

ip telnet-client, 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 708).

Syntax

[no] ip telnet-client

User level

admin

Context

general

Related commands

ip telnet, telnet

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

```
G350-001(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 fie size in Kb	**256-19456**	**18560**

User level

Read-write

Context

general

Example

```
G350-001# 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

ip unnumbered

Use the **ip unnumbered** command to configure an interface to borrow an IP address from another interface. 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	**Fast Ethernet** **Serial** **Vlan** **Loopback** **Tunnel** **Dialer**	
identifier	The identifier depends on the interface type: For Fast Ethernet: ***module/port*** For Serial: ***module/port:channel-group*[*.sub-interface*]** For Vlan: ***vlan-id*** For loopback: ***interface-number***	 channel-group: E1: **0-30** T1: **0-23** vlan-id: **1-3071** interface-number: integer **1-50**	

Parameter	Description	Possible Values	Default Value
	For Tunnel: ***interface-number***	interface-number: integer **1-50**	
	For Dialer: ***interface-number***	interface-number: integer **1**	

Context

Interface: Dialer, Serial (DS1 PPP L2, DS1 PPP L2-L3, DS1 FR-SUB L2, DS1 FR-SUB L2-L3, USP PPP L2, USP PPP L2-L3) Tunnel (L2, L2-L3)

User level

read-write

Example

```
G250-001(super-if:Dialer 1)# ip unnumbered 1 loopback 1
G250-001(super-if:Dialer 1)# ip unnumbered 2 vlan 1
G250-001(super-if:Dialer 1)# ip unnumbered 3 serial 2/1:1
G250-001(super-if:Dialer 1)# ip unnumbered 4 serial 2/1:1
```

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*

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 create virtual router #1 on the Vlan 2 interface:

```
G350-001(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:

```
G350-001(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”:

```
G350-001(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:

```
G350-001(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:

```
G350-001(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:

```
G350-001(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:

```
G350-001(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:

```
G350-001(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

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:

```
G350-001(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 treatment of packets carrying an IP option that enter the current interface. 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:

```
G350-001(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-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 this command to specify that the current rule applies to all packets *except* those having the specified IP protocol.

Syntax

[no] ip-protocol *protocol_name* | *protocol_number*

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

Example

To specify that rule 22 applies to all packets having an IP protocol of IGMP:

```
G350-001(ACL 330/ip rule 22)# 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

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	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:

```
G350-001(ACL 330)# ip-rule 22
G350-001(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

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	ip-rule number 10,000 (last rule in the ordered list of rules)		

User level

read-write

Context

ip crypto-list

Example

```
G350-001(Crypto 901)# ip-rule 21
G350-001(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

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

```
G350-001(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-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 Fast Ethernet 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:

```
G350-001(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

```
G350-001(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

```
G350-001(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

```
G350-001(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

```
G350-001(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

```
G350-001(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

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 Fast Ethernet 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: FastEthernet
crypto isakmp peer

Example

To register a remote VPN peer with an object tracker:

```
G350-001(config-peer:149.49.70.1)# keepalive-track 5
```

To register the FastEthernet interface with an object tracker:

```
G350-001(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

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 hosts that send packets to the tunnel that the tunnel is down, although 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

```
G350-001(super if:Tunnel 1)# tunnel keepalive 10 3
```

Related commands

tunnel checksum, tunnel destination, tunnel key, tunnel path-mtu-discovery, tunnel source, tunnel ttl

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:

```
G350-001(if:Serial 2/1)# keepalive 300
```

Related commands

encapsulation, ip address, ppp timeout ncp, ppp timeout retry, show interfaces

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**	
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

```
G350-001(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

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:

```
G350-001(DHCP 5)# lease 86400
```

Related commands

interface serial, ppp ipcp dns request, show interfaces,

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 min. to 24 hrs)**	**86,400**

User level

read-write

Context

crypto isakmp policy

Example

```
G350-001(config-isakmmp:1)# lifetime 100
```

Related commands

authentication, crypto isakmp policy, description (ISAKMP policy), encryption, group, hash, show crypto isakmp policy

---

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:

```
G350-001(super-banner-post-login)# line 3 "Welcome to the G350 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

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:

```
G350-001(controller:5/1)# linecode ami
```

Related commands

cablelength long, cablelength short, channel-group, clock source, controller, ds-mode, framing, interface serial, ip address, linecode (T1), remote, show controllers

---

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:

```
G350-001(controller:5/1)# linecode ami
```

Related commands

cablelength long, cablelength short, channel-group, clock source, controller, ds-mode, framing, interface serial, ip address, linecode (E1), remote, show controllers

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

Example

To set the load calculation interval to 60 seconds:

```
G350-001(if:Serial 2/1:1)# 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

local-address

Use the **local-address** command to set the local IP address for the IPSec tunnels derived from this 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--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

Examples

```
G350-001(crypto 901)# local-address 192.168.49.1
G350-001(crypto 901)# local-address FastEthernet 10/2.0
G350-001(crypto 901)# local-address Serial 2/1:10
```

Related commands

description (ip rule), destination-ip, ip crypto-list, ip-rule (VPN), protect crypto map, source-ip, show ip crypto-list

---

loopback diag

Use the **loopback diag** command to activate a Loopback signal on the Serial interface. Use the **no** form of the command to deactivate the Loopback signal.

Syntax

[no] loopback diag

User level

read-write

Context

Interface: Controller

Example

To activate a Loopback signal on the current interface:

```
G350-001(if:Serial 5/1)# loopback diag
```

Related commands

loopback local, loopback remote

---

loopback local

Use the **loopback local** command to activate a Loopback signal on the Serial interface. Use the **no** form of the command to deactivate the Loopback signal.

Syntax

loopback local *loopback_type*

no loopback local

Parameters

Parameter	Description	Possible Values	Default Value
loopback_type	The type of information to loop back	**line**, **payload**	

User level

read-write

Context

Interface: Controller

Example

To activate a loopback signal with payload information:

```
G350-001(if:Serial 5/1)# loopback local payload
```

Related commands

loopback diag, loopback remote

loopback remote

Use the **loopback remote** command to request a remote station to activate a Loopback signal on the Serial interface. Use the **no** form of the command to deactivate the Loopback signal.

Syntax

loopback remote *loopback_type*

no loopback remote

Parameters

Parameter	Description	Possible Values	Default Value
loopback_type	The type of information to loop back	**line**, **payload**	

User level

read-write

Context

Interface: Controller (T1)

Example

To request that a loopback signal be sent with payload information:

```
G350-001(if:Serial 5/1)# loopback remote payload
```

Related commands

loopback diag, loopback local

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:

```
G350-001(super)# map-class frame-relay mySVoip1
G350-001(super-map-class)#
```

Related commands

clear frame-relay counters, frame-relay class-dlci, interface serial, show frame-relay map, show frame-relay pvc brief, show interfaces

---

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	IPSec VPN tunnel mode. This is the default setting.		
transport	IPSec VPN transport mode. **Note**: Specify this mode only for a GRE tunnel.		

User level

read-write

Context

crypto ipsec transform-set

Example

```
G350-001(config-transform:ts1)# mode tunnel
```

Related commands

crypto ipsec transform-set, set pfs, set security-association lifetime, show crypto ipsec transform-set

---

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)

Example

To specify the Maximum Transmission Unit for the Serial 2/1:1 interface to be 1000 bytes:

```
G350-001(if:Serial 2/1:1)# 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, show ppp authentication

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”:

```
G350-001(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)

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:

```
G350-001(name-server-list:1)# name-server 2 1.1.1.1
```

To delete all static DNS servers from list 1:

```
G350-001(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

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:

```
G350-001(router:rip)# network 192.168.37.0
```

Related commands

default-metric (RIP), distribution-list, redistribute (RIP), timers basic

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:

```
G350-001(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

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

Examples

```
G350-001(super)# next-hop list 1
G350-001(super)# next-hop DBR
```

Related commands

destination-ip, dscp (policy-based routing, packet sniffing, VPN), show ip next-hop-list, show isdn bri link

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:

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 type

Examples

```
G350-001(config-rtr icmp 1)# next-hop FastEthernet 10/2 interface-name
00:04:d0:af:12:4 mac-address
G350-001(config-rtr icmp 1)# next-hop Serial 2/1:1 interface-name
```

Related commands

dscp-table, fail-retries, frequency, interface-keepalive bypass-logic, rtr, source-address, success-retries, type, wait-interval

next-hop-interface

Use the **next-hop-interface** command to add the specified interface to the next hop path for this 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 that 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

```
G350-001(config-next hop list 1)# next-hop-interface 3 Serial 5/1:0
track 1
```

```
G350-001(config-next hop list 2)# next-hop-interface 5 FastEthernet
10/2
```

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 this 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
hop_number	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

```
G350-001(super)# next-hop-ip 2 149.49.200.2 track 3
```

Related commands

next-hop-interface, show next-hop

---

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:

```
G350-001(DHCP 5)# next-server 1.1.1.1
```

To clear the next server IP address:

```
G350-001(DHCP 5)# no next-server
```

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

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)

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

```
G350-001(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

---

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 190).

CAUTION:

This command erases all announcement files in the G250/G350 announcement directory.

Syntax

nvram initialize

User level

read-write

Context

general

Example

To reset the configuration parameters for the device:

```
G350-001(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

---

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	A 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

```
G350-001(config-track list 2)# object 3
```

Related commands

description (object tracking), threshold count, track, show track

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 following are exceptions: 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:

```
G350-001(DHCP 5)# option 42
G350-001(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

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”:

```
G350-001(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

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 Fast Ethernet interface:

```
G350-001(router:ospf)# passive-interface FastEthernet 10/2.1
```

To suppress OSPF routing updates on the interface at IP address 192.168.1.1:

```
G350-001(router:ospf)# passive-interface 192.168.1.1
```

Related commands

area, default-metric (OSPF), network (OSPF), redistribute (OSPF), timers spf

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 three seconds, timing out after five seconds:

```
G350-001(super)# ping 192.168.49.1 3 50 5 192.168.49.4
```

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)

Example

To define the VLAN 1 interface as the Primary Management Interface:

```
G350-001(super)# interface vlan 1
G350-001(super-if:Vlan 1)# pmi
```

Related commands

show pmi

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}

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	Reserved for future use		
none	Keyword indicating that no password is sent		

User level

read-write

Context

Interface: Console, USB

Example

To select the CHAP authentication protocol:

```
G350-001(if:CON)# ppp authentication chap
```

Related commands

async mode interactive, async mode terminal, async modem-type, async reset-modem (USB port), ip address, shutdown (interface), shutdown (USB modem), speed (PPP), timeout absolute

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: Fast Ethernet

Example

```
G350-001(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, show ppp authentication

---

ppp chap password

Use the **ppp chap password** command to set the CHAP password for authentication with a remote peer.

Note:

Executing the **copy running-config startup-config** command stores the configured CHAP password to the NVRAM and not to the 'startup-config' file.

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

ppp chap password *secret*

Parameters

Parameter	Description	Possible Values	Default Value
secret	The CHAP password.		

User level

Read-write

Context

Interface: Fast Ethernet

Example

```
G350-001(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, show ppp authentication

---

ppp chap refuse

Use the **ppp chap refuse** command to prevent authentication with CHAP, even when a chap secret is configured.

Syntax

ppp chap refuse

no ppp chap refuse

User level

Read-write

Context

Interface: Fast Ethernet

Example

```
G350-001(super-if:FastEthernet 10/2)# ppp chap refuse
```

Related commands

interface FastEthernet, ppp pap refuse

ppp chap-secret

Use the **ppp chap-secret** command to configure the shared secret used in PPP sessions with CHAP authentication.

Note:

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

Syntax

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

Example

To set the shared secret to “mypwd3”:

```
G350-001(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 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

[no] ppp ipcp dns request

User level

read-write

Context

Interface: Dialer, FastEthernet (PPPoE only)

Example

```
G350-001(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: Fast Ethernet

Example

```
G350-001(super-if:FastEthernet 10/2)# ppp pap refuse
```

Related commands

interface FastEthernet, 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:

Executing the **copy running-config startup-config** command stores the configured username/password to the NVRAM and not to the 'startup-config' file.

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: Fast Ethernet

Example

```
G350-001(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, show ppp authentication

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: Serial (DS1 PPP L2-L3, DS1 PPP L2, USP PPP L2-L3, USP PPP L2)

Example

To specify that PPP will allow 60 seconds for negotiation of a network protocol:

```
G350-001(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: Serial (DS1 PPP L2-L3, DS1 PPP L2, USP PPP L2-L3, USP PPP L2)

Example

To specify that PPP will wait up to 30 seconds for a response during negotiation:

```
G350-001(super)# ppp timeout retry seconds
```

Related commands

encapsulation, ip address, keepalive (PPP), ppp timeout ncp, show interfaces

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: Fast Ethernet

Example

```
G350-001(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, show ppp authentication

pppoe-client persistent max-attempts

Use the **pppoe-client persistent max-attempts** command to limit the number of consecutive connection establishment retires. 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.

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: Fast Ethernet

Example

```
G350-001(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, show ppp authentication

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

pppoe-client service-name *string*

no pppoe-client service-name *string*

Parameters

Parameter	Description	Possible Values	Default Value
string	The service name		

User level

Read-write

Context

Interface: Fast Ethernet

Example

```
G350-001(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, show ppp authentication

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.

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

pppoe-client wait-for-ipcp *seconds*

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: Fast Ethernet

Example

```
G350-001(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

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:

```
G350-001(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

pre-shared-key

Use the **pre-shared-key** CLI 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 on page 800** 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	
hexadecimal	Keyword indicating that the pre-shared key string is being specified in hexadecimal notation		

User level

read-write

Context

crypto isakmp peer

Examples

```
G350-001(config-peer:149.49.70.1)# pre-shared-key GNpi1odGNBrB5z4GJLzI
G350-001(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

priority-queue

Use the **priority-queue** command to enable priority queuing mode in a serial or Fast Ethernet interface. By default, priority queuing is off, and Weighted Fair VoIP Queuing (WFVQ) is enabled on all Serial interfaces and all Fast Ethernet interfaces for which traffic-shaping is enabled. If you disable priority queuing by using the **no** form of the **priority-queue** command, WFVQ is re-enabled.

Note:

The command **priority-queue** is not applicable for an interface on which Frame-Relay Traffic-Shaping is 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

Example

To enable priority queuing:

```
G350-001(if:Serial 2/1:1)# priority-queue
```

Related commands

fair-queue-limit, fair-voip-queue, voip-queue-delay

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

crypto map/ip-rule

Examples

```
G350-001(crypto 901/ip rule 21)# protect crypto map 5
G350-001(crypto 901/ip rule 22)# no protect
```

Related commands

description (ip rule), destination-ip, ip crypto-list, ip-rule (VPN), local-address, source-ip, show ip crypto-list

queue-limit

Use the **queue-limit** command to set the packet size of the various queues. Use the **no** form of the command to restore the packet size to its default value, using the interface bandwidth.

Note:

The **queue-limit** command is not applicable in fair-voip-queue mode.

Note:

The command **queue-limit** is not applicable for an interface on which Frame-Relay Traffic-Shaping 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

Example

To specify a size of 200 for queue 1:

```
G350-001(if:Serial 2/1:1)# queue-limit 1 200
```

Related commands

interface FastEthernet, interface serial, set qos bearer, set qos control, set qos signal, show ip qos-list, show queue, show voip-parameters, voip-queue-delay

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:

```
G350-001(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)

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:

```
G350-001(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)

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

```
G350-001(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

release voip-dsp

Use the **release voip-dsp** command to end a BTR test on the VoIP engine.

Note:
Status changes that occur during the test create SNMP traps.

Note:
View the results of the most recent BTR test with the **show mm** command (refer to show mm on page 683).

Syntax

release voip-dsp

User level

read-write

Context

general

Related commands

busyout voip-dsp, show mm, show voip-parameters, test voip-dsp

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:

```
G350-001(controller:5/1)# remote reset-performance-monitoring-counters
```

Related commands

cablelength long, cablelength short, channel-group, clock source, controller, ds-mode, framing, interface serial, ip address, linecode (E1), linecode (T1), show controllers

remove port

Use the **remove port** command to remove the virtual integrated port assignment from a trunk group in Standard Local Survivability (SLS). The port assignment is administered with the add port command.

Note:

This command is not supported on the G350.

Syntax

remove port *module-port*

Parameters

Parameter	Description	Possible Values	Default Value
module-port	The virtual integrated port assignment for this ***group-type***	See below	

Port assignments conform to this list:

G250 model	Analog loop-start trunks (*group-type* parameter is loop-start)	Analog DID trunks (*group-type* parameter is loop-start)
G250-Analog	V301, V302, V303, V304	V305, V306
G250-BRI	V301	V302, V303
G250-DCP	V301, V302, V303, V304	V305, V306
G250-DS1	V301	V302, V303

User level

read-write

Context

survivable-call-engine/trunk-group

Example

```
G250-100 (sls-trunk-group-<tgnum>)# remove port v301
```

Related commands

set dial, set tac, clear tac, add port, set supervision, set digit-treatment, set digits, show

rename announcement-file

Use the **rename announcement-file** command to rename an announcement file in the G250/G350 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_local_announcement1.wav“ to “to_local_announcement1.wav.“

```
G350-001# rename announcement-file from_local_announcement1.wav
to_local_announcement1.wav
```

Related commands

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

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

```
G350-001(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

---

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.

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 Avaya G250 and Avaya G350 Media Gateways and all its media modules		

User level

read-write

Context

general

Example

To reset the VoIP engine:

```
G350-001(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:

```
G350-001(super)# retstatus
Succeeded
G350-001(super)# retstatus
Failed
```

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 379).

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:

```
G350-003(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

rmon event, 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 378. 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:

```
G350-001(super)# rmon event 32 trap description resetTrap owner config
event 32 was created successfully
```

Related commands

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:

```
G350-001(super)# rmon history 32 10/2 interval 20 buckets 100 owner
config

history index 32 was created successfully
```

Related commands

rmon alarm, rmon event, show rmon alarm, show rmon event, show rmon history, show rmon statistics

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

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

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

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

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

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:

```
G350-001(cna-testplug 1)# rtp-echo-port 45230
```

Related commands

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

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

```
G350-001(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 threshold is 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	Sets all event thresholds to the specified number		
codec-loss	Sets the event threshold for the codec-loss metric		
codec-rtt	Sets the event threshold for the codec-rtt metric		
echo-return-loss	Sets the event threshold for the echo-return-loss metric		
loss	Sets the event threshold for the loss metric		
remote-loss	Sets the event threshold for the remote-loss metric		
rtt	Sets the event threshold for the rtt metric		
jitter	Sets the event threshold for the jitter metric		
remote-jitter	Sets the event threshold for the remote-jitter metric		
ssrc-change	Sets the event threshold for the ssrc-change metric		
num	The number of events		

User level

read-write

Context

General

Example

To set rtp-stat event-thresholds:

```
G350-001(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 fault/clear trap boundary:

```
G350-001(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

Example

To set the minimum statistic window to 50:

```
G350-001(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:

```
G350-001(super)#  rtp-stat qos-trap
The RTP statistics QoS trap is enabled
```

To disable QoS traps:

```
G350-001(super)# no rtp-stat qos-trap
The RTP statistics QoS trap is disabled.
```

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

```
G350-001(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:

```
G350-001 (super)# rtp-stat-service
The RTP statistics service is enabled.
```

To disable the RTP statistics application:

```
G350-001 (super)# no rtp-stat-service
The RTP statistics service is disabled.
```

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 384.

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 ***dbm***

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	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	The average codec loss measurement since the beginning of the RTP stream.		
loss	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	The average packet loss evaluation since the beginning of the RTP stream.		
remote-loss	The network loss according to the remote RTP receiver. The device learns of the remote packet loss from received RTCP messages.		
average-remote-loss	The average remote network loss measurement since the beginning of the RTP stream.		
percentage		**0.0-100.0**	

Parameter	Description	Possible Values	Default Value
codec-rtt	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	The network RTT. This metric does not include internal delay. The device learns of the RTT from RTCP messages.		
jitter	Variation in delay of packet delivery to the local peer.		
remote-jitter	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	The echo cancellation loss on the TDM bus.		
db		**0-100**	
all	Clears all configured thresholds.		

User Level

read-write

Context

General

Example

To set the echo return loss threshold to 5 dB:

```
G350-001(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

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 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:

```
G350-003(cna-testplug 1)# rtp-test-port 65120
```

Related commands

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

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

```
G350-001(config)# rtr 1
```

Related commands

rtr-schedule, show rtr configuration, show rtr operational-state, 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

```
G350-001(config)# rtr-schedule 1 start-time now life forever
```

Related commands

rtr, show rtr configuration, show rtr operational-state

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 400 for more information. The Media Server must configure the SAT port to 5023.

Syntax

sat

User level

read-only

Context

general

---

save config

Use the **save config** command to write the SLS data set in a G250 to non-volatile RAM (NVRAM).

Note:

This command is not supported on the G350.

Syntax

save config

User level

read-write

Context

You must be in the survivable-call-engine context before the **save config** command will work.

Example

```
G250-001(super-survivable-call-engine)# save config
Survivable-call-engine configuration is saved
```

Related commands

clear survivable-config, clear dial-pattern, clear extension, clear trunk-group, set date-format, set dial-pattern, set ip-codec-set, set max-ip-registrations, set survivable-call-engine, show date-format, show dial-pattern, show extension, show ip-codec-set, show last-pim-update, show max-ip-registrations, show survivable-call-engine, show trunk-group, survivable-call-engine

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:

```
G350-003(cna-testplug 1)# scheduler 4 124.12.221.43
```

Related commands

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

self-identity

Use the **self-identity** command to set the identity of this 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	Sets self-identity to the address of this device. This is the default setting		
fqdn-str	Sets self-identity to the Fully Qualified Domain Name of this device		

User level

read-write

Context

crypto isakmp peer

Example

```
G350-001(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

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

[no] server-name *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”:

```
G350-001(DHCP 5)# server-name "avaya"
```

To clear the optional server name:

```
G350-001(DHCP 5)# no server-name
```

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

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 Media Server SAT terminal, the SAT port must be configured to 5023 on the Media Server. For **session mgc** and **session icc**, the Media 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:

```
G350-001(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 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:

```
G350-001(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, dir, show boot bank, show download software status, show image version

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	**1**	
relay	Contact closure relay	**1**, **2**	
mgc	Contact closure is controlled by the call controller		
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:

```
G350-001(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:

```
G350-001(super)# set contact-closure pulse-duration 10/1:2 3
```

Related commands

set contact-closure admin, show contact-closure

set cor

Use the **set cor** command to administer the class-of-restriction values for each station that uses Standard Local Survivability (SLS).

Note:

This command is not supported on the G350.

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	

* 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."

User level

read-write

Context

survivable-call-engine/station

Example

```
G250-001 (sls-station-<extension>)# set cor unrestricted
```

Related commands

set type, set port, set trunk-destination, set password, set expansion-module, set swhook-flash, , show

set date-format

Use the **set date-format** command to set a date format for the SLS data set on the G250. The default date format is mm/dd/yy.

Note:

This command is not supported on the G350.

Syntax

set date format {mm/dd/yy | dd/mm/yy | yy/mm/dd}

User level

read-write

Context

survivable-call-engine

Example

```
G250-001(super-survivable-call-engine)# set date-format dd/mm/yy
Date Format is dd/mm/yy
```

Related commands

station, trunk-group, clear extension, show extension, clear trunk-group, show trunk-group, set max-ip-registrations, show max-ip-registrations, set pim-lockout, show pim-lockout, show, set fac, show fac, clear fac, show date-format, set ip-codec-set, copy running-config startup-config, clear survivable-config, show last-pim-update, survivable-call-engine

set dial

Use the **set dial** command to define the method for sending outbound digits in Standard Local Survivability (SLS).

Note:

This command is not supported on the G350.

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	

User level

read-write

Context

survivable-call-engine/trunk-group

Example

```
G250-001 (sls-trunk-group-<tgnum>)# set dial dtmf
```

Related commands

set tac, clear tac, add port, remove port, set digit-treatment, set digits, set supervision, show

set dial-pattern

Use the **`set dial-pattern`** command to configure up to 15 dial patterns in the SLS data set on the G250.

Note:

This command is not supported on the G350.

Syntax

`set dial-pattern` ***`dialed_string length type deny tgnum`***

Parameters

Parameter	Description	Possible Values	Default Value
dialed_string	Maximum of 18 characters: only 0-9, *, and X or x as a pre-string or mid-string replacement. X cannot be at the end of a dialed string.		
length	Length of the dialed string	Up to 28 digits	

Parameter	Description	Possible Values	Default Value
type	**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)		
deny	Indicates whether the call should be permitted or denied	**y** or **n**	
tgnum	The trunk group number	**1-2000**	

User level

read-write

Context

You must be in the survivable-call-engine context before the **`set dial-pattern`** command will work.

Example

```
G250-001(super-survivable-call-engine)# set dial-pattern 49139 10 locl
false 22

Dialed String: 49139
  Length: 10
  Type:  locl
  Deny Call:  false
  Trunk Group:  22
```

Related commands

clear survivable-config, clear dial-pattern, clear extension, clear trunk-group, save config, set date-format, set ip-codec-set, set max-ip-registrations, set survivable-call-engine, show date-format, show dial-pattern, show extension, show ip-codec-set, show last-pim-update, show max-ip-registrations, show survivable-call-engine, show trunk-group, survivable-call-engine

set digits

Use the **set digits** command to define the inserted dial string that is added to the start of the received DID incoming dial string in Standard Local Survivability (SLS).

Note:

You must have executed the set digit-treatment command before this command will work. This command is not supported on the G350.

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** **blank** (removes digits)	

* 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

survivable-call-engine/trunk-group

Examples

```
G250-001 (sls-trunk-group-<tgnum>)# set digits 538
G250-001 (sls-trunk-group-<tgnum>)# set digits ""
```

Related commands

set dial, set tac, clear tac, add port, remove port, set supervision, set digit-treatment, show

set digit-treatment

Use the **set digit-treatment** command to define the incoming digit treatment for analog DID trunks only in Standard Local Survivability (SLS).

Note:

This command is not supported on the G350.

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 treament) **absorb1** **absorb2** **absorb3** **absorb4** **absorb5** **insert1** **insert2** **insert3** **insert4**	

User level

read-write

Context

survivable-call-engine/trunk-group

Examples

```
G250-100 (sls-trunk-group-<tgnum>)# set digit-treatment absorb 1
G250-100 (sls-trunk-group-<tgnum>)# set digit-treatment blank
```

Related commands

set dial, set tac, clear tac, add port, remove port, set supervision, set digits, show

set dot1x m tlv

Use the **set dot1x lldp tlv** command to specify that if LLDP is enabled, then upon 802.1x authentication of a supplicant, the G250/G350 transmits the port LLDP information (PVID, Port Vlan) in the LLDP packet sent to the supplicant.

Note:

This command applies to all ports running the 802.1x protoccol.

Syntax

set dot1x lldp tlv {enable | disable}

Parameters

Parameter	Description	Possible Values	Default Value
enable	Enables transmission of port LLDP information in the LLDP packet sent to the supplicant.		
disable	Disables transmission of port LLDP information in the LLDP packet sent to the supplicant.		

User Level

read-write

Context

general

Example

```
G350-001(super)# set dot1x lldp tlv enable
```

Related commands

clear dot1x config, set dot1x max-req, set dot1x max-supp-per-port, set dot1x port-mode, set dot1x quiet-period, set dot1x re-authperiod, set dot1x server-timeout, set dot1x supp-timeout, set dot1x system-auth-control disable, set dot1x system-auth-control enable, set dot1x tx-period, set port dot1x initialize, set port dot1x port-control, set port dot1x port-mode, set port dot1x re-authenticate, set port dot1x re-authentication, show dot1x, show port dot1x, show port dot1x statistics, show port dot1x supp-mac

set dot1x max-req

Use the **set dot1x max-req** command to set the maximum number of times the port tries to retransmit requests to the Authenticated Station before the session is terminated.

Note:

Time period settings affect all external ports.

Note:

This command applies to all ports running the 802.1x protoccol.

Syntax

set dot1x max-req *count*

Parameters

Parameter	Description	Possible Values	Default Value
count	Number of attempts	**1-10**	**2**

User Level

admin

Context

general

Example

```
G350-001(super)# set dot1x max-req 5
```

Related commands

clear dot1x config, set dot1x m tlv, set dot1x max-supp-per-port, set dot1x port-mode, set dot1x quiet-period, set dot1x re-authperiod, set dot1x server-timeout, set dot1x supp-timeout, set dot1x system-auth-control disable, set dot1x system-auth-control enable, set dot1x tx-period, set port dot1x initialize, set port dot1x port-control, set port dot1x port-mode, set port dot1x re-authenticate, set port dot1x re-authentication, show dot1x, show port dot1x, show port dot1x statistics, show port dot1x supp-mac

set dot1x max-supp-per-port

Use the **set dot1x max-supp-per-port** command to specify the supported number of supplicants per port in MAC-based authentication.

Note:

If the configured **max-supp-per-port** is smaller than the current number of supplicants connected to one or more of the device's ports, a message notifies you that proceeding will de-authenticate the supplicants on those ports .

Note:

This command applies to all ports running the 802.1x protoccol.

Syntax

set dot1x max-supp-per-port *number*

Parameters

Parameter	Description	Possible Values	Default Value
number	The maximum number of supported supplicants per port, in MAC-based authentication mode	**1-8**	**2**

User Level

read-write

Context

general

Example

```
G350-001(super)# set dot1x max-supp-per-port 3
```

Related commands

clear dot1x config, set dot1x m tlv, set dot1x max-req, set dot1x port-mode, set dot1x quiet-period, set dot1x re-authperiod, set dot1x server-timeout, set dot1x supp-timeout, set dot1x system-auth-control disable, set dot1x system-auth-control enable, set dot1x tx-period, set port dot1x initialize, set port dot1x port-control, set port dot1x port-mode, set port dot1x re-authenticate, set port dot1x re-authentication, show dot1x, show port dot1x, show port dot1x statistics, show port dot1x supp-mac

set dot1x port-mode

Use the **set dot1x port-mode** command to specify the mode of authentication: port-based (single supplicant) or MAC-based (multiple supplicants). In port-based mode, only one station can authenticate the port and afterwards all MACs connected to the port have access to the network. In MAC-based mode, each of the MACs connected to the port is authenticated in order to get access to the network. The default value is **port-based-authentication**, which is backward compatible to the 802.1x operations mode in previous releases.

Note:

This command applies to all ports running the 802.1x protoccol.

Syntax

set dot1x port-mode [port-based-authentication | mac-based-authentication]

Parameters

Parameter	Description	Possible Values	Default Value
port-based-authentication	Sets authentication to port-based (single supplicant) mode		
mac-based-authentication	Sets authentication to MAC-based (multi supplicants) mode		

User Level

read-write

Context

general

Example

```
G350-001(super)# set dot1x port mode mac-based-authentication
```

Related commands

clear dot1x config, set dot1x m tlv, set dot1x max-req, set dot1x max-supp-per-port, set dot1x quiet-period, set dot1x re-authperiod, set dot1x server-timeout, set dot1x supp-timeout, set dot1x system-auth-control disable, set dot1x system-auth-control enable, set dot1x tx-period, set port dot1x initialize, set port dot1x port-control, set port dot1x port-mode, set port dot1x re-authenticate, set port dot1x re-authentication, show dot1x, show port dot1x, show port dot1x statistics, show port dot1x supp-mac

set dot1x quiet-period

Use the **set dot1x quiet-period** command to set the minimum time between authentication attempts.

Note:

Time period settings affect all external ports.

Syntax

set dot1x quiet-period *seconds*

Parameters

Parameter	Description	Possible Values	Default Value
seconds	Number of seconds.	**0-65535**	**60**

User Level

admin

Example

```
G350-001(super)# set dot1x quiet-period 45
```

Related commands

clear dot1x config, set dot1x m tlv, set dot1x max-req, set dot1x max-supp-per-port, set dot1x port-mode, set dot1x re-authperiod, set dot1x server-timeout, set dot1x supp-timeout, set dot1x system-auth-control disable, set dot1x system-auth-control enable, set dot1x tx-period, set port dot1x initialize, set port dot1x port-control, set port dot1x port-mode, set port dot1x re-authenticate, set port dot1x re-authentication, show dot1x, show port dot1x, show port dot1x statistics, show port dot1x supp-mac

set dot1x re-authperiod

Use the **set dot1x re-authperiod** command to set the idle time between re-authentication attempts.

Note:

Time period settings affect all external ports.

Syntax

set dot1x re-authperiod *seconds*

Parameters

Parameter	Description	Possible Values	Default Value
seconds	Number of seconds	**0-65535**	**3600**

User Level

admin

Context

general

Example

```
G350-001(super)# set dot1x re-authperiod 7200
```

Related commands

clear dot1x config, set dot1x m tlv, set dot1x max-req, set dot1x max-supp-per-port, set dot1x port-mode, set dot1x quiet-period, set dot1x server-timeout, set dot1x supp-timeout, set dot1x system-auth-control disable, set dot1x system-auth-control enable, set dot1x tx-period, set port dot1x initialize, set port dot1x port-control, set port dot1x port-mode, set port dot1x re-authenticate, set port dot1x re-authentication, show dot1x, show port dot1x, show port dot1x statistics, show port dot1x supp-mac

set dot1x server-timeout

Use the **set dot1x server-timeout** command to set the server retransmission timeout period for all ports. This is the maximum time that the port will wait for a reply from the Authentication Server.

Note:

Timeout settings affect all external ports.

Syntax

set dot1x server-timeout ***seconds***

Parameters

Parameter	Description	Possible Values	Default Value
seconds	Number of seconds	**0-65535**	**30**

User Level

admin

Context

general

Example

```
G350-001(super)# set dot1x server-timeout 15
```

Related commands

clear dot1x config, set dot1x m tlv, set dot1x max-req, set dot1x max-supp-per-port, set dot1x port-mode, set dot1x quiet-period, set dot1x re-authperiod, set dot1x supp-timeout, set dot1x system-auth-control disable, set dot1x system-auth-control enable, set dot1x tx-period, set port dot1x initialize, set port dot1x port-control, set port dot1x port-mode, set port dot1x re-authenticate, set port dot1x re-authentication, show dot1x, show port dot1x, show port dot1x statistics, show port dot1x supp-mac

set dot1x supp-timeout

Use the **set dot1x supp-timeout** command to set the maximum time that the switch will wait for a reply from the Authenticated Station before the session is terminated.

Note:

Timeout settings affect all external ports.

Syntax

set dot1x supp-timeout *seconds*

Parameters

Parameter	Description	Possible Values	Default Value
seconds	Number of seconds	**0-65535**	**30**

User Level

admin

Context

general

Example

```
G350-001(super)# set dot1x supp-timeout 15
```

Related commands

clear dot1x config, set dot1x m tlv, set dot1x max-req, set dot1x max-supp-per-port, set dot1x port-mode, set dot1x quiet-period, set dot1x re-authperiod, set dot1x server-timeout, set dot1x system-auth-control disable, set dot1x system-auth-control enable, set dot1x tx-period, set port dot1x initialize, set port dot1x port-control, set port dot1x port-mode, set port dot1x re-authenticate, set port dot1x re-authentication, show dot1x, show port dot1x, show port dot1x statistics, show port dot1x supp-mac

set dot1x system-auth-control disable

Use the **set dot1x system-auth-control disable** command to globally disable the PBNAC (802.1x) feature.

Syntax

set dot1x system-auth-control disable

User Level

admin

Context

general

Example

```
G350-001(super)# set dot1x system-auth-control disable
```

Related commands

clear dot1x config, set dot1x m tlv, set dot1x max-req, set dot1x max-supp-per-port, set dot1x port-mode, set dot1x quiet-period, set dot1x re-authperiod, set dot1x server-timeout, set dot1x supp-timeout, set dot1x system-auth-control enable, set dot1x tx-period, set port dot1x initialize, set port dot1x port-control, set port dot1x port-mode, set port dot1x re-authenticate, set port dot1x re-authentication, show dot1x, show port dot1x, show port dot1x statistics, show port dot1x supp-mac

set dot1x system-auth-control enable

Use the **set dot1x system-auth-control enable** command to globally enable the PBNAC (802.1x) feature.

Syntax

set dot1x system-auth-control enable

User Level

admin

Context

general

Example

```
G350-001(super)# set dot1x system-auth-control enable
```

Related commands

clear dot1x config, set dot1x m tlv, set dot1x max-req, set dot1x max-supp-per-port, set dot1x port-mode, set dot1x quiet-period, set dot1x re-authperiod, set dot1x server-timeout, set dot1x supp-timeout, set dot1x system-auth-control disable, set dot1x tx-period, set port dot1x initialize, set port dot1x port-control, set port dot1x port-mode, set port dot1x re-authenticate, set port dot1x re-authentication, show dot1x, show port dot1x, show port dot1x statistics, show port dot1x supp-mac

set dot1x tx-period

Use the **`set dot1x tx-period`** command to set the time interval between attempts to access the Authenticated Station.

Note:

Time period settings affect all external ports.

Syntax

`set dot1x tx-period` ***`seconds`***

Parameters

Parameter	Description	Possible Values	Default Value
`seconds`	Number of seconds	**0-65535**	**30**

User Level

admin

Context

general

Example

```
G350-001 (super)# set dot1x tx-period 15
```

Related commands

clear dot1x config, set dot1x m tlv, set dot1x max-req, set dot1x max-supp-per-port, set dot1x port-mode, set dot1x quiet-period, set dot1x re-authperiod, set dot1x server-timeout, set dot1x supp-timeout, set dot1x system-auth-control disable, set dot1x system-auth-control enable, set port dot1x initialize, set port dot1x port-control, set port dot1x port-mode, set port dot1x re-authenticate, set port dot1x re-authentication, show dot1x, show port dot1x, show port dot1x statistics, show port dot1x supp-mac

---

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

```
G350-001(config-crypto:1)# set dscp 10
G350-001(config-crypto:1)# no set dscp
```

Related commands

continuous-channel, description (crypto map), set peer (crypto map), set peer-group, set transform-set

set expansion-module

Use the **set expansion-module** command to allow a DCP or IP station to have an expansion module that provides for more button appearances in Standard Local Survivability (SLS).

Note:

This command not supported on the G350.

Syntax

set expansion-module {yes | no}

Parameters

Parameter	Description	Possible Values	Default Value
yes	This station can have an expansion module		
no	This station cannot have an expansion module		

User level

read-write

Context

survivable-call-engine/station

Example

```
G250-100 (sls-station-<extension>)# set expansion-module yes
```

Related commands

set type, set port, set cor, set password, set password, set swhook-flash, show

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:

In ETR mode, the TRK and LINE 1 ports are connected. All other telephone ports stop operating.

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 | manual-off}

Parameters

Parameter	Description	Possible Values	Default Value
module	Module number	**1-7**	
auto	Allow the gateway to control ETR mode automatically		
manual-on	Set ETR mode to on		
manual-off	Set ETR mode to off		

User level

read-write

Context

general

Example

To specify that the gateway will control ETR mode automatically on module 7:

```
G350-001(super)# set etr 7 auto
```

Related commands

show etr

set fac

Use the **set fac** command to administer the Feature Access Code for Standard Local Survivabiltiy (SLS) on the G250.

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. This command is not supported on the G350

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, 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

survivable-call-engine

Example

```
G250-001(super-survivable-call-engine)# set fac hold 234
Done!
```

Related commands

station, trunk-group, clear extension, show extension, clear trunk-group, show trunk-group, set max-ip-registrations, show max-ip-registrations, set pim-lockout, show pim-lockout, show, show fac, clear fac, set date-format, show date-format, set ip-codec-set, copy running-config startup-config, clear survivable-config, show last-pim-update, survivable-call-engine

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	Enable heartbeat monitoring		
disable	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 ip-codec-set

Use the **set ip-codec-set** command to configure an IP codec set within the SLS data set on the G250.

Note:

This command is not supported on the G350.

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

survivable-call-engine

Example

```
G250-001(super-survivable-call-engine)# set ip-codec-set g.711mu
IP codec g.711mu is set
```

Related commands

station, trunk-group, clear extension, show extension, clear trunk-group, show trunk-group, set max-ip-registrations, show max-ip-registrations, set pim-lockout, show pim-lockout, show, set fac, show fac, clear fac, set date-format, show date-format, copy running-config startup-config, clear survivable-config, show last-pim-update, survivable-call-engine

set lldp re-init-delay

Use the **lldp re-init-delay** command to set the reinitDelay. This sets 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

```
G250-001(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	Enable the LLDP application		
disable	Disable the LLDP application		

User level

read-write

Context

General

Example

```
G250-001(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 TxDelay. The TxDelay sets 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

```
G250-001(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 TxHoldMultiplier. This parameter is a multiplier on the TxInterval 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

```
G250-001(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.

Use the **no** form of the command to delete a number from the dial list.

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

```
G250-001(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 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** | **condition** {**all** | ***MsgFacility***} {**none** | ***severity***}}

Parameters

Parameter	Description	Possible Values	Default Value
enable	Enable logging to the file sink		
disable	Disable logging to the file sink		
condition	Define a filter rule for logging		
all	Apply the filter condition to all MsgFacilities		
MsgFacility	Apply the filter condition to a specific MsgFacility	**boot**, **dialer**, **policy,** **snmp**, **usb-modem,** **cascade**, **dnsc**, **ppp**, **stp**, **vlan**, **cdr**, **fan**, **pppoe**, **supply**, **voice**, **cli**, **filesys**, **qos**, **switchfabric**, **wan**, **cna_tp**, **ipsec**, **router**, **system**, **config**, **isakmp**, **rtp-stat**, **tftp**, **console**, **lag**, **saa**, **threshold**, **dhcps**, **poe**, **security**, **tracker**	

Parameter	Description	Possible Values	Default Value
none	Do not log messages to the file sink		
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)**	

User level

read-write

Context

general

Example

To filter VLAN messages sending only those having a severity of critical or greater:

```
G350-001(super)# set logging file condition vlan critical
```

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:

```
G350-001(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:

```
G350-001(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	Apply this filter to all message facility systems		
MsgFacility	Apply this filter to messages produced by a specific system	**boot**, **dialer**, **policy**, **snmp**, **usb-modem**, **cascade**, **dnsc**, **ppp**, **stp**, **vlan**, **cdr**, **fan**, **pppoe**, **supply**, **voice**, **cli**, **filesys**, **qos**, **switchfabric, wan**, **cna_tp**, **ipsec**, **router**, **system**, **config**, **isakmp**, **rtp-stat**, **tftp**, **console**, **lag**, **saa**, **threshold**, **dhcps**, **poe**, **security, tracker**	
none	Do not log any messages		

Parameter	Description	Possible Values	Default Value
severity	Only log messages whose severity level is equal to or more severe than the specified level (0 is the highest severity, 7 the lowest)	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:

```
G350-001(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/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	Enable logging for the Syslog server		
disable	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:

```
G350-001(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 specified Syslog server be sent to the mail output facility:

```
G350-001(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	Enable logging to the console session		
disable	Disable logging to the console session		
condition	Define a filter rule for logging		
all	Apply the filter condition to all MsgFacilities		
MsgFacility	Apply the filter condition to a specific MsgFacility	**boot**, **dialer**, **policy,** **snmp**, **usb-modem**, **cascade**, **dnsc**, **ppp**, **stp**, **vlan**, **cdr**, **fan**, **pppoe**, **supply**, **voice**, **cli**, **filesys**, **qos**, **switchfabric**, **wan**, **cna_tp**, **ipsec**, **router**, **system**, **config**, **isakmp**, **rtp-stat**, **tftp**, **console**, **lag**, **saa**, **threshold**, **dhcps**, **poe**, **security**, **tracker**	

Parameter	Description	Possible Values	Default Value
none	Do not 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, 7 the lowest)	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:

```
G350-001(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

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:

```
G350-001(super)# set logout 20
```

To disable the automatic disconnection of idle sessions:

```
G350-001(super)# set logout 0
```

Related commands

exit, reset, show logout

set max-ip-registrations

Use the **set max-ip-registrations** command to configure the maximum IP registrations allowed in the SLS data set

Note:

Since the VoIP resources on the G250 are limited, the maximum IP registrations should not be set for more than 12. This command is not supported on the G350.

Syntax

set max-ip-registrations *number*

Parameters

Parameter	Description	Possible Values	Default Value
number	Maximum number of IP registrations	**1-12**	**8**

User level

read-write

Context

survivable-call-engine

Example

```
G250-001(super-survivable-call-engine)# set max-ip-registrations 10
Maximum IP Registrations is set to 10
```

Related commands

station, trunk-group, clear extension, show extension, clear trunk-group, show trunk-group, show max-ip-registrations, set pim-lockout, show pim-lockout, show, set fac, show fac, clear fac, set date-format, show date-format, set ip-codec-set, copy running-config startup-config, clear survivable-config, show last-pim-update, survivable-call-engine

set mediaserver

Use the **set mediaserver** command to set media 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 media 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:

```
G350-563# 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:

```
G350-001(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 mss-notification rate

Use the **set mss-notification rate** command to configure the rate at which the G250/G350 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

```
G350-001(super)# set mss-notification rate 120
```

Related commands

DoS-classification, show rtp-stat config

set password

Use the **set password** command to administer a station password for an IP or DCP station using the administration identity of an IP Softphone in Standard Local Survivability (SLS).

Note:

You must first establish a station type (set type) before this command works. This command not supported on the G350.

Note:

Provisioning and Information Manager (PIM) establishes a secure session to safely deliver the security password for each station. The password is required for all IP phones in survivability mode.

Syntax

set password *password*

Parameters

Parameter	Description	Possible Values	Default Value
password	Password for an IP or DCP station	4-8 digits in range **0-9**	

User level

read-write

Context

survivable-call-engine/station

Example

```
G250-100 (sls-station-<extension>)# set password 12345
```

Related commands

set type, set port, set cor, set trunk-destination, set expansion-module, set swhook-flash, show

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

```
G350-001(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 (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		
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

```
G350-001(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

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

```
G350-001(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 pfs

Use the **set pfs** command to specify whether each IKE phase 2 negotiation will employ PFS (Perfect Forward Secrecy), 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	Specifies that IKE employs the 768-bit Diffie-Hellman prime modulus group.		
group2	Specifies that IKE employs the 1,024-bit Diffie-Hellman prime modulus group.		
group5	Specifies that IKE employs the 1536-bit Diffie-Hellman prime modulus group.		
group14	Specifies that IKE employs the 2048-bit Diffie-Hellman prime modulus group.		

User level

read-write

Context

crypto ipsec transform-set

Example

```
G350-001(config-transform:ts1)# set pfs group1
```

Related commands

crypto ipsec transform-set, mode, set security-association lifetime, show crypto ipsec transform-set

set pim-lockout

Use the **set pim-lockout** command to prevent Provisioning and Installation Manager (PIM) updates while you are working on SLS administration on the G250.

Note:

This command is not supported on the G350.

Syntax

set pim-lockout {yes | no}

User level

read-write

Context

survivable-call-engine

Example

```
G250-001(super-survivable-call-engine)# set pim-lockout yes
```

Related commands

station, trunk-group, clear extension, show extension, clear trunk-group, show trunk-group, set max-ip-registrations, show max-ip-registrations, show pim-lockout, show, set fac, show fac, clear fac, set date-format, show date-format, set ip-codec-set, copy running-config startup-config, clear survivable-config, show last-pim-update, survivable-call-engine

set port

Use the **set port** command to administer the virtual integrated port on a station for Standard Local Survivability (SLS).

Note:

This command is not supported on the G350.

Syntax

set port *module-port*

Parameters

Parameter	Description	Possible Values	Default Value
module-port	The virtual integrated port assignment for the appropriate G250 model.	Depends on class administered with the set type command; see below	

Assign a port from this list:

G250 model	Analog station ports*	DCP	IP
G250-Analog	V305, V306		No port assignments required
G250-BRI	V302, V303		
G250-DCP	V305, V306	V401-V412	
G250-DS1	V302, V303		

* These ports cannot be previously assigned as DID trunks.

User level

read-write

Context

survivable-call-engine/station

Example

```
G250-100 (sls-station-<extension>)# set port v305
```

Related commands

set type, set cor, set trunk-destination, set password, set expansion-module, set swhook-flash, show

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 autonegotiation.

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, 4/5-13 for ports 5 to 13 on module 4.		
no-flowcontrol	The port will advertise no pause capabilities.		
asym-tx-only	The port will advertise asymmetric Tx pause capabilities only.		
sym-only	The port will advertise symmetric pause capabilities only.		
sym-and-asym-rx	The port will advertise both symmetric and asymmetric Rx pause capabilities.		

User level

read-write

Context

general

Example

To specify that port 5 of module 2 will advertise asymmetric Tx pause capabilities only:

```
G350-001(super)# set port auto-negotiation-flowcontrol-advertisement
2/5 asym-tx-only

Port 2/5 pause capabilities was set
```

Related commands

set port disable, set port duplex, set port edge admin state, set port enable, 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 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	The port number. You can also specify a range of ports separated by a dash, for example, 4/5-13 for ports 5 to 13 on module 4.		
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 3 of module 5 to valuable:

```
G350-001(super)# set port classification 5/3 valuable
Port 5/3 classification has been changed.
```

Related commands

show port classification

set port disable

Use the **set port disable** command to disable a port or range of ports.

Syntax

set port disable *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, 4/5-13 for ports 5 to 13 on module 4.		

User level

read-write

Context

general

Example

To disable port 1 on module 4:

```
G350-001(super)# set port disable 4/1
Port 4/1 disabled.
```

Related commands

set port auto-negotiation-flowcontrol-advertisement, set port duplex, set port edge admin state, set port enable, 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 dot1x initialize

Use the **set port dot1x initialize** command to initialize 802.1x on a port.

Syntax

set port dot1x initialize *mod/port*

Parameters

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

User level

admin

Context

general

Example

```
G350-001(super)# set port dot1x initialize 2/3
dot1x port 4/1 initializing...
dot1x initialized on port 4/1.
```

Related commands

clear dot1x config, set dot1x m tlv, set dot1x max-req, set dot1x max-supp-per-port, set dot1x port-mode,, set dot1x quiet-period, set dot1x re-authperiod, set dot1x server-timeout, set dot1x supp-timeout, set dot1x system-auth-control disable, set dot1x system-auth-control enable, set dot1x tx-period, set port dot1x port-control, set port dot1x port-mode, set port dot1x re-authenticate, set port dot1x re-authentication, show dot1x, show port dot1x, show port dot1x statistics, show port dot1x supp-mac

set port dot1x port-control

Use the **set port dot1x port-control** command to set the dot1x parameter per port.

Syntax

set port dot1x port-control ***mod/port*** **{force-authorize | force-unauthorize | auto}**

Parameters

Parameter	Description	Possible Values	Default Value
mod	Number of the module		
port	Number of the port on the module		
force-authorize	The port is always in forwarding state		
force-unauthorize	The port is always in blocking state		
auto	Port blocking depends on authorization outcome		**auto**

User level

admin

Context

general

Example

```
G350-001(super)# set port dot1x port-control 1/2 auto
Port 4/1 dot1x port-control is set to auto.
```

Related commands

clear dot1x config, set dot1x m tlv, set dot1x max-req, set dot1x max-supp-per-port, set dot1x port-mode, set dot1x quiet-period, set dot1x re-authperiod, set dot1x server-timeout, set dot1x supp-timeout, set dot1x system-auth-control disable, set dot1x system-auth-control enable, set dot1x tx-period, set port dot1x initialize, set port dot1x port-mode, set port dot1x re-authenticate, set port dot1x re-authentication, show dot1x, show port dot1x, show port dot1x statistics, show port dot1x supp-mac

set port dot1x port-mode

Use the **set port dot1x port-mode** command to specify the port's mode of authentication: port-based (single supplicant) or MAC-based (multiple supplicants). In port-based mode, only one station can authenticate the port and afterwards all MACs connected to the port have access to the network. In MAC-based mode, each of the MACs connected to the port is authenticated in order to get access to the network. The default value is **port-based-authentication**.

Syntax

set dot1x port-mode *mod/port* [port-based-authentication | mac-based-authentication]

Parameters

Parameter	Description	Possible Values	Default Value
mod	Number of the module		
port	Number of the port on the module		
port-based-authentication	Sets port authentication to port-based (single supplicant) mode		
mac-based-authentication	Sets port authentication to MAC-based (multi supplicants) mode		

User Level

read-write

Context

general

Example

```
G350-001(super)# set dot1x port mode mac-based-authentication
```

Related commands

clear dot1x config, set dot1x m tlv, set dot1x max-req, set dot1x max-supp-per-port, set dot1x port-mode, set dot1x quiet-period, set dot1x re-authperiod, set dot1x server-timeout, set dot1x supp-timeout, set dot1x system-auth-control disable, set dot1x system-auth-control enable, set dot1x tx-period, set port dot1x initialize, set port dot1x port-control, set port dot1x re-authenticate, set port dot1x re-authentication, show dot1x, show port dot1x, show port dot1x statistics, show port dot1x supp-mac

set port dot1x re-authenticate

Use the **`set port dot1x re-authenticate`** command to set the port to re-authenticate.

Syntax

`set port dot1x re-authenticate` ***`mod/port`***

Parameters

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

User level

admin

Context

general

Example

```
G350-001(super)# set port dot1x re-authenticate 4/1
dot1x port 4/1 re-authenticating...
dot1x re-authentication successful...
dot1x port 4/1 authorized.
```

Related commands

clear dot1x config, set dot1x m tlv, set dot1x max-req, set dot1x max-supp-per-port, set dot1x port-mode, set dot1x quiet-period, set dot1x re-authperiod, set dot1x server-timeout, set dot1x supp-timeout, set dot1x system-auth-control disable, set dot1x system-auth-control enable, set dot1x tx-period, set port dot1x initialize, set port dot1x port-control, set port dot1x port-mode, set port dot1x re-authentication, show dot1x, show port dot1x, show port dot1x statistics, show port dot1x supp-mac

set port dot1x re-authentication

Use the **`set port dot1x re-authentication`** command to set the re-authentication mode per port.

Syntax

`set port dot1x re-authentication` ***`mod/port`*** **`{enable | disable}`**

Parameters

Parameter	Description	Possible Values	Default Value
`mod`	Number of the module		
`port`	Number of the port on the module		
`enable`	Keyword to enable automatic re-authentication		
`disable`	Keyword to disable automatic re-authentication		**disable**

User level

admin

Context

general

Example

```
G350-001(super)# set port dot1x re-authentication 1/2 enable
Port 1/2 re-authentication enabled.
```

Related commands

clear dot1x config, set dot1x m tlv, set dot1x max-req, set dot1x max-supp-per-port, set dot1x port-mode, set dot1x quiet-period, set dot1x re-authperiod, set dot1x server-timeout, set dot1x supp-timeout, set dot1x system-auth-control disable, set dot1x system-auth-control enable, set dot1x tx-period, set port dot1x initialize, set port dot1x port-control, set port dot1x port-mode, set port dot1x re-authenticate, show dot1x, show port dot1x, show port dot1x statistics, show port dot1x supp-mac

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 Fast Ethernet 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, 4/5-13 for ports 5 to 13 on module 4.		
full	Set full-duplex transmission		
half	Set half-duplex transmission		

User level

read-write

Context

general

Example

To set port 1 on module 4 to full duplex:

```
G350-001(super)# set port duplex 4/1 full
Port 4/1 set to full-duplex.
```

Related commands

set port auto-negotiation-flowcontrol-advertisement, set port disable, set port edge admin state, set port enable, 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.

Note:

This command is not supported on the G250.

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, 4/5-13 for ports 5 to 13 on module 4.		
admin_state	The type of the specified port	**edge-port**, **non-edge-port**	

User level

read-write

Context

general

Example

To specify that port 3 of module 10 is an edge port:

```
G350-001(super)# set port edge admin state 10/3 edge-port
```

Related commands

set port auto-negotiation-flowcontrol-advertisement, set port disable, set port duplex, set port enable, 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

Use the **set port enable** command to enable a port or a range of ports.

Syntax

set port enable [*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, 4/5-13 for ports 5 to 13 on module 4.		

User level

read-write

Context

general

Example

To enable port 3 of module 10:

```
G350-147# set port enable 10/3
Port 10/3 enabled.
```

Related commands

set port auto-negotiation-flowcontrol-advertisement, set port 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	Indicates 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	Indicates 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	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		
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.		

Parameter	Description	Possible Values	Default Value
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 1 receives administrative status from a remote device:

```
G350-147# set port flowcontrol receive 5/1 on

Port 5/1 flow control receive administration status set to on
(port will require far end to send flowcontrol)
```

To specify that port 1 cannot send administrative status to a remote device:

```
G350-147# set port flowcontrol send 5/1 off

Port 5/1 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 disable, set port duplex, set port edge admin state, set port enable, 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, 4/5-13 for ports 5 to 13 on module 4.		
value	Priority level	**0-7**	

User level

read-write

Context

general

Example

To set the priority level of port 1 on module 3 to 5:

```
G350-147# set port level 3/1 5
Port 3/1 level set to 5
```

Related commands

set port auto-negotiation-flowcontrol-advertisement, set port disable, set port duplex, set port edge admin state, set port enable, 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 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	LLDP agent will not transmit nor receive LLDP frames on this port.		
tx-only	LLDP agent will transmit LLDP frames on this port but it will not store any information about the remote systems connected.		
rx-only	LLDP agent will receive, but it will not transmit LLDP frames on this port		
rx-and-tx	LLDP agent will transmit and receive LLDP frames on this port (default)		**X**

User level

read-write

Context

General

Example

```
G250-001(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)		
enable	enable transmission of tlv parameter		
disable	disable transmission of tlv parameter		

Parameter	Description	Possible Values	Default Value
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.		
vlan-id	VLAN number. VLAN identifier of statically bound VLANs on the port. ● The vlan-id must exist and be bound to that port.	**1-4071**	

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

Example

```
G250-001(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, show lldp, show lldp config, show port lldp config, show port lldp vlan-name config

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, 4/5-13 for ports 5 to 13 on module 4 in the G350, or 10/3-5 for ETH LAN ports 3-5 on the front panel of the G250.		
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 3/1 to port 5/1 in the G350 for all packets sent and received:

```
G350-001(super)# set port mirror source-port 3/1 mirror-port 5/1
sampling always direction both
```

To set up port mirroring from port 10/3 to port 10/5 in the G250 for all packets sent and received:

```
G250-001(super)# set port mirror source-port 10/3 mirror-port 10/5
sampling always direction both
```

Related commands

clear port mirror, show port mirror

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, 4/5-13 for ports 5 to 13 on module 4 on the G350, or 10/5-8 for ETH LAN ports 5 to 8 on the front panel of the G250.		
name	The port name	maximum 16-character string	

User level

read-write

Context

general

Example

To name port 21 of module 4 to “arthur”

```
G350-147# set port name 4/21 arthur
Port 4/21 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 disable, set port duplex, set port edge admin state, set port enable, 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, 4/5-13 for ports 5 to 13 on module 4 on the G350, or 10/5-8 for ETH LAN ports 5 to 8 on the front panel of the G250.		
`enable`	Enable port negotiation protocol		
`disable`	Disable port negotiation protocol		

User level

read-write

Context

general

Example

To disable autonegotiation on port 1, module 4:

```
G350-147# set port negotiation 4/1 disable
Link negotiation protocol disabled on port 4/1.
```

Related commands

set port auto-negotiation-flowcontrol-advertisement, set port disable, set port duplex, set port edge admin state, set port enable, 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.

Note:

This command is not supported by the G250.

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, 4/5-13 for ports 5 to 13 on module 4.		

Parameter	Description	Possible Values	Default Value
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 2 is automatically detected:

```
G350-001(super)# set port point-to-point admin status 10/2 auto
```

Related commands

set port auto-negotiation-flowcontrol-advertisement, set port disable, set port duplex, set port edge admin state, set port enable, 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 powerinline

Use the **`set port powerinline`** command to enable or disable the load detection process on the port. The load detection process is used to power devices using Power over Ethernet (PoE).

Note:

This command is not supported by the G250-DCP.

Syntax

`set port powerinline` ***`module_number/port_number`*** **`{enable | disable}`**

Parameters

Parameter	Description	Possible Values	Default Value
module_number	The module number		
port_number	The port number. A range of ports can also be specified. For example, to specify ports 1-3 on module 3 of the G350, use the syntax 3/1-3. To specify ETH LAN ports 3-5 on the front panel of the G250, use the syntax 10/3-5.		
enable	Enable load detection on this port		
disable	Disable load detection on this port		

User level

read-write

Context

general

Example

To enable load detection on ports 3/1, 3/2, and 3/3 of the G350:

```
G350-001(super)# set port powerinline 3/1-3 enable
```

To enable load detection on ports 10/3, 10/4, and 10/5 of the G250:

```
G350-001(super)# set port powerinline 10/3-5 enable
```

Related commands

set port powerinline priority, set port powerinline type, set powerinline trap disable, set powerinline trap enable, show powerinline

set port powerinline priority

Use the **set port powerinline priority** command to configure the priority level of powering the port.

Note:

The order in which ports in the same priority group are powered is not sequential.

Note:

This command is not supported by the G250-DCP.

Syntax

set port powerinline priority *module_number/port_number priority*

Parameters

Parameter	Description	Possible Values	Default Value
module_number	The module number		
port_number	The port number. A range of ports can be specified. For example, to specify ports 1-3 on module 3 on the G350, use the syntax 3/1-3. To specify ETH LAN ports 3-5 on the front panel of the G250, use the syntax 10/3-5.		
priority	The priority level of powering the port	**Critical**, **High**, **Low**	

User level

read-write

Context

general

Example

To set powering priority to High for ports 3/1, 3/2, and 3/3 on the G350:

```
G350-001(super)# set port powerinline priority 3/1-3 high
```

To set powering priority to High for ports 10/3, 10/4, and 10/5 on the G250:

```
G350-001(super)# set port powerinline priority 10/3-5 high
```

Related commands

set port powerinline, set port powerinline type, set powerinline trap disable, set powerinline trap enable, show powerinline

set port powerinline type

Use the **set port powerinline type** command to set the type of powered device connected to the PoE port.

Note:

This command is not supported on the G250-DCP.

Syntax

set port powerinline type *module/port_number string*

Parameters

Parameter	Description	Possible Values	Default Value
module	Number of the module.		
port_number	Number of the port on the module.		
string	A description of the type of powered device connected to this port.		

User level

admin

Context

general

Examples

```
G350-001(super)# set port powerinline type 6/1-3 telephone
G250-001(super)# set port powerinline type 10/5 telephone
```

Related commands

set port powerinline, set port powerinline priority, set powerinline trap disable, set powerinline trap enable, show powerinline

set port redundancy

Use the **set port redundancy** command to globally enable or disable port redundancy on the device. Using this command does not delete existing redundancy entries.

Note:

This command is not supported by the G250.

Syntax

set port redundancy {enable|disable}

Parameters

Parameter	Description	Possible Values	Default Value
enable	Enable port redundancy on the device		
disable	Disable port redundancy on the device		

User level

read-write

Context

general

Example

To enable port redundancy:

```
G350-147# set port redundancy enable
All redundancy schemes are now enabled
```

Related commands

set port redundancy on|off, set port redundancy-intervals, show port redundancy

set port redundancy on|off

Use the **set port redundancy on|off** 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.

Note:

This command is not supported by the G250.

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 12 of module 4 acts as a backup port for port 7 on module 3, and to name the redundancy pair red1:

```
G350-147# set port redundancy 3/7 4/12 on red1

red1: Port 4/12 is redundant to port 3/7.
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, 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.

Note:

This command is not supported by the G250.

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`	Do not 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:

```
G350-147# set port redundancy-intervals 100 20
```

Related commands

set port redundancy, set port redundancy on|off, show port redundancy

set port spantree

Use the **set port spantree** command to enable or disable spanning tree for specific ports.

Note:

This command is not supported by the G250.

Syntax

set port spantree {enable|disable} [*module/port*]

Parameters

Parameter	Description	Possible Values	Default Value
enable	Keyword specifying that spanning tree mode should be enabled		
disable	Keyword specifying that spanning tree mode should be disabled		
module	The module number		
port	The port number		

User level

read-write

Context

general

Example

To enable spanning tree on port 1 of module 3:

```
P480-1# set port spantree enable 3/1
port 3/1 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 will be allowed to forward traffic if two ports with different costs cause a loop.

Note:

This command is not supported by the G250.

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 4/2 to 4096:

```
G350-147# set port spantree cost 4/2 4096
port 4/2 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).

Note:

This command is not supported by the G250.

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 2 of module 10 to send a hello packet:

```
G350-001(super)# set port spantree force-protocol-migration 10/2
```

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.

Note:

This command is not supported by the G250.

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 4 of module 3 to 128:

```
G350-147# set port spantree priority 3/4 128
port 3/4 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 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, 4/5-13 for ports 5 to 13 on module 4.		
10MB	Keyword that sets the specified port to a speed of 10 Mbps		
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 1 on module 4 to 100 Mbps

```
G350-147# set port speed 4/1 100MB
Port 4/1 speed set to 100 Mbps.
```

Related commands

set port auto-negotiation-flowcontrol-advertisement, set port disable, set port duplex, set port edge admin state, set port enable, 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

---

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

Examples

To bind ports 4 through 6 of module 3 in the G350 to VLAN 2:

```
G350-001# set port static-vlan 3/4-6 2

VLAN 2 is bound to port 3/4
VLAN 2 is bound to port 3/5
VLAN 2 is bound to port 3/6
```

To bind ports 3 through 5 on the front panel of the G250 to VLAN 2:

```
G250-001# set port static-vlan 10/3-5 2

VLAN 2 is bound to port 10/3
VLAN 2 is bound to port 10/4
VLAN 2 is bound to port 10/5
```

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 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, 4/5-13 for ports 5 to 13 on module 4 of the G350. To specify ETH LAN ports 3-5 on the front panel of the G250, use the syntax 10/3-5.		
enable	Enable uplink/downlink traps		
disable	Disable uplink/downlink traps		

User level

read-write

Context

general

Example

To enable uplink and downlink traps for port 2 of module 3 on the G350:

```
G350-147# set port trap 3/2 enable
Port 3/2 up/down trap enabled.
```

Related commands - SNMP access configuration

ip snmp-server, set snmp community, set snmp retries, set snmp timeout, show port trap, show snmp, show snmp engineID, show snmp group, show snmp retries, show snmp timeout, show snmp user, show snmp user summary, 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

clear snmp trap, set snmp 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 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, 4/5-13 for ports 5 to 13 on module 4.		

User level

read-write

Context

general

Example

To set the VLAN ID for ports 1 to 5 on module 10, to 1:

```
G350-147# set port vlan 1 10/1-5

Port 10/1 does not exist!
Port 10/2 does not exist!
Port 10/3 added to VLAN 1
Port 10/4 added to VLAN 1
Port 10/5 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. A list of ports can be entered using the form **n-m**. For example, specify **5/4-8** to indicate module 5, ports 4 through 8 on the G350. To specify ETH LAN ports 3-5 on the front panel of the G250, use the syntax 10/3-5.		
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 5 through 9 on module 5 will only support the VLANs manually configured for those ports:

```
G350-001# set port vlan-binding-mode 5/5-9 static

Set Port vlan binding method:5/5
Set Port vlan binding method:5/6
Set Port vlan binding method:5/7
Set Port vlan binding method:5/8
Set Port vlan binding method:5/9
```

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 powerinline trap disable

Use the **`set powerinline trap disable`** command to disable PoE trap generation.

Note:

This command is not supported on the G250-DCP.

Syntax

`set port powerinline trap disable` ***`module`***

Parameters

Parameter	Description	Possible Values	Default Value
`module`	Number of the module.		

User level

admin

Example

```
G350-001(super)# set powerinline trap disable 6
```

Related commands

set port powerinline, set port powerinline priority, set port powerinline type, set powerinline trap enable, show powerinline

set powerinline trap enable

Note:

This command is not supported by the G250-DCP.

Use the **set powerinline trap enable** command to enable the generation of PoE traps and configure the Usage Threshold value.

Syntax

set powerinline trap enable *module [threshold]*

Parameters

Parameter	Description	Possible Values	Default Value
module	Number of the module.		
threshold	(Optional) Power consumption usage for generating traps, in percent.	**1-99**	**99**

User level

admin

Context

general

Example

```
G350-001(super)# set powerinline trap enable 6 70
```

Related commands

set port powerinline, set port powerinline priority, set port powerinline type, set powerinline trap disable, show powerinline

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 492).

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:

```
G350-001(super)# set qos bearer bbedscp 43
```

Related commands

interface FastEthernet, interface serial, queue-limit, set qos control, set qos signal, show ip qos-list, show queue, show voip-parameters, voip-queue-delay

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:

```
G350-001(super)# set qos control local
```

Related commands

interface FastEthernet, interface serial, queue-limit, set qos bearer, set qos control, set qos signal, show ip qos-list, show queue, show voip-parameters, voip-queue-delay

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			
disable			
refresh			
secs	The refresh time in seconds	**1-99**	**15**
retry			
noretry			
guaranteed			
controlled			

User level

read-write

Context

general

Example

To set the refresh rate to 15 seconds:

```
G350-001(super)# set qos rsvp refresh 15
```

To specify no retry upon failure:

```
G350-001(super)# set qos rsvp failure noretry
```

To specify controlled load service:

```
G350-001(super)# set qos rsvp profile controlled
```

To enable RSVP:

```
G350-001(super)# set qos rsvp enable
```

Related commands

show qos-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:

```
G350-001(super)# set qos rtcp monip 132.123.23.12
```

To set the reporting period to 10 seconds:

```
G350-001(super)# set qos rtcp reportper 10
```

To set the listening port number to 5000:

```
G350-001(super)# set qos rtcp listenport 5000
```

To enable reporting capability:

```
G350-001(super)# set qos rtcp enable
```

Related commands - RTCP

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:

```
G350-001(super)# set qos signal dscp 43
```

Related commands

interface FastEthernet, interface serial, queue-limit, set qos bearer, set qos control, show ip qos-list, show queue, show voip-parameters, voip-queue-delay

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:

```
G350-001(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:

```
G350-001# 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:

```
G350-001# 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**:

```
G350-147# 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:

```
G350-147# 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:

```
G350-001# 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

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	Set the total search timer		
primary-search	Set the primary search timer		
minutes	Number of minutes	**1-60**	total-search: **30** primary-search: **1**
transition-point	Set the entry point		
value		**1-4**	**1**

User level

read-write

Context

general

Example

To set the primary search timer to 20 minutes:

```
G350-001(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

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	Specify the lifetime in seconds		
seconds	The lifetime, in seconds	**120-86,400**	
kilobytes	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	Unlimited lifetime		

User level

read-write

Context

crypto ipsec transform-set

Example

```
G350-001(config-transform:ts1)# set security-association lifetime
seconds 300
```

Related commands

crypto ipsec transform-set, mode, set pfs, show crypto ipsec transform-set

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 | trap [*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		
trap	Keyword specifying an SNMP trap		
community_string	Specifies the name of the SNMP community. If no community string is specified, the community string configured for that access type is cleared.		

User level

read-write

Context

general

Example

To set the read-only community string to 'read':

```
G350-001(super)# set snmp community read-only read
SNMP read-only community string set
```

Related commands - SNMP access configuration

ip snmp-server, set snmp retries, set snmp timeout, show port trap, show snmp, show snmp engineID, show snmp group, show snmp retries, show snmp timeout, show snmp user, show snmp user summary, 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

clear snmp trap, set port trap, set snmp 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.

Note:

This command is not supported by the G250.

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:

```
G350-001(super)# set snmp retries 100
```

Related commands - SNMP access configuration

ip snmp-server, set snmp community, set snmp timeout, show port trap, show snmp, show snmp engineID, show snmp group, show snmp retries, show snmp timeout, show snmp user, show snmp user summary, 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

clear snmp trap, set port trap, set snmp 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.

Note:

This command is not supported by the G250.

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:

```
G350-001(super)# set snmp timeout 60
```

Related commands - SNMP access configuration

ip snmp-server, set snmp community, set snmp retries, show port trap, show snmp, show snmp engineID, show snmp group, show snmp retries, show snmp timeout, show snmp user, show snmp user summary, 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

clear snmp trap, set port trap, set snmp trap, show snmp, snmp trap link-status, snmp-server enable notifications, snmp-server host, snmp-server informs

set snmp trap

Use the **set snmp trap** command to define an SNMPv1 trap receiver, or configure its settings.

Syntax

set snmp trap receiver {**enable**|**disable**} [*categorylist*]

Parameters

Parameter	Description	Possible Values	Default Value
receiver	The IP address of the trap receiver		
enable	Keyword specifying that the trap receiver is enabled		
disable	Keyword specifying that the trap receiver is disabled (this is the default		

Parameter	Description	Possible Values	Default Value
category list	List of trap categories to be enabled or disabled for the specified trap receiver.	**All**— all traps affected by enable/disable **config fault, trafic_treshold, module_De-Enrollment, module_Enrollment, delete_SW_redundancy_entry, create_SW_redundancy_entry, temperature_warninggeneral_threshold, cam_change, duplicate_ip, ip_vlan_violation, link_aggregation_connection_fault, link_aggregation_connection_return,link_aggregation_partial_fault, link_aggregation_partial_return,delete_lagcreate_new_lag, active_policy_list_change, policy_access_control_violation,BUPS_module_fault, BUPS_module_fault_return, BUPS_fans_module_fault, BUPS_fans_module_fault_return, fans_module_fault, fans_module_fault_returncascade_up_connection_fault, cascade_up_connection_fault_return,cascade_down_connection_fault_return, cascade_down_connection_fault**	

User level

admin

Context

general

Related commands - SNMP access configuration

ip snmp-server, set snmp community, set snmp retries, set snmp timeout, show port trap, show snmp, show snmp engineID, show snmp group, show snmp retries, show snmp timeout, show snmp user, show snmp user summary, 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

clear snmp trap, set 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 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 this bridge.

Note:

This command is not supported by the G250.

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:

```
G350-001(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.

Note:

This command is not supported by the G250.

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:

```
G350-147# set spantree enable
bridge spanning tree enabled.
```

To disable spanning tree:

```
G350-147# set spantree disable
bridge spanning tree disabled.
```

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.

Note:

This command is not supported by the G250.

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:

```
G350-001(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.

Note:

This command is not supported by the G250.

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:

```
G350-401# 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.

Note:

This command is not supported by the G250.

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:

```
G350-001(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.

Note:
This command is not supported by the G250.

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:

```
G350-001(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.

Note:

This command is not supported by the G250.

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:

```
G350-001(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.

Note:

This command is not supported by the G250.

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:

```
G350-101# 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

set supervision

Use the **set supervision** command to define the incoming signaling supervision mode for analog DID trunks only in Standard Local Survivability (SLS).

Note:

This command is not supported on the G350.

Syntax

set supervision ***sup-type***

Parameters

Parameter	Description	Possible Values	Default Value
sup-type	The incoming signaling supervision mode for DID trunks	**immediate** **wink**	

User level

read-write

Context

survivable-call-engine/trunk-group

Example

```
G250-100 (sls-trunk-group-<tgnum>)# set supervision wink
```

Related commands

set dial, set tac, clear tac, add port, remove port, set digit-treatment, set digits, show

set survivable-call-engine

Use the **set survivable-call-engine** command to enable or disable SLS.

Note:

This command is not supported on the G350.

Note:

If you disable SLS using the **set survivable-call-engine** command, the ETR function is enabled only after the G250 has registered with an entry from the Media Gateway Controller (MGC) list.

Syntax

set survivable-call-engine {enable | disable}

Parameters

Parameter	Description	Possible Values	Default Value
enable	Enable SLS		
disable	Disable SLS		

User level

read-write

Context

survivable-call-engine

Example

```
G250-001(super-survivable-call-engine)# set survivable-call-engine
enable
Survivable Call Engine is enabled
```

Related commands

clear survivable-config, clear dial-pattern, clear extension, clear trunk-group, save config, set date-format, set dial-pattern, set ip-codec-set, set max-ip-registrations, show date-format, show dial-pattern, show extension, show ip-codec-set, show last-pim-update, show max-ip-registrations, show survivable-call-engine, show trunk-group, survivable-call-engine

set swhook-flash

Use the **set swhook-flash** command to enable Standard Local Survivability (SLS) to recognize the switchhook flash signal from a particular analog station and to provide subsequent transfer service.

Note:

This command is not supported on the G350.

Syntax

set swhook-flash {yes | no}

Parameters

Parameter	Description	Possible Values	Default Value
yes	SLS recognizes the switchhook signal and transfers the call.		
no	SLS does not recognize the switchhook signal and does not transfer the call.		

User level

read-write

Context

survivable-call-engine/station

Example

```
G250-100 (sls-station-<extension>)# set swhook-flash yes
```

Related commands

set type, set port, set cor, set password, set password, set expansion-module, show

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		
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:

```
G350-001(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		
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:

```
G350-001(super)# set sync source primary
```

If the secondary interface is not configured, the sync source set operation will fail.

```
G350-001(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 sync source switching.

Syntax

set sync switching {enable | disable}

Parameters

Parameter	Description	Possible Values	Default Value
enable	Enable automatic sync source switching		
disable	Disable automatic sync source switching		

User level

read-write

Context

general

Example

To enable sync source switching:

```
G350-001(super)# set sync switching enable
```

Related commands

clear sync interface, set sync interface, set sync source, show sync timing

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 descriptive contact of the system to “Larry Williams”

```
G350-147# 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 descriptive location of the system to “tech-support”:

```
G350-147# 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 this 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 should be typed inside quotes. The name is cleared if you leave this field blank.		

User level

read-write

Context

general

Examples

To set the descriptive name of the system to “G350-HQ”:

```
G350-001(super)# set system name “G350-HQ”
*** Set system name ***
system name set
```

Related commands

set system contact, set system location

set tac

Use the **set tac** command to administer the trunk-access codes for Standard Local Survivability (SLS). You must issue this command before the trunk group is enabled in the SLS database.

Note:

This command is not supported on the G350.

Syntax

set tac *tac*

Parameters

Parameter	Description	Possible Values	Default Value
tac	This unique dial string identifies the trunk group (circumvents normal ARS dial string analysis)	a string of 1-4 digits (can include “#” and “*” as the leading digit only)	

User level

read-write

Context

survivable-call-engine/trunk-group

Example

```
G250-100 (sls-trunk-group-<tgnum>)# set tac 88
```

Related commands

set dial, clear tac, add port, remove port, set digit-treatment, set digits, set supervision, show

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:

```
G350-001(super)# set terminal recovery password disable
```

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 236.

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

```
G350-001(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

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, 4/5-13 for ports 5 to 13 on module 4 of the G350. To specify ETH LAN ports 3-5 on the front panel of the G250, use the syntax 10/3-5.		
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 3 of module 3 in the G350:

```
G350-001(super)# set trunk 3/3 dot1q
Dot1Q VLAN tagging set on port 3/3.
```

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 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 queuing in Standard Local Survivability (SLS).

Note:

This command is not supported on the G350 and does not apply to analog DID trunks.

Syntax

set trunk-destination {*yes* | *no*}

Parameters

Parameter	Description	Possible Values	Default Value
yes	This extension can receive incoming analog loop-start trunk calls		
no	This extension cannot receive incoming analog loop-start trunk calls		

User level

read-write

Context

survivable-call-engine/station

Example

```
G250-100 (sls-station-<extension>)# set trunk-destination yes
```

Related commands

set type, set port, set cor, set password, set expansion-module, set swhook-flash, show

set type

Use the **`set type`** command to administer specific phone models for Standard Local Survivability (SLS).

Note:

This command is not supported on the G350.

Syntax

`set type` ***`model`***

Parameters

Parameter	Description	Possible Values	Default Value
`model`	Model type	Depends on class: see below	

Choose a model type from this list:

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

survivable-call-engine/station

Example

```
G250-100 (sls-station-<extension>)# set type ip4625
```

Related commands

set port, set cor, set trunk-destination, set password, set expansion-module, set swhook-flash, show

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:

```
G350-100# 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 status, show system, show temp, show timeout, show utilization, show voltages, test led

---

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	**1-3071**	
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”:

```
G350-147# 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

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.

Note:

This command is not supported by the G250.

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:

```
G350-001(super)# set web aux-files-url http://176.2.3.66/DMweb
```

Related commands

show web aux-files-url

show

The show command works in both the station and trunk-group second-level subcontexts under the survivable-call-engine context. In both subcontexts the command lists all of the station (extension) and trunk group parameters for Standard Local Survivability (SLS.)

Note:

This command is not supported on the G350.

Syntax

show

User level

read-only

Context

survivable-call-engine

Example

In the station context:

```
G250-100 (sls-station-<extension>)# show
Extension Type       Port             Cor          Trk-Des Exp-Mod Flash Passwd
--------- ---------- ---------------- ------------ ------- ------- ----- ------
49138     ip4620sw   abc.def.ghi.123  unrestricted yes     no      -     ******
```

In the trunk-group context:

```
G250-100 (sls-trunk-group<tgnum>)# show
Group Type       Dial   Tac  Ports               Supervision Treat   Insert
----- ---------- ------ ---- ------------------- ----------- ------- ------
1     loop-start dtmf   99   v301                -           -       -
```

Output fields - station context

Field	Description
Extension	The extension number of the phone (1-7 digits).
Type	The telephone model.
Port	The module/port location.

Field	Description
Cor	Class of restriction assigned to the station, which determines the range of dialling 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 queuing.
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.

Output fields - trunk-group context

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**

Field	Description
Treat	The incoming digit treatment for analog DID trunks only.
Insert	The dial string that is added to the start of the received DID incoming dial string.

Related commands

station, trunk-group, clear extension, show extension, clear trunk-group, show trunk-group, set max-ip-registrations, show max-ip-registrations, set pim-lockout, show pim-lockout, set fac, show fac, clear fac, set date-format, show date-format, set ip-codec-set, copy running-config startup-config, clear survivable-config, show last-pim-update, survivable-call-engine

show announcements files

Use the **show announcements files** command to display the announcements files stored in the G250/G350 announcement directory.

Syntax

```
show announcements-files [brief]
```

Parameters

Parameter	Description	Possible Values	Default Value
brief	Displays less detail		

User level

Read only

Context

general

Example

```
G350-003(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
G350-003(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 scp announcement-file, erase announcement-file, rename announcement-file, show download announcement-file status, show upload announcement-file status

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

```
G350-001(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 banner login

Use the **show banner login** command to display the banner that is displayed before the login prompt.

Syntax

show banner login

User level

admin

Context

general

Example

To display the banner that will be displayed before the login prompt:

```
G350-001(super)# show banner login

Welcome to G350 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 displayed after a user logs in successfully.

Syntax

show banner post-login

User level

admin

Context

general

Example

To display the banner that will be shown after a successful login:

```
G350-001(super)# show banner post-login

*** Welcome to the G350 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

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:

```
G350-001(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, dir, set boot bank, show download software status, show image version

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

```
G350-001(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 for a specific VLAN or for all VLANs.

Syntax

show cam mac ***mac_address*** [***vlan_number***]

Parameters

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

User level

read-only

Context

general

Example

To display all entries in VLAN 1 that match the MAC address 00:40:c2:00:66:b0:

```
G350-001(super)# show cam mac 00:40:c2:00:66:b0 1
```

Related commands

clear cam, show cam

---

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

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 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

```
G350-001(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 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

```
G350-001(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 max-frame-size, capture start, capture stop, capture-service, clear capture-buffer, ip capture-list, name, show capture

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

```
G350-001(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.
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.

Name	Description
ID	The MAC address of the G250/G350, 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.
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.

Related commands

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

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:

```
G350-001(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 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	**7**	
port	Contact closure module port to display	**20**	
relay	Relay number	**1,2**	

User level

read-only

Context

general

Example

To display information about all contact closure relays:

```
G350-001(super)# show contact-closure
Module port relay admin           pulse-duration   status
------ ---- ----- --------------- ---------------  ------
7       20    1   call-controller 3 seconds        triggered
7       20    2   manual          toggle           off
```

To display information about contact closure relay 2:

```
G350-001(super)# show contact-closure 7/20:2
Module port relay admin           pulse-duration   status
------ ---- ----- --------------- ---------------  ------
7       20    2   manual          toggle           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

---

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:

```
G350-001(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 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 195.

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 5:

```
G350-001(super)# show controllers remote 5/1 1h-data
```

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:

```
G350-001(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 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
list			
crypto-list-id	The crypto-list whose SA configuration should be displayed.		
rule			
rule-id	The ip-rule in the crypto-list whose SA configuration should be displayed.		

Parameter	Description	Possible Values	Default Value
address	Show SA configuration by peer IP address.		
detail	Display detailed output.		

User level

read-only

Context

general

Examples

1. To display the IPSec SA database and related information (in this example, active SAs exist for the rule):

```
G350-001(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

...
```

2. To display the IPSec SA database and related information in detail (in this example, IP Payload Compression (IPPCP) is used):

```
G350-001(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 it was received on.
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 that 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 that 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, due to the length being not aligned to the cipher block. • **Replay failed *** — The number of packets discarded after being received through this tunnel, due to anti-replay verification failure. • **Sa expired *** — The number of packets discarded after being received through this tunnel, due to the SA KB lifetime being smaller then the external IP packet total length. • **Auth failed *** — The number of packets discarded after being received through this tunnel, due to 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, due to bad ESP trailer format received failure. • **Invalid identity *** — The number of packets discarded after being received through this tunnel, due to invalid identity. That is, the inner (original) IP header address doesn't 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 not covered by any of 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 PFS (Perfect Forward Secrecy) 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

```
G350-001(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

```
G350-001(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

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.

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

```
G350-001(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

```
G350-001(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

```
G350-001(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

```
G350-001(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 not (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 csu loopbacks

Use the **show csu loopbacks** command to view the state of the server SAT-controlled CSU loopbacks on a media module.

Note:

This command is not supported by the G250, except for the G250-DS1.

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 v2:

```
G350-001(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.

Note:

This command is not supported by the G250, except for the G250-DS1.

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:

```
G350-001(super)# show csu status v4

TI version of csu status:

CSU NETWORK INTERFACE STATUS
------------------------------------------------------------------
LOS:ON00F:OFF
EER:OFFL00PD:OFF
AIS:OFFPDV:OFF
LOF:OFFYEL:ON

E1 version of csu status:

CSU NETWORK INTERFACE STATUS
------------------------------------------------------------------
LOS:ON00F:OFF
EER:OFFL00PD:OFF
AIS:OFFPDV:OFF
LOF:OFFLMA:OFF
RMA:OFFLCM:ON
```

Output fields

Name	Description
LOS	Loss of signal
OOF	Out of frame
EER	Excessive error rate
LOF	Loss of frame
AIS	Alarm indication signal
YEL	Yellow
PDV	Pulse density violation (same as BPV)
LOOPD	Looped
LMA	Local multiframe alignment
RMA	Remote multiframe alignment
LCM	Loss of CRC multiframe

Related commands

show csu loopbacks

show date-format

Use the **show date-format** command to display the current date format in effect for the SLS data set in the G250.

Note:

This command is not supported on the G350.

Syntax

show date-format

User level

read-write

Context

survivable-call-engine

Example

```
G250-001(super-survivable-call-engine)# show date-format
Date Format is mm/dd/yy
```

Related commands

station, trunk-group, clear extension, show extension, clear trunk-group, show trunk-group, set max-ip-registrations, show max-ip-registrations, set pim-lockout, show pim-lockout, show, set fac, show fac, clear fac, set date-format, set ip-codec-set, copy running-config startup-config, clear survivable-config, show last-pim-update, survivable-call-engine

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 dial-pattern

Use the **show dial-pattern** command to list all dial-pattern strings in the SLS data set on the G250 in tabular format.

Note:

This command is not supported on the G350.

Syntax

show dial-pattern

User level

read-write

Context

survivable-call-engine

Example

```
G250-001(super-survivable-call-engine)# show dial-pattern
Dialed String     Length    Type   Deny Call    Trunk Group
-------------     ------    ----   ----------   -----------
9139              6         op     true         22
22310             10        emer   false        123
```

Output fields

Field	Description
Dialed String	The administered ARS dial string.
Length	The 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.

Field	Description
Deny Call	Indicates whether the call should be permitted (true) or denied (false).
Trunk Group	The trunk-group number (1-2000) associated with this dial string.

Related commands

clear survivable-config, clear dial-pattern, clear extension, clear trunk-group, save config, set date-format, set dial-pattern, set ip-codec-set, set max-ip-registrations, set survivable-call-engine, show date-format, show extension, show ip-codec-set, show last-pim-update, show max-ip-registrations, show survivable-call-engine, show trunk-group, survivable-call-engine

show dot1x

Use the **show dot1x** command to display the system dot1x capabilities, protocol version, and timer values.

Syntax

show dot1x

User level

admin

Context

general

Example

```
G350-001(super)# show dot1x
PAE Capabilities                          Authenticator Only
Protocol Version                          1
System-auth-control                       enabled
Max supplicants per port                  2
LLDP Transmission VLAN mode               disabled

Module  Max Supp   Total Supps  Authenticated Supps  Authenticating Supps
------  ---------  -----------  -------------------  --------------------
6       200        39           39                    0
```

Output fields

Name	Description
PAE Capabilities	The capabilities of the Port Access Entity
Protocol Version	The protocol version in use
System-auth-control	Whether 802.1x authorization is enabled.
Max supplicants per port	The configured maximum number of supplicants per port (relevant for MAC-based authentication only).
LLDP Transmission VLAN mode	Whether LLDP transmission VLAN mode is enabled.
Module	Number of the module and port.
Max Supp	The overall maximum number of supplicants the G250/G350 can support.
Total Supps	The number of currently connected supplicants.
Authenticated Supps	The number of authenticated supplicants connected to the G250/G350.
Authenticating Supps	The number of supplicants connected to the G250/G350 being authenticated (not authenticated yet).

Related commands

clear dot1x config, set dot1x m tlv, set dot1x max-req, set dot1x max-supp-per-port, set dot1x port-mode, set dot1x quiet-period, set dot1x re-authperiod, set dot1x server-timeout, set dot1x supp-timeout, set dot1x system-auth-control disable, set dot1x system-auth-control enable, set dot1x tx-period, set port dot1x initialize, set port dot1x port-control, set port dot1x port-mode, set port dot1x re-authenticate, set port dot1x re-authentication, show port dot1x, show port dot1x statistics, show port dot1x supp-mac

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 G250/G350 announcement directory.

Syntax

show download announcement-file status

User level

read-only

Context

general

Example

In the following example, no download command has been issued:

```
G350-001(super)# show download announcement-file status
Module #9
===========
No dest file for download operation - no download operation was done.
In the following example, a download command has been issued:
G350-001(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 scp announcement-file, erase announcement-file, rename announcement-file, show announcements files, show upload announcement-file status

---

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

```
G350-001(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 scp license-file, copy tftp license-file, show license 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

```
G350-001(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, 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

- If no download has been performed:

```
G350-001# 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:

```
G350-001# 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 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 upload phone-script-file status, show ip tftp-server files

show download software status

Use the **show download software status** command to display the status of the current Device Manager software 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:

```
G350-001(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, dir, set boot bank, show boot bank, show image version

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:

```
G350-001(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 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:

```
G350-001(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 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 ds-mode:

```
G350-001(super)# show ds-mode

Current ds-mode:    T1
Configured ds-mode: T1
```

Related commands

ds-mode

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

```
G350-001(super)# show dynamic-cac
Current RBBL : 256 kbps
event : 0 Days, 1:21:00
Last event BBL : 256 kbps
```

Related commands

dynamic-cac

---

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 etr

Use the **show etr** command to view the status of Emergency Transfer Relay (ETR) mode.

Note:

In ETR mode, the TRK and LINE 1 ports are connected. All other telephone ports stop operating.

Syntax

show etr

User level

read-only

Context

general

Example

To display the ETR status:

```
G350-001(super)# show etr
Module: 7
Admin State: auto
Module status: in service
Trunk line  line status
----- ----  -----------
1     2     off hook
```

Related commands

set etr

show extension

Use the **show extension** command to display extension-specific SLS data parameters. If no parameters are specified, all administered extensions are listed.

Note:

This command is not supported on the G350.

Syntax

show extension [all | ***extension*** | ***{extension +n}*****]**

Parameters

Parameter	Description	Possible Values	Default Value
all	Lists all administered extensions		
extension	Lists only the numbered extension		
extension +n	Lists the numbered extension + “n” entries		

User level

read-write

Context

survivable-call-engine

Example

```
G250-001(super-survivable-call-engine)# show extension all
Extension Type       Port       Cor          Trk-Des Exp-Mod Flash  Passwd
--------- ----       ----       ---          ------- ------- -----  ------
11111     ip4620sw   0.0.0.0    unrestricted  yes     no      -     ******
11112     ip4620sw   0.0.0.0    unrestricted  yes     no      -     ******
11117     ip4610sw   0.0.0.0    internal      yes     yes     -     ******
12111     analog2500 v305       unresticted   yes     -       yes    -
G250-001(super-survivable-call-engine)# show extension 11111
Extension Type       Port       Cor          Trk-Des Exp-Mod Flash  Passwd
--------- ----       ----       ---          ------- ------- -----  ------
11111     ip4620sw   0.0.0.0    unrestricted  yes     no      -     ******
G250-001(super-survivable-call-engine)# show extension 11111 +2
Extension Type       Port       Cor          Trk-Des Exp-Mod Flash  Passwd
--------- ----       ----       ---          ------- ------- -----  ------
11111     ip4620sw   0.0.0.0    unrestricted  yes     no      -     ******
11112     ip4620sw   0.0.0.0    unrestricted  yes     no      -     ******
11117     ip4610sw   0.0.0.0    internal      yes     yes     -     ******
```

Output fields

Field	Description
Extension	The extension number of the phone (1-7 digits).
Type	The station type.
Port	The module/port location.

Field	Description
Cor	The Class of Restriction. Possible classes include: • emergency • internal • local • toll • unrestricted
Trunk-Des	Indicates whether to permit (y) or deny (n) 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.
Password	Asterisks (*) indicate an administered password.

Related commands

station, trunk-group, clear extension, clear trunk-group, show trunk-group, set max-ip-registrations, show max-ip-registrations, set pim-lockout, show pim-lockout, show, set fac, show fac, clear fac, set date-format, show date-format, set ip-codec-set, copy running-config startup-config, clear survivable-config, show last-pim-update, survivable-call-engine

show fac

Use the **`show fac`** command to list the administered Feature Access Codes for Standard Local Survivabiltiy (SLS) on the G250.

Note:

This command is not supported on the G350.

Syntax

`show fac`

User level

read-only

Context

survivable-call-engine

Example

```
G250-001(super-survivable-call-engine)# show fac

Feature       Access Code
------------- -----------
hold           234
Done!
```

Related commands

station, trunk-group, clear extension, show extension, clear trunk-group, show trunk-group, set max-ip-registrations, show max-ip-registrations, set pim-lockout, show pim-lockout, show, set fac, clear fac, set date-format, show date-format, set ip-codec-set, copy running-config startup-config, clear survivable-config, show last-pim-update, survivable-call-engine

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:

```
G350-001(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 status, show system, show temp, show timeout, show utilization, show voltages, test led

---

show flows

Use the **show flows** command to display information about the real-time status of micro-flows within output queues for the current interface.

Note:

This command is only applicable in fair-voip-queue mode.

Syntax

show flows *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

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

Examples

```
G350-001(super)# show flows FastEthernet 10/2
G350-001(super)# show flows Serial 3/1:2
```

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:

```
G350-001(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

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 a Serial interface:

```
G350-001(super)# show frame-relay fragment interface "Serial 5/1"
```

Related commands

clear frame-relay counters, frame-relay class-dlci, interface serial, map-class frame-relay, show frame-relay map, 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:

```
G350-001(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:

```
G350-001(super)# show frame-relay map

Showing 2 frame-relay map entries
Interface StateInterface Type DLCI DLCI Type DLCI State
----------- ------ -------------- ---- --------- ------
Serial 1.1 downpoint-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":

```
G350-001(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 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:

```
G350-001(super)# show frame-relay pvc brief
```

Related commands

clear frame-relay counters, frame-relay class-dlci, interface serial, map-class frame-relay, show frame-relay map, show interfaces

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:

```
G350-001(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 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:

```
G350-001(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 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:

```
G350-001(super)# show icc-vlan
VLAN 1
```

Related commands

icc-vlan

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 software versions:

```
G350-001(super)# show image version

Bank   Version
----   -------
A       3.9.7
B       3.12.10

Module number: 1
```

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, dir, set boot bank, show boot bank, show download software status

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** For Serial(USP): **2/1** For Serial (DS1): module/port: **2/1** channel-group: E1: **0-30** T1: **0-23** For VLAN: **1-3071** 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:

```
G350-001(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, show frame-relay map, 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 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		

Parameter	Description	Possible Values	Default Value
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)

Example

To display detailed information about all access control lists:

```
G350-001(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:

```
G350-001(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:

```
G350-001(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

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

```
G350-001(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 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:

```
G350-001(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 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:

```
G350-001(super)# show ip arp
```

To display one host ARP mapping:

```
G350-001(super)# show ip arp 192.168.49.1
```

To display a range of ARP mappings:

```
G350-001(super)# show ip arp 192.168.49.1 255.255.255.0
```

To display ARP mappings for the VLAN 1 interface:

```
G350-001(super)# show ip arp “Vlan 1”
```

To display static ARP mapping:

```
G350-001(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 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:

```
G350-001(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

show ip-codec-set

Use the **show ip-codec-set** command to display the IP Codec Set as administered in the SLS data set.

Note:

This command is not supported on the G350.

Syntax

show ip-codec-set

User level

read-write

Context

survivable-call-engine

Example

```
G250-001(super-survivable-call-engine)# show ip-codec-set
     IP Codec:     g.711mu Priority 1 Silence n Frames 20
```

Output fields

Field	Description
IP codec	The administered codec type (`g.711mu` or `g.711a`)
Priority	The numeric priority of the codec
Silence	Indicates whether silence suppression is applied (y) or not (n)
Frames	The frame size: 20 mSec

Related commands

clear survivable-config, clear dial-pattern, clear extension, clear trunk-group, save config, set date-format, set dial-pattern, set ip-codec-set, set max-ip-registrations, set survivable-call-engine, show date-format, show dial-pattern, show extension, show last-pim-update, show max-ip-registrations, show survivable-call-engine, show trunk-group, survivable-call-engine

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	Show all active crypto-lists.		
all	Show all crypto-lists.		
detail	Display detailed configuration information.		

User level

read-only

Context

general

Examples

To display the configuration of a specific crypto-list:

```
G350-001(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:

```
G350-001(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.
Description	Crypto map description.

Name	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 not (No).

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

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 context of the interface)

`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: Fast Ethernet 10/2
general

Examples

Example 1:

```
G350-001(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:                           G350-1
Client Identifier:                   01:11:22:33:44:55:66
Requested Options:                   default - router(3)
                                     Dns-servers(6)
                                     Domain-name(15)
Track-id:                            1
```

Example 2:

```
G350-001(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.
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).

Name	Description
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.

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: Fast Ethernet 10/2,
general

Examples

Example 1 shows the usage of the command in the interface context:

```
G350-001(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
```

Example 2 shows the usage of the command in the general context:

```
G350-001# 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

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**	

Parameter	Description	Possible Values	Default Value
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:

```
G350-001(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:

```
G350-001(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:

```
G350-001(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:

```
G350-001(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

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:

```
G350-001(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 that 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:

```
G350-001(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
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

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

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 number 1:

```
G350-001(super)# show ip distribution access-lists 1
```

To display the content of all current distribution lists:

```
G350-001(super)# show ip distribution access-lists
```

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

```
G350-001(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         Fast Ethernet 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.
Interface	The interface running the PPP or DHCP protocol that discovered the DNS server (where applicable).

Field	Description
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.

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

```
G350-001(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 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:

```
G350-001(super)# show ip icmp

ICMP error messages status is ENABLE
```

Related commands

ip icmp-errors

show ip interface

Use the **show ip interface** command to display information about an IP interface.

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		

Parameter	Description	Possible Values	Default Value
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

Examples

To display information for the Fast Ethernet interface:

```
G350-001(super)# show ip interface "FastEthernet 10/2"
```

To display information for the sub-interface 0 of the Fast Ethernet interface:

```
G350-001(super)# show ip interface "FastEthernet 10/2.0"
```

To display all IP interfaces:

```
G350-001(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 will appear:
`Internet address will be negotiated using IPCP`, or `Address determined by IPCP`.

If DHCP client was configured on the interface, the following will appear:
`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

Examples

In the following example, PPP is activated on the FastEthernet interface and no IP address has been gathered:

```
G350-001(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   2/1:1        51.0.0.1            8   manual    up
Console               10.3.0.1           24   manual    down
Usb                  10.3.0.3           24   manual    down
```

In the following example, PPP is activated on the FastEthernet interface and an IP address has been gathered:

```
G350-001(super)# show ip interface brief
Showing 1 Interface
        Interface             Address     Mask Method        Status
------------------------ --------------- ---- ------ --------------------
FastEth  10/2              10.0.0.50         32 IPCP        up
```

In the following example, no IP address has been gathered for the interface configured with DHCP client:

```
G350-001(super)# show ip interface brief
Showing 1 Interface
        Interface             Address     Mask Method        Status
------------------------ --------------- ---- ------ --------------------
FastEth  10/2              unassigned        32 DHCP        down
```

In the following example, an IP address has been gathered for the interface configured with DHCP client:

```
G350-001(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

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**	

User level

read-only

Context

ip pbr-list ip-rule

Examples

```
G350-001(super)# show ip next-hop-list all
Index Name
----- ---------
1 list #1
3 list #3
```

```
G350-001(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 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:

```
G350-001(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	Displays information about the autonomous system boundary router summary LSAs		
router	Displays information about the router LSAs		
network	Displays information about the network LSAs		
network-summary	Displays information about the network LSAs summary		
external	Displays information about the external LSAs		

User level

read-only

Context

general

Example

To display OSPF database information for all router types:

```
G350-001(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:

```
G350-001(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 or for all interfaces.

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 neighbor information for all interfaces:

```
G350-001(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 pbr-list

Use the **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

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)

Example

```
G350-001(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

show ip protocols

Use the **show ip protocols** command to display parameters and statistics of the IP routing protocol process.

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:

```
G350-001(super)# show ip protocols
```

To display RIP details:

```
G350-001(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

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)

Example

To display information about all QoS lists:

```
G350-001(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 on all the interfaces:

```
G350-001(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        PortOperation
----- -------- --- ---------------- --------------- ------- ----------
Deflt  Any     Src  Any AnyTrust-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, queue-limit, set qos bearer, set qos control, set qos signal, show queue, show voip-parameters, voip-queue-delay

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:

```
G350-001(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

show ip route

Use the **show ip route** command to display information about the IP routing table.

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:

```
G350-001(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 a single route:

```
G350-001(super)# show ip route 137.32.50.13
```

To display a range of routes:

```
G350-001(super)# show ip route 137.44.50.13 255.255.255.0
```

Related commands

clear ip route, ip default-gateway, ip route, 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:

```
G350-001(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 route, 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.

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:

```
G350-001(super)# show ip route static
```

To display a single static route:

```
G350-001(super)# show ip route static 137.32.50.13
```

To display a range of static routes:

```
G350-001(super)# show ip route static 137.44.50.13 255.255.255.0
```

```
G350-001(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 route, 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:

```
G350-001(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 route, 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:

```
G350-001(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 route, show ip route, show ip route best-match, show ip route summary, traceroute

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:

```
G350-001(super)# show ip rtp header-compression

IP RTP header compression statistics:

Interface Serial 2/1:1.1:
  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).

Name	Description
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:

```
G350-001(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
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)

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-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:

```
G350-001(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 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

```
G350-001(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

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:

```
G350-001(super)# show ip tcp header-compression
IP TCP header compression statistics:
Interface Serial 2/1:1.1:
  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:

```
G350-001(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

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

```
G350-001(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 G250 or G350 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 statistics:

```
G350-003(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
Total TFTP server errors	The total number of download/upload errors

Name	Description
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

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 ip traffic

Use the **`show ip traffic`** command to display IP counters information.

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:

```
G350-001(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
```

show ip vrrp

Use the **show ip vrrp** command to display VRRP information for a specific VLAN or for all VLANs.

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:

```
G350-001(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:

```
G350-001(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

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:

```
G350-001(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:

```
G350-001(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:

```
G350-001(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

---

show keepalive-icmp

Use the **show keepalive-icmp** command to display information about the extended keepalive settings.

Syntax

show keepalive

User level

read-only

Context

Interface: FastEthernet

Example

```
G350-001(if:FastEthernet 10/2)# show keepalive

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

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 on the G250.

Note:

This command is not supported on the G350.

Syntax

show last-pim-update

User level

read-write

Context

survivable-call-engine

Example

```
G250-001(super-survivable-call-engine)# show last-pim-update
Last PIM update occured at 15:47:0 on 2/28/2005
```

Related commands

station, trunk-group, clear extension, show extension, clear trunk-group, show trunk-group, set max-ip-registrations, show max-ip-registrations, set pim-lockout, show pim-lockout, show, set fac, show fac, clear fac, set date-format, show date-format, set ip-codec-set, copy running-config startup-config, clear survivable-config, survivable-call-engine

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

```
G350-001(super)# show license status
License was installed.
```

Related commands

copy ftp license-file, copy scp license-file, copy tftp license-file, show download license-file status

show list

Use the **show list** command to display information about the specified 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:

```
G350-001(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 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:

```
G350-001(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., G350 Media Gateway, 10/100BaseTx-Pwr
System name = System number 1
System description = Avaya Inc., G350 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.
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.

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

```
G250-001(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 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:

```
G350-001(super)# show logging file condition
*****************************************************
*** Message logging configuration of FILE     sink ***

Sink Is Enabled
Sink default severity: Informational

Facility             ! 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.

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:

```
G350-001(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:

```
G350-001(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:

```
G350-001(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

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:

```
G350-001(super)# show logout
CLI timeout is 15 minutes
```

Related commands

exit, reset, set logout

---

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:

```
G350-001(super)# show map-class frame-relay
Showing 1 frame-relay map-class entry
Map Class Name     CIR       BC        BE      Fragment
-------------- --------- --------- ---------  ---------
default            56000        7000          0            0
```

Related commands

show controllers, show frame-relay fragment, show frame-relay lmi, show frame-relay pvc, show frame-relay traffic, show interfaces, show ip interface

show max-ip-registrations

Use the **show max-ip-registrations** command to display the maximum IP registration administration in the SLS data on the G250.

Note:

This command is not supported on the G350.

Syntax

show max-ip-registrations

User level

read-write

Context

survivable-call-engine

Example

```
G250-001(super-survivable-call-engine)# show max-ip-registrations
Maximum IP Registrations is 12
```

Related commands

station, trunk-group, clear extension, show extension, clear trunk-group, show trunk-group, set max-ip-registrations, set pim-lockout, show pim-lockout, show, set fac, show fac, clear fac, set date-format, show date-format, set ip-codec-set, copy running-config startup-config, clear survivable-config, show last-pim-update, survivable-call-engine

show mediaserver

Use the **show mediaserver** command to show media server configuration information.

Syntax

show mediaserver

User level

read-only

Context

general

Example

To display media server configuration information:

```
G350-001(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 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 685.

Syntax

show mg list_config

User level

read-only

Context

general

Example

To display the list of installed equipment:

```
G350-001(super)# show mg list_config
SLOT  TYPE   CODE    SUFFIX  HW VINTAGE  FW VINTAGE
----  ------ ------  ------  ----------  -----------
v0    G350   PC1053  B       00          0.0.15(B)
v1     -- Not Installed --
v2     -- Not Installed --
v3     -- Not Installed --
v4     -- Not Installed --
```

```
v5      -- Not Installed --
v6      -- Not Installed --
v7      -- Initilalizing --
```

Related commands

set utilization cpu, show faults, show mgc, show mm, show module, show recovery, show restart-log, show status, 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:

```
G350-001(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 status, 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.

On the G250, 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:

```
survivable-call-engine
```

If SLS is disabled, the following message appears at the end of the MGC list:

```
survivable-call-engine    disabled
```

Note:

SLS is not supported by the G350 or the G250-BRI.

Syntax

show mgc list

User level

read-only

Context

general

Example

To display the list of media gateway controllers:

```
G350-001(super)# show mgc list

CONFIGURED MGC HOST
---------------------
135.8.48.220
135.34.54.2
149.49.70.230
```

```
-- Not Available --
```

The following example shows output for the **show mgc list** command in the G250:

```
G250-001(super)# show mgc list

CONFIGURED MGC HOST
---------------------
135.8.48.220
135.34.54.2
149.49.70.230
-- Not Available --
survivable-call-engine
```

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 (--Not Available--) is not used on the G250. • The fifth element is either: - survivable-call-engine — SLS is enabled. - survivable-call-engine 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 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:

```
G350-001(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 status, 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. To view information about all Media Modules, do not specify a Media Module.

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 3:

```
G350-001(super)# show module v3
SLOT TYPE       CODE     SUFFIX  HW VINTAGE  FW VINTAGE
---- ---------  ----     ------  ----------  ----------
v3   DS1        MM710    A       4           5
```

To show information about all media modules:

```
G350-001(super)# show module
SLOT TYPE       CODE     SUFFIX  HW VINTAGE  FW VINTAGE
---- ---------  ----     ------  ----------  ----------
v0   G350       DAF1     A       00          10(B)
v1   ICC        S8300    A       4           6
v2   DCP        MM712    A       3           3
v3   DS1        MM710    A       4           5
v4   -- Not Installed -
v5   -- Not Installed -
v6   PoE        MM314
v7   Analog     (on-board)
```

Related commands

set utilization cpu, show faults, show mg list_config, show mgc, show mm, show recovery, show restart-log, show status, show system, show temp, show timeout, show utilization, show voltages, test led

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

```
G350-001(super)# show mss-notification rate
```

Related commands

DoS-classification, set security-association lifetime

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

```
G350-001(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

---

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.

Note:
This command is not supported on the G350.

Syntax

show pim-lockout

User level

read-only

Context

survivable-call-engine

Example

```
G250-001(super-survivable-call-engine)# show pim-lockout
PIM lockout = yes
```

Related commands

station, trunk-group, clear extension, show extension, clear trunk-group, show trunk-group, set max-ip-registrations, show max-ip-registrations, set pim-lockout, show, set fac, show fac, clear fac, set date-format, show date-format, set ip-codec-set, copy running-config startup-config, clear survivable-config, show last-pim-update, survivable-call-engine

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:

```
G350-001(super)# show pmi
Active PMI     : interface Vlan 1 (172.16.1.139)
Configured PMI : interface Vlan 1 (172.16.1.139)
```

Related commands

pmi

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, 4/5-13 for ports 5 to 13 on module 4.		

User level

read-only

Context

general

Example

To display the status for port 4 on module 3:

```
G350-001(super)# show port 3/4

Port Name    Status  Vlan Level  Neg    Dup. Spd. Type
---- ------- ------- ---- ----- ------- ---- ---- -------------
3/4 NO NAME no link   1    0   enable  half 10M  10/100BaseTx 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	Autonegotiation status of the port — **enabled, disabled**
Dup	Duplex setting for the port — **full, half**
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**

Related commands

show port point-to-point status

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

set 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:

```
G350-001(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 disable, set port duplex, set port edge admin state, set port enable, 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 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, 4/5-13 for ports 5 to 13 on module 4.		

User level

read-only

Context

general

Example

To display information for port 8 of module 4 on the G350:

```
G350-001(super)# show port classification 4/8
Port   Port Classification
------ ---------------------
4/8    regular
```

To display information for port 6 on the front panel of the G250:

```
G250-001(super)# show port classification 10/6
Port   Port Classification
------ ---------------------
10/6    regular
```

Related commands

set port classification

show port dot1x

Use the **show port dot1x** command to display the configurable values associated with the authenticator Port Access Entity (PAE) and backend authenticator.

Syntax

show port dot1x ***[mod[/port]]***

Parameters

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

User level

admin

Context

general

Example

```
G350-001(super)# show port dot1x 3/3
Port   PortAuth  Port     Re   Quiet  ReAuth Server  Supp    Tx     Max
Number Mode      Control  Auth Period Period Timeout Timeout Period Req
------ --------- -------- ---- ------ ------ ------- ------- ------ ---
 3/3   MAC-Based Auto     Disa 60     3600   30      30      30     2

Port   Total Authenticated Authenticating
Number Supps  Supps        Supps
------ ----- ------------- --------------
 3/3   1     0             1
```

Note:

For an explanation of the output fields, see the table describing the output of the **show port dot1x** command in the chapter *Accessing the Avaya G250/G350 Media Gateway*, in *Administration for the Avaya G250 and Avaya G350 Media Gateways*, 03-300436.

Related commands

clear dot1x config, set dot1x m tlv, set dot1x max-req, set dot1x max-supp-per-port, set dot1x port-mode, set dot1x quiet-period, set dot1x re-authperiod, set dot1x server-timeout, set dot1x supp-timeout, set dot1x system-auth-control disable, set dot1x system-auth-control enable, set dot1x tx-period, set port dot1x initialize, set port dot1x port-control, set port dot1x port-mode, set port dot1x re-authenticate, set port dot1x re-authentication, show dot1x, show port dot1x statistics, show port dot1x supp-mac

show port dot1x statistics

Use the **show port dot1x statistics** command to display all the port dot1x statistics.

Syntax

show port dot1x statistics ***[mod[/port]]***

Parameters

Parameter	Description	Possible Values	Default Value
mod	(Optional) Number of the module.		
port	(Optional) Number of the port on the module.		

User level

admin

Context

general

Example

```
MG-1(develop)# show port dot1x statistics 1/1
Port Tx_Req/Id Tx_Req Tx_Total Rx_Start Rx_Logff Rx_Resp/Id Rx_Resp
---- --------- ------ -------- -------- -------- ---------- -------
1/1      2       5        0       0        0          0         0
Port Rx_Invalid Rx_Len_Err Rx_Total Last_Rx_Frm_Ver Last_Rx_Frm_Src_Mac
---- ---------- ---------- -------- --------------- -------------------
1/1      0          0         0            0         1d-80-00-00-00-00
```

Output fields

Field	Description
Port	Port and module numbers.
Tx_Req/Id	Number of EAP request/identity frames sent from the port.
Tx_Req	Number of EAP request frames (excluding request/identity frames) sent from the port.
Tx_Total	Total number of EAP frames of any type that have been sent from the port.
Rx_Start	Number of valid EAP start frames received by the port.
Rx_Logff	Number of EAP logoff frames received by the port.
Rx_Resp/Id	Number of EAP request/identity frames received by the port.
Rx_Resp	Number of valid EAP request frames (excluding response/identity frames) received by the port.
Rx_Invalid	Number of EAP frames of unrecognized frame type received by the port.
Rx_Len_Err	Number of EAP frames of invalid packet body length received by the port.
Rx_Total	Total number of valid EAP frames of any type received by the port.
Last_Rx_Frm_Ver	Number of frames in 802.1x version 1 format received by the port.
Last_Rx_Frm_Src_Mac	Source MAC address of the most recently received EAP frame.

Related commands

clear dot1x config, set dot1x m tlv, set dot1x max-req, set dot1x max-supp-per-port, set dot1x port-mode, set dot1x quiet-period, set dot1x re-authperiod, set dot1x server-timeout, set dot1x supp-timeout, set dot1x system-auth-control disable, set dot1x system-auth-control enable, set dot1x tx-period, set port dot1x initialize, set port dot1x port-control, set port dot1x port-mode, set port dot1x re-authenticate, set port dot1x re-authentication, show dot1x, show port dot1x, show port dot1x supp-mac

show port dot1x supp-mac

Use the **show port dot1x supp-mac** command to display all the port dot1x supplicant MACs.

Syntax

show port dot1x supp-mac [*mod*[*/port*]]

Parameters

Parameter	Description	Possible Values	Default Value
mod	(Optional) Number of the module.		
port	(Optional) Number of the port on the module.		

User level

read-only

Context

general

Example

```
G350-001(super)# show  port dot1x supp-mac
Port   Supplicant        Port Auth  Auth    BEnd  Supplicant
Number MAC               Mode       State   State Status
------ ----------------- ---------- ------- ----- ----------
 6/1   00-10-5a-18-94-e3 MAC-Based  Authed  Idle  Auth
 6/2   N/A               MAC-Based  N/A     N/A   N/A
 6/3   N/A               Port-Based Init    Init  Unauth
```

Output fields

Field	Description
Port Number	Number of the module and port.
Supplicant MAC	The MAC address of the supplicant.
Port Auth Mode	The port authentication mode: Port-based (single supplicant) or MAC based (multiple supplicants).

Field	Description
Auth State	The authentication state. Possible states are: • Init • F-auth • F-Unauth • Disconnected • Connecting • Authenticating • Authenticated • Aborting • Held
BEnd State	The current state of the Backend Authentication machine. Possible states are: • Request • Response • Success • Fail • Timeout • Idle • Initialize
Supplicant Status	The current state of the supplicant. Possible states are: • Auth • Nonauth • N/A

Related commands

clear dot1x config, set dot1x m tlv, set dot1x max-req, set dot1x max-supp-per-port, set dot1x port-mode, set dot1x quiet-period, set dot1x re-authperiod, set dot1x server-timeout, set dot1x supp-timeout, set dot1x system-auth-control disable, set dot1x system-auth-control enable, set dot1x tx-period, set port dot1x initialize, set port dot1x port-control, set port dot1x port-mode, set port dot1x re-authenticate, set port dot1x re-authentication, show dot1x, show port dot1x, show port dot1x statistics

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.

Note:

This command is not supported by the G250.

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, 4/5-13 for ports 5 to 13 on module 4.		

User level

read-only

Context

general

Example

To show edge state for all ports:

```
G350-001(super)# show port edge state
```

Related commands

set port auto-negotiation-flowcontrol-advertisement, set port disable, set port duplex, set port edge admin state, set port enable, 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 G350:

```
G350-101(super)# show port flowcontrol 3/4

Port   Send-Flowcontrol Receive-Flowcontrol
Admin Oper       Admin Oper
------ ----- ----       ----- ----
3/4   off   off        off   off
```

To display flowcontrol information for the front panel of the G250:

```
G250-101(super)# show port flowcontrol 10/4

Port   Send-Flowcontrol Receive-Flowcontrol
Admin Oper       Admin Oper
------ ----- ----       ----- ----
10/4   off   off        off   off
```

Related commands

set port auto-negotiation-flowcontrol-advertisement, set port disable, set port duplex, set port edge admin state, set port enable, 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.
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.

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

```
G350-001(super)# show port lldp config
Port    Port      Port         System   System      System     Management
Number  Status    Description  Name     Description Capability Address      PVID
------  --------  -----------  -------  ----------- ---------- ------------ ------
 6/1    disable   disable      disable  enable      enable     enable       enable
 6/2    txAndRx   disable      disable  enable      enable     disable      disable
 6/3    txAndRx   disable      disable  disable     disable    disable      disable
 6/4    txAndRx   disable      disable  disable     disable    disable      disable
 6/5    txAndRx   disable      disable  disable     disable    disable      disable
 6/6    txAndRx   disable      disable  disable     disable    disable      disable
 6/7    txAndRx   disable      disable  disable     disable    disable      disable
 6/8    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.
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.

Field	Description
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.

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

```
G250-001(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,

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:

```
G350-001(super)# show port mirror
```

Related commands

clear port mirror, set port mirror

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.

Note:

This command is not supported by the G250.

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:

```
G350-001(super)# show port point-to-point status
```

Related commands

show port

---

show port redundancy

Use the **show port redundancy** command to display information about software port redundancy pairs defined on the media gateway.

Note:

This command is not supported by the G250.

Syntax

show port redundancy

User level

read-only

Context

general

Example

To display port redundancy information:

```
G350-001(super)# show port redundancy
Redundancy Name     Primary Port        Secondary Port      Status
-----------------   -------------       ----------------    --------
bud3/48                   3/47   secondary
jack3/46                   3/45  secondary
tony3/1                    3/2   primary
wayne3/34                   3/33  secondary
Minimum Time between Switchovers: 1
Switchback interval: 3
```

Related commands

set port redundancy, set port redundancy on|off, set port redundancy-intervals

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, 4/5-13 for ports 5 to 13 on module 4.		

User level

read-only

Context

general

Example

To display trap information for port 1 of module 4:

```
G350-001(super)# show port trap 4/1
Port 4/1 up/down trap is disabled
```

Related commands - SNMP access configuration

ip snmp-server, 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 user summary, 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

clear snmp trap, set port trap, set snmp trap, show snmp, snmp trap link-status, snmp-server enable notifications, snmp-server host, snmp-server informs

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, 4/5-13 for ports 5 to 13 on module 4.		

User level

read-only

Context

general

Example

To display VLAN binding information for all ports:

```
G350-001(super)# show port vlan-binding-mode

port 2/1 is statically bound
port 2/2 is statically bound
port 2/3 is statically bound
port 2/4 is statically bound
port 2/5 is statically bound
port 2/6 is statically bound
port 2/7 is statically bound
port 2/8 is statically bound
port 2/9 is statically bound
port 2/10 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 powerinline

Use the **show powerinline** command to display the current inline power status of the specified module or port. If no port is specified, information for all ports is displayed.

Note:

This command is not supported by the G250-DCP.

Syntax

show powerinline [*module_number/port_number*]

Parameters

Parameter	Description	Possible Values	Default Value
module_number	The module number		
port_number	The port number		

User level

read-only

Context

general

Example

To display power information for ports on module 6 of the G350:

```
G350-001(super)# show powerinline 6
Actual powerinline power consumption is 30W.
Powerinline power consumption trap threshold is 207 (99%) Watts.
Powerinline traps are enabled
Port  Inline Operational Status  Powering Priority  PD Type
----  -------------------------  -----------------  --------
6/1   Fault                      Low                telephone
6/2   Searching                  Low                telephone
```

Related commands

set port powerinline, set port powerinline priority, set port powerinline type, set powerinline trap disable, set powerinline trap enable

show ppp authentication

Use the **show ppp authentication** command to show the PPP authentication status.

Syntax

show ppp authentication

User level

Read only

Context

Ethernet interface

Example

```
G350-001(super)# show ppp authentication
PAP sent-username: configured
CHAP refuseCHAP hostname: G350
CHAP password: not configured
```

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, pppoe-client wait-for-ipcp

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|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		
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		
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:

```
G350-001(super)# show protocol
Protocols                          Status
------------                       --------
SSH-CLIENT                          ON
TELNET-CLIENT                       OFF
SNMPv1                              ON
SNMPv3                              ON
TELNET                              ON
HTTP                                ON
RECOVERY-PASSWORD                   ON
FTP-CLIENT                          ON
TFTP                                OFF
DHCP                                ON
DNS-CLIENT                          ON
```

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 and RTCP information:

```
G350-001(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

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

Examples

```
G250-001(super)# show queue FastEthernet 10/2
G350-001(super)# show queue Serial 3/1:2
```

Related commands

interface FastEthernet, interface serial, queue-limit, set qos bearer, set qos control, set qos signal, show ip qos-list, show voip-parameters, voip-queue-delay

show queueing

Use the **show queueing** command to display the priority queue size, in packets.

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 Fast Ethernet interface when traffic shaping has been configured.

Example

```
G350-001(super)# show queueing
Current priority queue configuration:

Interface     VOI   Est. Delay    Q.1(High   Q.    Q.    Q.4(Low   DE
Name          P     [ms]          )          2     3     )         Buf
Serial 2/1    OFF   OFF           524        52    52    524       -
                                             4     4
Serial 5/     OFF   OFF           507        50    50    507       507
1:1                                          7     7
```

```
Current voip fair queue configuration:

  Interface     Total       Flow        Dynami    Max voip    Priorit
  Name          discard     discard     c         delay       y
                threshold   threshold   Queue     (ms)        queues
  Serial 3/     256         64          16        20          1
  1:1
```

Output fields

Field	Description
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.
Max voip delay [ms]	Maximum delay for voip bearer. Configurable through the **voip-queue-delay** command.
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 - WFVQ

interface FastEthernet, interface serial, priority-queue

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:

```
G350-001(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

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:

```
G350-001(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 status, 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:

```
G350-001(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 status, show system, show temp, show timeout, show utilization, show voltages, test led

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:

```
G350-001(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

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 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:

```
G350-001(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

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:

```
G350-001(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

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:

```
G350-001(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

rmon alarm, rmon event, rmon history, show rmon alarm, show rmon event, show rmon history

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 current configuration of the RTP statistics application:

```
G350-001(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 G250 and Avaya G350 Media Gateways*, 03-300436.

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:

```
G350-001(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 G250 and Avaya G350 Media Gateways*, 03-300436.

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.

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	Displays only active sessions		
active-events	Displays only active sessions experiencing bad QoS conditions		

Parameter	Description	Possible Values	Default Value
history	Displays only terminated sessions		
events	Displays only terminated sessions that experienced bad QoS conditions		
destination-ip	Displays only sessions to this destination subnet		
remote-subnet	The destination subnet		
remote-subnet-mask	The destination subnet mask		
host	Displays only sessions to this specific address		
rem-addr	The specific IP address		
last	Displays 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:

```
G350-001(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:

```
G350-001(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 G250 and Avaya G350 Media Gateways*, 03-300436.

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

The following summary shows two active sessions, one with QoS problems (35):

```
G350-001(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      2/1      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 G250 and Avaya G350 Media Gateways*, 03-300436.

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:

```
G350-001(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 G250 and Avaya G350 Media Gateways*, 03-300436.

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 G250/G350 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		
last	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:

```
G350-001(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 G250/G350
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 packest 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

show rtr configuration

Use the **show rtr configuration** command to display RTR configuration values, including all defaults, for a specific RTR operation or for all RTR operations.

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

```
G350-001(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 or for all RTR operations.

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

```
G350-001(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
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.

Field	Description
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.

Related commands

rtr, rtr-schedule, show rtr configuration

show running-config

Use the **show running-config** command to display the G250/G350's current configuration.

Syntax

show running-config

User level

read-only

Context

general

Example

To display the current configuration:

```
G350-001(super)# show running-config

G350-001(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 self-test-status

Use the **show self-test-status** command to display the results of the power-up self test sequence.

Syntax

show self-test-status

User level

read-only

Context

general

Example

```
G350-001(super)# show self-test-status
Device successfully passed the power-up self test sequence.
```

Related commands

enhanced security, show system, zeroize

show snmp

Use the **show snmp** command to display SNMP configuration information.

Syntax

show snmp

User level

read-only

Context

general

Example

```
G350-001(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    Notificatio   Trap/    User
                   l              n             Inform   Name
 129.22.22.22      v1     noaut    all           trap     ReadCommN
 UDP port: 162            h
 DM
 129.11.33.44      v2c    noaut    all           inform   WriteComm
 UDP port: 162            h                               N
```

Related commands - SNMP access configuration

ip snmp-server, set snmp community, set snmp retries, set snmp timeout, show port trap, show snmp engineID, show snmp group, show snmp retries, show snmp timeout, show snmp user, show snmp user summary, 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

clear snmp trap, set port trap, set snmp 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

---

show snmp engineID

Use the **show snmp engineID** command to display the SNMP engine ID for the G250/G350.

Syntax

show snmp engineid

User level

admin

Context

general

Example

To display the SNMP engine ID:

```
G350-001(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-server, set snmp community, set snmp retries, set snmp timeout, show port trap, show snmp, show snmp group, show snmp retries, show snmp timeout, show snmp user, show snmp user summary, 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

clear snmp trap, set port trap, set snmp 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.

Syntax

show snmp group

User level

admin

Context

general

Example

```
G350-001(super)# show snmp group

Group Name: defaultROgroup Context:
Security Model: v1
Security Level: noauth
Context Match: exact
Read View: defaultUserView
Write View:
Notify View: defaultUserView
Group Name: defaultROgroup Context:
Security Model: v2c
Security Level: noauth
Context Match: exact
Read View: defaultUserView
Write View:
Notify View: defaultUserView
```

Related commands - SNMP access configuration

ip snmp-server, set snmp community, set snmp retries, set snmp timeout, show port trap, show snmp, show snmp engineID, show snmp retries, show snmp timeout, show snmp user, show snmp user summary, 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

clear snmp trap, set port trap, set snmp 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.

Note:

This command is not supported by the G250.

Syntax

show snmp retries

User level

read-only

Context

general

Example

To display the number of retry attempts:

```
G350-001(super)# show snmp retries
the SNMP Retries Number is 100
```

Related commands - SNMP access configuration

ip snmp-server, set snmp community, set snmp retries, set snmp timeout, show port trap, show snmp, show snmp engineID, show snmp group, show snmp timeout, show snmp user, show snmp user summary, 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

clear snmp trap, set port trap, set snmp 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.

Note:

This command is not supported by the G250.

Syntax

show snmp timeout

User level

read-only

Context

general

Example

To display the timeout value:

```
G350-001(super)# show snmp timeout
the SNMP Timeout is 60
```

Related commands - SNMP access configuration

ip snmp-server, set snmp community, set snmp retries, set snmp timeout, show port trap, show snmp, show snmp engineID, show snmp group, show snmp retries, show snmp user, show snmp user summary, 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

clear snmp trap, set port trap, set snmp 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 the specified SNMP user.

Syntax

show snmp user *username* [*remote EngineID*]

Parameters

Parameter	Description	Possible Values	Default Value
username	The username of the user whose information you wish to display		
remote EngineID	The engine ID of the remote user		

User level

admin

Context

general

Example

```
G350-001(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-server, set snmp community, set snmp retries, set snmp timeout, show port trap, show snmp, show snmp engineID, show snmp group, show snmp retries, show snmp timeout, show snmp user summary, 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

clear snmp trap, set port trap, set snmp 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 user summary

Use the **show snmp user summary** command to display configuration information for all SNMP users.

Syntax

show snmp user summary

User level

admin

Context

general

Related commands - SNMP access configuration

ip snmp-server, set snmp community, set snmp retries, set snmp timeout, show port trap, 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

clear snmp trap, set port trap, set snmp trap, show snmp, snmp trap link-status, snmp-server enable notifications, snmp-server host, snmp-server informs

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	The SNMPv3 username		

User level

admin

Context

general

Example

```
G350-001(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-server, set snmp community, set snmp retries, set snmp timeout, show port trap, show snmp, show snmp engineID, show snmp group, show snmp retries, show snmp timeout, show snmp user, show snmp user summary, 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

clear snmp trap, set port trap, set snmp 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.

Syntax

show snmp view

User level

admin

Context

general

Example

```
G350-001(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-server, set snmp community, set snmp retries, set snmp timeout, show port trap, show snmp, show snmp engineID, show snmp group, show snmp retries, show snmp timeout, show snmp user, show snmp user summary, 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

clear snmp trap, set port trap, set snmp 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 spantree

Use the **show spantree** command to display spanning-tree information. If no port is specified, information for all ports is displayed.

Note:

This command is not supported by the G250.

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:

```
G350-001(super)# show spantree

Spanning tree enabled
Designated Root:  00-40-0d-88-06-c8
Designated Root Priority: 32768
Designated Root Cost: 20
Designated Root Port: 1/1
Root Max Age: 20   Hello Time: 2

Bridge ID MAC ADDR: 00-40-0d-92-04-b4
Bridge ID priority: 32768

Port   State         Cost       Priority
------ ------------- ---------- ------------
4 /1   Forwarding    20         128
4 /2   not-connected 20         128
4 /3   LAG-member    20         128
```

```
4 /4    LAG-member     20          128
4 /5    not-connected  20          128
4 /6    not-connected  20          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
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
Port-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

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

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:

```
G350-001(super)# show startup-config

G350-001(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 status

Use the **show status** command to display the status of the current file copy process to or from the device.

Syntax

show {download | upload} {software [*mmID*] | config} status

Parameters

Parameter	Description	Possible Values	Default Value
download	Keyword specifying that the download status is displayed		
upload	Keyword specifying that the upload status is displayed		
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:

```
G350-001(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 survivable-call-engine

Use the **show survivable-call-engine** command to display SLS status (enabled or disabled).

Note:
This command is not supported on the G350.

Syntax

show survivable-call-engine

User level

read-write

Context

survivable-call-engine

Example

```
G250-001(super)# show survivable-call-engine

Survivable Call Engine is enabled.
```

Related commands

clear survivable-config, clear dial-pattern, clear extension, clear trunk-group, save config, set date-format, set dial-pattern, set ip-codec-set, set max-ip-registrations, set survivable-call-engine, show date-format, show dial-pattern, show extension, show ip-codec-set, show last-pim-update, show max-ip-registrations, show trunk-group, survivable-call-engine

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:

```
G350-001(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

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:

```
G350-001(super)# show system
System Name          :
System Location      :
System Contact       :
Uptime (d,h:m:s)     : 0,7:36:43
MV Time              : N/A
MAC Address          : 00:04:0d:29:c5:11
WAN MAC address      : 00:04:0d:29:c5:10
Serial No            : 03IS12345678
Model No             : G350 Chassis
HW Vintage           : 00
HW Suffix            : B
FW Vintage           : 0.0.15
HW Ready for FIPS     : Yes
```

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 status, show temp, show timeout, show utilization, show voltages, test led

Related commands - FIPS

enhanced security, show self-test-status, zeroize

---

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

```
G350-001(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
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

Output fields

Field	Description
Connections closed normally	The total number of connections closed in the normal manner, using FIN and ACK from both sides
Connections closed on RST	The total number of connections closed on RST from either side
Total discards	The total number of discarded packets
ACK for SYN verification failed	The number of packets discarded due to 3rd ACK verification failure
FIN out-of-sync	The number of packets in which the FIN sequence number was out of the receive window
ACK for FIN out-of-sync	The number of packets in which FIN was previously received but its ACK ack number didn't match the FIN's sequence number
RST out-of-sync	The number of packets in which RST was received but its sequence number did not match
Active sessions	The total number of active inbound sessions
SYN-SENT	The number of sessions that received a valid 3rd ACK from remote peer, and sent SYN to the local peer
ESTABLISHED	The number of established sessions
FIN-WAIT-IN	The number of sessions in which FIN was sent by the local peer
FIN_WAIT_OUT	The number of sessions in which FIN was sent by the remote peer
FINT_WAIT_INOUT	The number of sessions in which FIN was sent by the remote peer and the local peer, but no corresponding ACK has yet been received from either or both sides

Related commands

clear tcp syn-cookies counters, tcp syn-cookies

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:

```
G350-001(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 status, 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:

```
G350-001(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 status, show system, show temp, show utilization, show voltages, test led

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

```
G350-001(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

G350-001(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)
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

Related commands

rtr, track

---

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 G250/G350 device:

```
G350-001(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:

```
G350-001(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

show traffic-shape queue, 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 G250/G350 device:

```
G350-001(super)# show traffic-shape queue

  Traffic queued in shaping queue on 5/1:11.11 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
```

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.

Field	Description
Byte Limit	Maximum number of bytes sent per internal interval.
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.

Related commands

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 G250/G350 device:

```
G350-001(super)# show traffic-shape statistics
                       Queue Packets   Bytes     Packets   Bytes     Shaping
Interface         VC   Depth                     Delayed   Delayed   Active
----------------- ---- ----- -------- ---------- --------- -------- ---------
Serial 5/1:11.11    16     0      455     220218       375    182250    No
Serial 5/0:11.11    20    55      455     220218       375    182250    yes
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 5/11 interface:

```
G250-001(super)# show traffic-shape statistics Serial 5/11:11.11
                       Queue Packets   Bytes     Packets   Bytes     Shaping
Interface         VC   Depth                     Delayed   Delayed   Active
----------------- ---- ----- -------- ---------- --------- -------- ---------
Serial 5/1:11.11    16     0      455     220218       375    182250    No
```

Output fields:

Field	Description
Interface	Interface or sub-interface type and 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

show traffic-shape, show traffic-shape queue

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*[-*port*]]]

Parameters

Parameter	Description	Possible Values	Default Value
module	Number of the module		
port	Number of the port on the module. You can specify a range of ports. For example, use the syntax 4/1-3 to specify ports 1 through 3 on module 4.		

User level

read-only

Context

general

Example

To display binding information for ports 1-3 of module 4:

```
G350-001(super)# show trunk 4/1-3

Port   Mode  Binding mode Native vlan Vlans allowed on trunk
------ ----- ------------- ----------- ----------------
Port   Mode  Binding mode Native vlan Vlans allowed on trunk
------ ----- ------------- ----------- ---------------------
Port   Mode  Binding mode Native vlan Vlans allowed on trunk
------ ----- ------------- ----------- ---------------------
4/3   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 trunk-group

Use the **`show trunk-group`** command to display trunk group administration in Standard Local Survivability (SLS).

Note:

This command is not supported on the G350.

Syntax

`show trunk-group` ***`list`***

Parameters

Parameter	Description	Possible Values	Default Value
`list`	Lists all administered trunk groups Lists only the numbered trunk group Lists the numbered trunk group + “n” entries	**all** **trunk-group** **extension + n**	

User level

read-only

Context

survivable-call-engine

Example

```
G250-001(super-survivable-call-engine)# 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).
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.

Related commands

station, trunk-group, clear extension, show extension, clear trunk-group, set max-ip-registrations, show max-ip-registrations, set pim-lockout, show pim-lockout, show, set fac, show fac, clear fac, set date-format, show date-format, set ip-codec-set, copy running-config startup-config, clear survivable-config, show last-pim-update, survivable-call-engine

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 G250/G350 announcement directory to the Voice Announcements Manager.

Syntax

show upload announcement-file status

User level

read-only

Context

general

Example

In the following example, an upload command has been issued and the upload succeeds:

```
G350-001(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 the following example, an upload command has been issued, but the upload fails:

```
G350-001(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 the following example, no upload command has been issued:

```
G350-001(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 scp announcement-file, erase announcement-file, rename announcement-file, show announcements files, show download announcement-file status

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

If no download was done:

```
G350-001(super)# show upload dhcp-binding-file status

Module #10

===========

No dest file for download operation - no download operation was done.
```

If download was done:

```
G350-001(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
```

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

- If no upload has been performed:

```
G350-001# 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:
G350-003(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 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 status

Use the **show upload status** command to display status information regarding the upload of 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:

```
G350-001(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

show username

Use the **show username** command to display local user accounts.

Syntax

show username

User level

admin

Context

general

Example

To display all the defined user accounts:

```
G350-001(super)# show username
User account   password   access-type
-----------  --------  ------------
root          *****     admin
gkohll        *****     read-only
readwrite      *****      read-write
```

Related commands

username

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:

```
G350-001(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 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	**1-3071**	
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:

```
G350-001(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:

```
G350-001(super)# show vlan 1

VLAN ID Vlan-name
------- --------------------------------
1       V1

Switch Ports currently bound to this vlan:
In module 10: 3
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

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:

```
G350-001(super)# show voip-parameters

VOIP ENGINE PARAMETERS
------------------------------------------------------------
IP (PMI)             : 172.16.1.139
DSP Firmware Version: 200
DSP Hardware Vintage: 1.0
Fault Status         : No Fault Messages
Additional Status    : No Status Messages

CURRENT STATE
------------------------------------------------------------
In Use      : 0 channels, 0 of 300 points (0.0% used)
DSPs State : Idle
Admin State: Release
```

Related commands - VoIP testing

busyout voip-dsp, release voip-dsp, test voip-dsp

Related commands - QoS

interface FastEthernet, interface serial, queue-limit, set qos bearer, set qos control, set qos signal, show ip qos-list, show queue, voip-queue-delay

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:

```
G350-001(super)# show voltages
Voltage Actual  Status  Usage
------- ------  ------  -----
-48.0   -48.761 OK    5V DC2DC, Analog/DCP ports, Fans
5.0     4.947   OK      3.3V DC2DC,1.8V DC-to-DC,Modules logic,
TDM buses TSI
3.3     3.277   OK      2.5V voltage regulator, Motherboard logic
2.5     2.533   OK      CPU & companion chip I/O
1.8     1.787   OK      1.6V voltage regulator,
CPU & companion chip core
1.6     1.583   OK      VoIP DSP
```

Related commands

set utilization cpu, show faults, show mg list config, show mgc, show mm, show module, show recovery, show restart-log, show status, show system, show temp, show timeout, show utilization, test led

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.

Note:

This command is not supported by the G250.

Syntax

show web aux-files-url

User level

read-only

Context

general

Example

To display the URL of the Web server:

```
G350-001(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

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:

```
G350-001(cna-testplug 1)# no shutdown
```

Related commands

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

---

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-L3, DS1 PPP L2, DS1 FR L2, DS1 FR-SUB L2-L3, DS1 FR-SUB L2, USP PPP L2, USP PPP L2-L3, USP FR L2, USP FR-SUB L2, USP FR-SUB L2-L3), FastEthernet (L2, L2-L3), VLAN (L2-L3, L2), Console, Loopback (L2-L3, L2), Controller, Tunnel (L2-L3, L2)

Example

To shutdown the VLAN 2 interface:

```
G350-001(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 modem-type, async reset-modem (Console port), ip address, ppp authentication, speed (PPP), 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

```
G350-001(super-if:USB-Modem)# shutdown
```

Related commands

async reset-modem (USB port), ip address, ppp authentication, shutdown (USB modem), speed (PPP), timeout absolute

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: 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), Tunnel (L2, L2-L3)

Related commands - SNMP access configuration

ip snmp-server, set snmp community, set snmp retries, set snmp timeout, show port trap, show snmp, show snmp engineID, show snmp group, show snmp retries, show snmp timeout, show snmp user, show snmp user summary, 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

clear snmp trap, set port trap, set snmp trap, show snmp, snmp-server enable notifications, snmp-server host, snmp-server informs

snmp-server community

Use the **snmp-server community** command to enable 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

User level

admin

Context

general

Example

G350-001(super)# snmp-server community

Related commands - SNMP access configuration

ip snmp-server, set snmp community, set snmp retries, set snmp timeout, show port trap, show snmp, show snmp engineID, show snmp group, show snmp retries, show snmp timeout, show snmp user, show snmp user summary, 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

clear snmp trap, set port trap, set snmp 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 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***} [**udp-port** ***port***] [***notification_type_list***]

no snmp-server dynamic-trap-manager ***notification_type_list***

Parameters

Parameter	Description	Possible Values	Default Value
traps	Specifies that the dynamic trap manager sends messages without requesting acknowledgement. This is the default.		
informs	Specifies that the dynamic trap manager sends messages requiring acknowledgement.		
v1	Specifies that the dynamic trap manager uses SNMP v1 functionality. This is the default.		
v2c	Specifies that the dynamic trap manager uses SNMP v2c functionality.		
community	The community string for accessing SNMP services.		
port	The udp port of the SNMP host.		
notification_type_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**

User Level

admin

Context

general

Example

```
G350-001(super)# snmp-server dynamic-trap-manager 10.1.2.4 traps v2c
public all
```

Related commands - SNMP access configuration

ip snmp-server, set snmp community, show snmp, show snmp engineID, show snmp group, 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

clear snmp trap, set port trap, set snmp 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 enable notifications

Use the **snmp-server enable notifications** command to enable the sending of all traps and informs from the G350. Use the **no** form of the command to disable the sending of all traps and informs from the G350.

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

G350-001(super)# snmp-server enable notifications

Related commands - SNMP access configuration

ip snmp-server, set snmp community, set snmp retries, set snmp timeout, show port trap, show snmp, show snmp engineID, show snmp group, show snmp retries, show snmp timeout, show snmp user, show snmp user summary, 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

clear snmp trap, set port trap, set snmp 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 engineID

Use the **`snmp-server engineID`** command to specify the SNMP Engine ID for the G350. 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 G250/G350 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

G350-001(super)# snmp-server engineid 00:02:00:81:00:d0:00:4c:18:00

Related commands - SNMP access configuration

ip snmp-server, set snmp community, set snmp retries, set snmp timeout, show port trap, show snmp, show snmp engineID, show snmp group, show snmp retries, show snmp timeout, show snmp user, show snmp user summary, 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

clear snmp trap, set port trap, set snmp 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 {auth|noauth|priv}} [read readviewname] [write writeviewname] [notify notifyviewname]

no snmp-server group groupname [v1|v2c|v3 {noauth|auth|priv}]

Parameters

Parameter	Description	Possible Values	Default Value
groupname	A character string of at most 32 characters specifying the group name		
v1	The group is limited to SNMP v1 functionality		
v2c	The group is limited to SNMP v2c functionality		
v3	The group has full SNMP v3 functionality (this is the default)		
auth	The group authenticates packets		
noauth	The group does not authenticate packets (this is the default)		
priv	The group authenticates and encrypts packets		
readviewname	A character string of at most 64 characters 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.		
writeviewname	A character string of at most 64 characters 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.		
notifyviewname	A character string of at most 64 characters 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.		

User level

admin

Context

general

Example

```
G350-001(super)# snmp-server group 12groupRO v3 auth read view1 notify
view2
```

Related commands - SNMP access configuration

ip snmp-server, set snmp community, set snmp retries, set snmp timeout, show port trap, show snmp, show snmp engineID, show snmp group, show snmp retries, show snmp timeout, show snmp user, show snmp user summary, 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

clear snmp trap, set port trap, set snmp 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 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* | *hostname*} {traps | informs} {{{v1 | v2c} *community*} | {v3 [auth | noauth | priv] *user*}} [udp-port port] [notification-type-list]

no snmp-server host *host_address* [{traps|informs} *notification-type-list*]

Parameters

Parameter	Description	Possible Values	Default Value
host_address	The IP address of the SNMP host.		
hostname	A character string no longer than 32 characters, specifying the hostname of the SNMP host.		
traps	Send traps to this host (messages not requiring acknowledgement). This is the default.		
informs	Send informs to this host (messages requiring acknowledgement).		
v1	Use SNMP v1 functionality with this host.		
v2c	Use SNMP v2c functionality with this host.		
community	The community string to use to connect to the specified host (for v1 or v2c).		
v3	Use SNMP v3 functionality with this host.		
auth	Authenticate messages to this host.		
noauth	Do not authenticate messages to this host (this is the default).		
priv	Authenticate and encrypt messages to this host.		
user	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 -type-list	List of notification types that are enabled for this host. Use the no form of the command to disable specific notification types. The default is none.	**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

```
G350-001(super)# snmp-server host 10.1.2.4 informs v3 auth John
udp-port 789 config generic
```

Related commands - SNMP access configuration

ip snmp-server, set snmp community, set snmp retries, set snmp timeout, show port trap, show snmp, show snmp engineID, show snmp group, show snmp retries, show snmp timeout, show snmp user, show snmp user summary, 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

clear snmp trap, set port trap, set snmp 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*] [timeout *timeout*] [pending *pending*]

Parameters

Parameter	Description	Possible Values	Default Value
retries	The maximum number of times to resend an inform message		3
timeout	The number of seconds to wait for an acknowledgement before resending an inform message		3
pending	The maximum allowable number of inform messages that can be waiting for acknowledgement at any given time. When the maximum is reached, the oldest pending inform messages are discarded.		25

User level

admin

Context

general

Example

```
G350-001(super)# snmp-server informs retries 5 timeout 3
```

Related commands - SNMP access configuration

ip snmp-server, set snmp community, set snmp retries, set snmp timeout, show port trap, show snmp, show snmp engineID, show snmp group, show snmp retries, show snmp timeout, show snmp user, show snmp user summary, 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

clear snmp trap, set port trap, set snmp trap, show snmp, snmp trap link-status, snmp-server enable notifications, snmp-server host

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 SNMPEngineID groupname* {v1|v2c|v3}
[auth {md5|sha} *auth-password* [*priv des56 priv-password*]]

no snmp-server remote-user *username* [*groupname* {v1|v2c|v3}]

Parameters

Parameter	Description	Possible Values	Default Value
username	A character string no longer than 32 characters, specifying the username of this user		
SNMPEngineID	The remote device Engine ID for this user		
groupname	A character string no longer than 32 characters, specifying the groupname this user is associated with		
v1	The user is authorized for SNMP v1 functionality in the specified group		
v2c	The user is authorized for SNMP v2c functionality in the specified group		
v3	The user is authorized for SNMP v3 functionality in the specified group		
auth			
md5	Use the MAC-MD5-96 authentication protocol		
sha	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			
des56			
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

```
G350-001(super)# snmp-server remote-user john
 00:02:00:81:00:d0:00:4c:18:00 L2Group
```

Related commands - SNMP access configuration

ip snmp-server, set snmp community, set snmp retries, set snmp timeout, show port trap, show snmp, show snmp engineID, show snmp group, show snmp retries, show snmp timeout, show snmp user, show snmp user summary, 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

clear snmp trap, set port trap, set snmp 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*]] [volatile]

no snmp-server user *username* [*groupname* {v1|v2c|v3}]]

Parameters

Parameter	Description	Possible Values	Default Value
username	A character string no longer than 32 characters, specifying the username of this user		
groupname	A character string no longer than 32 characters, specifying the groupname this user is associated with		
v1	The user is authorized for SNMP v1 functionality in the specified group		

Parameter	Description	Possible Values	Default Value
v2c	The user is authorized for SNMP v2c functionality in the specified group		
v3	The user is authorized for SNMP v3 functionality in the specified group		
md5	Use the MAC-MD5-96 authentication protocol		
sha	Use the HMAC-SHA-96 authentication protocol		
auth-password	A character string between 8 and 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 between 8 and 64 characters specifying the privacy password. The minimum length is 8 characters.		
volatile	Specifies that the user configurations are only set temporarily, until the system is reset. After reset, the user settings return to their previous values.		

User level

admin

Context

general

Example

```
G350-001(super)# snmp-server user john L2Group v3 auth md5 katmandu
 priv des56 uktanatan
```

Related commands - SNMP access configuration

ip snmp-server, set snmp community, set snmp retries, set snmp timeout, show port trap, show snmp, show snmp engineID, show snmp group, show snmp retries, show snmp timeout, show snmp user, show snmp user summary, 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

clear snmp trap, set port trap, set snmp 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. A 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.

Syntax

snmp-server view *viewname oidtree* {included|excluded}

no snmp-server view *viewname* [*oidtree*]

Parameters

Parameter	Description	Possible Values	Default Value
viewname	The name of the view		
oidtree	The subtree to be included in or excluded from this view. Oidtree 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

```
G350-001(super)# snmp-server view internet 1.3.6.1 included
```

Related commands - SNMP access configuration

ip snmp-server, set snmp community, set snmp retries, set snmp timeout, show port trap, show snmp, show snmp engineID, show snmp group, show snmp retries, show snmp timeout, show snmp user, show snmp user summary, 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

clear snmp trap, set port trap, set snmp 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

---

source-address

Use the **source-address** command to set the source IP address for RTR operations. Use the **no** form of this command to restore the default setting, which is to use the output interface's IP address.

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 type

Examples

```
G350-001(config-rtr icmp 1)# source-address 135.64.102.5
```

Related commands

dscp-table, fail-retries, frequency, next-hop (object tracking), rtr, success-retries, type, wait-interval

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 all packets *except* those coming from the specified IP address.

Syntax

[no] source-ip {host *ip_address* | any | *ip_address wildcard*}

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		
wildcard	A range of IP addresses		

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:

```
G350-110(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

---

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, USB

Example

To set the PPP baud rate to 9600:

```
G350-001(if:CON)# speed 9600
```

Related commands

async mode interactive, async mode terminal, async modem-type, ip address, ppp authentication, shutdown (interface), shutdown (USB modem), timeout absolute

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)

Example

To set the interface speed to 100MB:

```
G350-001(if:FastEthernet 10/2)# speed 100MB
```

Related commands

autoneg, duplex, shutdown (interface), traffic-shape rate

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

```
G350-001(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

station

Use the **station** command within the survivable-call-engine context to enter a second-level subcontext for administering stations for Standard Local Survivability (SLS). After issuing this command the prompt changes to (sls-station-<extension>). Type **exit** to leave the station context, which returns you to the survivable-call-engine context.

Note:

This command is not supported on the G350.

Syntax

station *extension class*

Parameters

Parameter	Description	Possible Values	Default Value
extension	A 1-7 digit unique numeric string	“0” through “9;” an extension can begin with the digit “0.”	
class	Station class	analog dcp ip	

User level

read-write

Context

survivable-call-engine

Example

```
G250-001(super-survivable-call-engine)# station 23456 analog
G250-001(super-sls-station-<extension>)#
```

Related commands

Depending on the class of station the following sub-commands are available:

Command	Analog	DCP	IP
set type	X	X	X
set port	X	X	
set cor	X	X	X
set trunk-destination	X	X	X
set password		X	X
set expansion-module		X	X
set swhook-flash	X		
show	X	X	X

trunk-group, clear extension, show extension, clear trunk-group, show trunk-group, set max-ip-registrations, show max-ip-registrations, set pim-lockout, show pim-lockout, show, set fac, show fac, clear fac, set date-format, show date-format, set ip-codec-set, copy running-config startup-config, clear survivable-config, show last-pim-update, survivable-call-engine

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:

```
G350-001(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:

```
G350-001(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

---

success-retries

Use the **success-retries** command to specify how many consecutive answered probes change the status of an RTR operation device from down to up. Use the **no** form of this command to restore the value to the default.

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 type

Example

```
G350-001(config-rtr icmp 1)# success-retries 3
```

Related commands

dscp-table, fail-retries, frequency, next-hop (object tracking), rtr, source-address, type, wait-interval

---

suggest-key

Use the **suggest-key** utility command to 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.

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	The type of key to be generated.	**alphanumeric** or **hexadecimal**	**alphanumeric**

User level

read-write

Context

crypto isakmp peer

Examples

```
G350-001(config-peer:149.49.70.1)# suggest-key
The suggest key: GNpi1odGNBrB5z4GJLz156jDmRWAGFES
```

```
G350-001(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

---

survivable-call-engine

Use the **survivable-call-engine** command to enter the survivable-call-engine context. In this context, you can administer the standard local survivablility (SLS) data set from the G250 CLI. Type **exit** to leave the survivable call engine context.

Note:

This command not supported on the G350.

Two second-level subcontexts within the survivable-call-engine context permit SLS station (extension) and trunk group administration. Type these commands to enter the respective context:

- **station *extension* [class]** to enter the station context
- **trunk-group *tgnum* [type]** to enter the trunk-group context

Syntax

survivable-call-engine

User level

read-only

Context

general

Example

```
G250-001(super)# survivable-call-engine
G250-001(super-survivable-call-engine)#
```

Related commands

station, trunk-group, clear extension, show extension, clear trunk-group, show trunk-group, set max-ip-registrations, show max-ip-registrations, set pim-lockout, show pim-lockout, show, set fac, show fac, clear fac, set date-format, show date-format, set ip-codec-set, copy running-config startup-config, clear survivable-config, show last-pim-update

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 specify that the rule applies to all ports other than the defined port.

Note:

Issuing this command also sets the protocol to be TCP, if it is not already.

Syntax

tcp destination-port any | **{{eq** | **lt** | **gt}**
{*port_name* | *port_number*}} | **{range *start_port end_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

Example

To specify that the current rule applies to all packets whose destination port is 300:

```
G350-001(ACL 330/ip rule 22)# 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:

```
G350-001(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 specify that the rule applies to all ports other than the defined port.

Note:

Issuing this command also sets the protocol to be TCP, if it is not already.

Syntax

[no] 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

Example

To specify that rule 22 applies to all packets whose source port is greater than 95:

```
G350-001(ACL 330/ip rule 22)# 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

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:

```
G350-001(config)# tcp syn-cookies
To enable tcp syn-cookies copy the running configuration to the
start-upconfiguration file, and reset the device.
G350-001(config)# copy running-config startup-config
G350-001(config)# reset
...
! Coming up from reset - syn-cookies are now enabled
```

To disable SYN cookies:

```
G350-001(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

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:

```
G350-001(super)# tech
Password:
G350-001(tech)#
```

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:

```
G350-001(super)# telnet 133.23.6.66
```

Related commands

ip telnet, ip telnet-client

---

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:

```
G350-001(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 6 characters:

```
G350-001(super)# terminal width 6
```

Related commands

banner login, banner post-login, clear screen, hostname, line, show banner login, show banner post-login, terminal length

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:

```
G350-001(super)# test led
```

The Box level ALM, CPU and MDM LEDs should be BLINKING for 5 seconds each.

Related commands

set utilization cpu, show faults, show mg list config, show mgc, show mm, show module, show recovery, show restart-log, show status, show system, show temp, show timeout, show utilization, show voltages

test voip-dsp

Use the **test voip-dsp** command to start a BTR test on the VoIP engine. Also refer to: busyout voip-dsp on page 51, and release voip-dsp on page 372.

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.

Note:

To view the results of the most recent BTR test, refer to show mm on page 683.

Syntax

test voip-dsp

User level

read-write

Context

general

Example:

To start a BTR test:

```
G350-001(super)# test voip-dsp
DSP TEST RESULTS
-------------------------
DSP 0                   PASS
DSP 1                   PASS
```

Related commands

busyout voip-dsp, release voip-dsp, show voip-parameters

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 G250/G350. 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:

```
G350-001(cna-testplug 1)# test-rate-limit 70 20
```

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)

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

Examples

To specify that for list 5, the state will change from down to up if 4 or more hosts are up:

```
G350-001(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:

```
G350-001(config-track list 5)# threshold count down 2
```

Related commands

description (object tracking), object, track, show track

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

Example

To set the PPP timeout to 30 minutes:

```
G350-001(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 modem-type, async reset-modem (USB port), ip address, ppp authentication, shutdown (interface), shutdown (USB modem), speed (PPP)

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:

```
G350-001(router:rip)# timers basic 30 180
```

Related commands

default-metric (RIP), distribution-list, network (RIP), redistribute (RIP)

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:

```
G350-001(router:ospf)# timers spf 5
```

Related commands

area, default-metric (OSPF), network (OSPF), passive-interface, redistribute (OSPF)

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

Parameter	Description	Possible Values	Default Value
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**
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:

```
G250-001(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 route, show ip route, show ip route best-match, show ip route static, show ip route summary, show ip route track-table

---

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.		

Parameter	Description	Possible Values	Default Value
and	Specifies 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	Specifies 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

Examples

To configure object tracker 1 which tracks RTR 2:

```
G350-001(config)# track 1 rtr 2
G350-001(config-track rtr 1)#
```

To create Track List 5 and specify that its state should be calculated using the Boolean OR argument:

```
G350-001(config)# track 5 list boolean or
G350-001(config-track list 5)#
```

To create Track List 3 and specify that its state should be calculated using a threshold calculation:

```
G350-001(config)# track 3 list threshold count
G350-001(config-track list 3)#
```

Related commands

description (object tracking), object, rtr, threshold count, show track

---

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:

```
G350-001(if:FastEthernet 10/2)# traffic-shape rate 128000
```

Related commands

autoneg, duplex, shutdown (interface), speed (interface)

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:

```
G350-001(if:Serial 5/1)# transmitter-delay 10
```

Related commands

bandwidth, idle-character, ignore dcd, interface serial, invert txclock, nrzi-encoding

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:

```
G350-001(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--
```

trunk-group

Use the **trunk-group** command within the survivable call engine context to enter a second-level subcontext for administering trunks for Standard Local Survivability (SLS). After issuing this command, the prompt changes to (`sls-trunk-group-<tgnum>`). Type **exit** to leave the trunk-group context, which returns you to the survivable-call-engine context.

Note:

This command is not supported on the G350.

Syntax

trunk-group *tgnum* [group-type]

Parameters

Parameter	Description	Possible Values	Default Value
tgnum	The required trunk group number. • G250-Analog and G250-DCP: maximum 2 analog DID trunk groups • G250-BRI and B250 DS1: maximum 1 analog loop-start and 2 analog DID trunk groups.	**1-2000**	
group-type	The trunk group type. This argument is required to enter the trunk-group context.	**loop-start did** (analog)	

User level

read-write

Context

survivable-call-engine

Example

```
G250-001(super-survivable-call-engine)# trunk-group 200 loop-start
G250-001(sls-trunk-group-<tgnum>)#
```

Related commands

Depending on the group type the following sub-commands are available once you are inside the trunk-group context:

Command	Analog loop start	Analog DID
set dial	X	X
set tac	X	X
clear tac	X	X
add port	X	X
remove port	X	X
set digit-treatment		X
set digits		X

1 of 2

Command	Analog loop start	Analog DID
set supervision		X
show	X	X
		2 of 2

station, clear extension, show extension, clear trunk-group, show trunk-group, set max-ip-registrations, show max-ip-registrations, set pim-lockout, show pim-lockout, show, set fac, show fac, clear fac, set date-format, show date-format, set ip-codec-set, copy running-config startup-config, clear survivable-config, show last-pim-update, survivable-call-engine

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

```
G350-001(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

```
G350-001(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

```
G350-001(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

```
G350-001(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

```
G350-001(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	Specifies 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

```
G350-001(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

```
G350-001(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

```
G350-001(super)# tunnel ttl 16
```

Related commands

keepalive (GRE tunnel), tunnel checksum, tunnel destination, tunnel key, tunnel path-mtu-discovery, tunnel source

type

Use the **type** command to specify which type of operation an RTR 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

Examples

```
G350-001(config-rtr 1)# type echo protocol ipIcmpEcho 137.42.11.1
G350-001(config-rtr icmp 1)#
```

```
G350-001(config-rtr 2)# type tcpConnect dest-ipaddr 147.42.11.1
dest-port 80
G350-001(config-rtr tcp 2)#
```

Related commands

dscp-table, fail-retries, frequency, next-hop (object tracking), rtr, source-address, success-retries, wait-interval

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 specify that the rule applies to all ports *other* than the defined port.

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}***

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

Example

To specify that rule 22 applies to all packets whose destination port is 300:

```
G350-001(ACL 330/ip rule 22)# 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 specify that the rule applies to all ports other than the defined port.

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}***

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

Example

To specify that rule 22 applies to all packets whose source port is greater than 95:

```
G350-001(ACL 330/ip rule 22)# 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

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. But you can modify its basic password.

Note:

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

Syntax

username *name* password *passwd* access-type *access_type*

no username *name*

Parameters

Parameter	Description	Possible Values	Default Value
name	New user name	**minimum four character string**	
passwd	User's password	minimum four character string	
access_type	Access type definition	**read-only**, **read-write**, **admin**	

User level

admin

Context

general

Example

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

```
G350-001(super)# username john password johnny access-type read-write
User account added.
```

You cannot change the access type of the root user:

```
G350-001(super)# username root password secret access-type read-write
ERROR: User account root has always an administrator access type.
```

To change the password of the root user:

```
G350-001(super)# username root password secret access-type admin
User account modified.
```

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

show username

---

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):

```
G350-001(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):

```
G350-001(dhcp 5/option 19)# value raw hex 01
```

To set a non-encapsulated value in ASCII format for vendor-specific option 1:

```
G350-001(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:

```
G350-001(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

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:

```
G350-001(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

---

voip-queue

Use the **voip-queue** command to select custom queueing for VoIP traffic. By default, VoIP queuing is off, and Weighted Fair VoIP Queuing (WFVQ) is enabled on all Serial interfaces and all Fast Ethernet 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

Example

To enable VoIP queuing:

```
G350-001(if:Serial 2/1:1)# voip-queue
```

Related commands

fair-queue-limit, fair-voip-queue, voip-queue, voip-queue-delay

voip-queue-delay

Use the **voip-queue-delay** command to set the maximum query delay for which to estimate.

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-classs frame-relay context, to control the specific DLCI queueing parameters.

Syntax

voip-queue-delay *queue_delay_ms*

Parameters

Parameter	Description	Possible Values	Default Value
queue_delay_ms	The maximum amount of time that voice traffic is allowed to wait in the queue	**1-1000**	

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

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:

```
G350-001(super)# voip-queue-delay 30
```

Related commands - QoS

interface FastEthernet, interface serial, queue-limit, set qos bearer, set qos control, set qos signal, show ip qos-list, show queue, show voip-parameters, voip-queue-delay

Related commands - WFVQ

fair-queue-limit, fair-voip-queue, voip-queue-delay

---

wait-interval

Use the **wait-interval** command to specify how long to 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:

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 type

Example

```
G350-001(config-rtr icmp 1)# wait-interval 3 seconds
```

Related commands

dscp-table, fail-retries, frequency, next-hop (object tracking), rtr, source-address, success-retries, type

---

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 G250/G350 announcement directory.

Syntax

zeroize

User level

admin

Context

general

Example

To clear all secret parameters and initialize the NVRAM to its factory defaults:

```
G350-001(super)# zeroize

This command will  restore factory defaults, and disconnect your
existing session.

               *** Zeroize *** - do you want to continue (Y/N)? Y
```

Related commands

enhanced security, show self-test-status, show system

Topical Index of Commands

Numerical

802.1x protocol
- clear dot1x config . . . 70
- set dot1x lldp tlv . . . 410
- set dot1x max-req . . . 411
- set dot1x max-supp-per-port . . . 412
- set dot1x port-mode . . . 413
- set dot1x quiet-period . . . 414
- set dot1x reauthperiod . . . 415
- set dot1x server-timeout . . . 416
- set dot1x supp-timeout . . . 417
- set dot1x system-auth-control disable . . . 418
- set dot1x system-auth-control enable . . . 418
- set dot1x tx-period . . . 419
- set port dot1x initialize . . . 454
- set port dot1x port-control . . . 455
- set port dot1x port-mode . . . 456
- set port dot1x re-authenticate . . . 457
- set port dot1x re-authentication . . . 458
- show dot1x . . . 574
- show port dot1x . . . 692
- show port dot1x statistics . . . 693
- show port dot1x supp-mac . . . 695

A

Announcement files
- copy announcement-file scp . . . 102
- copy scp announcement-file . . . 123
- erase announcement-file . . . 189
- rename announcement-file . . . 374
- show announcements files . . . 536
- show download announcement-file status . . . 575
- show upload announcement-file status . . . 764

ARP table
- arp . . . 37
- arp timeout . . . 38
- clear arp-cache . . . 62
- ip max-arp-entries . . . 260
- ip proxy-arp . . . 276
- show ip arp . . . 607
- show ip reverse-arp . . . 643

Auxiliary files
- set web aux-files-url . . . 533
- show web aux-files-url . . . 773

B

Backup interfaces
- backup delay . . . 44
- backup interface . . . 45

BOOTP relay, *see* DHCP and BOOTP relay

BRI links, *see* Link status

Broadcast relay
- interface FastEthernet . . . 219
- interface serial . . . 221
- interface vlan . . . 224
- ip directed-broadcast . . . 248
- ip netbios-rebroadcast . . . 261

C

CAC, *see* Dynamic CAC

Call admission control, *see* Dynamic CAC

CAM table
- clear cam . . . 64
- show cam . . . 540
- show cam mac . . . 541

Chatter, *see* CNA test plugs

CLI sessions
- exit . . . 191
- reset . . . 376
- set logout . . . 439
- show logout . . . 677

CNA test plugs
- clear counters . . . 66
- cna-testplug . . . 96
- cna-testplug-service . . . 97
- control-port . . . 100
- rtp-echo-port . . . 383
- rtp-test-port . . . 393
- scheduler . . . 397
- show cna testplug . . . 545
- shutdown . . . 773
- test-rate-limit . . . 811

Configuration files
- copy ftp startup-config . . . 114
- copy running-config ftp . . . 120
- copy running-config scp . . . 121
- copy running-config startup-config . . . 122
- copy running-config tftp . . . 122
- copy startup-config ftp . . . 128
- copy startup-config scp . . . 129
- copy startup-config tftp . . . 130

Configuration files, (continued)
copy tftp startup-config . . . 136
erase startup-config . . . 190
nvram initialize . . . 346
show copy status . . . 552
show download status . . . 580
show erase status . . . 583
show logging file condition . . . 673
show running-config . . . 733
show startup-config . . . 746
Connectivity
ping . . . 351
Contact closure
set contact-closure admin . . . 402
set contact-closure pulse-duration . . . 403
show contact-closure . . . 549
Contents Address Memory, *see* CAM table
Converged Network Analyzer, *see* CNA test plugs
CSU loopbacks
show csu loopbacks . . . 569
show csu status . . . 570

D

Default gateway
default gateway . . . 238
Default settings
zeroize . . . 843
Device status
set utilization cpu . . . 531
show faults . . . 587
show mg list_config . . . 680
show mgc . . . 681
show mm . . . 683
show module . . . 685
show recovery . . . 715
show restart-log . . . 716
show status . . . 747
show system . . . 749
show temp . . . 753
show timeout . . . 753
show utilization . . . 768
show voltages . . . 772
test led . . . 810
DHCP and BOOTP relay
interface FastEthernet . . . 219
ip bootp-dhcp server . . . 233
interface vlan . . . 224
ip bootp-dhcp server . . . 233
ip bootp-dhcp network . . . 232
ip bootp-dhcp relay . . . 233
DHCP binding
copy dhcp-binding ftp . . . 106
copy dhcp-binding scp . . . 107
copy dhcp-binding tftp . . . 108
DHCP client
clear ip dhcp-client statistics . . . 74
ip address dhcp . . . 229
ip dhcp client client-id . . . 240
ip dhcp client hostname . . . 241
ip dhcp client lease . . . 242
ip dhcp client request . . . 243, 244
release dhcp . . . 371
renew dhcp . . . 375
show ip dhcp-client . . . 613
show ip dhcp-client statistics . . . 616
DHCP server
clear ip dhcp-server binding . . . 75
clear ip dhcp-server statistics . . . 76
ip dhcp activate pool . . . 239
ip dhcp ping packets . . . 246
ip dhcp ping timeout . . . 246
ip dhcp pool . . . 245
bootfile . . . 50
client-identifier . . . 94
default-router . . . 154
dns-server . . . 174
domain-name . . . 175
end-ip-addr . . . 187
lease . . . 325
name . . . 336
next-server . . . 344
option . . . 348
value . . . 838
server-name . . . 399
show ip dhcp-pool . . . 618
start-ip-addr . . . 796
subnet-mask . . . 798
vendor-specific-option . . . 839
class-identifier . . . 62
value . . . 838
ip dhcp-server . . . 247
show ip dhcp-server bindings . . . 623
show ip dhcp-server statistics . . . 624
Dial backup, *see* Dialer interface
Dialer interface
interface dialer . . . 218
dialer modem-interface . . . 163
dialer order . . . 164
dialer persistent . . . 165
dialer persistent delay . . . 165
dialer persistent initial delay . . . 166
dialer persistent max-attempts . . . 167
dialer persistent re-enable . . . 168
dialer string . . . 168
dialer wait-for-ipcp . . . 169
ip address negotiated . . . 230
ppp ipcp dns request . . . 357
Directed broadcast forwarding, *see* Broadcast relay

Display
banner login . . . 47
banner post-login . . . 47
clear screen . . . 87
hostname . . . 211
line . . . 326
show banner login . . . 538
show banner post-login . . . 539
terminal length . . . 808
terminal width . . . 809
DNS resolver
clear ip domain statistics . . . 77
ip domain list . . . 254
ip domain lookup . . . 255
ip domain name-server-list . . . 255
description (DNS resolver) . . . 156
name-server . . . 337
ip domain retry . . . 256
ip domain timeout . . . 257
nslookup . . . 345
show ip domain . . . 626
show ip domain statistics . . . 628
Dot1x, *see* 802.1x protocol
Dynamic CAC
dynamic-cac . . . 183
show dynamic-cac . . . 582
Dynamic trap manager
snmp-server dynamic-trap-manager . . . 778

E

E1/T1 interfaces
cablelength long . . . 51
cablelength short . . . 52
channel-group . . . 60
clock source . . . 95
controller . . . 100
ds-mode . . . 180
framing . . . 207
interface serial . . . 221
ip address . . . 228
linecode (E1) . . . 327
linecode (T1) . . . 328
remote . . . 372
show controllers . . . 550
show ds-mode . . . 582
Emergency transfer relay, *see* ETR
Ethernet port configuration
set port auto-negotiation-flowcontrol-advertisement . . . 451
set port disable . . . 453
set port duplex . . . 459
set port edge admin state . . . 460
Ethernet port configuration, (continued)
set port enable . . . 461
set port flowcontrol . . . 462
set port level . . . 464
set port name . . . 469
set port negotiation . . . 470
set port point-to-point admin status . . . 471
set port speed . . . 483
show port auto-negotiation-flowcontrol-advertisement . . . 690
show port edge state . . . 696
show port flowcontrol . . . 697
ETR
set etr . . . 422
show etr . . . 584

F

Fan
fan speed low . . . 194
no fan speed level low . . . 194
FIPS
enhanced security . . . 188
show self-test-status . . . 734
show system . . . 749
zeroize . . . 843
Firmware management
copy ftp EW_archive . . . 109
copy ftp module . . . 111
copy ftp SW_imageA . . . 115
copy ftp SW_imageB . . . 116
copy tftp EW_archive . . . 131
copy tftp module . . . 133
copy tftp SW_imageA . . . 137
copy tftp SW_imageB . . . 138
dir . . . 170
set boot bank . . . 401
show boot bank . . . 539
show download software status . . . 579
show image version . . . 597
Firmware, *see* Firmware management
Fragmentation
clear fragment . . . 73
fragment chain . . . 197
fragment size . . . 198
fragment timeout . . . 199
show fragment . . . 589
Frame relay encapsulation
clear frame-relay counters . . . 73
frame-relay class-dlci . . . 200

Frame relay encapsulation, (continued)
interface serial . . . 221
encapsulation . . . 184
frame-relay interface-dlci . . . 201
frame-relay lmi-n391dte . . . 202
frame-relay lmi-n392dte . . . 203
frame-relay lmi-n393dte . . . 204
frame-relay lmi-type . . . 205
frame-relay priority-dlci-group . . . 206
frame-relay traffic-shaping . . . 207
ip address . . . 228
map-class frame-relay . . . 333
bc out . . . 48
be out . . . 49
cir out . . . 61
show frame-relay map . . . 593
show frame-relay pvc brief . . . 595
show interfaces . . . 598

G

GRE tunneling
interface FastEthernet . . . 219
interface tunnel . . . 222
keepalive (GRE tunnel) . . . 322
tunnel checksum . . . 824
tunnel destination . . . 825
tunnel key . . . 827
tunnel path-mtu-discovery . . . 828
tunnel source . . . 830
tunnel ttl . . . 831
tunnel dscp . . . 826
tunnel mode . . . 828

H

Header compression, *see* IPHC header compression, Van Jacobson header compression
HTTP server
ip http . . . 258

I

ICC configuration
icc-vlan . . . 212
show icc-vlan . . . 597
ICMP errors
ip icmp-errors . . . 259
show ip icmp . . . 630
ICMP keepalive
keepalive-icmp . . . 316
keepalive-icmp failure-retries . . . 317
keepalive-icmp interval . . . 318
keepalive-icmp source-address . . . 318
ICMP keepalive, (continued)
keepalive-icmp success-retries . . . 319
keepalive-icmp timeout . . . 320
show keepalive-icmp . . . 667
IP interface configuration
description (interface) . . . 155
interface Console . . . 217
interface dialer . . . 218
interface FastEthernet . . . 219
interface Loopback . . . 220
interface serial . . . 221
interface tunnel . . . 222
interface usb . . . 223
interface vlan . . . 224
ip address . . . 228
ip admin-state . . . 231
ip broadcast-address . . . 234
load-interval . . . 329
show ip interface brief . . . 633
IP phone upgrades
clear ip tftp-server statistics . . . 80
copy ftp phone-image . . . 112
copy ftp phone-script . . . 113
copy phone-script ftp . . . 117
copy phone-script scp . . . 118
copy phone-script tftp . . . 119
copy scp phone-script . . . 126
copy tftp phone-image . . . 134
copy tftp phone-script . . . 135
erase phone-image . . . 189
ip tftp-server file-system size . . . 301
show application-memory . . . 537
show download phone-image-file status . . . 577
show download phone-script-file status . . . 578
show ip tftp-server files . . . 659
show ip tftp-server statistics . . . 660
show upload phone-script-file status . . . 766
IP unnumbered
ip unnumbered . . . 302
IPHC header compression
clear ip rtp header-compression . . . 78
clear ip tcp header-compression . . . 79
ip rtp compression-connections . . . 287
ip rtp header-compression . . . 288
ip rtp max-period . . . 290
ip rtp max-time . . . 291
ip rtp non-tcp-mode . . . 292
ip rtp port-range . . . 293
ip tcp compression-connections . . . 297
show ip rtp header-compression . . . 649
show ip rtp header-compression brief . . . 651
show ip tcp header-compression . . . 656

K

Keepalive, *see* ICMP keepalive
keepalive-track, *see* VPN, WAN Ethernet port configuration

L

License files
- copy ftp license-file . . . 110
- copy scp license-file . . . 125
- copy tftp license-file . . . 132
- show download license-file status . . . 576
- show license status . . . 669

Link status
- show isdn bri link . . . 665
- show isdn link summary . . . 666
- show isdn pri link . . . 666

LLDP
- set lldp re-init-delay . . . 426
- set lldp system-control . . . 426
- set lldp tx-delay . . . 427
- set lldp tx-hold-multiplier . . . 428
- set lldp tx-interval . . . 429
- set port lldp . . . 465
- set port lldp tlv . . . 466
- show lldp . . . 670
- show lldp config . . . 672
- show port lldp config . . . 699
- show port lldp vlan-name config . . . 701

Log file, *see* Logging

Logging
- clear logging file . . . 81
- clear logging server . . . 82
- set logging file . . . 430
- set logging server . . . 431
- set logging server access-level . . . 432
- set logging server condition . . . 433
- set logging server enable/disable . . . 435
- set logging server facility . . . 436
- set logging session . . . 437
- show logging file content . . . 674
- show logging server condition . . . 675
- show logging session condition . . . 677

Loopback signals
- loopback diag . . . 331
- loopback local . . . 331
- loopback remote . . . 332

Loopbacks, *see* CSU loopbacks

M

Media Gateway Controller, *see* MGC configuration

MGC configuration
- clear mgc list . . . 83
- session . . . 400
- set icc-monitoring . . . 424
- set mediaserver . . . 441
- set mgc list . . . 442
- set reset-times . . . 501
- show icc-monitoring . . . 596
- show mediaserver . . . 679
- show mgc . . . 681
- show mgc list . . . 682

Modem configuration
- interface Console . . . 217
  - async mode interactive . . . 39
  - async mode terminal . . . 39
  - async modem-init-string . . . 40
  - async modem-type . . . 41
  - async reset-modem . . . 42
  - ip peer address . . . 274
  - ppp authentication . . . 352
  - shutdown (interface) . . . 774
  - speed (PPP) . . . 794
  - timeout absolute . . . 813
- interface USB
  - async modem-init-string . . . 40
  - async reset-modem . . . 42
  - ip peer address . . . 274
  - ppp authentication . . . 352
  - shutdown (USB modem) . . . 775
  - speed (PPP) . . . 794
  - timeout absolute . . . 813
- interface usb . . . 223
- ppp chap-secret . . . 356

Modem dial backup, *see* Dialer interface

MSS notifications
- DoS-classification . . . 181
- set mss-notification rate . . . 443
- show mss-notification rate . . . 686

N

NetBIOS rebroadcast, *see* Broadcast relay
NVRAM, *see* Configuration files

O

Object tracking
- rtr . . . 394
  - type . . . 832
    - dscp (object tracking) . . . 175
    - fail-retries . . . 192
    - frequency . . . 208
    - next-hop (object tracking) . . . 341
    - source-address . . . 792
    - success-retries . . . 799
    - wait-interval . . . 842
  - rtr-schedule . . . 395
  - show rtr configuration . . . 729
  - show rtr operational-state . . . 731
  - show track . . . 754
  - track . . . 818
    - description (object tracking) . . . 161
    - object . . . 347
    - threshold count . . . 812

Open Shortest Path First, *see* OSPF

OSPF
- ip ospf authentication . . . 264
- ip ospf authentication-key . . . 265
- ip ospf cost . . . 266
- ip ospf dead-interval . . . 267
- ip ospf hello-interval . . . 268
- ip ospf message-digest-key . . . 269
- ip ospf network point-to-multipoint . . . 270
- ip ospf priority . . . 270
- ip ospf router-id . . . 271
- router ospf . . . 381
  - area . . . 36
  - default-metric (OSPF) . . . 152
  - network (OSPF) . . . 339
  - passive-interface . . . 350
  - redistribute (OSPF) . . . 370
  - timers spf . . . 815
- show ip ospf . . . 636
- show ip ospf database . . . 636
- show ip ospf interface . . . 638
- show ip ospf neighbor . . . 639
- show ip protocols . . . 641

P

Packet sniffing
- capture buffer-mode . . . 53
- capture buffer-size . . . 54
- capture filter-group . . . 55
- capture interface . . . 55
- capture max-frame-size . . . 56
- capture start . . . 57
- capture stop . . . 58
- capture-service . . . 59
- clear capture-buffer . . . 64
- ip capture-list . . . 235
  - composite-operation . . . 98
  - cookie . . . 101
  - copy capture-file ftp . . . 103
  - copy capture-file scp . . . 104
  - copy capture-file tftp . . . 105
  - ip-rule . . . 313
    - destination-ip . . . 162
    - dscp . . . 176, 177
    - fragment . . . 196
    - icmp . . . 213
    - ip-protocol . . . 312
    - source-ip . . . 793
    - tcp destination-port . . . 802
    - tcp source-port . . . 804
    - udp destination-port . . . 833
    - udp source-port . . . 835
  - owner . . . 349
  - show ip capture-list . . . 608
  - show upload status . . . 767
- name . . . 336
- show capture . . . 543
- show capture-buffer hex . . . 544
- show ip capture-list . . . 608

Password, *see* Users

PMI
- pmi . . . 352
- show pmi . . . 688

PoE
- set port powerinline . . . 472
- set port powerinline priority . . . 474
- set port powerinline type . . . 475
- set powerinline trap disable . . . 489
- set powerinline trap enable . . . 490
- show powerinline . . . 707

Policy
ip access-control-list . . . 226
cookie . . . 101
ip-fragments-in . . . 310
ip-option-in . . . 311
ip-rule . . . 313
composite-operation . . . 98
destination-ip . . . 162
dscp . . . 176, 177
fragment . . . 196
icmp . . . 213
show composite-operation . . . 548
show ip-rule . . . 653
source-ip . . . 793
tcp destination-port . . . 802
tcp established . . . 803
tcp source-port . . . 804
udp destination-port . . . 833
udp source-port . . . 835
name . . . 336
owner . . . 349
show composite-operation . . . 548
show ip-rule . . . 653
show list . . . 669
ip access-group . . . 227
ip policy-list-copy . . . 275
ip qos-group . . . 276
ip qos-list . . . 277
composite-operation . . . 98
cos . . . 139
dscp . . . 176, 177
fragment . . . 196
name . . . 336
show composite-operation . . . 548
cookie . . . 101
dscp-table . . . 179
composite-operation . . . 98
name . . . 336
show dscp-table . . . 581
ip-rule . . . 313
composite-operation . . . 98
destination-ip . . . 162
icmp . . . 213
show composite-operation . . . 548
show dscp-table . . . 581
show ip-rule . . . 653
source-ip . . . 793
tcp destination-port . . . 802
tcp source-port . . . 804
udp destination-port . . . 833
udp source-port . . . 835
name . . . 336
owner . . . 349
show composite-operation . . . 548

Policy, ip-rule, (continued)
show dscp-table . . . 581
show ip-rule . . . 653
show list . . . 669
ip simulate . . . 294
pre-classification . . . 364
show ip qos-list . . . 642
Policy-based routing
ip next-hop-list . . . 263
next-hop-interface . . . 342
next-hop-ip . . . 343
show next-hop . . . 686
ip pbr-group . . . 272
ip pbr-list . . . 273
ip-rule . . . 313
destination-ip . . . 162
dscp . . . 176, 177
fragment . . . 196
next-hop (policy-based routing) . . . 340
show ip next-hop-list . . . 635
show ip-rule . . . 653
name . . . 336
owner . . . 349
show ip-rule . . . 653
show list . . . 669
show ip active-lists . . . 604
show ip active-pbr-lists . . . 606
show ip pbr-list . . . 640
Port classification
set port classification . . . 452
show port classification . . . 691
Port mirroring
clear port mirror . . . 84
set port mirror . . . 468
show port mirror . . . 702
Port redundancy
set port redundancy . . . 476
set port redundancy on|off . . . 477
set port redundancy-intervals . . . 478
show port redundancy . . . 704
Port status
show port . . . 688
show port point-to-point status . . . 703
Power over Ethernet, *see* PoE
PPP encapsulation
interface dialer . . . 218
interface FastEthernet (PPPoE only) . . . 219
interface serial . . . 221
encapsulation . . . 184
ip address . . . 228
keepalive (PPP) . . . 323
ppp timeout ncp . . . 359
ppp timeout retry . . . 360
show interfaces . . . 598
PPP over Ethernet, *see* PPPoE

PPPoE
interface FastEthernet . . . 219
encapsulation pppoe . . . 185
ip address negotiated . . . 230
mtu . . . 335
ppp chap hostname . . . 353
ppp chap password . . . 354
ppp ipcp dns request . . . 357
ppp pap-sent username . . . 358
pppoe-client persistent delay . . . 360
pppoe-client persistent max-attempts . . . 361
pppoe-client service-name . . . 362
pppoe-client wait-for-ipcp . . . 363
show ppp authentication . . . 708
ppp chap refuse . . . 355
ppp pap refuse . . . 357
PRI links, *see* Link status
Primary management interface, *see* PMI
Proxy ARP
ip proxy-arp . . . 276

Q

QoS
interface FastEthernet . . . 219
voip-queue-delay . . . 841
interface serial . . . 221
voip-queue-delay . . . 841
queue-limit . . . 368
set qos bearer . . . 490
set qos control . . . 492
set qos signal . . . 495
show queue . . . 712
show voip-parameters . . . 771
QoS, *see* RTP, RTCP, RSVP, WFVQ

R

RADIUS authentication
clear radius authentication server . . . 86
set radius authentication . . . 496
set radius authentication retry-number . . . 497
set radius authentication retry-time . . . 498
set radius authentication secret . . . 498
set radius authentication server . . . 499
set radius authentication udp-port . . . 500
show radius authentication . . . 714
Recovery password
set terminal recovery password . . . 526
Redundancy, *see* Port redundancy
RIP
ip distribution access-list . . . 249
ip rip authentication key . . . 278
ip rip authentication mode . . . 279
ip rip default-route-mode . . . 280
ip rip poison-reverse . . . 281
ip rip rip-version . . . 282
ip rip send-receive-mode . . . 283
ip rip split-horizon . . . 284
router rip . . . 382
default-metric (RIP) . . . 152
distribution-list . . . 173
network (RIP) . . . 338
timers basic . . . 814
show ip protocols . . . 641
RMON monitoring
rmon alarm . . . 378
rmon event . . . 379
rmon history . . . 380
show rmon alarm . . . 717
show rmon event . . . 718
show rmon history . . . 719
show rmon statistics . . . 720
Route redistribution
default-metric (interface route metric value) . . . 153
redistribute (OSPF) . . . 370
redistribute (RIP) . . . 369
Routing information protocol, *see* RIP
Routing table configuration
clear ip route . . . 77
ip default-gateway . . . 238
ip route . . . 285
show ip route . . . 644
show ip route best-match . . . 646
show ip route static . . . 647, 648
show ip route summary . . . 648
traceroute . . . 816
RSVP
set qos rsvp . . . 493
show qos-rtcp . . . 710
RTCP
set qos rtcp . . . 494
show qos-rtcp . . . 710
RTP
interface serial . . . 221
RTP header compression, *see* IPHC header compression
RTP MIB, *see* RTP statistics

RTP statistics
rtp-stat clear . . . 383
rtp-stat event-threshold . . . 384
rtp-stat fault . . . 386
rtp-stat min-stat-win . . . 387
rtp-stat qos-trap . . . 388
rtp-stat qos-trap-rate-limit . . . 389
rtp-stat service . . . 390
rtp-stat threshold . . . 390
show rtp-stat config . . . 721
show rtp-stat detailed . . . 722
show rtp-stat sessions . . . 723
show rtp-stat summary . . . 725
show rtp-stat thresholds . . . 726
show rtp-stat traceroute . . . 727
RTR, *see* Object tracking

S

SAA, *see* Object tracking
SAT
sat . . . 395
Session logs, *see* Logging
SLS survivability
survivable-call-engine . . . 801
clear dial-pattern . . . 69
clear extension . . . 71
clear survivable-config . . . 89
clear trunk-group . . . 91
save config . . . 396
set date-format . . . 405
set dial-pattern . . . 406
set ip-codec-set . . . 425
set max-ip-registrations . . . 440
set survivable-call-engine . . . 517
show date-format . . . 572
show dial-pattern . . . 573
show extension . . . 584
show ip-codec-set . . . 609
show last-pim-update . . . 668
show max-ip-registrations . . . 679
show survivable-call-engine . . . 748
show trunk-group . . . 762
trunk-group
clear tac . . . 90
SNMP access configuration
ip snmp-server . . . 295
set snmp community . . . 503
set snmp retries . . . 504
set snmp timeout . . . 505
show port trap . . . 705
show snmp . . . 735
show snmp engineID . . . 736
show snmp group . . . 737
show snmp retries . . . 738
SNMP access configuration, (continued)
show snmp timeout . . . 739
show snmp user . . . 740
show snmp user summary . . . 741
show snmp usertogroup . . . 741
show snmp view . . . 743
snmp-server community . . . 777
snmp-server engineID . . . 780
snmp-server group . . . 781
snmp-server remote-user . . . 787
snmp-server user . . . 789
snmp-server view . . . 791
SNMP trap configuration
clear snmp trap . . . 87
set port trap . . . 485
set snmp trap . . . 506
show snmp . . . 735
snmp trap link-status . . . 776
snmp-server enable notifications . . . 779
snmp-server host . . . 783
snmp-server informs . . . 786
Software management, *see* Firmware management
Spanning tree
set port spantree . . . 479
set port spantree cost . . . 480
set port spantree force-protocol-migration . . . 481
set port spantree priority . . . 482
set spantree default-path-cost . . . 508
set spantree enable/disable . . . 509
set spantree forward-delay . . . 510
set spantree hello-time . . . 511
set spantree max-age . . . 512
set spantree priority . . . 513
set spantree tx-hold-count . . . 514
set spantree version . . . 515
show spantree . . . 744
SSH protocol
clear ssh-client known-hosts . . . 88
crypto key generate . . . 150
disconnect ssh . . . 172
ip ssh . . . 296
show ip ssh . . . 654
Standard Local Survivability, *see* SLS survivability
Status of the device, *see* Device status
Switch Ethernet ports, *see* Ethernet port configuration
Synchronization
clear sync interface . . . 89
set sync interface . . . 519
set sync source . . . 520
set sync switching . . . 521
show sync timing . . . 749
SYN-cookies
clear tcp syn-cookies counters . . . 91
show tcp syn-cookies . . . 750
tcp syn-cookies . . . 806

Syslog, *see* Logging
System Access Terminal, *see* SAT
System identification
set system contact . . . 522
set system location . . . 523
set system name . . . 524

T

TCP header compression, *see* IPHC header compression, Van Jacobson header compression
Telnet access
ip telnet . . . 299
ip telnet-client . . . 300
telnet . . . 807
Terminal display, *see* Display
TFTP server
IP phone upgrades, *see* IP phone upgrades
ip tftp-server . . . 300
ip tftp-server file-system size . . . 301
Traffic shaping
show traffic-shape . . . 756
show traffic-shape queue . . . 757
show traffic-shape statistics . . . 759

U

Upgrading firmware, *see* Firmware management
Users
show username . . . 768
username . . . 837
USP configuration
interface serial . . . 221
bandwidth . . . 46
idle-character . . . 215
ignore dcd . . . 216
invert txclock . . . 226
nrzi-encoding . . . 345
transmitter-delay . . . 821

V

Van Jacobson header compression
clear ip tcp header-compression . . . 79
ip tcp compression-connections . . . 297
ip tcp header-compression . . . 297
show ip tcp header-compression . . . 656
Verifying WAN configuration
show controllers . . . 550
show frame-relay fragment . . . 589
show frame-relay lmi . . . 590
show frame-relay pvc . . . 593
show frame-relay traffic . . . 596
show interfaces . . . 598
show ip interface . . . 630
show map-class frame-relay . . . 678
Virtual Private Networks, *see* VPN
VLAN configuration
clear port static-vlan . . . 85
clear vlan . . . 93
icc-vlan . . . 212
set port static-vlan . . . 484
set port vlan . . . 486
set port vlan-binding-mode . . . 488
set trunk . . . 527
set vlan . . . 532
show cam vlan . . . 542
show port vlan-binding-mode . . . 706
show trunk . . . 761
show vlan . . . 769
VoIP QoS, *see* QoS
VoIP testing
busyout voip-dsp . . . 51
release voip-dsp . . . 372
show voip-parameters . . . 771
test voip-dsp . . . 810
VPN
clear crypto isakmp . . . 67
clear crypto sa . . . 68
clear crypto sa counters . . . 69
crypto ipsec df-bit . . . 140
crypto ipsec minimal-pmtu . . . 141
crypto ipsec nat-transparency udp-encapsulation 141
crypto ipsec transform-set . . . 142
mode . . . 334
set pfs . . . 448
set security-association lifetime . . . 502
crypto isakmp invalid-spi-recovery . . . 144
crypto isakmp nat keepalive . . . 144
crypto isakmp peer . . . 145
continuous-channel . . . 99
description (ISAKMP peer) . . . 158
initiate mode aggressive . . . 216
isakmp-policy . . . 315
keepalive (VPN) . . . 324
keepalive-track . . . 321
pre-shared-key . . . 365
self-identity . . . 398
suggest-key . . . 800
crypto isakmp peer-group . . . 146
description (ISAKMP peer group) . . . 159
set peer (peer group) . . . 446
crypto isakmp policy . . . 148
authentication . . . 43
description (ISAKMP policy) . . . 157
encryption . . . 186
group . . . 209
hash . . . 210
lifetime . . . 325
crypto isakmp suggest-key . . . 149

VPN, (continued)
crypto map . . . 151
continuous-channel . . . 99
description (crypto map) . . . 156
set dscp . . . 420
set peer (crypto map) . . . 445
set peer-group . . . 447
set transform-set . . . 526
interface
ip crypto-group . . . 236
ip crypto-list . . . 237
ip-rule . . . 314
description (ip rule) . . . 160
destination-ip . . . 162
protect crypto map . . . 367
source-ip . . . 793
local-address . . . 330
show crypto ipsec sa . . . 553
show crypto ipsec transform-set . . . 561
show crypto isakmp peer . . . 563
show crypto isakmp peer-group . . . 564
show crypto isakmp policy . . . 565
show crypto isakmp sa . . . 566
show crypto map . . . 568
show ip active-lists . . . 604
show ip crypto-list . . . 610
VPN license, *see* License files
VRRP
ip vrrp . . . 303
ip vrrp address . . . 304
ip vrrp auth-key . . . 305
ip vrrp override addr owner . . . 306
ip vrrp preempt . . . 306
ip vrrp primary . . . 307
ip vrrp priority . . . 308
ip vrrp timer . . . 309
router vrrp . . . 382
show ip vrrp . . . 663

W

WAN Ethernet port configuration
autoneg . . . 451
interface FastEthernet . . . 219
autoneg . . . 44
duplex . . . 182
keepalive-track . . . 321
shutdown (interface) . . . 774
speed (interface) . . . 795
traffic-shape rate . . . 820
WAN interfaces, *see* E1/T1 interfaces, USP interfaces, PPP encapsulation, PPPoE, Frame relay encapsulation, Verifying WAN configuration
Weighted Fair VoIP Queuing, *see* WFVQ
WFVQ
interface FastEthernet . . . 219
fair-queue-limit . . . 192
fair-voip-queue . . . 193
priority-queue . . . 366
voip-queue . . . 840
voip-queue-delay . . . 841
interface serial . . . 221
fair-queue-limit . . . 192
fair-voip-queue . . . 193
priority-queue . . . 366
voip-queue . . . 840
voip-queue-delay . . . 841
show queueing . . . 713