下一代智能防火墙

Web配置手册

（适用于F5600-14G-4F）



非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分全部，

并不得以任何形式传播。本文档中的信息可能变动，恕不另行通知。

修订时间：2017年4月20日

|  |
| --- |
|  |

目录

[1 W入门命令 1](#_Toc434414251)

[1.1 系统时间命令 1](#_Toc434414252)

[1.1.1 date 1](#_Toc434414253)

[1.1.2 ntp 1](#_Toc434414254)

[1.1.3 ntpupdate 2](#_Toc434414255)

[1.1.4 show date 2](#_Toc434414256)

[1.1.5 show ntp config 3](#_Toc434414257)

[1.1.6 show timezone 3](#_Toc434414258)

[1.1.7 timezone 4](#_Toc434414259)

[1.2 系统升级命令 4](#_Toc434414260)

[1.2.1 copy ftp 4](#_Toc434414261)

[1.3 配置文件命令 5](#_Toc434414262)

[1.3.1 save config 5](#_Toc434414263)

[1.3.2 copy startup-config backup-config 6](#_Toc434414264)

[1.3.3 copy backup-config startup-config 6](#_Toc434414265)

[1.3.4 copy running-config backup-config 7](#_Toc434414266)

[1.3.5 copy running-config startup-config 7](#_Toc434414267)

[1.3.6 copy file ftp 8](#_Toc434414268)

[1.3.7 copy file tftp 9](#_Toc434414269)

[1.3.8 copy ftp 9](#_Toc434414270)

[1.3.9 copy tftp 10](#_Toc434414271)

[1.3.10 erase startup-config 10](#_Toc434414272)

[1.4 管理员命令 11](#_Toc434414273)

[1.4.1 authorized 11](#_Toc434414274)

[1.4.2 authorized-table 12](#_Toc434414275)

[1.4.3 guish admin unique 13](#_Toc434414276)

[1.4.4 guish autosave 13](#_Toc434414277)

[1.4.5 guish maxclient 14](#_Toc434414278)

[1.4.6 guish timeout 14](#_Toc434414279)

[1.4.7 user administrator authorized-address 15](#_Toc434414280)

[1.4.8 user administrator local 15](#_Toc434414281)

[1.4.9 user administrator ldap 16](#_Toc434414282)

[1.4.10 user administrator radius 17](#_Toc434414283)

[1.5 常用系统管理命令 18](#_Toc434414284)

[1.5.1 clear user 18](#_Toc434414285)

[1.5.2 ping 18](#_Toc434414286)

[1.5.3 ping6 19](#_Toc434414287)

[1.5.4 show version 20](#_Toc434414288)

[1.5.5 tcpsyn 21](#_Toc434414289)

[1.5.6 traceroute 22](#_Toc434414290)

[1.5.7 who 23](#_Toc434414291)

[2 接口 24](#_Toc434414292)

[2.1 以太网端口配置命令 24](#_Toc434414293)

[2.1.1 allow access 24](#_Toc434414294)

[2.1.2 auto-negotiate 25](#_Toc434414295)

[2.1.3 duplex 25](#_Toc434414296)

[2.1.4 ip address 26](#_Toc434414297)

[2.1.5 ip address dhcp 27](#_Toc434414298)

[2.1.6 ip address pppoe 27](#_Toc434414299)

[2.1.7 ipv6 address 28](#_Toc434414300)

[2.1.8 mtu 28](#_Toc434414301)

[2.1.9 show interface 29](#_Toc434414302)

[2.1.10 shutdown 30](#_Toc434414303)

[2.1.11 speed 30](#_Toc434414304)

[2.2 聚合接口配置命令 31](#_Toc434414305)

[2.2.1 aggregate-group 31](#_Toc434414306)

[2.2.2 interface 32](#_Toc434414307)

[2.3 VLAN接口配置命令 32](#_Toc434414308)

[2.3.1 interface 32](#_Toc434414309)

[2.4 透明网桥配置命令 33](#_Toc434414310)

[2.4.1 bridge forward-delay 33](#_Toc434414311)

[2.4.2 bridge hello-time 34](#_Toc434414312)

[2.4.3 bridge max-age 34](#_Toc434414313)

[2.4.4 bridge priority 35](#_Toc434414314)

[2.4.5 bridge stp 35](#_Toc434414315)

[2.4.6 bridge-group 36](#_Toc434414316)

[2.4.7 interface 36](#_Toc434414317)

[2.4.8 show bridge-group 37](#_Toc434414318)

[2.5 隧道接口配置命令 38](#_Toc434414319)

[2.5.1 interface tunnel 38](#_Toc434414320)

[2.5.2 show interface 39](#_Toc434414321)

[2.5.3 tunnel destination 40](#_Toc434414322)

[2.5.4 tunnel source 41](#_Toc434414323)

[3 DHCP命令 42](#_Toc434414324)

[3.1 DHCP命令 42](#_Toc434414325)

[3.1.1 bind 42](#_Toc434414326)

[3.1.2 dhcprelay 42](#_Toc434414327)

[3.1.3 exclude 44](#_Toc434414328)

[3.1.4 share-net 44](#_Toc434414329)

[3.1.5 share-net dns 45](#_Toc434414330)

[3.1.6 share-net domain 46](#_Toc434414331)

[3.1.7 share-net subnet 47](#_Toc434414332)

[3.1.8 share-net wins 48](#_Toc434414333)

[3.1.9 show dhcp config 49](#_Toc434414334)

[3.1.10 show dhcp ip active 49](#_Toc434414335)

[4 路由配置 51](#_Toc434414336)

[4.1 静态路由配置命令 51](#_Toc434414337)

[4.1.1 ip route 51](#_Toc434414338)

[4.2 路由显示命令 52](#_Toc434414339)

[4.2.1 show ip route 52](#_Toc434414340)

[4.2.2 show ip route *address* 54](#_Toc434414341)

[4.3 策略路由命令 55](#_Toc434414342)

[4.3.1 proute 55](#_Toc434414343)

[4.3.2 proute insert 56](#_Toc434414344)

[4.3.3 proute move 58](#_Toc434414345)

[4.3.4 show proute 58](#_Toc434414346)

[4.4 ISP路由命令 59](#_Toc434414347)

[4.4.1 isp network 59](#_Toc434414348)

[4.4.2 subnet 60](#_Toc434414349)

[4.5 RIP 60](#_Toc434414350)

[4.5.1 default-information originate 60](#_Toc434414351)

[4.5.2 default-metric 61](#_Toc434414352)

[4.5.3 distance 62](#_Toc434414353)

[4.5.4 ip rip authentication key-chain 62](#_Toc434414354)

[4.5.5 ip rip authentication mode 63](#_Toc434414355)

[4.5.6 ip rip authentication string 65](#_Toc434414356)

[4.5.7 ip rip receive 65](#_Toc434414357)

[4.5.8 ip rip send 67](#_Toc434414358)

[4.5.9 ip rip split-horizon 68](#_Toc434414359)

[4.5.10 key 68](#_Toc434414360)

[4.5.11 key chain 69](#_Toc434414361)

[4.5.12 key-string 70](#_Toc434414362)

[4.5.13 network 71](#_Toc434414363)

[4.5.14 passive-interface 72](#_Toc434414364)

[4.5.15 redistribute 73](#_Toc434414365)

[4.5.16 router rip 74](#_Toc434414366)

[4.5.17 show ip rip 74](#_Toc434414367)

[1.1.1 show ip rip status 75](#_Toc434414368)

[4.5.18 version 78](#_Toc434414369)

[4.6 OSPF命令 79](#_Toc434414370)

[4.6.1 area { *ip-address* | *router-id* } authentication 79](#_Toc434414371)

[4.6.2 area { ip-address | router-id } range 80](#_Toc434414372)

[4.6.3 distance 81](#_Toc434414373)

[4.6.4 default-metric 82](#_Toc434414374)

[4.6.5 default-information originate 83](#_Toc434414375)

[4.6.6 ip ospf authentication 84](#_Toc434414376)

[4.6.7 ip ospf authentication-key 84](#_Toc434414377)

[4.6.8 ip ospf cost 85](#_Toc434414378)

[4.6.9 ip ospf dead-interval 85](#_Toc434414379)

[4.6.10 ip ospf hello-interval 86](#_Toc434414380)

[4.6.11 ip ospf message-digest-key 87](#_Toc434414381)

[4.6.12 ip ospf network 87](#_Toc434414382)

[4.6.13 ip ospf priority 88](#_Toc434414383)

[4.6.14 ip ospf retransmit-interval 89](#_Toc434414384)

[4.6.15 ip ospf transmit-delay 89](#_Toc434414385)

[4.6.16 network 90](#_Toc434414386)

[4.6.17 redistribute 91](#_Toc434414387)

[4.6.18 router-id 92](#_Toc434414388)

[4.6.19 router ospf 92](#_Toc434414389)

[4.6.20 show ip ospf 93](#_Toc434414390)

[4.6.21 show ip ospf database 94](#_Toc434414391)

[4.6.22 show ip ospf interface 95](#_Toc434414392)

[4.6.23 timers spf 96](#_Toc434414393)

[5 VRF 98](#_Toc434414394)

[5.1 VRF配置命令 98](#_Toc434414395)

[5.1.1 ip vrf 98](#_Toc434414396)

[5.1.2 ip vrf forwarding 98](#_Toc434414397)

[5.1.3 ip route vrf 99](#_Toc434414398)

[5.1.4 show ip route vrf 100](#_Toc434414399)

[5.1.5 show ip vrf 101](#_Toc434414400)

[6 NAT 103](#_Toc434414401)

[6.1 NAT地址池配置命令 103](#_Toc434414402)

[6.1.1 ip nat pool 103](#_Toc434414403)

[6.1.2 ip address 103](#_Toc434414404)

[6.2 源NAT配置命令 104](#_Toc434414405)

[6.2.1 ip nat source 104](#_Toc434414406)

[6.3 目的NAT配置命令 105](#_Toc434414407)

[6.3.1 ip nat destination 105](#_Toc434414408)

[6.4 静态NAT配置命令 106](#_Toc434414409)

[6.4.1 ip nat static 106](#_Toc434414410)

[6.5 NAT规则移动配置命令 107](#_Toc434414411)

[6.5.1 ip nat { static | source | destination } move 107](#_Toc434414412)

[7 DNS命令 108](#_Toc434414413)

[7.1 DNS命令 108](#_Toc434414414)

[7.1.1 clear dns cache 108](#_Toc434414415)

[7.1.2 dns 108](#_Toc434414416)

[7.1.3 dns host-name 109](#_Toc434414417)

[7.1.4 dns server 110](#_Toc434414418)

[7.1.5 show dns cache 110](#_Toc434414419)

[7.1.6 show dns cache statistics 111](#_Toc434414420)

[7.1.7 show running-config dns 112](#_Toc434414421)

[8 无线3G命令 113](#_Toc434414422)

[8.1 无线3G命令 113](#_Toc434414423)

[8.1.1 access-type 113](#_Toc434414424)

[8.1.2 auth password 114](#_Toc434414425)

[8.1.3 auth username 114](#_Toc434414426)

[8.1.4 dialer mode 116](#_Toc434414427)

[8.1.5 dialer string 116](#_Toc434414428)

[8.1.6 show interface cell3g0 117](#_Toc434414429)

[9 地址探测 119](#_Toc434414430)

[9.1 地址探测配置命令 119](#_Toc434414431)

[9.1.1 show track 119](#_Toc434414432)

[9.1.2 track（系统视图） 120](#_Toc434414433)

[9.2 地址探测组配置命令 122](#_Toc434414434)

[9.2.1 description 122](#_Toc434414435)

[9.2.2 member 122](#_Toc434414436)

[9.2.3 mode strict 123](#_Toc434414437)

[9.2.4 show track-group 124](#_Toc434414438)

[9.2.5 track-group 125](#_Toc434414439)

[9.3 接口状态探测 125](#_Toc434414440)

[9.3.1 track（接口模式） 125](#_Toc434414441)

[9.4 地址探测和HA联动 126](#_Toc434414442)

[9.4.1 track（HA视图） 126](#_Toc434414443)

[10 安全策略 128](#_Toc434414444)

[10.1 安全策略配置命令 128](#_Toc434414445)

[10.1.1 policy 128](#_Toc434414446)

[10.2 安全策略修改命令 129](#_Toc434414447)

[10.2.1 application 129](#_Toc434414448)

[10.2.2 dest-address 129](#_Toc434414449)

[10.2.3 disable 130](#_Toc434414450)

[10.2.4 enable 130](#_Toc434414451)

[10.2.5 in-interface 131](#_Toc434414452)

[10.2.6 out-interface 131](#_Toc434414453)

[10.2.7 schedule 132](#_Toc434414454)

[10.2.8 service 132](#_Toc434414455)

[10.2.9 source-address 133](#_Toc434414456)

[10.2.10 timeout 133](#_Toc434414457)

[10.2.11 user 134](#_Toc434414458)

[10.3 安全策略移动命令 135](#_Toc434414459)

[10.3.1 policy move 135](#_Toc434414460)

[10.4 修改默认安全策略命令 136](#_Toc434414461)

[10.4.1 policy default-action 136](#_Toc434414462)

[11 对象管理命令参考 138](#_Toc434414463)

[11.1 地址对象命令 138](#_Toc434414464)

[11.1.1 address 138](#_Toc434414465)

[11.1.2 address-group 138](#_Toc434414466)

[11.1.3 exclude ip address 139](#_Toc434414467)

[11.1.4 excule ip range 140](#_Toc434414468)

[11.1.5 excule ip subnet 140](#_Toc434414469)

[11.1.6 ip address 141](#_Toc434414470)

[11.1.7 ip range 141](#_Toc434414471)

[11.1.8 ip subnet 142](#_Toc434414472)

[11.1.9 member 143](#_Toc434414473)

[11.1.10 show address 143](#_Toc434414474)

[11.1.11 show address-group 144](#_Toc434414475)

[11.2 服务对象命令 145](#_Toc434414476)

[11.2.1 icmp type 145](#_Toc434414477)

[11.2.2 member 146](#_Toc434414478)

[11.2.3 protocol 146](#_Toc434414479)

[11.2.4 service 147](#_Toc434414480)

[11.2.5 service-group 147](#_Toc434414481)

[11.2.6 show service 148](#_Toc434414482)

[11.2.7 show service-group 152](#_Toc434414483)

[11.2.8 tcp dst-port 152](#_Toc434414484)

[11.2.9 udp dst-port 153](#_Toc434414485)

[11.3 时间表命令 154](#_Toc434414486)

[11.3.1 day 154](#_Toc434414487)

[11.3.2 day start 155](#_Toc434414488)

[11.3.3 periodic 155](#_Toc434414489)

[11.3.4 schedule-day 156](#_Toc434414490)

[11.3.5 schedule-month 157](#_Toc434414491)

[11.3.6 schedule-once 157](#_Toc434414492)

[11.3.7 schedule-week 158](#_Toc434414493)

[11.3.8 show schedule-day 158](#_Toc434414494)

[11.3.9 show schedule-month 159](#_Toc434414495)

[11.3.10 show schedule-once 160](#_Toc434414496)

[11.3.11 show schedule-week 161](#_Toc434414497)

[11.4 关键字命令 162](#_Toc434414498)

[11.4.1 content 162](#_Toc434414499)

[11.4.2 description 162](#_Toc434414500)

[11.4.3 keyword 163](#_Toc434414501)

[11.4.4 show keyword 163](#_Toc434414502)

[12 应用控制 165](#_Toc434414503)

[12.1 应用对象配置命令 165](#_Toc434414504)

[12.1.1 application 165](#_Toc434414505)

[12.1.2 application-group 165](#_Toc434414506)

[12.1.3 description 166](#_Toc434414507)

[12.1.4 member application 166](#_Toc434414508)

[12.1.5 priority 167](#_Toc434414509)

[12.1.6 show application 168](#_Toc434414510)

[12.1.7 show application-category 169](#_Toc434414511)

[12.1.8 show application-group 170](#_Toc434414512)

[12.1.9 show application-summary 171](#_Toc434414513)

[12.2 应用控制策略配置命令 172](#_Toc434414514)

[12.2.1 app-policy 172](#_Toc434414515)

[12.2.2 app-policy disable 173](#_Toc434414516)

[12.2.3 app-policy enable 174](#_Toc434414517)

[13 类与网站策略 175](#_Toc434414518)

[13.1 URL分类 175](#_Toc434414519)

[13.1.1 show url-category 175](#_Toc434414520)

[13.1.2 url 176](#_Toc434414521)

[13.1.3 url-category 176](#_Toc434414522)

[13.2 网站策略配置命令 177](#_Toc434414523)

[13.2.1 website-policy 177](#_Toc434414524)

[13.2.2 website-policy disable 178](#_Toc434414525)

[13.2.3 website-policy enable 178](#_Toc434414526)

[13.2.4 website-policy malware 179](#_Toc434414527)

[14 用户和用户认证 180](#_Toc434414528)

[14.1 用户配置命令 180](#_Toc434414529)

[14.1.1 bind ip 180](#_Toc434414530)

[14.1.2 bind ip exclude 180](#_Toc434414531)

[14.1.3 clear user-recognition 181](#_Toc434414532)

[14.1.4 description 182](#_Toc434414533)

[14.1.5 enable 182](#_Toc434414534)

[14.1.6 enable bind 183](#_Toc434414535)

[14.1.7 match user 183](#_Toc434414536)

[14.1.8 member 184](#_Toc434414537)

[14.1.9 show user 185](#_Toc434414538)

[14.1.10 show user-group 186](#_Toc434414539)

[14.1.11 show user-param 187](#_Toc434414540)

[14.1.12 show user-recognition 188](#_Toc434414541)

[14.1.13 user 189](#_Toc434414542)

[14.1.14 user-group 190](#_Toc434414543)

[14.1.15 user-param 191](#_Toc434414544)

[14.2 用户认证配置命令 192](#_Toc434414545)

[14.2.1 authenticate 192](#_Toc434414546)

[14.2.2 enable authenticate 193](#_Toc434414547)

[14.2.3 show user-policy 193](#_Toc434414548)

[14.2.4 user-policy 194](#_Toc434414549)

[14.2.5 user-policy move 196](#_Toc434414550)

[14.2.6 user-webauth force-timeout 196](#_Toc434414551)

[14.2.7 user-webauth hello-url 197](#_Toc434414552)

[14.2.8 user-webauth keepalive-timeout 198](#_Toc434414553)

[14.2.9 user-webauth login-multi 198](#_Toc434414554)

[14.2.10 user-webauth login-single 199](#_Toc434414555)

[14.3 配置认证服务器 199](#_Toc434414556)

[14.3.1 bindtype 199](#_Toc434414557)

[14.3.2 cnid 200](#_Toc434414558)

[14.3.3 dn 201](#_Toc434414559)

[14.3.4 filter 201](#_Toc434414560)

[14.3.5 ldap（LDAP配置视图） 202](#_Toc434414561)

[14.3.6 ldap（系统视图） 202](#_Toc434414562)

[14.3.7 radius-server 203](#_Toc434414563)

[14.3.8 server-group 204](#_Toc434414564)

[14.3.9 show radius-server 205](#_Toc434414565)

[14.3.10 show server-group 206](#_Toc434414566)

[14.3.11 user-portal-server 207](#_Toc434414567)

[15 流量管理 209](#_Toc434414568)

[15.1 线路配置命令 209](#_Toc434414569)

[15.1.1 limit 209](#_Toc434414570)

[15.1.2 match interface 209](#_Toc434414571)

[15.1.3 maxbandwidth 210](#_Toc434414572)

[15.1.4 qos-profile line 211](#_Toc434414573)

[15.2 管道配置命令 211](#_Toc434414574)

[15.2.1 bandwidth 211](#_Toc434414575)

[15.2.2 match 212](#_Toc434414576)

[15.2.3 maxbandwidth 213](#_Toc434414577)

[15.2.4 move 213](#_Toc434414578)

[15.2.5 perip 214](#_Toc434414579)

[15.2.6 priority 214](#_Toc434414580)

[15.2.7 qos-profile channel 215](#_Toc434414581)

[15.2.8 schedule 216](#_Toc434414582)

[15.3 白名单配置命令 216](#_Toc434414583)

[15.3.1 qos-profile white-list 216](#_Toc434414584)

[16 安全防护 218](#_Toc434414585)

[16.1 异常报文攻击防护配置命令 218](#_Toc434414586)

[16.1.1 ip defend attack 218](#_Toc434414587)

[16.1.2 ip defend attack log 219](#_Toc434414588)

[16.2 扫描攻击防护配置命令 220](#_Toc434414589)

[16.2.1 ip defend port-scan interface 220](#_Toc434414590)

[16.2.2 ip defend scan log 221](#_Toc434414591)

[16.3 flood攻击配置命令 222](#_Toc434414592)

[16.3.1 ip defend 222](#_Toc434414593)

[16.3.2 ip defend { synflood | udpflood | icmpflood | dnsflood } interface 223](#_Toc434414594)

[16.4 IPMAC绑定配置命令 224](#_Toc434414595)

[16.4.1 ipmac 224](#_Toc434414596)

[16.4.2 ipmac log 225](#_Toc434414597)

[16.5 防arp攻击配置命令 225](#_Toc434414598)

[16.5.1 anti-arp broadcast 225](#_Toc434414599)

[16.5.2 anti-arp broadcast interface 226](#_Toc434414600)

[16.5.3 anti-arp broadcast interval 226](#_Toc434414601)

[16.5.4 anti-arp flood 227](#_Toc434414602)

[16.5.5 anti-arp flood block-time 227](#_Toc434414603)

[16.5.6 anti-arp flood threshold 228](#_Toc434414604)

[16.5.7 anti-arp learning-arp 228](#_Toc434414605)

[16.5.8 anti-arp spoof 229](#_Toc434414606)

[16.6 黑名单配置命令 230](#_Toc434414607)

[16.6.1 blist add 230](#_Toc434414608)

[16.6.2 show blist 230](#_Toc434414609)

[17 会话限制 232](#_Toc434414610)

[17.1 会话限制配置命令 232](#_Toc434414611)

[17.1.1 ip connection limit 232](#_Toc434414612)

[17.1.2 show ip connection limit config 232](#_Toc434414613)

[17.1.3 show ip connection statistics 233](#_Toc434414614)

[17.1.4 show ip connection limit 234](#_Toc434414615)

[18 CA中心命令 235](#_Toc434414616)

[18.1 CA中心命令 235](#_Toc434414617)

[18.1.1 pki ca crl export tftp 235](#_Toc434414618)

[18.1.2 pki ca crl generate 235](#_Toc434414619)

[18.1.3 pki ca crl update-period 236](#_Toc434414620)

[18.1.4 pki ca root-certificate cert\_key import tftp 236](#_Toc434414621)

[18.1.5 pki ca root-certificate export tftp 237](#_Toc434414622)

[18.1.6 pki ca root-certificate pkcs12 import tftp 238](#_Toc434414623)

[18.1.7 show pki ca crl 239](#_Toc434414624)

[18.1.8 show pki ca root-certificate 240](#_Toc434414625)

[18.1.9 show running-config pki 241](#_Toc434414626)

[18.2 用户证书命令 242](#_Toc434414627)

[18.2.1 no pki ca user-certificate 242](#_Toc434414628)

[18.2.2 pki ca user-certificate copy 243](#_Toc434414629)

[18.2.3 pki ca user-certificate export tftp 243](#_Toc434414630)

[18.2.4 pki ca user-certificate revoke 244](#_Toc434414631)

[18.2.5 pki ca user-certificate sign 245](#_Toc434414632)

[18.2.6 show pki ca user-certificate 245](#_Toc434414633)

[19 证书命令 248](#_Toc434414634)

[19.1 本地证书命令 248](#_Toc434414635)

[19.1.1 no pki local certificate 248](#_Toc434414636)

[19.1.2 pki local certificate cert\_key import tftp 248](#_Toc434414637)

[19.1.3 pki local certificate export tftp 249](#_Toc434414638)

[19.1.4 pki local certificate pkcs12 import tftp 250](#_Toc434414639)

[19.1.5 show pki local certificate 251](#_Toc434414640)

[19.2 本地CA证书命令 253](#_Toc434414641)

[19.2.1 no pki local ca 253](#_Toc434414642)

[19.2.2 pki local ca export tftp 253](#_Toc434414643)

[19.2.3 pki local ca import tftp 254](#_Toc434414644)

[19.2.4 show pki local ca 255](#_Toc434414645)

[19.3 本地CRL命令 256](#_Toc434414646)

[19.3.1 no pki local crl 256](#_Toc434414647)

[19.3.2 pki local crl export tftp 257](#_Toc434414648)

[19.3.3 pki local crl import tftp 258](#_Toc434414649)

[19.3.4 show pki local crl 258](#_Toc434414650)

[19.4 自动获取CRL命令 260](#_Toc434414651)

[19.4.1 pki local crl auto-get 260](#_Toc434414652)

[19.4.2 show pki local crl auto-get 261](#_Toc434414653)

[20 SNMP命令 263](#_Toc434414654)

[20.1 SNMP命令 263](#_Toc434414655)

[20.1.1 community 263](#_Toc434414656)

[20.1.2 show snmpv3 usm-user 264](#_Toc434414657)

[20.1.3 snmp 264](#_Toc434414658)

[20.1.4 snmpv3 usm-user 265](#_Toc434414659)

[20.1.5 syslocation 266](#_Toc434414660)

[20.1.6 trap 267](#_Toc434414661)

[20.1.7 trap version 267](#_Toc434414662)

[20.1.8 version 268](#_Toc434414663)

[20.1.9 write-community 269](#_Toc434414664)

[21 日志命令参考 271](#_Toc434414665)

[21.1 日志命令 271](#_Toc434414666)

[21.1.1 log facility 271](#_Toc434414667)

[21.1.2 log local 272](#_Toc434414668)

[21.1.3 log server addr 273](#_Toc434414669)

[21.1.4 log server crypt 274](#_Toc434414670)

[21.1.5 log server enable 274](#_Toc434414671)

[21.1.6 log server port 275](#_Toc434414672)

[21.1.7 log server second 276](#_Toc434414673)

[21.1.8 log server third 277](#_Toc434414674)

[21.1.9 log server upto 277](#_Toc434414675)

[21.1.10 log source addr 279](#_Toc434414676)

[21.1.11 show log config 280](#_Toc434414677)

[22 HA 282](#_Toc434414678)

[22.1 HA配置命令 282](#_Toc434414679)

[22.1.1 auto\_sync 282](#_Toc434414680)

[22.1.2 disable 283](#_Toc434414681)

[22.1.3 enable backup-master 283](#_Toc434414682)

[22.1.4 ha-config 283](#_Toc434414683)

[22.1.5 hainterface 284](#_Toc434414684)

[22.1.6 keepalive 284](#_Toc434414685)

[22.1.7 manage-ip 285](#_Toc434414686)

[22.1.8 monitor 286](#_Toc434414687)

[22.1.9 preempt 287](#_Toc434414688)

[22.1.10 show ha state 288](#_Toc434414689)

[22.1.11 standby 289](#_Toc434414690)

[22.1.12 swap 290](#_Toc434414691)

[22.1.13 sync config 290](#_Toc434414692)

[22.1.14 sync lib 291](#_Toc434414693)

[23 接口状态同步组 292](#_Toc434414694)

[23.1 接口状态同步组命令 292](#_Toc434414695)

[23.1.1 interface sync group 292](#_Toc434414696)

[24 IPv6命令参考 294](#_Toc434414697)

[24.1 IPv6路由命令 294](#_Toc434414698)

[24.1.1 ipv6 route 294](#_Toc434414699)

[24.1.2 show ipv6 route 295](#_Toc434414700)

[24.1.3 show ipv6 route connected 295](#_Toc434414701)

[24.1.4 show ipv6 route *ipv6-address* 296](#_Toc434414702)

[24.1.5 show ipv6 route *ipv6-prefix* 297](#_Toc434414703)

[24.1.6 show ipv6 route static 298](#_Toc434414704)

[24.1.7 show ipv6 route summary 298](#_Toc434414705)

[25 IPv6邻居发现命令参考 300](#_Toc434414706)

[25.1 IPv6路由命令 300](#_Toc434414707)

[25.1.1 clear ipv6 neighbor 300](#_Toc434414708)

[25.1.2 ipv6 nd dad attempts 300](#_Toc434414709)

[25.1.3 ipv6 nd nud ns-retrans-interval 301](#_Toc434414710)

[25.1.4 ipv6 nd nud reachable-time 301](#_Toc434414711)

[25.1.5 ipv6 nd ra-interval 302](#_Toc434414712)

[25.1.6 ipv6 nd send-ra 303](#_Toc434414713)

[25.1.7 show ipv6 nd nud-params 303](#_Toc434414714)

[25.1.8 show ipv6 neighbor 304](#_Toc434414715)

[26 IPv6隧道命令参考 306](#_Toc434414716)

[26.1 IPv6隧道命令 306](#_Toc434414717)

[26.1.1 interface tunnel 306](#_Toc434414718)

[26.1.2 show tunnel 306](#_Toc434414719)

[26.1.3 show tunnel ipv6ip 307](#_Toc434414720)

[26.1.4 tunnel destination 308](#_Toc434414721)

[26.1.5 tunnel source 309](#_Toc434414722)

[27 IPv6命令参考 310](#_Toc434414723)

[27.1 IPv6策略命令 310](#_Toc434414724)

[27.1.1 dest-address 310](#_Toc434414725)

[27.1.2 enable 310](#_Toc434414726)

[27.1.3 in-interface 311](#_Toc434414727)

[27.1.4 out-interface 311](#_Toc434414728)

[27.1.5 policy6 312](#_Toc434414729)

[27.1.6 policy6 default-action 313](#_Toc434414730)

[27.1.7 policy6 insert 314](#_Toc434414731)

[27.1.8 policy6 move 314](#_Toc434414732)

[27.1.9 schedule 315](#_Toc434414733)

[27.1.10 service 316](#_Toc434414734)

[27.1.11 show running-config ipv6-policy 316](#_Toc434414735)

[27.1.12 source-address 317](#_Toc434414736)

# 入门命令

## 系统时间命令

### date

**date**命令用来配置系统时间。

【命令】

**date** year month day hour minute second

【视图】

用户视图

【参数】

*year*：年，取值范围为2006～2030。

*month*：月，取值范围为1～12。

*day*：天，取值范围为1～31。

*hour*：小时，取值范围为0～23。

*minute*：分钟，取值范围为0～59。

*second*：秒，取值范围为0～59。

【举例】

# 配置系统时间。

host# date 2014 7 3 15 51 20

【相关命令】

show date

### ntp

**ntp**命令用来配置通过时间服务器配置系统时间。

**no ntp**命令用来删除时间服务器配置。

【命令】

**ntp** *word interval-time*

**no ntp**

【视图】

系统视图

【参数】

*word*：NTP服务器的IP地址，或者域名。

*interval-time*：从NTP服务器获取时间的间隔，取值范围为5～65535，单位为秒。

【举例】

# 配置从asia.pool.ntp.org获取时间。

host# configure terminal

host(config)# ntp asia.pool.ntp.org 60

【相关命令】

**show date**

**show ntp config**

### ntpupdate

**ntpupdate**命令用来立刻从NTP服务器获取时间。

【命令】

**ntpupdate** *word*

【视图】

用户视图

【参数】

*word*：指定的NTP服务器的IP地址，或者域名。

【举例】

# 立即从asia.pool.ntp.org获取时间。

host# ntpupdate asia.pool.ntp.org

### show date

**show date**命令用来显示系统时间。

【命令】

**show date**

【视图】

用户视图

【举例】

# 显示系统当前时间。

host# show date

ABS time :1404375911

UTC time :2014-07-03 08:25:11

Local time :2014-07-03 16:25:11

### show ntp config

**show ntp config**命令用来显示通过NTP服务器获取时间的配置信息。

【命令】

**show ntp config**

【视图】

用户视图

【举例】

# 显示NTP的配置信息。

host# show ntp config

timezone 57

ntp asia.pool.ntp.org 60

!

### show timezone

**show timezone**命令用来显示系统时区信息。

【命令】

**show timezone**

【视图】

用户视图

【举例】

# 显示系统时区的配置信息。

host# show timezone

timezone 57

!

### timezone

**timezone**命令用来配置系统的时区。

【命令】

**timezone** *zone*

【视图】

系统视图

【参数】

*zone*：时区，取值范围为1～75。

【使用指导】

北京、乌鲁木齐时区为57。

【举例】

# 配置系统时区为北京、乌鲁木齐。

host# configure terminal

host(config)# timezone 57

【相关命令】

* show date
* show timezone

## 系统升级命令

### copy ftp

**copy ftp**命令用来通过FTP服务器的匿名账户升级相关文件。

**copy ftp** *username**pasword*命令用来通过FTP服务器配置的用户名和密码升级相关文件。

【命令】

**copy ftp** *ip-address file-name*{ **version** | **applib** | **avlib** | **ipslib** | **urllib** }

**copy ftp** *username**pasword**ip-address file-name*{ **version** | **applib** | **avlib** | **ipslib** | **urllib** }

【视图】

用户视图

【参数】

*ip-address*：FTP服务器IP地址。

*file-name*：升级的文件名称。

*username*：FTP服务器的用户名。

*password*：FTP服务器的密码。

**version**：从FTP服务器升级版本。

**applib**：从FTP服务器升级应用识别库。

**avlib**：从FTP服务器升级av库。

**ipslib**：从FTP服务器升级ips库。

**urllib**：从FTP服务器升级url库。

**config**：从FTP服务器升级配置文件。

【使用指导】

在通过FTP服务器升级相关文件前，需要保证：

FTP服务器与设备网络可达。

FTP服务器上存在升级响应的文件。

【举例】

# 通过匿名用户从FTP服务器升级系统版本。

host#copy ftp 192.168.1.75 image.bin version

# 通过FTP用户从FTP服务器升级系统版本。

host#copy ftp admin admin 192.168.1.75 image.bin version

## 配置文件命令

### save config

**save config**命令用来保存系统当前的配置。

【命令】

**save config**

【视图】

用户视图

【使用指导】

当系统的配置发生更改，需要保存配置时，需要执行此命令。

【举例】

# 保存系统当前配置。

host# save config

Building configuration...

Save configuration ok !

【相关命令】

* copy startup-config backup-config
* copy backup-config startup-config
* copy running-config backup-config
* copy running-config startup-config
* erase startup-config

### copy startup-config backup-config

copy startup-config backup-config命令用来将启动配置进行备份。

【命令】

copy startup-config backup-config

【视图】

用户视图

【举例】

# 备份启动配置。

host# copy startup-config backup-config

【相关命令】

* save config
* copy backup-config startup-config
* copy running-config backup-config
* copy running-config startup-config
* erase startup-config

### copy backup-config startup-config

copy backup-config startup-config命令用来将备份配置恢复为启动配置。

【命令】

**copy backup-config startup-config**

【视图】

用户视图

【举例】

# 恢复备份配置为启动配置。

host# copy backup-config startup-config

【相关命令】

* save config
* copy startup-config backup-config
* copy running-config backup-config
* copy running-config startup-config
* erase startup-config

### copy running-config backup-config

copy running-config backup-config命令用来将当前有效配置保存为备份配置文件。

【命令】

copy running-config backup-config

【视图】

用户视图

【举例】

# 将当前有效配置保存为备份配置文件。

host# copy running-config backup-config

【相关命令】

* save config
* copy startup-config backup-config
* copy backup-config startup-config
* copy running-config startup-config
* erase startup-config

### copy running-config startup-config

copy running-config startup-config命令用来将系统当前有效配置保存为启动配置。

【命令】

copy running-config startup-config

【视图】

用户视图

【举例】

# 将系统当前有效配置保存为启动配置。

host# copy running-config startup-config

【相关命令】

* save config
* copy startup-config backup-config
* copy backup-config startup-config
* copy running-config backup-config
* erase startup-config

### copy file ftp

copy { running-config | startup-config } ftp命令用来通过FTP导出当前配置文件或启动配置文件。

【命令】

copy { running-config | startup-config } ftp *username password ip-address remote-file*

【视图】

用户视图

【参数】

running-config：导出当前系统配置文件。

startup-config：导出启动配置文件。

*username*：FTP服务器用户名。

*password*：FTP服务器密码。

*ip-address*：FTP服务器地址。

*remote-file*：导出后文件的保存名称。

【举例】

# 通过FTP导出当前系统配置文件。

host# copy running-config ftp admin admin 192.168.1.71 bk\_cfg.con

【相关命令】

copy { running-config | startup-config } tftp *ip-address remote-file*

### copy file tftp

copy { running-config | startup-config } tftp命令用来通过TFTP导出当前配置文件或启动配置文件。

【命令】

copy { running-config | startup-config } tftp *ip-address remote-file*

【视图】

用户视图

【参数】

**running-config**：导出当前系统配置文件。

**startup-config**：导出启动配置文件。

*ip-address*：TFTP服务器地址。

*remote-file*：导出后文件的保存名称。

【举例】

# 通过TFTP导出当前系统配置文件。

host# copy running-config tftp 192.168.1.71 bk\_cfg.con

【相关命令】

* **copy** { **running-config** | **startup-config** } **ftp** *username password ip-address remote-file*

### copy ftp

**copy ftp**命令用来通过FTP服务器导入配置文件。

【命令】

**copy ftp** *username password ip-address remote-file* **config**

【视图】

用户视图

【参数】

*username*：FTP服务器用户名。

*password*：FTP服务器密码。

*ip-address*：FTP服务器地址。

*remote-file*：从FTP服务器导入的文件名称。

【举例】

# 从FTP服务器导入配置文件。

host# copy ftp admin admin 192.168.1.71 bk\_cfg.con config

【相关命令】

* copy tftp

### copy tftp

**copy tftp**命令用来通过TFTP服务器导入配置文件。

【命令】

**copy tftp** *ip-address remote-file* **config**

【视图】

用户视图

【参数】

*ip-address*：TFTP服务器地址。

*remote-file*：从TFTP服务器导入的文件名称。

【举例】

# 从TFTP服务器导入配置文件。

host# copy tftp 192.168.1.71 bk\_cfg.con config

【相关命令】

* **copy ftp** username password ip-address remote-file **config**

### erase startup-config

erase startup-config命令用来清除启动配置。

【命令】

erase startup-config

【视图】

用户视图

【举例】

# 清除系统启动配置。

host# erase startup-config

Remove all the configuration(back to factory default), are you sure? [y]/n: y

【相关命令】

* save config
* copy startup-config backup-config
* copy backup-config startup-config
* copy running-config backup-config
* copy running-config startup-config

## 管理员命令

### authorized

**authorized**命令用来开启管理员权限表中的具体权限。

**no authorized**命令用来关闭管理员权限表中的具体权限。

【命令】

authorized { read | write } { all | system-config | log-report | admin-user |

access-user | updata | securit-policy | reboot }

no authorized { read | write } { all | system-config | log-report | admin-user |

access-user | updata | securit-policy | reboot }

【视图】

authorized-table视图

【参数】

**read**：配置读权限。

**write**：配置写权限。

**all**：具有所有的读或者写权限。

**system-config**：具有系统配置的权限，系统配置具有下面六中权限规定以外的所有权限，且具有对象管理的权限。

**log-report**：具有日志、netflow操作的权限。

**admin-user**：具有管理员用户、授权表、在线信息的操作权限。

**access-user**：具有接入用户的操作权限。

**updata**：具有升级的操作权限。

**securit-policy**：具有配置安全策略的操作权限。

**reboot**：具有重启系统的操作权限。

【举例】

# 给权限表reader配置权限。

host# configure terminal

host(config)# authorized-table reader

host(authorized-table)# authorized read all

【相关命令】

* show running-config

### authorized-table

authorized-table命令用来创建管理员权限表。

no authorized-table命令用来删除管理员权限表。

【命令】

**authorized-table**

**no authorized-table**

【缺省情况】

缺省情况下，有admin管理员权限表。该表配置了所有的读权限和写权限。

【视图】

系统视图

【使用指导】

默认的管理员账户，使用admin管理员权限表。

【举例】

# 创建一个reader管理员权限表。

host# configure terminal

host(config)# authorized-table reader

【相关命令】

* show running-config

### guish admin unique

**guish admin unique**命令用来开启管理员唯一性检查。

**no guish admin unique**命令用来关闭管理员唯一性检查。

【命令】

**guish admin unique**

**no guish admin unique**

【缺省情况】

缺省情况下，未开启管理员唯一性检查。

【视图】

系统视图

【使用指导】

该命令将使得第二个用相同管理员账号登录设备的IP登录失败。

【举例】

# 配置开启管理员唯一性检查。

host# configure terminal

host(config)# guish admin unique

### guish autosave

**guish autosave**命令用来启用自动保存配置。

**no guish autosave**命令用来关闭自动保存配置。

【命令】

**guish autosave**

**no guish autosave**

【视图】

系统视图

【举例】

# 启用自动保存。

host# configure terminal

host(config)# guish autosave

### guish maxclient

**guish maxclient**命令用来配置管理员最大登录数。

**no guish maxclient**命令用来删除管理员最大登录数。

【命令】

**guish maxclient** *max*

【缺省情况】

缺省情况下，管理员的最大登录数是20。

【视图】

系统视图

【参数】

*max*：管理员最大登录数，取值范围为1～20，默认为20。

【使用指导】

当执行**no guish maxclient**命令后，管理员最大登录数将恢复为默认值。

【举例】

# 配置管理员最大登录数。

host# configure terminal

host(config)# guish maxclient 15

### guish timeout

**guish timeout**命令用来配置管理员没有操作自动退出的时间长度。

【命令】

**guish timeout** *timeout*

【缺省情况】

缺省情况下，超时时间是10分钟。

【视图】

系统视图

【参数】

*timeout*：管理员没有操作自动退出的时间长度。取值范围为1～480分钟。默认值为10分钟。

【举例】

# 配置管理员自动退出时间为20分钟。

host# configure terminal

host(config)# guish timeout 20

### user administrator authorized-address

**user administrator authorized-address**命令用来配置管理员用户的管理地址。

**no user administrator authorized-address**命令用来删除管理员用户的管理地址。

【命令】

**user administrator** *user* **authorized-address** { **first** | **second** | **third** } *ip-address*

**user administrator** *user* **authorized-address** { **first** | **second** | **third** }*ip-address*/*prefix*

【视图】

系统视图

【参数】

*user*：管理员的名称，为已存在的管理员用户。

**first**：管理员的第一个管理地址。

**second**：管理员的第二个管理地址。

**third**：管理员的第三个管理地址。

*ip-address*：IP地址。

*prefix*：子网掩码。

【使用指导】

可以配置三个授权地址，该用户可以通过任意一个地址登录；或者配置网段管理地址，用户可以用该网段任何一个地址登录。

【举例】

# 配置管理员管理地址。

host# configure terminal

host(config)# user administrator admin authorized-address first 192.168.1.1

### user administrator local

**user administrator local**命令用来创建本地管理员用户。

**no user administrator**命令用来删除本地管理员用户。

【命令】

**user administrator** *user* **local** *password* **authorized-table** *name*[ **disable** ]

**no user administrator** *user*

【缺省情况】

缺省情况下，已存在本地管理员账户“admin”。

【视图】

系统视图

【参数】

*user*：本地管理员的名称，为1～31个字符的字符串，且不能包含“%!"#$&`\*+,/:;<=>?\^'{}!”。

*password*：本地管理员的密码，为6～63个字符的字符串，可以包含“[!@#$%&`-.](mailto:!@#$%&`-.)”。

*name*：权限表的名称。

**disable**：使该用户暂时无效。

【使用指导】

创建或者修改本地管理员用户的密码以及管理权限表，并可以通过**disable**选项使该用户暂时无效。

【举例】

# 配置一个test的本地管理员。

host# configure terminal

host(config)# user administrator test local test1! Authorized-table reader

### user administrator ldap

**user administrator ldap**命令用来创建ldap管理员用户。

**no user administrator** 命令用来删除ldap管理员用户。

【命令】

**user administrator** *user* **ldap** *server* **authorized-table** *name*[ **disable** ]

**no user administrator** *name*

【视图】

系统视图

【参数】

*user*：ldap管理员的名称，为1～31个字符的字符串，且不能包含“%!"#$&`\*+,/:;<=>?\^'{}!”。

*server*：ldap服务器的名称。

*name*：权限表的名称。

**disable**：使该用户暂时无效。

【使用指导】

*server*为已存在的ldap服务器名称。

【举例】

# 创建一个ldap管理员用户。

host# configure terminal

host(config)# ldap ldap1

host(config)#user administrator aa ldap ldap1 authorized-table reader

【相关命令】

* **ldap name**
* **ldap ip-address** [ **port** ]

### user administrator radius

user administrator radius命令用来创建radius管理员用户。

no user administrator命令用来删除radius管理员用户。

【命令】

user administrator *user* radius *server* authorized-table *name* [ disable ]

no user administrator *user*

【视图】

系统视图

【参数】

*user*：radius管理员的名称，为1～31个字符的字符串，且不能包含“%!"#$&`\*+,/:;<=>?\^'{}!”。

*server*：radius服务器的名称。

*name*：权限表的名称。

disable：使该用户暂时无效。

【使用指导】

*server*为已存在的radius server或者radius组。

【举例】

# 创建一个test\_radius的用户。

host# configure terminal

host(config)#radius-server test\_radius 1.1.1.1 aaa

host(config)#user administrator user\_radius radius test\_radius authorized-table reader

【相关命令】

* radius-server *name* ip-address *secret* [ port ]
* radius-server *name* group *group-name*

## 常用系统管理命令

### clear user

**clear user**命令用来清除已登录的用户。

【命令】

**clear user** *name* **address** *ip-address* **time** *time*

【视图】

用户视图

【参数】

*name*：登录用户的用户名。

*ip-address*：登录用户的IP地址。

*time*：登录用户的登录时间。

【使用指导】

*time*格式需要和**who**命令显示的格式一致。

【举例】

# 清除admin用户。

host(config)# clear user admin address 192.168.1.105 time 2014-07-4 19:34:46

### ping

**ping**命令用来诊断设备的网络情况。

【命令】

**ping -c** *request-times* **-s** *packet* **-i** *interval-time* **-t** *ttl* **-I** {*ip-address*|*domain-name*}

【视图】

用户视图

【参数】

*request-times*：ping请求的ICMP报文个数。取值范围为1～10000次，默认为5个。

*packet*：ICMP报文大小。取值范围为0～65507字节，默认为64字节。

*interval-time*：请求的时间间隔。取值范围为0～10秒，默认为1秒。

*ttl*：ICMP报文的TTL时间。取值范围为1～255秒。

*ip-address*：ping请求的地址。

*doman-name*：ping请求的域名。

【使用指导】

当**ping**域名时，需要配置DNS，具体请参考DNS配置。

【举例】

# ping百度。

host# ping www.baidu.com

PING 61.135.169.105 (61.135.169.105) 56(84) bytes of data.

seq ttl time(ms)

1 47 73.194

2 47 70.368

3 47 61.334

4 47 69.463

5 47 70.177

--- 61.135.169.105 ping statistics ---

5 packets transmitted, 5 received, 0% packet loss, time 4001ms

rtt min/avg/max/mdev = 61.334/68.907/73.194/3.998 ms

### ping6

**ping6**命令用来诊断设备的网络情况。

【命令】

**ping6 -c** *request-times* **-s** *packet* **-i** *interval-time* **-t** *ttl* **-I** *ipv6-address*

【视图】

用户视图

【参数】

*request-times*：ping请求的ICMP报文个数。取值范围为1～10000次，默认为5个。

*packet*：ICMP报文大小。取值范围为0～65507字节，默认为64字节。

*interval-time*：请求的时间间隔。取值范围为0～10秒，默认为1秒。

*ttl*：ICMP报文的TTL时间。取值范围为1～255秒。

*ipv6-address*：ping6请求的地址。

【举例】

# ping6 2003：2003：：1。

host# ping6 2003:2003::1

PING 2003:2003::1(2003:2003::1) 56 data bytes

seq ttl time(ms)

1 64 0.145

2 64 0.119

3 64 0.118

4 64 0.119

5 64 0.112

--- 2003:2003::1 ping statistics ---

5 packets transmitted, 5 received, 0% packet loss, time 4002ms

rtt min/avg/max/mdev = 0.112/0.122/0.145/0.016 ms

### show version

**show version**命令用来显示系统的版本信息。

【命令】

**show version**

【视图】

用户视图

【举例】

# 查看系统版本信息。

host# show version

Unkown, Build time is Jun 30 2014 16:25:16

System uptime: 3 days 21 hours 23 minutes

Firmware is 0630.bin

Application signature version: 20140620

Url category version: 20140422

IPS signature version: 20140620

Virus Productoon version: 20140422

Serial : 020100000114040228802760

Product : Unknown

Model : Unknown

Platform : Unknown

Basic Functionality : License valid

Application Audit and Control : License valid

URL Category : License valid

Malware URL Category : License valid

Virtual Private Network : License valid

Intrusion Prevention System : License valid

Virus Protection : License valid

Application Audit and Control Update Service : License valid

URL Category Update Service : License valid

Malware URL Category Update Service : License valid

Intrusion Prevention System Update Service : License valid

Virus Protection Update Service : License valid

### tcpsyn

**tcpsyn**命令用来进行TCP SYN报文的诊断。

【命令】

**tcpsyn -c** *request-times***<1-1000>** *ip-address**port***<0-65535>**

【视图】

用户视图

【参数】

*request-times*：TCP SYN报文请求次数。取值范围为1～1000次，默认为4次。

*ip-address*：TCP SYN报文的目的IP地址。

*port*：TCP SYN报文的目的端口号。

【举例】

# 向192.168.1.1发送TCP SYN报文。

host# tcpsyn -c 5 192.168.1.1 80

tcpsyn to 192.168.1.1:80

1 TCP ACK from 192.168.1.1:80

2 TCP ACK from 192.168.1.1:80

3 TCP ACK from 192.168.1.1:80

4 TCP ACK from 192.168.1.1:80

5 TCP ACK from 192.168.1.1:80

### traceroute

**traceroute**命令用来进行路由诊断。

【命令】

**traceroute -s** { *ip-address*| *domain-name* }

【视图】

用户视图

【参数】

*ip-address*：需要通过命令进行路由诊断的IP地址。

*domain-name*：需要通过命令进行路由诊断的域名。

【举例】

# traceroute百度。

host# traceroute www.baidu.com

traceroute to 61.135.169.125 (61.135.169.125), 30 hops max, 46 byte packets

1 192.168.2.1 (192.168.2.1) 1.222 ms 4.836 ms 4.839 ms

2 124.202.226.33 (124.202.226.33) 5.338 ms 2.688 ms 1.880 ms

3 10.255.26.225 (10.255.26.225) 5.663 ms 4.703 ms 3.477 ms

4 124.205.98.205 (124.205.98.205) 6.172 ms 4.949 ms 5.018 ms

5 124.205.98.217 (124.205.98.217) 5.004 ms 3.391 ms 4.993 ms

6 202.99.1.138 (202.99.1.138) 5.051 ms 6.706 ms \*

7 10.15.253.229 (10.15.253.229) 5.576 ms 5.798 ms 7.121 ms

8 \* \* \*

9 113.57.231.1 (113.57.231.1) 24.559 ms \* 25.419 ms

10 58.19.113.250 (58.19.113.250) 30.435 ms 25.320 ms 25.433 ms

11 210.5.142.234 (210.5.142.234) 71.182 ms 71.219 ms 70.708 ms

12 210.5.142.237 (210.5.142.237) 26.776 ms 25.325 ms 30.491 ms

13 58.19.112.17 (58.19.112.17) 71.150 ms 71.126 ms 71.331 ms

14 219.158.22.49 (219.158.22.49) 71.217 ms 71.235 ms 71.272 ms

15 123.126.0.90 (123.126.0.90) 71.070 ms 71.113 ms 72.854 ms

16 202.106.227.34 (202.106.227.34) 81.300 ms 76.106 ms 76.209 ms

17 \* \* \*

18 \* \* \*

19 \* \* \*

20 \* \* \*

21 \* \* \*

22 \* \* \*

23 123.125.248.98 (123.125.248.98) 70.982 ms !A \* \*

24 \* \* \*

25 \* \* \*

26 \* \* \*

27 \* \* \*

28 \* \* \*

29 \* \* \*

30 \* \* \*

### who

**who**命令用来查看当前有多少用户登录了设备。

【命令】

**who**

【视图】

用户视图

【使用指导】

当需要查看有多少用户、什么时间、登录IP、什么方式登录设备时，请执行此命令。

【举例】

# 查看当前登录用户。

host# who

Login style Username IP Login time

SSH admin 192.168.1.105 2014-07-04 12:25:13

GUI admin 192.168.1.105 2014-07-04 09:38:56

表 1-1 当前登录用户信息描述表

| 字段 | 描述 |
| --- | --- |
| Login style | 登录方式 |
| Usernae | 登录用户名 |
| Ip | 登录用户的IP地址 |
| Login time | 登录的时间 |

# 接口

## 以太网端口配置命令

### allow access

**allow access**命令用来配置端口管理访问方式。

**no allow access**命令用来取消端口管理访问方式。

【命令】

**allow access** { **center-monitor | http | https | ping | telnet | ssh | all** }

**no allow access** { **center-monitor | http | https | ping | telnet | ssh | all** }

【缺省情况】

缺省情况下，未使能任何访问方式。

【视图】

接口视图

【参数】

**center-monitor**：允许或者禁止集中网管来管理设备。

**http**：允许或者禁止通过HTTP方式管理设备。

**https**：允许或者禁止通过HTTPS方式管理设备。

**ping**：允许或者禁止外面设备ping本设备。

**telnet**：允许或者禁止通过telnet方式管理设备。

**ssh**：允许或者禁止通过ssh方式管理设备。

**all**：允许或者禁止外面设备开启所有访问控制。

【使用指导】

端口的管理访问是用来控制通过该端口访问和管理设备的权限。通过配置端口的管理访问可以限制对端口的某类访问，保护设备的安全运行。

以上这些权限在同一个端口上可以同时打开多个，可以组合使用。

【举例】

# ge0端口开启所有访问控制。

host# configure terminal

host(config)# interface ge0

host(config-ge0)#allow access all

### auto-negotiate

**auto-negotiate** 命令用来启用/禁用端口自协商。

【命令】

**auto-negotiate** { **on | off** }

【缺省情况】

缺省情况下，以太网接口的自协商模式为on。

【视图】

接口视图

【参数】

**on**：启用端口自协商功能。

**off**：禁用端口自协商功能。

【使用指导】

光类型接口不支持自协商off模式。

【举例】

# 关闭ge0接口的自协商功能。

host# configure terminal

host(config)# interface ge0

host(config-ge0)#auto-negotiate off

### duplex

**duplex**命令用来设置端口的双工模式。

【命令】

**duplex** { **full** | **half** }

【视图】

接口视图

【参数】

**full**：全双工。

**half**：半双工。

【使用指导】

只有在关闭端口的自协商功能的情况下，才能进行双工的配置。

与共享式HUB相连时，应设置以太网口为半双工方式；与交换式LAN SWITCH相连时，一般设置以太网口为全双工方式。

【举例】

# 设置ge0接口为全双工模式。

host# configure terminal

host(config)# interface ge0

host(config-ge0)#duplex full

### ip address

**ip address**命令用来配置端口的IP地址。

**no ip address**命令用来取消端口的IP地址。

【命令】

**ip address** *address* [ **secondary** ]

**no ip address** *address* [ **secondary** ]

【视图】

接口视图

【参数】

*address*：接口IP地址。

**secondary**：辅助IP地址。

【使用指导】

接口除了配置主IP外还能配置多个辅IP，用于一个物理端口下接多个网段的机器。

需要先配置主IP地址才能配置辅IP地址。

【举例】

# ge0端口配置静态IP地址10.1.1.10。

host# configure terminal

host(config)# interface ge0

host(config-ge0)#ip address 10.1.1.10/24

### ip address dhcp

**ip address dhcp**命令用来配置接口通过DHCP方式从DHCP服务器获取IP地址。

**no ip address dhcp**命令用来取消接口通过DHCP方式获取IP地址。

【命令】

**ip address dhcp metric** *metric-range* **gw** { **reset** | **default** } **dns** { **reset** | **default** }

【视图】

接口视图

【参数】

*metric-range*：通过DHCP获取地址的权重，取值范围1～255。

**reset**：使用DHCP服务器指定的网关或DNS。

**default**：使用系统原有的网管或DNS。

【举例】

# ge0端口配置dhcp模式获取IP地址。

host# configure terminal

host(config)# interface ge0

host(config-ge0)#ip address dhcp metric 1 gw reset dns reset

### ip address pppoe

**ip address pppoe**命令用来配置接口通过PPPOE方式从服务器获取IP地址。

**no ip address pppoe**命令用来取消接口通过PPPOE方式获取IP地址。

【命令】

**ip address pppoe** [ *address* ]

**no ip address pppoe**

【视图】

接口视图

【参数】

*address*：接口指定的IP地址。

【使用指导】

通过PPPOE从服务器获取IP地址，同时也能取到网关和DNS设置。

在启用PPPOE方式时可以指定IP地址；如不指定则通过PPPOE方式获取地址。

【举例】

# ge0端口配置为PPPOE模式。

host# configure terminal

host(config)# int ge0

host(config-ge0)#ip address pppoe

### ipv6 address

**ipv6 address**命令用来配置端口的IP地址。

**no ipv6 address**命令用来取消端口的IP地址。

【命令】

**ipv6 address** *address* [ **secondary** ]

**no ipv6 address** *address* [ **secondary** ]

【视图】

接口视图

【参数】

*address*：接口IP地址。

**secondary**：辅助IP地址。

【使用指导】

接口除了配置主IP外还能配置多个辅IP，用于一个物理端口下接多个网段的机器。

需要先配置主IP地址才能配置辅IP地址。

【举例】

# ge0端口配置静态IPv6地址2003:7856::1/64和一个辅IPv6地址4005:8899::1/64。

host# configure terminal

host(config)# interface ge0

host(config-ge0)#ipv6 address 2003:7856::1/64

host(config-ge0)#ipv6 address 4005:8899::1/64 secondary

### mtu

**mtu**命令用来配置端口的MTU值，用于控制接口的最大报文发送长度。

【命令】

**mtu** *mtu-range*

【缺省情况】

缺省情况下，MTU值为1500字节。

【视图】

接口视图

【参数】

*mtu-range*：MTU值，取值范围1280～1500字节。

【举例】

# 配置ge0端口的MTU值为1400字节。

host# configure terminal

host(config)# interface ge0

host(config-ge0)#mtu 1400

### show interface

**show interface**命令用来显示接口信息。

【命令】

**show interface** *interface-name*

【视图】

任意视图

【参数】

*interface-name*：接口名称。

【举例】

# 显示端口ge0的信息。

host# show interface ge0

----------------------------------------------------------------------

interface ge0

description:

Admin UP Link UP

MTU: 1400

MAC address: 00:21:45:c2:e7:40

Auto negotiate: OFF

Speed: 100 Duplex: FULL

media type: COMBO(COPPER)

Listen Mode: OFF

Link-local address: fe80::221:45ff:fec2:e740/64

表 2-1 show interface命令显示信息描述表

| 字段 | 描述 |
| --- | --- |
| Admin UP | 接口物理状态，有Link UP和Link DOWN两种情况 |
| MTU | 接口MTU值 |
| MAC address | 接口MAC地址 |
| Auto negotiate | 接口自协商方式，有ON和OFF两种方式 |
| Speed | 接口速率 |
| Listen | 接口监听模式，有ON和OFF两种方式 |
| Link-local address | 接口的链路本地地址 |

### shutdown

**shutdown**命令用来关闭端口收发包功能。

**no shutdown**命令用来打开端口收发包功能。

【命令】

**shutdown**

**no shutdown**

【缺省情况】

缺省情况下，端口为开启状态。

【视图】

接口视图

【举例】

# 关闭ge0接口。

host# configure terminal

host(config)# interface ge0

host(config-ge0)#shutdown

### speed

**speed**命令用来配置接口收发包的速率。

【命令】

**speed** { **10** | **100** | **1000** }

【视图】

接口视图

【参数】

**10**：端口收发包速率10M。

**100**：端口收发包速率100M。

**1000**：端口收发包速率1000M。

【使用指导】

只有在自协商模式为off时可配置。

【举例】

# 设置ge0接口的速率为100M。

host# configure terminal

host(config)# interface ge0

host(config-ge0)#speed 100

## 聚合接口配置命令

### aggregate-group

**aggregate-group**命令用来把端口加入聚合接口。

**no aggregate-group**命令用来把端口移除聚合接口。

【命令】

**aggregate-group** *id*

**no aggregate-group** *id*

【视图】

接口视图

【参数】

*id*：聚合接口，取值范围0～255。

【使用指导】

配置聚合接口后，需要将实际物理接口或VLAN接口加入聚合接口中，这些接口被称为聚合组端口。

所有加入到Aggregate接口的物理子接口都可以接收报文，并且在发送报文时，轮询发送，即从第一个物理子接口到最后一个物理子接口依次发送。

将一个端口加入聚合接口时，该端口的所有IP地址将被删除。

【举例】

# 将ge1加入聚合接口agg0内。

host# configure terminal

host(config)# interface ge1

host(config-ge1)#aggregate-group 0

### interface

**interface**命令用来创建接口，并进入接口视图，如果创建的接口已经存在，则直接进入接口视图。

**no interface**命令用来删除指定接口。

【命令】

**interface** *name*

**no interface** *name*

【视图】

系统视图

【参数】

*name*：聚合接口名，以agg开头，后面添加0～255的数字。

【举例】

# 创建聚合接口agg0。

host# configure terminal

host(config)# interface agg0

## VLAN接口配置命令

### interface

**interface**命令用来创建VLAN接口，并进入接口视图，如果创建的接口已经存在，则直接进入接口视图。

**no interface**命令用来删除指定的VLAN接口。

【命令】

**interface** *name***.***vlanid*

**no interface** *name***.***vlanid*

【视图】

系统视图

【参数】

*name*：接口名称。

*vlanid*：VLAN ID，范围1～4094。

【使用指导】

如果要让设备识别带VLAN标识的包，需要创建一个以太网子接口，并且为其指定一个VLAN ID，则可以通过该子接口接收/转发带VLAN的包。

【举例】

# 创建一个物理以太网接口ge的VLAN子接口，VLAN ID为10。

host# configure terminal

host(config)# interface ge0.10

## 透明网桥配置命令

### bridge forward-delay

**bridge max-time**命令用来修改透明网桥转发时延。

【命令】

**bridge forward-delay***delay-time*

【缺省情况】

缺省情况下，缺省时间为15S。

【视图】

透明网桥视图

【参数】

*delay -time*：端口状态转换时延，范围4～30秒。

【使用指导】

端口转换时延是指开启STP后，端口从listening到learning到forwarding变化的时间间隔。

【举例】

# 修改网桥bvi0的状态转换时延为20秒。

host# configure terminal

host(config)# interface bvi0

host(config-bvi0)#bridge forward-delay 20

### bridge hello-time

**bridge hello-time**命令用来修改透明网桥配置发送bpdu hello时间。

【命令】

**bridge hello-time** *hello-time*

【缺省情况】

缺省情况下，缺省时间为2S。

【视图】

透明网桥视图

【参数】

*hello-time*：发送hello bpdu时间间隔，范围1～10秒。

【举例】

# 修改网桥bvi0的hello-time为2秒。

host# configure terminal

host(config)# interface bvi0

host(config-bvi0)#bridge hello-time 2

### bridge max-age

**bridge max-age**命令用来修改透明网桥最大老化时间。

【命令】

**bridge max-age** *age-time*

【缺省情况】

缺省情况下，缺省时间为20S。

【视图】

透明网桥视图

【参数】

*age-time*：最大老化时间，范围6-40秒。

【举例】

# 修改网桥bvi0的age-time为30秒。

host# configure terminal

host(config)# interface bvi0

host(config-bvi0)#bridge max-age 30

### bridge priority

**bridge priority**命令用来修改网桥的优先级。

【命令】

**bridge priority** *priority-rang*

【缺省情况】

缺省情况下，优先级默认为32767。

【视图】

透明网桥视图

【参数】

*priority-rang*：桥接口优先级，范围为0～65535。

【举例】

# 修改网桥bvi0的优先级为1000。

host# configure terminal

host(config)# interface bvi0

host(config-bvi0)#bridge priority 1000

### bridge stp

**bridge stp**命令用来开启或关闭网桥STP功能。

【命令】

**bridge stp** { **enable** | **disable** }

【缺省情况】

缺省情况下， 网桥STP功能为disable。

【视图】

透明网桥视图

【参数】

**enable**：开启stp功能。

**disable**：关闭stp功能。

【举例】

# 开启网桥bvi0的STP功能。

host# configure terminal

host(config)# interface bvi0

host(config-bvi0)#bridge stp enable

### bridge-group

**bridge-group**命令用来把端口加入透明网桥接口。

**no bridge-group**命令用来把端口移除透明网桥接口。

【命令】

**bridge-group** *id*

**no bridge-group** *id*

【视图】

接口视图

【参数】

*id*：聚合接索引，取值范围0～255。

【举例】

# 将ge1作为网桥组端口加入网桥。

host# configure terminal

host(config)# interface ge1

host(config-ge1)#bridge-group 0

### interface

**interface**命令用来创建透明网桥接口，并进入网桥视图，如果创建的网桥接口已经存在，则直接进入网桥接口视图。

**no interface**命令用来删除指定的网桥接口。

【命令】

**interface** *name*

**no interface** *name*

【视图】

系统视图

【参数】

*name*：聚合接口名，以bvi开头，后面添加0～255的数字。

【使用指导】

配置透明网桥后，需要将实际物理接口或VLAN接口加入网桥中，这些接口被称为网桥组端口。

网桥组端口的ID由两部分组成：1字节的优先级和1字节的端口号。当网桥有两个端口都连接在LAN上从而形成回路时，可以通过网桥端口ID来影响端口的选择，ID越小的端口越有可能成为指定端口。因此，如果网桥端口的优先级越小，则网桥端口的ID越小，越有可能成为指定端口。

同一个接口只能加入到一个网桥组。

将一个端口加入网桥时，该端口的所有IP地址将被删除。

【举例】

# 创建一个网桥接口bvi0。

host# configure terminal

host(config)# interface bvi0

### show bridge-group

**show bridge-group**命令用来指定桥组信息。

【命令】

**show bridge-group** *group-id*

【视图】

任意视图

【参数】

*Group-id*：网桥组ID，范围0～255。

【使用指导】

分别显示了桥组名、STP启用状态、桥ID、指定的根、FDB老化时间及该桥组所包含的端口及端口的状态。

【举例】

# 显示网桥组bvi0的信息。

host# show bridge-group 0

Bridge: bvi0

STP: enabled

bridge id : 0001.002145c2e741

designated root : 0001.002145c2e741

Ageing time: 300

Hello time: 2

Max age: 20

Forward delay: 20

Bridge ports:

ge1 <forwarding>

表 2-2 show bridge-group命令显示信息描述表

| 字段 | 描述 |
| --- | --- |
| Bridge | 桥组名称 |
| STP | 接口STP的状态，有enable和disable两种 |
| bridge id | 指定桥ID |
| designated root | 指定根桥 |
| Hello time | 发送hello包的间隔 |
| Max age | 最大老化时间 |
| Forward delay | 状态转换时延 |
| Bridge ports | 桥接口 |

## 隧道接口配置命令

### interface tunnel

**interface tunnel**命令用来创建隧道接口，并进入隧道视图，如果创建的隧道接口已经存在，则直接进入隧道接口视图。

**no interface tunnel**命令用来删除指定的隧道接口。

【命令】

**interface** **tunnel** *tunnel-id* **mode** { **ipsec** | **ipv6ip** { **manual** | **6to4** | **isatap** }}

**no interface tunnel** *tunnel-name*

【视图】

系统视图

【参数】

*tunnel-id*：tunnel接口id，范围为0～1023。

*tunnel-name*：隧道名称。

**ipsec**：ipsec封装方式。

**ipv6ip**：ipv6封装模式。

**manual**：手动隧道。

**6to4**：6to4隧道

**isatap**：isatap隧道。

【使用指导】

每个接口都能分别配置不同的封装模式，但每次只能配置一种方式，且在接口创建时就指定，不能修改。

IPv6手动隧道是点到点的隧道模式，隧道的两端都必须配置才能成功通信，否则隧道的另一端会认为该报文不是自己的报文而被丢弃。手动隧道必须由管理员手动配置封装IPv6报文的IPv4源和目的地址。

6to4采用特殊的IPv6地址使在IPv4海洋中的IPv6孤岛能相互连接。此时IPv6的出口路由器与其他的IPv6域建立隧道连接。IPv4隧道的末端可从IPv6域的地址前缀中自动提取，因为站点的IPv4地址包含在IPv6地址前缀中。

ISATAP ( Intra-Site Automatic Tunnel Addressing Protocol，站内自动隧道[寻址](http://baike.baidu.com/view/1303626.htm)协议)是一种地址分配和[主机](http://baike.baidu.com/view/23880.htm)到[主机](http://baike.baidu.com/view/23880.htm)、主机到[路由器](http://baike.baidu.com/view/1360.htm)和[路由器](http://baike.baidu.com/view/1360.htm)到主机的自动[隧道技术](http://baike.baidu.com/view/626368.htm)，它为IPv6主机之间提供了跨越IPv4内部网络的[单播](http://baike.baidu.com/view/492261.htm)IPv6连通性 ISATAP一般用于IPv4网络中的IPv6/IPv4[节点](http://baike.baidu.com/view/47398.htm)间的通信。

【举例】

# 创建一个6to4模式的tunnel接口。

host# configure terminal

host(config)# interface tunnel 2 mode ipv6ip 6to4

### show interface

**show interface**命令用来显示接口信息。

【命令】

**show interface** *tunnel-name*

【视图】

任意视图

【参数】

*tunnel -name*：隧道接口名称。

【举例】

# 显示端口tunnel0的信息。

host# show interface tunnel0

----------------------------------------------------------------------

interface tunnel0

description:

Admin UP Link DOWN

MTU: 1480

tunnel mode: manual(ipv6)

tunnel source-dev: ge0 (192.168.1.85)

tunnel destination addr: 10.1.1.1

表 2-3 show interface命令显示信息描述表

| 字段 | 描述 |
| --- | --- |
| Admin UP | 接口物理状态，Link UP和Link DOWN两种情况 |
| MTU | 接口MTU值 |
| tunnel mode | 隧道模式，有manual，6to4和isatap三种 |
| tunnel source-dev | 隧道的源接口或地址 |
| tunnel destination addr | 隧道的目的地址 |

### tunnel destination

**tunnel destination**命令用来指定隧道接口的目的地址。

**no tunnel destination**命令用来删除隧道接口的目的地址。

【命令】

**tunnel destination** *address*

**no tunnel destination**

【视图】

隧道接口视图

【参数】

*address*：隧道目的地址。

【使用指导】

只有配置为manual模式的隧道才能配置目的地址。

【举例】

# 创建tunnel0隧道，并配置它的目的地址为10.1.1.1。

host# configure terminal

host(config)# interface tunnel 0 mode ipv6ip manual

host(config-tunnel0)#tunnel destination 10.1.1.1

### tunnel source

**tunnel source**命令用来指定隧道接口的源地址或源接口。

**no tunnel source**命令用来删除隧道接口的源地址或源接口。

【命令】

**tunnel source** { *address* | *interface-name* }

**no tunnel source**

【视图】

隧道接口视图

【参数】

*address*：隧道源地址。

*interface-name*：接口名称。

【举例】

# 配置一个6to4模式的tunnel接口，并将ge0接口作为隧道源接口。

host# configure terminal

host(config)# interface tunnel 2 mode ipv6ip 6to4

host(config-tunnel2)#tunnel source ge0

# DHCP命令

## DHCP命令

### bind

**bind**命令用来配置IP和MAC绑定。

**no bind**命令用来删除IP和MAC绑定。

【命令】

**bind** *name**mac-address ip-address*

**no bind** *name*

【视图】

DHCP视图

【参数】

*name*：IP和MAC的绑定名称。为1～31个字符的字符串，且不能包含“%!"#$&`\*+,/:;<=>?\^'{}!”。

*mac-address*：MAC地址。

*ip-address*：IP地址。

【使用指导】

该命令可以设置指定的IP地址与指定的MAC地址捆绑，指定的MAC地址与IP地址一一对应。在IP分配时，对应的MAC地址只分配对应的IP地址。

【举例】

# 配置一条名为“test”的IP和MAC绑定。

host# configure terminal

host(config)# dhcp

host(config-dhcp)# bind test 00:01:7a:fb:9a:db 1.1.1.2

【相关命令】

* show dhcp config

### dhcprelay

**dhcprelay**命令用来在接口上开启DHCP代理的功能。

**no dhcprelay**命令用来在接口上关闭DHCP代理的功能。

【命令】

**dhcprelay ip-address**

**no dhcprelay**

【缺省情况】

缺省情况下，任何接口上的DHCP代理功能均未开启。

【视图】

接口视图

【使用指导】

仅当某接口状态为UP状态时，才可在该接口上开启DHCP代理功能。

【举例】

# 开启ge4接口上的DHCP代理功能。

host# configure terminal

host(config)# interface ge4

host(config-ge4)# dhcp

host(config-ge4)# dhcprelay 172.1.1.10

【相关命令】

* show running-config interface

dhcpserver enable

**dhcpserver enable**命令用来在接口上开启DHCP服务器功能。

**no dhcpserver enable**命令用来在接口上关闭DHCP服务器功能。

【命令】

**dhcpserver enable**

**no dhcpserver enable**

【缺省情况】

缺省情况下，任何接口上的DHCP服务器功能均未开启。

【视图】

接口视图

【使用指导】

仅当某接口状态为UP状态时，才可在该接口上开启DHCP服务器功能。

【举例】

# 开启ge4接口上的DHCP服务器功能。

host# configure terminal

host(config)# interface ge4

host(config-ge4)#dhcpserver enable

【相关命令】

* show running-config interface

### exclude

**exclude**命令用来配置排除的地址范围。

**no exclude**命令用来删除排除的地址范围。

【命令】

**exclude** *ip-address1 ip-address2*

**no exclude** *ip-address1 ip-address2*

【视图】

DHCP视图

【参数】

*ip-address1*：排除地址范围的起始IP地址。

*ip-address2*：排除地址范围的结束IP地址。

【使用指导】

排除地址范围内的IP地址将不会被分配给客户端。

【举例】

# 配置排除地址范围。

host# configure terminal

host(config)# dhcp

host(config-dhcp)# exclude 1.1.1.10 1.1.1.20

【相关命令】

* show dhcp config

### share-net

**share-net** *name**ip-address1 ip-address2* **infinite**命令用来配置指定子网的地址池，及其租约为无限期。

**share-net** *name**ip-address1 ip-address2**days* **days** *hours* **hours** *minutes* **mins**命令用来配置指定子网的地址池，及指定其租约时间。

**no share-net** *name**ip-address1 ip-address2*命令用来删除指定子网的地址池。

【命令】

**share-net** *name**ip-address1 ip-address2* **infinite**

**share-net** *name**ip-address1 ip-address2**days* **days** *hours* **hours** *minutes* **mins**

**no share-net** *name**ip-address1 ip-address2*

【视图】

DHCP视图

【参数】

*name*：子网名称。

*ip-address1*：子网对应的地址池的起始IP地址。

*ip-address2*：子网对应的地址池的结束IP地址。

*days*：租约时间为有限期时的单位天，取值范围为0～100天。

*hours*：租约时间为有限期时的单位小时，取值范围为0～23小时。

*minutes*：租约时间为有限期时的单位分钟，取值范围为0～59分钟。

【举例】

# 配置子网“abc123”的IP地址池及租约时间。

host# configure terminal

host(config)# dhcp

host(config-dhcp)# share-net abc123 1.1.1.2 1.1.1.100 infinite

host(config-dhcp)# share-net abc123 1.1.2.1 1.1.2.100 2 days 3 hours 40 mins

【相关命令】

* show dhcp config

### share-net dns

**share-net** *name* **dns**命令用来配置子网的DNS。

**no share-net** *name* **dns**命令用来删除子网的DNS。

【命令】

**share-net name dns** *ip-address&*<1-2>

**no share-net name dns**

【视图】

DHCP视图

【参数】

*name*：子网名称。

*ip-address*：子网的DNS IP地址。如果使用该命令，则至少配置1个，最多配置2个。

【使用指导】

如果配置了DNS，DHCP服务器将在为客户端分配IP地址时，一同通知给客户端。

【举例】

# 配置子网“abc123”的DNS。

host# configure terminal

host(config)# dhcp

host(config-dhcp)# share-net abc123 dns 8.8.8.8

【相关命令】

* show dhcp config

### share-net domain

**share-net** *name* **domain**命令用来配置子网的域名。

**no share-net** *name* **domain**命令用来删除子网的域名。

【命令】

**share-net** *name* **domain** *domain*

**no share-net** *name* **domain**

【视图】

DHCP视图

【参数】

*name*：子网名称。

*domain*：子网对应的域名。为1～31个字符的字符串，且不能包含“%!"#$&`\*+,/:;<=>?\^'{}!”。

【举例】

# 配置子网“abc123”的域名。

host# configure terminal

host(config)# dhcp

host(config-dhcp)# share-net abc123 domain abc123.com

【相关命令】

* show dhcp config

share-net gateway

**share-net** *name* **gateway**命令用来为指定的子网配置缺省网关IP地址。

**no share-net** *name* **gateway**命令用来为指定的子网删除缺省网关IP地址。

【命令】

**share-net** *name* **gateway** *ip-address*

**no share-net** *name* **gateway**

【视图】

DHCP视图

【参数】

*name*：子网名称。

*ip-address*：子网的缺省网关地址。

【使用指导】

如果配置了缺省网关，DHCP服务器将在为客户端分配IP地址时，一同通知给客户端。

【举例】

# 配置子网“abc123”的缺省网关。

host# configure terminal

host(config)# dhcp

host(config-dhcp)# share-net abc123 gateway 192.168.1.1

【相关命令】

* show dhcp config

### share-net subnet

**share-net** *name* **subnet** *ip-address*/*prefix*命令用来创建子网及子网网段。

**no share-net** *name* **subnet**命令用来删除指定子网的子网网段。

**no share-net**命令用来删除指定的子网的所有配置。

【命令】

**share-net** *name* **subnet** *ip-address*/*prefix*

**no share-net** *name*

**no share-net** *name* **subnet**

【视图】

DHCP视图

【参数】

*name*：子网名称。为1～31个字符的字符串，且不能包含“%!"#$&`\*+,/:;<=>?\^'{}!”。

*ip-address/prefix*：子网网段。

【使用指导】

当某接口作为DHCP服务器时，需要配置该项，才可为内网用户自动分配IP地址。

【举例】

# 创建一个子网“abc123”及子网网段。

host# configure terminal

host(config)# dhcp

host(config-dhcp)# share-net abc123 subnet 1.1.1.1/24

【相关命令】

* show dhcp config

### share-net wins

**share-net** *name* **wins**命令用来配置子网的WINS。

**no share-net** *name* **wins**命令用来删除子网的WINS。

【命令】

**share-net** *name* **wins** *ip-address***&<1-2>**

**no share-net** *name* **wins**

【视图】

DHCP视图

【参数】

*name*：子网名称。

*ip-address*：子网的WNS IP地址。如果使用该命令，则至少配置1个，最多配置2个。

【使用指导】

如果配置了WINS，DHCP服务器将在为客户端分配IP地址时，一同通知给客户端。

【举例】

# 配置子网“abc123”的WINS。

host# configure terminal

host(config)# dhcp

host(config-dhcp)# share-net abc123 wins 1.1.1.1

【相关命令】

* show dhcp config

### show dhcp config

**show dhc config**命令用来显示DHCP的配置信息。

【命令】

**show dhc config**

【视图】

任意视图

【举例】

# 显示DHCP的配置信息。

host# show dhcp config

dhcp

share-net abc123 subnet 1.1.1.1/24

share-net abc123 gateway 192.168.1.1

share-net abc123 dns 8.8.8.8

share-net abc123 wins 1.1.1.1

share-net abc123 domain abc123.com

bind test 00:01:7a:fb:9a:db 1.1.1.2

exclude 1.1.1.10 1.1.1.20

!

### show dhcp ip active

**show dhcp ip active**命令用来查看IP地址的分配详情。

【命令】

**show dhcp ip active**

【视图】

任意视图

【举例】

# 显示DHCP的IP地址分配详情。

host# show dhcp ip active

------------------------------

ipaddr:        192.168.6.100

macaddr:       3c:df:bd:8c:74:46

start\_time:    2014-07-03 14:22:45

end\_time:      Infinite

interface:     ge8

------------------------------

ipaddr:        192.168.6.101

macaddr:       f0:f6:1c:4b:9c:24

start\_time:    2014-07-03 11:23:21

end\_time:      2014-10-01 11:23:21

interface:     ge8

表 3-1 域名缓存统计显示信息描述表

| 字段 | 描述 |
| --- | --- |
| ipaddr | 分配的IP地址 |
| macaddr | 使用该IP的MAC地址 |
| start\_time | 该IP被分配启用的时间 |
| end\_time | 该IP的失效时间 |
| interface | 分配该IP的接口 |

# 路由配置

## 静态路由配置命令

### ip route

**ip route**命令用来配置静态路由。

**no ip route**命令用来删除静态路由。

【命令】

**ip route** { *network*/*prefix-len* | *network mask* | *isp* } { *nexthop* | *interface* | **null0** } [ *ad* ] [ **weight** *weights* ]

**ip route** { *network* | *isp* } [ *nexthop* | *interface* ] **blackhole**

**no ip route** { *network*/*prefix-len* | *network mask* | *isp* } { *nexthop* | *interface* | **null0** } [ *ad* ] [ **weight** *weights* ]

【缺省情况】

缺省情况下，未配置静态路由。

【视图】

系统视图

【参数】

*network*：目的网段地址。

*prefix-len*：网络掩码长度。

*mask*：网络掩码。

*isp*：ISP路由址库。

*nexthop*：下一跳地址。

*interface*：路由出接口。

**null0**：无出接口，即该路由为黑洞路由。

**blackhole**：黑洞路由。

*ad*：管理距离，范围1～255，静态路由缺省为1，直连路由缺省为0。

**weight**：路由的权重。

*weights*：权重值，范围是1～255。缺省是1。

【使用指导】

静态路由是由用户配置的路由。当用户确信到达某个网段应该先转发到某个地址时，可以通过**ip route** 命令配置这个静态路由，同时可以配置该静态路由的权重，用于负载分担。

【举例】

# 配置静态路由，目的网段地址是1.1.1.0、掩码是24位、下一跳是192.168.1.1。

host# configure terminal

host(config)# ip route 1.1.1.0/24 192.168.1.1

【相关命令】

* show ip route

## 路由显示命令

### show ip route

**show ip route**命令用来显示系统路由表。

【命令】

show ip route [ **summary** | **connected** | **static** | **rip** | **ospf** | **supernets-only** ]

【视图】

用户视图

【参数】

**summary**：显示汇总路由。

**connected**：显示直连路由。

**static**：显示静态路由。

**rip**：显示RIP路由。

**ospf**：显示OSPF路由。

**supernets-only**：显示超网路由。

【举例】

# 显示系统路由表。

host # show ip route

Codes: C - connected, S - static, R - RIP, O - OSPF,

P - PPPOE route, D - DHCP route, I - ISP route,

L - LLB route, > - selected route, \* - FIB route

S>\* 1.1.1.0/24 [1/0] via 192.168.1.1 weight 1, ge0

S 3.0.0.0/24 [1/0] via 3.3.3.3 weight 1 inactive

C>\* 3.3.3.0/24 is directly connected, ge0

S>\* 4.0.0.0/24 [1/0] via 192.168.1.1 weight 1, ge0, bh

S>\* 5.0.0.0/24 [1/0] is directly connected, Null0, bh

C>\* 127.0.0.0/8 is directly connected, lo

S>\* 192.168.0.0/16 [1/0] via 192.168.1.1 weight 1, ge0

C>\* 192.168.1.0/24 is directly connected, ge0

表 4-1 show ip route 命令显示信息描述表

| 字段 | 描述 | |
| --- | --- | --- |
| Codes | 路由类型和状态标示 | |
| C | 直连路由 |
| S | 静态路由 |
| R | RIP路由 |
| O | OSPF路由 |
| P | PPPOE路由 |
| D | DHCP路由 |
| I | ISP路由 |
| > | 路由已经被优选 |
| \* | 路由已经加入FIB表 |
| X.X.X.X/X | 目的网段 | |
| [X/Y] | X表示距离矢量，Y表示路由的度量 | |
| via | 下一条地址 | |
| is directly connected | 路由指定了出接口 | |
| weight | 下一跳的权重值 | |
| inactive | 路由没有激活 | |
| interface | 路由出接口 | |
| bh | 黑洞路由 | |

# 显示路由汇总信息。

host# show ip route summary

Route Source Routes FIB

connected 3 3

static 6 4

------

Totals 9 7

表 4-2 show ip route summary命令显示信息描述表

| 字段 | 描述 |
| --- | --- |
| Route Source | 路由类型 |
| Routes | 路由个数 |
| FIB | 已经加入FIB表的路由个数 |
| Totals | 总个数 |

### show ip route *address*

**show ip route** *address*命令用来显示和特定地址相关的路由表。

【命令】

**show ip route** {*address* | *network*[ **longer-prefixes** ] }

【视图】

用户视图

【参数】

*address*：显示地址所属路由表项。

*network*：显示和网络匹配的路由表项，格式为X.X.X.X/Y。

**longer-prefixes**:显示和网络掩码最长匹配的路由表项。

【使用指导】

**longer-prefixes**表示最长匹配。如果network输入3.3.0.0/16，只显示目的网段是3.3.0.0/16的地址。如果加上**longer-prefixes**参数，可以匹配3.3.3.0/24的地址。因为3.3.3.0和16位掩码相与，结果也是3.3.0.0。

【举例】

# 显示3.3.1.1所属路由表项。

host# show ip route 3.3.1.1

Routing entry for 3.3.0.0/16

Known via "static", distance 1, metric 0, best

\* 3.3.3.1, via ge0

表 4-3 **show ip route** *address*命令显示信息描述表

| 字段 | 描述 |
| --- | --- |
| Routing entry for | 路由表项 |
| Known via | 地址类型 |
| distance | 管理距离 |
| metric | 度量值 |
| best | 路由是否被优选 |
| \* X.X.X.X | 下一跳地址 |
| via | 后接出接口 |

## 策略路由命令

### proute

**proute**命令用来添加策略路由。

**no proute**命令用来删除策略路由。

【命令】

**proute** { *if\_in* | **any** } { *sip* | **any** } { *dip* | **any** } { *sev* | **any** } { *user* | **any** } { *app* | **any** } { *schedule* | **always** } { *nexthop* | *interface* } [ *id* ] [ **weight** *weights* ]

**no poute** *id*

【缺省情况】

缺省情况下，未配置策略路由。

【视图】

系统视图

【参数】

if\_in：流量入接口。

**any**：任何入接口

*sip*：流量的源IP地址。

**any**：任何源地址。

*dip*：流量的目的IP地址。

**any**：任何目的地址。

*sev*：流量匹配的服务组。

**any**：任何服务组。

*user*：流量所属用户。

**any**：任何用户

*app*：流量所属应用。

**any**：任何应用。

*schedule*：流量所属时间对象。

**always**：任何时间。

*nexthop*：下一跳地址。

*interface*：路由出接口。

*id*：策略路由ID号，范围是1～65535。缺省从1开始分配，依次递增。

**weight**：策略路由权重。

*weights*：策略路由的权重值，范围是1～255，默认是1。

【使用指导】

策略路由可以在流量进入设备的时候生效，也可以对于设备本地发起的流量生效，当入接口为any时，可以匹配本地接口发起的流量。

【举例】

# 将来自192.168.1.0/24网段的数据包路由至设备200.0.0.2上。

host# configure terminal

host(config)# address SRC1

host(config-ge0)# ip subnet 192.168.1.0/24

host(config-ge0)# exit

host(config)# proute any SRC1 any any any any always 200.0.0.2

【相关命令】

* show proute

### proute insert

**proute** **insert**命令用来插入一条策略路由。

【命令】

**proute** **insert** { *if\_in* | **any** } { *sip* | **any** } { *dip* | **any** } { *sev* | **any** } { *user* | **any** } { *app* | **any** } { *schedule* | **always** } { *nexthop* | *interface* } [ *id* ] [ **weight** *weights* ] **before** *compare-id*

【缺省情况】

缺省情况下，未配置策略路由。

【视图】

系统视图

【参数】

if\_in：流量入接口。

**any**：任何入接口

*sip*：流量的源IP地址。

**any**：任何源地址。

*dip*：流量的目的IP地址。

**any**：任何目的地址。

*sev*：流量匹配的服务组。

**any**：任何服务组。

*user*：流量所属用户。

**any**：任何用户

*app*：流量所属应用。

**any**：任何应用。

*schedule*：流量所属时间对象。

**always**：任何时间。

*nexthop*：下一跳地址。

*interface*：路由出接口。

*id*：策略路由ID号，范围是1～65535。缺省从1开始分配，依次递增。

**weight**：策略路由权重。

*weights*：策略路由的权重值，范围是1～255，默认是1。

**before**：在指定ID之前插入ID。

*compare-id*：要插入位置的ID号。

【使用指导】

策略路由的匹配是有先后顺序的，具体顺序和**show proute**顺序相同。

【举例】

# 将来自192.168.1.0/24网段的数据包路由至设备200.0.0.2上，并且将此策略路由插入到ID为10的策略路由之前。

host# configure terminal

host(config)# address SRC1

host(config-ge0)# ip subnet 192.168.1.0/24

host(config-ge0)# exit

host(config)# proute insert any SRC1 any any any any always 200.0.0.2 before 10

【相关命令】

* show proute

### proute move

**proute** **move**命令用来移动策略路由匹配顺序。

【命令】

**proute move** *id*{ **before** | **after** }compare-*id*

【视图】

系统视图

【参数】

*id*：策略路由ID号，范围是1～65535。缺省从1开始分配，依次递增。

**after:** 在指定ID之后插入策略路由。

**before**:在指定ID之前插入策略路由。

*compare-id*：要插入位置的ID号。

【使用指导】

策略路由的匹配是有先后顺序的，具体顺序和**show proute**顺序相同。

【举例】

# 将ID为5的策略路由插入到ID为10的策略路由之前。

host# configure terminal

host(config)# proute move 5 before 10

【相关命令】

* show proute

### show proute

**show proute**命令用来显示配置的策略路由。

【命令】

**show proute**

【视图】

用户视图

【举例】

# 用来显示配置的策略路由。

host# show proute

proute any ge0 any any any any always 192.168.1.1 1 active

表 4-4 show proute命令显示信息描述表

| 字段 | 描述 |
| --- | --- |
| active | 策略路由是否可以使用 |

## ISP路由命令

### isp network

**isp network**命令用来配置ISP路由地址库。

**no isp network**命令用来删除ISP路由地址库。

【命令】

**isp network** *name*

**no isp network** *name*

【缺省情况】

缺省情况下，设备内部预置了联通(ChinaUnicom)、移动(ChinaMobile)、电信(ChinaTelecom)和教育网(ChinaMobile)四个ISP路由地址库。

【视图】

系统视图

【参数】

*name*：ISP路由地址库名称，为1～31个字符组成的字符串，不能与预定义的ChinaUnicom、ChinaMobile 、ChinaTelecom、ChinaMobile相同。

【使用指导】

配置了ISP路由地址库后，会进入ISP路由配置视图。

【举例】

# 配置名字为ISP1的ISP路由。

host# configure terminal

host(config)# isp network ISP1

host(config-isp)#

【相关命令】

* subnet

### subnet

**subnet**命令用来配置ISP路由地址库的子网地址。

**no subnet**命令用来删除ISP路由地址库的子网地址。

【命令】

**subnet** *networks*

**no subnet** *networks*

【缺省情况】

缺省情况下，设备内部预置了联通(ChinaUnicom)、移动(ChinaMobile)、电信(ChinaTelecom)和教育网(ChinaMobile)四个ISP路由地址库。

【视图】

ISP路由视图

【参数】

*networks*：ISP路由的子网地址，为X.X.X.X/Y格式。

【使用指导】

用户自定义的ISP，每个ISP最多有200个地址网段。

【举例】

#在名字为ISP1的ispISP路由址库中，加入子网202.06.0.0/24

host# configure terminal

host(config)# isp network ISP1

host(config-isp)# subnet 202.106.0.0/24

【相关命令】

* isp network

## RIP

### default-information originate

**default-information originate**命令用来配置发布一条默认路由。

**no default-information originate**命令用来删除发布默认路由。

【命令】

**default-information originate**

**no default-information originate**

【缺省情况】

缺省情况下，不发布默认路由。

【视图】

RIP配置视图

【举例】

# 配置RIP发送一条默认路由。

host# configure terminal

host(config)# router rip

host(config-router)# default-information originate

【相关命令】

* show ip route status

### default-metric

**default-metric**命令用来配置重发布路由的默认度量。

**no default-metric**命令用来恢复重发布路由的默认度量值。

【命令】

**default-metric** *metric*

**no default-metric** [ *metric* ]

【缺省情况】

缺省情况下，重发布路由的默认度量是1。

【视图】

RIP配置视图

【参数】

*metric*：度量值，范围是1～16。

【使用指导】

**default-metric**设置的度量值被**redistribute**使用，如果**redistribute**没有配置metric，则按照**default-metric**重发布。

【举例】

# 配置配置重发布路由的默认度量为2。

host# configure terminal

host(config)# router rip

host(config-router)# default-metric 2

【相关命令】

* show ip route status

### distance

**distance**命令用来配置RIP的管理距离。

**no distance**命令用来恢复RIP的管理距离的缺省值。

【命令】

**distance** *ad*

【缺省情况】

缺省情况下，RIP的管理距离是120。

【视图】

RIP配置视图

【参数】

*ad*：RIP要配置的管理距离，范围是1～255，缺省是120。

【使用指导】

在路由器中可能会运行多个IGP路由协议，如果想让RIP路由具有比从其它路由协议学来的路由更高的优先级，需要配置小的管理距离。管理距离的高低将最后决定IP路由表中的路由是通过哪种路由算法获取的最佳路由。

【举例】

# 配置RIP的管理距离为100。

host# configure terminal

host(config)# router rip

host(config-router)# distance 100

【相关命令】

* show ip route status

### ip rip authentication key-chain

**ip rip authentication key-chain**命令用来配置key的认证钥匙链。

**no ip rip authentication key-chain**命令用来删除配置key认证钥匙链。

【命令】

**ip rip authentication key-chain** *keychain*

**no ip rip authentication key-chain** *keychain*

【缺省情况】

缺省情况下，未配置接口认证钥匙链。

【视图】

接口视图

【参数】

*keychain*：认证钥匙链的名称。

【使用指导】

RIP配置认证是在接口上进行的，首先选择认证方式，然后指定所使用的钥匙链或密文。

接口的key-chain和key-string配置只能二选一。

明文认证时，首选key-string，如果没有key-string，选择key-chain。

密文认证时，首选key-chain，如果没有key-chain，选择key-string。

【举例】

# 配置接口选择认证钥匙链key1认证。

host# configure terminal

host(config)# interface ge0

host(config-ge0)#ip rip authentication key-chain key1

【相关命令】

* key chain
* key
* key-string
* ip rip authentication mode
* ip rip authentication string

### ip rip authentication mode

**ip rip authentication mode**命令用来配置接口的RIP认证模式。

**no ip rip authentication mode**命令用来关闭接口的RIP认证。

【命令】

**ip rip authentication mode** { **md5** | **text** }

**no ip rip authentication mode** { **md5** | **text** }

【缺省情况】

缺省情况下，接口的RIP没有配置认证。

【视图】

接口视图

【参数】

**md5**：认证密文以md5方式发送。

**text**：认证的密文以明文方式发送。

【使用指导】

RIP配置认证是在接口上进行的，首先选择认证方式，然后指定所使用的钥匙链或密文。

RIP中每一个路由更新报文最大可包含25条路由，做了明文认证后只能包含24条，做了MD5认证后只能包含23条。

明文认证时，被认证方发送key chian时，发送最低ID值的key，并且不携带ID；认证方接收到 key后，和自己key chain的全部key进行比较，只要有一个key匹配就通过对被认证方的认证。

密文认证时，被认证方发送key时，发送最低ID值的key，并且携带了ID，认证方接收到key后，首先在自己key chain中查找是否具有相同ID的key，如果有相同ID的key并且key相同就通过认 证，key值不同就不通过认证。如果没有相同ID的key，就查找该ID往后的最近ID的key；如果没有往后的ID，认证失败。

【举例】

# 配置接口ge0的rip认证方式是md5。

host# configure terminal

host(config)# interface ge0

host(config-ge0)#ip rip authentication mode md5

【相关命令】

* key chain
* key-string
* key
* ip rip authentication key-chain
* ip rip authentication string

### ip rip authentication string

**ip rip authentication string**命令用来配置key的认证字符串。

**no ip rip authentication string**命令用来删除配置的key认证字符串。

【命令】

**ip rip authentication string** *key-string*

**no ip rip authentication string** [ *key-string* ]

【缺省情况】

缺省情况下，未配置接口认证字符串。

【视图】

接口视图

【参数】

*key-string*：要配置的认证字符串。

【使用指导】

RIP配置认证是在接口上进行的，首先选择认证方式，然后指定所使用的钥匙链或密文。

接口的key-chain和key-string配置只能二选一。

明文认证时，首选key-string，如果没有key-string，选择key-chain。

密文认证时，首选key-chain，如果没有key-chain，选择key-string。

【举例】

# 配置接口认证字符串为123456。

host# configure terminal

host(config)# interface ge0

host(config-ge0)#ip rip authentication string 123456

【相关命令】

* key chain
* key
* key-string
* ip rip authentication mode
* ip rip authentication string

### ip rip receive

**ip rip receive**命令用来配置接口报文接收版本。

**no ip rip receive**命令用来恢复接口接收报文版本的缺省值。

【命令】

**ip rip send receive** {**1 | 2** }

**no ip rip send receive** {**1 | 2** }

【缺省情况】

缺省情况下，接口按照RIP-2发送报文，按照RIP-1和RIP-2接收报文。

【视图】

接口视图

【参数】

**1**：接口只接收版本号为1的RIP报文。

**2**：接口只接收版本号为2的RIP报文。

【使用指导】

用户可以在RIP视图下配置RIP版本，也可在接口上配置RIP版本：

当全局和接口都没有进行RIP版本配置时，接口发送RIP-1广播报文，可以接收RIP-1广播、单播报文、RIP-2广播/组播/单播报文。

如果接口没有进行RIP版本配置，接口运行的RIP版本将以全局配置的版本为准，如果希望接口配置的RIP版本与全局配置的不一样，则进入接口视图配置接口运行的RIP版本。

当接口运行的RIP版本为RIP-1时，发送RIP-1广播报文，可以接收RIP-1广播/单播报文。

当接口运行的RIP版本为RIP-2且工作在组播方式时，发送RIP-2组播报文，可以接收RIP-2广播/组播/单播报文。

当接口运行的RIP版本为RIP-2且工作在广播方式时，发送RIP-2广播报文，可以接收RIP-1广播/单播报文、RIP-2广播/组播/单播报文。

【举例】

# 配置ge0只接受版本号为1的RIP报文。

host# configure terminal

host(config)# interface ge0

host(config-ge0)#ip rip receive version 1

【相关命令】

* show ip rip status

### ip rip send

**ip rip send**命令用来配置接口发送报文版本号。

**no ip rip send**命令用来恢复接口发送报文版本的缺省值。

【命令】

**ip rip send version** {**1 | 2** }

**no ip rip send version** {**1 | 2** }

【缺省情况】

缺省情况下，接口按照RIP-2发送报文，按照RIP-1和RIP-2接收报文。

【视图】

接口视图

【参数】

**1**：接口只发送版本号为1的RIP报文。

**2**：接口只发送版本号为2的RIP报文。

【使用指导】

用户可以在RIP视图下配置RIP版本，也可在接口上配置RIP版本：

当全局和接口都没有进行RIP版本配置时，接口发送RIP-1广播报文，可以接收RIP-1广播、单播报文、RIP-2广播/组播/单播报文。

如果接口没有进行RIP版本配置，接口运行的RIP版本将以全局配置的版本为准，如果希望接口配置的RIP版本与全局配置的不一样，则进入接口视图配置接口运行的RIP版本。

当接口运行的RIP版本为RIP-1时，发送RIP-1广播报文，可以接收RIP-1广播/单播报文。

当接口运行的RIP版本为RIP-2且工作在组播方式时，发送RIP-2组播报文，可以接收RIP-2广播/组播/单播报文。

当接口运行的RIP版本为RIP-2且工作在广播方式时，发送RIP-2广播报文，可以接收RIP-1广播/单播报文、RIP-2广播/组播/单播报文。

【举例】

# 配置ge0只发送版本号为1的RIP报文。

host# configure terminal

host(config)# interface ge0

host(config-ge0)#ip rip send version 1

【相关命令】

* show ip rip status

### ip rip split-horizon

**ip rip split-horizon**命令用来配置RIP水平分割。

**no ip rip split-horizon**命令用来删除RIP水平分割配置。

【命令】

**ip rip split-horizon** [ **poisoned-reverse** ]

**no ip rip split-horizon** [ **poisoned-reverse** ]

【缺省情况】

缺省情况下，接口下未配置水平分割。

【视图】

接口视图

【参数】

**poisoned-reverse**：启用毒性逆转。

【使用指导】

配置水平分割可以使得从一个接口学到的路由不能通过此接口向外发布，用于避免相邻路由器间的路由环路。

配置毒性逆转后，从一个接口学到的路由还可以从这个接口向外发布，但这些路由的度量值会设置为16（即不可达），可以用于避免相邻路由器间的路由环路。

【举例】

# 配置接口ge0上，启用毒性逆转。

host# configure terminal

host(config)# interface ge0

host(config-ge0)#ip rip split-horizon poisoned-reverse

【相关命令】

* show ip route status

### key

**key** 命令用来添加秘钥。

**no key** 命令用来删除配置的秘钥。

【命令】

**key** *id*

**no key** *id*

【缺省情况】

缺省情况下，未配置认证秘钥。

【视图】

钥匙链视图

【参数】

*id*：配置的秘钥的ID，范围是0～2147483647。

【使用指导】

配置了key后，会进入钥匙配置视图。

明文认证时，被认证方发送key chian时，发送最低ID值的key，并且不携带ID；认证方接收到 key后，和自己key chain的全部key进行比较，只要有一个key匹配就通过对被认证方的认证。

密文认证时，被认证方发送key时，发送最低ID值的key，并且携带了ID,认证方接收到key后，首先在自己key chain中查找是否具有相同ID的key，如果有相同ID的key并且key相同就通过认 证，key值不同就不通过认证。如果没有相同ID的key，就查找该ID往后的最近ID的key；如果没有往后的ID，认证失败。

【举例】

# 添加认证钥匙链key1，钥匙链中添加钥匙10。

host# configure terminal

host(config)# key chain key1

host(config-keychain)# key 10

host(config-keychain-key)#

【相关命令】

* key chain
* key-string
* ip rip authentication mode
* ip rip authentication key-chain
* ip rip authentication string

### key chain

**key chain**命令用来配置认证钥匙链。

**no key chain**命令用来删除认证钥匙链。

【命令】

**key chain** *name*

**no key chain** *name*

【缺省情况】

缺省情况下，未配置认证钥匙链。

【视图】

系统视图

【参数】

*name*：认证钥匙链名称，为1～31字符组成的字符串。

【使用指导】

RIP-2才支持认证，有明文认证和密文认证两种方法，这两种方法中均需要配置钥匙链key-chain或者key-string。

配置了认证钥匙链后，会进入钥匙链视图。

【举例】

# 添加认证钥匙链key1。

host# configure terminal

host(config)# key chain key1

host(config-keychain)#

【相关命令】

* key
* key-string
* ip rip authentication mode
* ip rip authentication key-chain
* ip rip authentication string

### key-string

**key-string**命令用来配置key的认证密文。

**no key-string**命令用来删除配置key认证的密文。

【命令】

**key-string** *string*

**no key-string** [*string* ]

【缺省情况】

缺省情况下，未配置key认证的密文。

【视图】

钥匙视图

【参数】

*string*：key的认证密文。

【使用指导】

明文认证时，被认证方发送key chian时，发送最低ID值的key，并且不携带ID；认证方接收到 key后，和自己key chain的全部key进行比较，只要有一个key匹配就通过对被认证方的认证。

密文认证时，被认证方发送key时，发送最低ID值的key，并且携带了ID，认证方接收到key后，首先在自己key chain中查找是否具有相同ID的key，如果有相同ID的key并且key相同就通过认 证，key值不同就不通过认证。如果没有相同ID的key，就查找该ID往后的最近ID的key；如果没有往后的ID，认证失败。

【举例】

# 添加认证钥匙链key1，钥匙链中添加秘钥10，key的认证密文是123456。

host# configure terminal

host(config)# key chain key1

host(config-keychain)# key 10

host(config-keychain-key)# key-string 123456

【相关命令】

* key chain
* key
* ip rip authentication mode
* ip rip authentication key-chain
* ip rip authentication string

### network

**network**命令用来配置RIP发布网络。

**no network**命令用来删除RIP发布网络。

【命令】

**network** { *ip-address* | *interface* }

**no network** { *ip-address* | *interface* }

【缺省情况】

缺省情况下，未配置发布网络。

【视图】

RIP配置视图

【参数】

*ip-address*：要发布的网络号，格式为X.X.X.X/Z，所有匹配这个网段的网络，都将被发布。

*interface*：要发布网络的接口，配置后，接口上的IP网络将被发布出去。

【举例】

# 配置将设备所有接口网络发布出去。

host# configure terminal

host(config)# router rip

host(config-router)# network 0.0.0.0/0

【相关命令】

* show ip rip status

### passive-interface

**passive-interface**命令用来配置接口的工作状态。

**no passive-interface**命令用来恢复接口的工作状态为缺省状态。

【命令】

**passive-interface** { *interface* **| default** }

【缺省情况】

缺省情况下，接口可以发送路由更新报文。

【视图】

RIP配置视图

【参数】

*interface*：要配置成被动状态的接口名称。

**default**：配置所有接口为被动状态。

【使用指导】

配置接口工作在被动模式，即接口只接收路由更新报文而不发送路由更新报文。

【举例】

# 配置ge0的工作模式为被动模式。

host# configure terminal

host(config)# router rip

host(config-router)# passive-interface ge0

【相关命令】

* show ip rip status

### redistribute

**redistribute**命令用来重发布其他路由协议的路由。

**no ip route**命令用来删除重发布其他路由协议的路由。

【命令】

**redistribute** { **connected** | **static** | **ospf** }[ **metric** *metric*]

**no redistribute** { **connected** | **static** | **ospf** }[ **metric** *metric*]

【缺省情况】

缺省情况下，未配置路由重发布。

【视图】

RIP配置视图

【参数】

**connected**：重发布直连路由。

**static**：重发布静态路由。

**ospf**：重发布OSPF路由。

**metric**：重发布路由的默认度量值。

*metric*：度量值，范围是1～16，缺省使用缺省度量。

【使用指导】

如果没有配置**metric**，则按照系统缺省度量重发布路由。

【举例】

#配置重发布直连路由。

host# configure terminal

host(config)# router rip

host(config-router)# redistribute connected

【相关命令】

* show ip route status

### router rip

**router rip**命令用来开启RIP路由协议。

**no router rip**命令用来关闭RIP路由协议。

【命令】

**router rip**

**no router rip**

【缺省情况】

缺省情况下，未开启RIP路由协议。

【视图】

系统视图

【使用指导】

**router rip**配置后，会进入RIP配置视图。

【举例】

# 配置启用RIP路由协议。

host# configure terminal

host(config)# router rip

host(config-router)#

### show ip rip

**show ip rip**命令显示RIP路由信息。

【命令】

**show ip rip**

【视图】

用户视图

【举例】

# 显示RIP路由信息。

host# show ip rip

Codes: R - RIP, C - connected, S - Static, O - OSPF, B - BGP

Sub-codes:

(n) - normal, (s) - static, (d) - default, (r) - redistribute,

(i) - interface

Network Next Hop Metric From Tag Time

R(d) 0.0.0.0/0 0.0.0.0 1 self 0

C(i) 3.3.3.0/24 0.0.0.0 1 self 0

S(r) 5.0.0.0/24 0.0.0.0 1 self 0

R(n) 10.0.0.0/24 192.168.1.1 2 192.168.1.20 0 02:52

C(i) 192.168.1.0/24 0.0.0.0 1 self 0

表 4-5 show ip rip命令显示信息描述表

| 字段 | 描述 | |
| --- | --- | --- |
| Codes: | 路由条目类型 | |
| R | 来自RIP |
| C | 来自直连路由 |
| S | 来自静态路由 |
| O | 来自OSPF |
| B | 来自BGP |
| Sub-codes: | 路由条目子类型 | |
| n | 普通条目 |
| s | 静态条目 |
| d | 默认路由条目 |
| r | 重定向条目 |
| i | 接口条目 |
| Network | 目的网段 | |
| Next Hop | 下一跳 | |
| Metric | 路由度量 | |
| From | 条目来自 | |
| Tag | 条目标签 | |
| Time | 条目超时时间 | |

### show ip rip status

**show ip rip status**命令用来显示RIP状态。

【命令】

**show ip rip status**

【视图】

用户视图

【举例】

# 显示RIP状态。

host# show ip rip status

Routing Protocol is "rip"

Sending updates every 30 seconds with +/-50%, next due in 25 seconds

Timeout after 180 seconds, garbage collect after 120 seconds

Outgoing update filter list for all interface is not set

Incoming update filter list for all interface is not set

Default redistribution metric is 2

Redistributing: static

Default version control: send version 2, receive any version

Interface Send Recv Key-chain

ge0 1 2 1 2

lo 2 1 2

Routing for Networks:

0.0.0.0/0

ge0

Routing Information Sources:

Gateway BadPackets BadRoutes Distance Last Update

192.168.1.20 0 0 120 00:00:29

Distance: (default is 120)

表 4-6 show ip rip status命令显示信息描述表

| 字段 | 描述 |
| --- | --- |
| Routing Protocol is | 路由协议 |
| Sending updates every | RIP的更新定时器时间 |
| next due in | 距下个更新的时间 |
| Timeout after | 超时时间 |
| garbage collect after | 垃圾回收时间 |
| Default redistribution metric | 重发布的默认路由 |
| Redistributing | 路由重发布配置 |
| Default version control | RIP全局报文版本控制 |
| send version | 发送报文的RIP版本 |
| receive | 接受报文的RIP版本 |
| Interface | 配置了RIP的接口名称 |
| Send | 接口发送报文的RIP版本 |
| Recv | 接口接受报文的RIP版本 |
| Key-chain | 接口认证的钥匙链 |
| Routing for Networks | 配置的RIP发送网络 |
| Routing Information Sources | RIP邻居 |
| Gateway | 邻居的IP地址 |
| BadPackets | 错误报文 |
| BadRoutes | 错误的路由条目 |
| Distance | 邻居RIP的管理距离 |
| Last Update | 收到上次更新距现在的时间 |
| Distance | RIP管理距离 |

timers

**timers**命令用来配置RIP定时器。

**no timers**命令用来恢复RIP定时器的默认值。

【命令】

**timers basic** *update-timer timeout-timer garbag-collection-timer*

**no timers basic** [*update-timer timeout-timer garbag-collection-timer* ]

【缺省情况】

缺省情况下，定时更新时间缺省为30秒，超时时间缺省为180秒，垃圾收集时间缺省为120秒。

【视图】

RIP配置视图

【参数】

*update-timer*：更新时间，范围是5～2147483647，单位是秒，缺省是30。

*timeout-timer*：超时时间，范围是5～2147483647，单位是秒，缺省是180。

*garbag-collection-timer*：垃圾回收时间，范围是5～2147483647，单位是秒，缺省是120。

【使用指导】

更新时间：每次定时器超时，启用了RIP的接口会发送应答信息。

超时时间：如果定时器超时后，还未收到可刷新现有路由的更新，则将该路由的度量设置为 16，从而将其标记为无效路由。在清除计时器超时以前，该路由仍将保留在路由表中。

垃圾回收时间：当定时器超时后，标记为无效的路由将被删除。

【举例】

# 配置RIP更新时间设为5秒，超时时间设为10秒，垃圾回收时间是30秒。

host# configure terminal

host(config)# router rip

host(config-router)# timers basic 5 10 30

【相关命令】

* show ip route status

### version

**version**命令用来配置RIP协议版本号。

**no version**命令用来恢复缺省的RIP协议版本号。

【命令】

**version** { **1** | **2** }

**no version**

【缺省情况】

缺省情况下，RIP协议是版本2。

【视图】

RIP配置视图

【参数】

**1**：配置RIP协议版本号为1。

**2**：配置RIP协议版本号为2。

【使用指导】

用户可以在RIP视图下配置RIP版本，也可在接口上配置RIP版本：

当全局和接口都没有进行RIP版本配置时，接口发送RIP-1广播报文，可以接收RIP-1广播、单播报文、RIP-2广播/组播/单播报文。

如果接口没有进行RIP版本配置，接口运行的RIP版本将以全局配置的版本为准，如果希望接口配置的RIP版本与全局配置的不一样，则进入接口视图配置接口运行的RIP版本。

当接口运行的RIP版本为RIP-1时，发送RIP-1广播报文，可以接收RIP-1广播/单播报文。

当接口运行的RIP版本为RIP-2且工作在组播方式时，发送RIP-2组播报文，可以接收RIP-2广播/组播/单播报文。

当接口运行的RIP版本为RIP-2且工作在广播方式时，发送RIP-2广播报文，可以接收RIP-1广播/单播报文、RIP-2广播/组播/单播报文。

【举例】

# 配置RIP的版本为2。

host# configure terminal

host(config)# router rip

host(config-router)# version 2

【相关命令】

* show ip rip status

## OSPF命令

### area { *ip-address* | *router-id* } authentication

**area** { *ip-address* | *router-id* } **authentication**命令用来配置OSPF区域认证方式。

**no area** { *ip-address* | *router-id* } **authentication**命令用来删除OSPF区域认证方式。

【命令】

**area** { *ip-address* | *router-id* } **authentication** [ **message-digest** ]

**no area** { *ip-address* | *router-id* } **authentication**

【缺省情况】

缺省情况下，OSPF区域不进行认证。

【视图】

OSPF配置视图

【参数】

*ip-address*：OSPF所属的区域ID，为点分十进制形式。

*router-id*：OSPF所属的区域ID，为十进制数字形式。取值范围为0～4294967295。

**message-digest**：OSPF区域认证采用密文认证的方式。

【使用指导】

执行**no area** { *ip-address* | *router-id* } **authentication**命令后，将恢复为默认的不认证方式。

OSPF支持在同一区域内进行认证。一个区域中所有的路由器的认证类型必须一致（不认证、明文认证、MD5密文认证）。认证提供基于密码的保护，防止未经授权对区域进行的访问。在配置区域认证时，必须对区域的所有接口单独配置认证密码。当接口的认证方式和接口所在区域的认证不一致时，优先考虑接口配置的认证方式。

【举例】

# 配置OSPF区域认证。

host# configure terminal

host(config)#router ospf

host(config-router)# area 0 authentication

【相关命令】

* show running-config ospf

### area { ip-address | router-id } range

**area** { *ip-address* | *router-id* } **range** *ip-address1*/*prefix1*[ **not-advertise** ]命令用来配置OSPF区域间路由聚合，并且不宣告聚合后的路由。

**area** { *ip-address* | *router-id* } **range** *ip-address1*/*prefix1* **advertise cost** *metric*命令用来配置OSPF 区域间路由聚合，并配置聚合路由的宣告metric。

**area** { *ip-address* | *router-id* } **range** *ip-address1*/*prefix1* **substitute** *ip-address2*/*prefix2*命令用来配置OSPF区域间路由聚合，并且将地址范围转换成地址宣告。

**no area** { *ip-address* | *router-id* } **range** *ip-address1*/*prefix1* **advertise cost**命令用来取消路由聚合宣告的cost。

【命令】

**area** { *ip-address* | *router-id* } **range** *ip-address1*/*prefix1*[ **not-advertise** ]

**area** { *ip-address* | *router-id* } **range** *ip-address1*/*prefix1* **advertise cost** *metric*

**area** { *ip-address* | *router-id* } **range** *ip-address1*/*prefix1* **substitute** *ip-address2*/*prefix2*

**no area** { *ip-address* | *router-id* } **range** *ip-address1*/*prefix1* **advertise cost**

【视图】

OSPF配置视图

【参数】

*ip-address*：进行聚合的区域ID，为点分十进制形式。

*router-id*：进行聚合的区域ID，为数字形式，取值范围为0～4294967295。

*ip-address1*/*prefix1*：地址范围。

*metric*：聚合路由的宣告metric。

*ip-address2*/*prefix2*：将地址范围转换成该地址宣告。

**not-advertise**：不宣告聚合后的路由。

【使用指导】

区域间的路由聚合是为了减少区域间路由数量，它使ABR通告一条聚合的域间路由到其他区域，而被聚合的路由不被宣告出去。在OSPF中，ABR向其他区域发送路由信息时，以网段为单位生成Type 3 LSA。如果该区域中存在一些连续的网段，则可以配置ABR将这些连续的网段聚合成一个网段。这样ABR只发送一条聚合后的LSA，所有落入本命令指定的聚合网段范围的LSA将不再会被单独发送出去，这样可减少其他区域中链路状态数据库（LSDB）的规模。如果该网段范围用关键字not-advertise限定，则到这一个网段路由的聚合路由将不会被广播出去。这个网段是由IP地址/掩码的方式说明的。接收聚合网段和对网段的限定，可减少区域间路由信息的交流量。

【举例】

# 配置OSPF区域间路由聚合。

host# configure terminal

host(config)# router ospf

host(config-router)# area 0 range 1.1.1.1/24 not-advertise

【相关命令】

* show running-config ospf

### distance

**distance**命令用来配置OSPF协议优先级。

**distance ospf intra-area**命令用来配置OSPF协议的域内、域间、AS外部路由的优先级。

**no distance**命令用来删除OSPF协议优先级。

【命令】

**distance** *distance*

**distance** **ospf intra-area** *intra-area***inter-area** *inter-area* **external** *external*

**no distance**

【缺省情况】

缺省情况下，默认值为110。

【视图】

OSPF配置视图

【参数】

*distance*：OSPF的管理距离(协议优先级)。取值范围为1～255。

*intra-area*：域内路由的OSPF优先级。取值范围为1～255。

*inter-area*：域间路由的OSPF优先级。取值范围为1～255。

*external*：AS外部路由的OSPF优先级。取值范围为1～255。

【使用指导】

使用**no distance**取消配置，使其恢复到默认值110。

一个协议的优先级指的是一个路由信息来源的可信度等级。优先级是一个1～255的整数，通常情况下，值越高可信度越低。值为255就意味着路由信息源根本不可信，应该被忽略。

【举例】

# 配置优先级为100。

host# configure terminal

host(config)# router ospf

host(config-router)# distance 100

【相关命令】

* show running-config ospf

### default-metric

**default-metric**命令用来配置OSPF重发布外部路由时的缺省metric。

**no default-metric**命令用来删除OSPF重发布外部路由时的缺省metric。

【命令】

**default-metric** *metric*

**no default-metric**

【视图】

OSPF配置视图

【参数】

*metric*：重发布路由的默认metric，取值范围为1～16777214。

【举例】

# 配置默认metric。

host# configure terminal

host(config)# router ospf

host(config-router)# default-metric 20

【相关命令】

* show running-config ospf

### default-information originate

**default-information originate metric**命令用来配置OSPF重发布默认路由。

**default-information originate always metric**命令用来强制发布默认路由，即使路由表中没有默认路由。

**no default-information originate**用来删除默认路由。

【命令】

**default-information originate metric** *metric* **metric-type** { **1** | **2** }

**default-information originate always metric** *metric* **metric-type** { **1** | **2** }

**no default-information originate**

【缺省情况】

缺省情况下，重发布的路由为第二类外部路由，即metric-type默认为2。

【视图】

OSPF配置视图

【参数】

*metric*：重发布路由的metric。取值范围为1～16777214。

**1：**重发布路由的类型为第一类外部路由。

**2：**重发布路由的类型为第二类外部路由。

【使用指导】

一旦配置了路由重分布，路由器就自动成为自治系统边界路由器。但是缺省情况下，不会发布缺省路由，可以强制自治系统边界路由器发布缺省路由。但这时路由器表中必须包含缺省路由。如果路由表中没有缺省路由，而要强制自治系统边界路由器产生缺省路由，使用always参数。

【举例】

# 配置OSPF重发布默认路由。

host# configure terminal

host(config)# router ospf

host(config-router)# default-information originate metric 20 metric-type 2

【相关命令】

* show running-config ospf

### ip ospf authentication

**ip ospf authentication**命令用来配置OSPF接口的认证方式。

**no ip ospf authentication**命令用来删除OSPF接口的认证方式。

【命令】

**ip ospf authentication** [ **message-digest** ]

**no ip ospf authentication**

【缺省情况】

缺省情况下，不进行接口认证。

【视图】

接口视图

【参数】

**message-digest**：不用该参数表示明文认证，使用该参数表示密文认证。

【使用指导】

执行**no ip ospf authentication**命令后将恢复至不启用认证的方式。

【举例】

# 配置启用OSPF接口认证。

host# configure terminal

host(config)# interface ge4

host(config-ge4)#ip ospf authentication message-digest

【相关命令】

* show running-config interface

### ip ospf authentication-key

**ip ospf authentication-key**命令用来配置OSPF接口上用于明文认证的密钥。

**no ip ospf authentication-key**命令用来删除OSPF接口上用于明文认证的密钥。

【命令】

**ip ospf authentication-key** *password*

**no ip ospf authentication-key**

【视图】

接口视图

【参数】

*password*：用于明文认证的密钥。

【举例】

# 配置OSPF认证密钥。

host# configure terminal

host(config)# interface ge0

host(config-ge0)#ip ospf authentication-key aaa

【相关命令】

* show running-config interface

### ip ospf cost

**ip ospf cost**命令用来配置OSPF接口发送报文的开销。

**no ip ospf cost**命令用来删除OSPF接口发送报文的开销。

【命令】

**ip ospf cost** *cost*

**no ip ospf cost**

【视图】

接口视图

【参数】

*cost*：OSPF接口发送报文的开销，取值范围为1～65535。

【举例】

# 配置OSPF接口发送报文的开销。

host# configure terminal

host(config)# interface ge4

host(config-ge4)# ip ospf cost 3

【相关命令】

* show running-config interface

### ip ospf dead-interval

**ip ospf dead-interval**命令用来配置OSPF接口邻居失效定时器。

**no ip ospf dead-interval**命令用来删除OSPF接口邻居失效定时器。

【命令】

**ip ospf dead-interval** *interval*

**no ip ospf dead-interval**

【缺省情况】

缺省情况下，默认值为40秒。

【视图】

接口视图

【参数】

*interval*：接口邻居失效定时器，取值范围为1～65535秒，默认值为40。

【使用指导】

使用**no ip ospf dead-interval**可以删除该配置，将恢复到默认值40秒。

Dead-interval的值至少是Hello-interval值的4倍。

同一网段的路由器的Dead-interval必须相同。

【举例】

# 配置接口邻居失效定时器。

host# configure terminal

host(config)# interface ge4

host(config-ge4)# ip ospf dead-interval 32

【相关命令】

* show running-config interface

### ip ospf hello-interval

**ip ospf hello-interval**命令用来配置OSPF接口Hello报文定时器。

**no ip ospf hello-interval**命令用来删除OSPF接口Hello报文定时器。

【命令】

**ip ospf hello-interval** *interval*

**no ip ospf hello-interval**

【缺省情况】

缺省情况下，发送间隔为10秒。

【视图】

接口视图

【参数】

*interval*：Hello报文发送间隔时间，取值范围为1～65535，默认为10秒。

【使用指导】

使用**no ip ospf hello-interval**可以删除该配置，将恢复到默认值10秒。

同一网段的路由其Hello-interval必须相同。

【举例】

# 配置Hello报文发送间隔。

host# configure terminal

host(config)# interface ge0

host(config-ge0)# ip ospf hello-interval 8

【相关命令】

* show running-config interface

### ip ospf message-digest-key

**ip ospf message-digest-key**命令用来配置OSPF接口上用于密文认证的密钥。

**no ip ospf message-digest-key**命令用来删除OSPF接口上用于密文认证的密钥。

【命令】

**ip ospf message-digest-key** *key-id* **md5** *key*

**no ip ospf message-digest-key** *key-id*

【视图】

接口视图

【参数】

*key-id*：key的ID号，取值范围为1～255。

*key*：key字符串，可以为字母、数字、字符。

【举例】

# 配置OSPF认证密钥。

host# configure terminal

host(config)# interface ge4

host(config-ge4)#ip ospf message-digest-key 1 md5 aaaa!@#$51234

【相关命令】

* show running-config interface

### ip ospf network

**ip ospf network**命令用来配置接口的OSPF网络类型。

**no ip ospf f dead-interval**命令用来删除接口的OSPF网络类型。

【命令】

**ip ospf network** { **broadcast** | **point-to-point** }

**no ip ospf f dead-interval**

【视图】

接口视图

【参数】

**broadcast**：设置接口OSPF网络类型为广播型网络。

**point-to-point**：设置接口OSPF网络类型为点对点型网络。

【举例】

# 配置接口OSPF网络类型。

host# configure terminal

host(config-router)# inter ge4

host(config-ge4)#ip ospf network broadcast

【相关命令】

* show running-config interface

### ip ospf priority

**ip ospf priority**命令用来配置OSPF接口的优先级。

**no ip ospf priority**命令用来删除OSPF接口的优先级。

【命令】

**ip ospf priority** *priority*

**no ip ospf priority**

【视图】

接口视图

【参数】

*priority*：接口的优先级，取值范围为0～255。

【举例】

# 配置OSPF接口优先级。

host# configure terminal

host(config)# interface ge4

host(config-ge4)#ip ospf priority 10

【相关命令】

* show running-config interface

### ip ospf retransmit-interval

**ip ospf retransmit-interval**命令用来配置OSPF接口LSA重传间隔。

**no ip ospf retransmit-interval**命令用来删除OSPF接口LSA重传间隔。

【命令】

**ip ospf retransmit-interval** *interval* **<3-65535>**

**no ip ospf retransmit-interval**

【缺省情况】

缺省情况下，重传间隔为5秒。

【视图】

接口视图

【参数】

*interval*：LSA重传间隔时间，取值范围为3～65535秒。默认为5秒。

【使用指导】

使用**no ip ospf retransmit-interval**命令删除配置后，将恢复到默认值5秒。

【举例】

# 配置LSA重传间隔。

host# configure terminal

host(config)# interface ge4

host(config-ge4)# ip ospf retransmit-interval 3

【相关命令】

* show running-config interface

### ip ospf transmit-delay

**ip ospf transmit-delay**命令用来配置OSPF接口LSA发送延迟。

**no ip ospf transmit-delay**命令用来删除OSPF接口LSA发送延迟。

【命令】

**ip ospf transmit-delay** *delay***<1-65535>**

**no ip ospf transmit-delay**

【缺省情况】

缺省情况下，默认值为1秒。

【视图】

接口视图

【参数】

*delay*：LSA发送延迟，取值范围为1～65535，默认值为1秒。

【使用指导】

使用**no ip ospf transmit-delay**命令可以删除该配置，将恢复到默认值1秒。

【举例】

# 配置LSA发送延迟。

host# configure terminal

host(config)# interface ge0

host(config-ge0)# ip ospf transmit-delay 2

【相关命令】

* show running-config interface

### network

**network**命令用来配置OSPF的接口及其所属的区域。

**no network**命令用来删除OSPF的接口及其所属的区域。

【命令】

**network** *ip-address*/*prefix* **area** { *ip-address* | *router-id* }

**no network** *ip-address*/*prefix* **area** { *ip-address* | *router-id* }

【视图】

OSPF配置视图

【参数】

*ip-address*/*prefix*：OSPF接口所属的网段。

*ip-address*：OSPF所属的区域ID，为点分十进制形式。

*router-id*：OSPF所属的区域ID，数字形式，取值范围为0～4294967295。

【使用指导】

声明网段后，在从属于*ip-address*/*prefix*网段的接口上启用OSPF。

【举例】

# 配置OSPF接口及所属区域。

host# configure terminal

host(config)# router ospf

host(config-router)# network 10.0.1.0/24 area 0

【相关命令】

* show running-config ospf

### redistribute

**redistribute**命令用来配置OSPF路由重发布。

**no redistribute**命令用来删除OSPF路由重发布。

【命令】

**redistribute** { **connected** | **static** | **rip** } **metric** *metric* **metric-type** { **1** | **2** }

**no redistribute** { **connected** | **static** | **rip** }

【缺省情况】

缺省情况下，重发布的路由为第二类外部路由，即metric-type默认为2。

【视图】

OSPF配置视图

【参数】

**connected**：重发布路由类型为直连路由。

**static：**重发布路由类型为静态路由。

**rip：**重发布路由类型为rip路由。

*metric*：重发布路由的metric，取值范围为1～16777214。

**1：**重发布路由的类型为第一类外部路由。

**2：**重发布路由的类型为第二类外部路由。

【举例】

# 配置OSPF路由重发布。

host# configure terminal

host(config)# router ospf

host(config-router)# redistribute connected metric 1 metric-type 2

【相关命令】

* show running-config ospf

### router-id

**router-id**命令用来配置OSPF路由器的Router-ID。

**no router-id**命令用来删除OSPF路由器的Router-ID。

【命令】

**router-id** *ip-address*

**no router-id**

【缺省情况】

缺省情况下，路由器先挑选IP地址最大的环回地址。若无环回地址，则选择状态up的接口地址大的作为本路由器的Router-ID。

【视图】

OSPF配置视图

【参数】

*ip-address*：OSPF的Router-ID，为点分十进制形式。

【使用指导】

**no router-id**可以删除Router-ID的设置，Router-ID将会重新自动选举，重启后生效。

OSPF协议需要路由器的Router-ID，作为本路由器在自治系统中的唯一标识。一般在协议任务启动 后，会自动选出一个Router-ID。通常路由器先挑选IP地址最大的环回地址。若无环回地址，则选择状态up的接口地址大的作为本路由器的Router-ID。也可以指定一个Router-ID。

【举例】

# 配置Router-ID。

host# configure terminal

host(config)# router ospf

host(config-router)# router-id 1.1.1.1

【相关命令】

* show running-config ospf

### router ospf

**router ospf**命令用来启用OSPF路由协议。

**no router ospf**命令用来关闭OSPF路由协议。

【命令】

**router ospf**

**no router ospf**

【缺省情况】

默认情况下，未启用OSPF路由协议。

【视图】

系统视图

【使用指导】

启用OSPF后，才可对OSPF作进一步的配置。

【举例】

# 启用OSPF。

host# configure terminal

host(config)# router ospf

【相关命令】

* show running-config ospf

### show ip ospf

**show ip ospf**命令用来查看OSPF信息及邻居信息。

【命令】

**show ip ospf**

【视图】

用户视图

【举例】

# 查看OSPF信息及邻居信息。

host# show ip ospf

OSPF Routing Process, Router ID: 1.1.1.1

Supports only single TOS (TOS0) routes

This implementation conforms to RFC2328

RFC1583Compatibility flag is disabled

OpaqueCapability flag is disabled

Initial SPF scheduling delay 20 millisec(s)

Minimum hold time between consecutive SPFs 100 millisec(s)

Maximum hold time between consecutive SPFs 30 millisec(s)

Hold time multiplier is currently 1

SPF algorithm last executed 4h09m59s ago

SPF timer is inactive

Refresh timer 10 secs

This router is an ASBR (injecting external routing information)

Number of external LSA 3. Checksum Sum 0x0001af66

Number of opaque AS LSA 0. Checksum Sum 0x00000000

Number of areas attached to this router: 1

Reference bandwidth unit is 100 mbps

Area ID: 0.0.0.0 (Backbone)

Number of interfaces in this area: Total: 0, Active: 0

Number of fully adjacent neighbors in this area: 0

Area has no authentication

SPF algorithm executed 1 times

Number of LSA 1

Number of router LSA 1. Checksum Sum 0x00002928

Number of network LSA 0. Checksum Sum 0x00000000

Number of summary LSA 0. Checksum Sum 0x00000000

Number of ASBR summary LSA 0. Checksum Sum 0x00000000

Number of NSSA LSA 0. Checksum Sum 0x00000000

Number of opaque link LSA 0. Checksum Sum 0x00000000

Number of opaque area LSA 0. Checksum Sum 0x00000000

### show ip ospf database

**show ip ospf database**命令用来查看OSPF LSA数据库。

【命令】

**show ip ospf database**

【视图】

用户视图

【举例】

# 查看LSA数据库。

host# show ip ospf database

OSPF Router with ID (1.1.1.1)

Router Link States (Area 0.0.0.0)

Link ID ADV Router Age Seq# CkSum Link count

1.1.1.1 1.1.1.1 1279 0x80000009 0x2928 0

AS External Link States

Link ID ADV Router Age Seq# CkSum Route

0.0.0.0 1.1.1.1 1009 0x80000008 0x7f34 E2 0.0.0.0/0 [0x0]

172.16.0.0 1.1.1.1 1109 0x80000009 0x39cf E2 172.16.0.0/16 [0x0]

192.168.2.0 1.1.1.1 669 0x80000009 0xf663 E2 192.168.2.0/24 [0x0]

表 4-7 LSA数据库显示信息描述表

| 字段 | 描述 |
| --- | --- |
| Link ID | LSA的Link state ID |
| ADV Router | 发送LSA路由器的Route-ID |
| Age | LSA的老化时间 |
| Seg | LSA的序列号 |
| CkSum | LSA的校验和 |
| Link count | LSA的连接数 |
| Route | 路由类型及外部路由的目的网段 |

### show ip ospf interface

**show ip ospf interface**命令用来查看OSPF接口信息。

【命令】

**show ip ospf interface** *if-name*

【视图】

用户视图

【参数】

*if-name*：接口名称。

【举例】

# 查看接口ge0的OSPF信息。

host# show ip ospf interface ge0

ge0 is up, line protocol is up

Internet Address 100.0.1.2/24,Area 0.0.0.0

Router ID 200.0.0.1, Network Type BROADCAST, Cost: 10

Transmit Delay is 1 sec, State DR, Priority 1

Designated Router (ID) 200.0.0.1,Interface Address 100.0.1.2

Backup Designated Router (ID) 200.0.0.2,Interface Address 100.0.1.1

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5

Hello due in 00:00:05

表 4-8 show ip ospf interface显示信息描述表

| 字段 | 描述 |
| --- | --- |
| Internet Address | 接口地址 |
| Area | 所属区域 |
| Router ID | router id |
| Network Type | 网络类型 |
| Cost | 开销值 |
| Transmit Delay | 传输延时时间 |
| State | DR状态 |
| Priority | DR选举优先级 |
| Designated Router | DR的ID和地址 |
| Backup Designated Router | BDR的ID和版本 |
| Timer intervals configured | OSPF定时器配置 |
| Hello due | 上个Hello距现在的时间 |

### timers spf

**timers spf**命令用来配置OSPF接收拓扑结构改变之后和启动最短路径优先（OSPF）之间的延迟时间和配置连续两次SPF计算之间的时间。

**no timers spf**命令用来删除OSPF路由计算定时器的配置。

【命令】

**timers throttle spf** *spf-delay* *spf-holdtime max-holdtime*

**no timers throttle spf**

【缺省情况】

缺省情况下，默认值spf-delay为5秒，spf-holdtime为10秒。

【视图】

OSPF配置视图

【参数】

*spf-delay*：spf延时时间，取值范围为0～600000秒，默认值为5秒。

*spf-holdtime*：spf连续两次计算间隔时间，取值范围为0～600000秒，默认值为10秒。

*max*-holdtime：最大间隔时间，取值范围为0～600000秒。

【使用指导】

使用**no timers spf**可以取消该配置，使其恢复到默认值spf-delay为5秒，spf-holdtime为10秒。

【举例】

# 配置spf算法定时器。

host# configure terminal

host(config)# router ospf

host(config-router)# timers throttle spf 20 10 30

【相关命令】

* show running-config ospf

# VRF

## VRF配置命令

### ip vrf

**ip vrf**命令用来添加一条VRF。

**no ip vrf**命令用来删除已经创建的VRF。

【命令】

**ip vrf** *name*

**no ip vrf** *name*

【缺省情况】

缺省情况下，不启用VRF。

【视图】

系统视图

【参数】

*name*：VRF的名字，不超过31个字符，不允许输入%!"#$&`\*+,/:;<=>?\^'{}!字符。

【使用指导】

设备能够创建的VRF数目由平台规格决定。

【举例】

# 创建一个名为test的VRF。

host# configure terminal

host(config)# ip vrf test

【相关命令】

* show ip vrf

### ip vrf forwarding

**ip vrf forwarding**命令用来把接口加入VRF。

**no ip vrf forwarding**命令用来从VRF删除接口。

【命令】

**ip vrf forwarding** *name*

**no ip vrf forwarding**

【缺省情况】

缺省情况下，接口不会加入VRF。

【视图】

接口视图

【参数】

*name*：接口要加入的VRF的名字，不超过31个字符，不允许输入%!"#$&`\*+,/:;<=>?\^'{}!字符。

【使用指导】

接口要从一个VRF下转移到另一个VRF，可以直接在接口下执行ip vrf forwarding命令。

接口加入或离开VRF，接口的IP配置会被删除。

【举例】

# 将接口ge0加入到VRF test中。

host# configure terminal

host(config)# interface ge0

host(config-ge0)#ip vrf forwarding test

### ip route vrf

**ip route vrf**命令用来添加一条VRF路由。

**no ip route vrf** 命令用来删除已经创建的VRF路由。

【命令】

**ip route vrf** *name**ip-address* { *interface* | *nexthop* }

**no ip route vrf** *name ip-address* { *interface* | *nexthop* }

【缺省情况】

缺省情况下，不启用VRF。

【视图】

系统视图

【参数】

*name*：VRF的名字。

*ip-address*：目的网段。

*interface*：出接口。

*nexthop*：下一跳地址。

【举例】

# 创建一个名为test的vrf，并且创建一条静态路由。

host#configure terminal

host(config)# ip vrf test

host(config)# ip route vrf test 0.0.0.0/0 10.1.1.1

【相关命令】

* show ip route vrf *name*

### show ip route vrf

**show ip route vrf** 命令用来查看VRF路由。

【命令】

**show ip route vrf** *name*

【视图】

用户视图

【参数】

*name*：已经创建的VRF的名字。

【举例】

# 显示VRF test的路由信息。

Codes: C - connected, S - static, R - RIP, O - OSPF,

P - PPPOE route, D - DHCP route, I - ISP route,

L - LLB route, > - selected route, \* - FIB route

S>\* 10.0.0.0/24 [1/0] via 192.168.1.1 weight 1, ge0

S 20.0.0.0/24 [1/0] via 30.0.0.1 weight 1 inactive

S>\* 30.0.0.0/24 [1/0] is directly connected, ge0

C>\* 192.168.1.0/24 is directly connected, ge0

表 5-1 show ip route vrf命令显示信息描述表

| 字段 | 描述 | |
| --- | --- | --- |
| Codes | 路由类型和状态标示 | |
| C | 直连路由 |
| S | 静态路由 |
| R | RIP路由 |
| O | OSPF路由 |
| P | PPPOE路由 |
| D | DHCP路由 |
| I | ISP路由 |
| > | 路由已经被优选 |
| \* | 路由已经加入FIB表 |
| X.X.X.X/X | 目的网段 | |
| [X/Y] | X表示距离矢量，Y表示路由的度量 | |
| via | 下一条地址 | |
| is directly connected | 路由制定了出接口 | |
| weight | 下一跳的权重值 | |
| inactive | 路由没有激活 | |
| interface | 路由出接口 | |

### show ip vrf

**show ip vrf**命令用来查看所有或者指定的VRF信息。

【命令】

**show ip vrf** [ *name* ]

【视图】

用户视图

【参数】

*name*：VRF的名字。

【举例】

# 显示VRF test的详细信息。

host# show ip vrf test

Name ID Interfaces

test 1 ge0

表 5-2 show ip vrf命令显示信息描述表

| 字段 | 描述 |
| --- | --- |
| Name | VRF的名称 |
| ID | VRF的内部ID号 |
| Interfaces | VRF中包含的接口 |

# NAT

## NAT地址池配置命令

### ip nat pool

**ip nat pool** 命令用来创建地址池，并进入地址池视图，如果创建的地址池已经存在，则进入地址池视图。

**no ip nat pool** 命令用来删除已创建的地址池。

【命令】

**ip nat pool** *pool-name*

**no ip nat pool** *pool-name*

【视图】

系统视图

【参数】

*pool-name*：地址池名称。

【举例】

# 创建名为abc的地址池。

host# configure termina

host(config)# ip nat pool abc

### ip address

**ip address** 命令用来向地址池中添加地址。

**no ip address** 命令用来删除地址池中的地址。

【命令】

**ip address***start-ip end-ip*

**no address** *start-ip end-ip*

【缺省情况】

缺省情况下，地址池为空。

【视图】

地址池节点视图

【参数】

*start-ip*：开始IP地址。

*end-ip*：结束IP地址。

【使用指导】

地址池中地址个数不能超过256个。

【举例】

# 向名为abc的地址池添加地址范围 1.1.1.1 到1.1.1.5。

host# configure termina

host(config)# ip nat pool abc

host(ip-nat-pool)# ip address 1.1.1.1 1.1.1.5

## 源NAT配置命令

### ip nat source

**ip nat source** 命令用来配置源NAT规则。

**no ip nat source** 命令用来删除源NAT规则。

【命令】

**ip nat source** *interface-name* { *source-address |* **any**} { *destination-address |* **any** } *service* { **pool** *|* **interface** *|* **no\_trans**} [ **log** ] [ *id* ]

**no ip nat source** *id*

【视图】

系统视图

【参数】

*interface-name*：接口名称。

*source-address*：源地址对象或地址组对象名称。

*destination- address*：目的地址对象或地址组对象名称。

**any**：任意地址或地址组对象。

*service*：源NAT匹配的服务，可以引用服务或者服务组对象名称。

**pool**：地址转换类型，转换成NAT地址池的地址。

**interface**：地址转换类型 ，转换后的地址为出接口地址。

**no\_trans**：地址转换类型，不进行转换。

**log**：是否产生日志，1为产生，0为不产生。

*id*：规则id，转换规则的唯一标识。

【使用指导】

源NAT是一种单向的针对源地址的映射，主要用于内网访问外网，减少公有地址的数目，隐藏内部地址。

【举例】

# 在ge0口上创建一条源NAT规则，转后的地址为地址池abc中的地址。

host# configure termina

host(config)# ip nat pool abc

host(ip-nat-pool)# ip address 192.168.1.1 192.168.1.5

host(ip-nat-pool)# exit

host(config)# ip nat source ge0 any any any abc

## 目的NAT配置命令

### ip nat destination

**ip nat destination**命令用来配置目的NAT规则。

**no ip nat destination** 命令用来删除目的NAT规则。

【命令】

**ip nat destination** *interface-name* { *source-address |* **any**} { *destination-address |* **any** } *service-name* { **pool** *|* **no\_trans**} [ **service** *service-id* ] [ **log** ] [ *id* ]

**no ip nat destination** *id*

【视图】

系统视图

【参数】

*interface-name*：接口名称。

*source-address*：源地址对象或地址组对象名称。

*destination- address*：目的地址对象或地址组对象名称。

**any**：任意地址或地址组对象。

*service-name*：源NAT匹配的服务，可以引用服务或者服务组对象名称。

**pool**：地址转换类型，转换成NAT地址池的地址。

**interface**：地址转换类型 ，转换后的地址为出接口地址。

**no\_trans**：地址转换类型，不进行转换。

*service-id*： 转换后的端口。

**log**：是否产生日志，1为产生，0为不产生。

*id*：规则id，转换规则的唯一标识。

【举例】

# 在ge0口上创建一条源NAT规则，转后的地址为地址池abc中的地址。

host# configure termina

host(config)# ip nat pool abc

host(ip-nat-pool)# ip address 192.168.1.1 192.168.1.5

host(ip-nat-pool)# exit

host(config)# ip nat destination ge0 any any any abc

## 静态NAT配置命令

### ip nat static

**ip nat static**命令用来配置静态NAT规则。

**no ip nat static** 命令用来删除静态NAT规则。

【命令】

**ip nat static** *interface-name local-address global-addr*ess [ *id* ]

**no ip nat static** *id*

【视图】

系统视图

【参数】

*interface-name*：接口名称。

*local-address*：内网地址。

*global- address*：外网地址。

*id*：规则id，转换规则的唯一标识。

【举例】

# 在ge0口上创建一条内网地址192.68.1.1到外网地址1.1.1.1的转换规则。

host# configure termina

host(config)# ip nat static ge0 192.168.1.1 1.1.1.1

## NAT规则移动配置命令

### ip nat { static | source | destination } move

ip nat { static | source | destination } move命令用来移动配置的NAT规则。

【命令】

ip nat { static | source | destination } move *id* { before | after } *ref-id*

【视图】

系统视图

【参数】

static：静态NAT规则。

source：源NAT规则。

destination：目的NAT规则。

before：参考规则之前。

after：参考规则之后。

*id*：规则id，转换规则的唯一标识。

*ref-id*：参考规则id。

【举例】

# 将源id为1的源NAT移到id为2的源NAT规则之后。

host# configure termina

host(config)# ip nat source move 1 after 2

# DNS命令

## DNS命令

### clear dns cache

**clear dns cache**命令用来清除DNS的动态缓存条目。

【命令】

**clear dns cache**

【视图】

用户视图

【使用指导】

在需要手动清除动态缓存时，使用该命令。

该命令会在DNS服务器配置被更改时，自动被调用。

【举例】

# 清除缓存的动态域名。

host# clear dns cache

### dns

**dns enable**命令用来开启DNS功能。

**dns disable**命令用来关闭DNS功能。

【命令】

**dns enable**

**dns disable**

【缺省情况】

缺省情况下，未开启DNS功能。

【视图】

系统视图

【使用指导】

设备的内网用户通过设备解析域名时，或者设备其它模块需要域名解析时，需要开启该功能。

【举例】

# 配置开启DNS。

host# configure terminal

host(config)# dns enable

【相关命令】

* show running-config dns

### dns host-name

**dns host-name**命令用来添加静态域名。

**no dns server**命令用来删除静态域名。

【命令】

**dns host-name** *domain ip-address*&<1-2>

**no dns server** *domain*

【缺省情况】

缺省情况下，未配置任何静态域名。

【视图】

系统视图

【参数】

*domain*：域名信息。可输入数字、字母、“-”、“.”，每级域名长度不超过63个字符，最后一级域名不少于2个字符，不多于6个字符。总共最多可输入255个字符。

*ip-address*：域名对应的IP地址。可以配置1到2个，至少1个。IP地址不可重复。

【使用指导】

设备内网用户访问某些特定IP地址，或限定设备内网用户访问某些特定域名，可以通过该命令实现。

【举例】

# 配置一条静态域名。

host# configure terminal

host(config)# dns host-name www.gateway.com 192.168.1.1

【相关命令】

* show dns cache

### dns server

**dns server**命令用来配置DNS服务器地址。

**no dns server**命令用来删除DNS服务器地址。

【命令】

**dns server** *ip-address*&<1-4>

**no dns server**

【缺省情况】

缺省情况下，未配置DNS服务器。

【视图】

系统视图

【参数】

*ip-address*：DNS服务器地址。可以配置1到4个，IP地址不可重复。

【使用指导】

设备的内网用户通过设备解析域名时，或者设备其它模块需要域名解析时，如果DNS缓存中没有该条目，需要配置DNS服务器，由DNS向该服务器请求DNS解析。

最多可配置4个DNS服务器，且每个DNS服务器地址不可重复。

DNS服务器配置更改时，将自动清除DNS动态缓存记录。

【举例】

# 配置DNS服务器。

host# configure terminal

host(config)# dns server 8.8.8.8 8.8.4.4

【相关命令】

* show running-config dns
* show dns server

### show dns cache

**show dns cache**命令用来显示DNS所有的缓存信息。

【命令】

**show dns cache**

【视图】

用户视图

【举例】

# 显示缓存的域名。

host# show dns cache

Host Name TTL(s) Type IP address

----------------------------------------------------------------------------------------

www.gateway.com 0 Static 192.168.1.1

----------------------------------------------------------------------------------------

Total:1

表 7-1 域名缓存显示信息描述表

| 字段 | 描述 |
| --- | --- |
| Host Name | 域名信息 |
| TTL | 域名存在时间，单位为秒 |
| Type | 缓存类型，手动添加的为Static，动态获取的为Dynamic |
| IP address | 域名对应的IP地址 |
| Static | 域名类型为静态域名 |
| Dynamic | 域名类型为动态域名 |
| Total | 缓存条目总数 |

### show dns cache statistics

**show dns cache statistics**命令用来显示缓存的统计信息。

【命令】

**show dns cache statistics**

【视图】

用户视图

【举例】

# 显示缓存的统计信息。

host# show dns cache statistics

DNS cache statistics:

Total:1

Static:1

Dynamic:0

表 7-2 名缓存统计显示信息描述表

| 字段 | 描述 |
| --- | --- |
| Total | 域名缓存条目总数 |
| Static | 静态域名缓存条目总数 |
| Dynamic | 动态域名缓存条目总数 |

### show running-config dns

**show running-config dns**命令用来查看DNS的相关配置信息。

【命令】

**show running-config dns**

【视图】

用户视图

【举例】

# 显示DNS的配置信息。

host# show running-config dns

dns enable

dns server 8.8.8.8

dns host-name www.gateway.com 192.168.1.1

!

# 无线3G命令

## 无线3G命令

### access-type

**access-type**命令用来选择3G的接入方式。

【命令】

**access-type** { **apn** | **vpdn** }

【缺省情况】

缺省情况下，3G的接入方式为apn方式。

【视图】

cell3g0视图

【参数】

**apn：**接入点方式。

**vpdn：**虚拟专线方式。

【使用指导】

通常普通的上网使用**apn**方式；当需要私网时采用**vpdn**方式。如无特殊需求，建议使用**apn**方式。

**apn**方式无需额外配置拨号串、用户名、密码；**vpdn**需要配置专有的拨号串、用户名、密码。

【举例】

# 配置为apn接入方式。

host# configure terminal

host(config)# interface cell3g0

host(config-cell3g0)# access-type apn

【相关命令】

* **dialer string** dial-string
* **auth username** name
* **auth password** password
* **show running-config interface**

### auth password

**auth password**命令用来配置vpdn接入方式时认证使用的密码。

【命令】

**auth password** *password*

【视图】

cell3g0视图

【参数】

*password*：使用vpdn接入方式时，3G所使用的认证密码。可输入字母、数字、符号，最多可输入31个字符。

【使用指导】

当3G使用vpdn接入方式时，需要配置该密码。

【举例】

# 配置vpdn接入时的用户名。

host# configure terminal

host(config)# interface cell3g0

host(config-cell3g0)#access-type vpdn

host(config-cell3g0)#dialer password abc123~@#

【相关命令】

* access-type vpdn
* show running-config interface

### auth username

**auth username**命令用来配置vpdn接入方式时认证使用的用户名。

【命令】

**auth username** *name*

【视图】

cell3g0视图

【参数】

*name*：使用vpdn接入方式时，3G所使用的认证用户名。为1～31个字符的字符串，且不能包含“%!"#$&`\*+,/:;<=>?\^'{}!”。

【使用指导】

当3G使用vpdn接入方式时，需要配置该用户名。

【举例】

# 配置vpdn接入时的用户名。

host# configure terminal

host(config)# interface cell3g0

host(config-cell3g0)#access-type vpdn

host(config-cell3g0)#dialer username abc123

【相关命令】

* access-type vpdn
* show running-config interface

demand idle-disconnect time

**demand idle-disconnect time**命令用来配置按需拨号的断线时间间隔。

【命令】

**demand idle-disconnect time** *time*

【缺省情况】

缺省情况下，按需拨号断开连接的时间间隔为10分钟。

【视图】

cell3g0视图

【参数】

*time*：按需拨号成功后，在该段时间内没有流量，则自动断开连接。取值范围为5～1800秒，默认为10分钟。

【使用指导】

本命令配合按需在线方式使用。

【举例】

# 配置按需在线的断开时间。

host# configure terminal

host(config)# interface cell3g0

host(config-cell3g0)#demand idle-disconnect time 300

【相关命令】

* dialer mode demand
* show running-config interface

### dialer mode

**dialer mode**命令用来配置3G上网的在线方式。

【命令】

**dialer mode** { **always-online** | **demand** }

【缺省情况】

缺省情况下，3G的在线方式为**demand**。

【视图】

cell3g0视图

【参数】

**always-online**：常在线上网方式。

**demand**：按需拨号上网方式。

【使用指导】

设备通过3G上网需要设备上有3G上网卡。

**always-online**在线方式是3G卡拨号成功后保持一直在线的状态，不断开连接；**demand**在线方式是根据设备上是否有流量产生进行拨号上网，当一定时间内没有流量后，3G卡自动断开连接。建议采用**demand**的在线方式。

【举例】

# 配置为按需拨号的在线方式。

host# configure terminal

host(config)# interface cell3g0

host(config-cell3g0)#dialer mode demand

【相关命令】

* demand idle-disconnect time *time*
* show running-config interface

### dialer string

**dialer string**命令用来配置vpdn接入方式时的拨号串。

【命令】

**dialer string** *dial-string*

【视图】

cell3g0视图

【参数】

*dial-string*：使用vpdn接入方式时，3G所使用的拨号串。可输入字母、数字、符号，最多可输入31个字符。

【使用指导】

当3G使用vpdn接入方式时，需要配置该拨号串。

【举例】

# 配置vpdn接入时的拨号串。

host# configure terminal

host(config)# interface cell3g0

host(config-cell3g0)#access-type vpdn

host(config-cell3g0)#dialer string ss1!~@

【相关命令】

* access-type vpdn
* show running-config interface

### show interface cell3g0

**show interface cell3g0**命令用来显示3G的信息。

【命令】

**show interface cell3g0**

【视图】

用户视图

【举例】

# 插上3G卡之后，显示3G信息。

host# show interface cell3g0

----------------------------------------------------------------------

interface cell3g0

description:

Admin UP Link UP

kernel ID: 272

MTU: 1500

modem info:

Modem state : In place

Equipment type : E261

Manufacturers : Huawei

Equipment serial number : 861586005822354

Hardware version : V3.1

Software version : 11.126.16.10.112

Transmission ability : +CGSM,+DS,+ES

uim info:

UIM card status : In place

ISMI information : 460015462747415

network info:

Cellular network state : LINK DOWN

Access network : CHINA\_UNICOM

Signal strength : 2

# 地址探测

## 地址探测配置命令

### show track

**show track**命令用来显示配置的地址探测。

【命令】

**show track [track-name]**

【视图】

用户视图

【举例】

# 显示配置的所有地址探测。

host # show track

Name Target Out device Type Interval Retry Used Status

1 www.baidu.com any ping 4 4 No Success

2 www.baidu.com any ping 10 4 No Success

3 2.2.2.2 any ping 1 1 No Failed

123 1.1.1.100 any ping 10 4 No Failed

表 9-1 show track显示信息描述表

| 字段 | 描述 |
| --- | --- |
| Name | 地址探测名称 |
| Target | 地址探测的目标 |
| Out device | 地址探测报文的发送接口 |
| Type | 探测类型 |
| Interval | 探测报文间隔时间 |
| Retry | 探测报文在超时前的重试次数 |
| Used | 地址探测是否被其他模块使用 |
| Yes | 地址探测被其他模块使用，无法删除 |
| No | 地址探测没有被其他模块使用，可以删除 |
| Status | 地址探测的状态 |
| Tracking | 地址探测正在探测，还没有探测结果返回 |
| Success | 地址探测成功 |
| Failed | 地址探测失败 |

# 显示一条地址探测。

host (config)# show track 123

Name: 123

Status: Failed

Target: 1.1.1.100

Out device: any

Type: ping Interval:10

Retry: 4 Used:No

表 9-2 show track [ *track-name* ]显示信息描述表

| 字段 | 描述 |
| --- | --- |
| Name | 地址探测名称 |
| Target | 地址探测的目标 |
| Out device | 地址探测报文的发送接口 |
| Type | 探测类型 |
| Interval | 探测报文间隔时间 |
| Retry | 探测报文在超时前的重试次数 |
| Used | 地址探测是否被其他模块使用 |
| Yes | 地址探测被其他模块使用，无法删除 |
| No | 地址探测没有被其他模块使用，可以删除 |
| Status | 地址探测的状态 |
| Tracking | 地址探测正在探测，还没有探测结果返回 |
| Success | 地址探测成功 |
| Failed | 地址探测失败 |

### track（系统视图）

**track**命令用来配置地址探测。

**no track**命令用来删除地址探测。

【命令】

**track** *track-name* **ping {** *domain-name* **|** *ip-address***} { any |** *interface-name***}** *interval**retry*

**track** *track-name* **tcp {** *domain-name* **|** *ip-address***}** *port* **{ any |** *interface-name***}** *interval**retry*

**track** *track-name* **dns** *domain-name* **{ any |** *interface-name***}** *interval**retry*

**no track** *track-name*

【缺省情况】

缺省情况下，未配置地址探测。

【视图】

**track**视图

【参数】

*track-name*：地址探测的名称，取值最大31个字符，且不能包含“%!"#$&`\*+,/:;<=>?\^'{}!”。

**ping**：配置使用PING协议的地址探测。

**tcp**：配置使用TCP协议的地址探测。

**dns**：配置使用DNS查询方式的地址探测。

*domain-name*：探测目标的域名，取值最大255个字符，只能使用英文字符，数字和“\_.”。域名使用“.”分割，每个部分的长度不能大于63，且不能使用\_开头，最后一个部分的长度是2到6。

*ip-address*：探测目标的IP地址，地址不能不能是0.0.0.0，255.255.255.255，127.0.0.0，169.254.0.0-169.254.255.254，224.0.0.0-239.255.255.255。

*port*：TCP探测的端口号。

**any**：探测可以使用任何接口作为出接口。

*interface-name*：探测只能使用指定接口作为出接口。

*interval*：探测报文的间隔时间，范围是1到600。

*retry*：在探测失败前，探测报文可以重试发送的次数，范围是1到10。

【使用指导】

需要注意的是：

地址探测配置后，会每间隔interval秒向探测报文发送探测，当在interval \* retry的时间内没有收到合法的探测报文，探测失败。

已经被配置为地址探测出接口的接口不能配置和地址探测联动。

子接口已经被配置为地址探测出接口的接口不能配置和地址探测联动。

已经配置了和地址探测联动的接口不能作为地址探测的出接口。

已经配置了和地址探测联动的接口的子接口不能作为地址探测出接口。【举例】

# 配置ping类型探测192.168.1.1的地址探测。

host# track gw ping 192.168.1.1 any 10 4

## 地址探测组配置命令

### description

**description**命令用来添加地址探测组描述。

**no description**命令用来删除地址探测组描述。

【命令】

**description** *desc*

**no description**

【缺省情况】

缺省情况下，地址探测组没有描述。

【视图】

地址探测组视图

【参数】

*desc*：地址探测组的描述，最大长度为127，且不能包含“%!"#$&`\*+,/:;<=>?\^'{}!”。。

【举例】

# 配置地址探测组的描述为internet。

host# configure terminal

host (config)# track-group g1

host (config-track-group)# description internet

### member

**member**用来添加地址地址探测组的组成员。

**no member**用来删除地址探测组的组成员。

【命令】

**member** *track-name*

**no member**

【缺省情况】

缺省情况下，地址探测组没有组成员。

【视图】

地址探测组视图

【参数】

*track-name*：地址探测的名称，取值最大31个字符，且不能包含“%!"#$&`\*+,/:;<=>?\^'{}!”。

【使用指导】

一个地址探测组内最多智能配置10个地址探测组成员。

当地址探测组内没有成员时，探测组的状态表示功状态。

【举例】

# 向地址探测组内加入一个成员。

host# configure terminal

host (config)# track-group g1

host (config-track-group)# member m1

### mode strict

**mode strict**命令用来配置地址探测组为严格模式。

**no mode strict**命令用来配置地址探测组为非严格模式。

【命令】

**mode strict**

**no mode strict**

【视图】

地址探测组视图

【使用指导】

需要注意的是：

当地址探测组为严格模式时，只要地址探测组成员中有一个是失败状态，地址探测组的状态也变成败状态。

当地址探测组为非严格模式时，只要地址探测组成员中有一个是成功状态，地址探测组的状态也成为成功状态。

无论是严格模式还是非严格模式，当地址探测组没有成员时，状态为成功状态。

【举例】

# 进入将地址探测组配置为严格模式。

host# configure terminal

host (config)# track-group g1

host (config-track-group)# mode strict

### show track-group

**show track-group** 命令用来显示地址探测组。

【命令】

**show track-group** [ *group-name* ]

【视图】

用户视图

【参数】

*group-name*：地址探测组的名称，取值最大31个字符，且不能包含“%!"#$&`\*+,/:;<=>?\^'{}!”。

【举例】

# 显示配置的所有地址探测组成员。

host # show track-group

Name: g1

Mode: non-strict Status: Success

Member:

1 www.baidu.com ping Success

2 www.baidu.com ping Success

123 1.1.1.100 ping Failed

Used: No

表 9-3 show track-group [ *group-name* ]显示信息描述表

| 字段 | 描述 |
| --- | --- |
| Name | 地址探测组名称 |
| Mode | 地址探测组模式 |
| non-strict | 非严格模式 |
| strict | 严格模式 |
| Status | 地址探测组的状态 |
| Failed | 地址探测组状态为失败 |
| Success | 地址探测组状态为成功 |
| Member | 地址探测组成员，下方显示成员的名称，目标，类型，状态 |
| Used | 地址探测是否被其他模块使用 |
| Yes | 地址探测被其他模块使用，无法删除 |
| No | 地址探测没有被其他模块使用，可以删除 |
| Status | 地址探测的状态 |

### track-group

**track-group**命令用来创建地址探测组并进入地址探测组模式。

**no track-group**命令用来删除地址探测组。

【命令】

**track-group** *group-name*

**no track-group** *group-name*

【缺省情况】

缺省情况下，未配置地址探测组。

【视图】

系统视图

【参数】

*group-name*：地址探测组的名称，取值最大31个字符，且不能包含“%!"#$&`\*+,/:;<=>?\^'{}!”。

【举例】

# 配置地址探测组并进入地址探测组模式。

host# configure terminal

host (config)# track-group g1

host (config-track-group)#

## 接口状态探测

### track（接口模式）

**track**命令配置地址探测和接口联动。

**no track**命令用来删除地址探测和接口联动。

【命令】

**track** *track-name*

**no track** *track-name*

【缺省情况】

缺省情况下，地址探测没有和接口联动。

【视图】

接口视图

【参数】

*track-name*：要和接口联动的地址探测或者地址探测组名称，取值最大31个字符，且不能包含“%!"#$&`\*+,/:;<=>?\^'{}!”。

【使用指导】

当地址探测失败后，和探测联动的接口会将接口关闭。地址探测恢复成功后，和探测联动的接口将恢复。

需要注意的是：

如果地址探测的出接口和此条地址探测联动，会造成探测失败后，接口因为已经关闭，探测报文永远无法发送出去的问题。所以禁止地址探测的出接口和此条地址探测联动。

已经被配置为地址探测出接口的接口不能配置和地址探测联动。

子接口已经被配置为地址探测出接口的接口不能配置和地址探测联动。

已经配置了和地址探测联动的接口不能作为地址探测的出接口。

已经配置了和地址探测联动的接口的子接口不能作为地址探测出接口。

【举例】

# 配置ge0和地址探测m1联动。

host# configure terminal

host(config)# interface ge0

host(config-ge0)# track m1

## 地址探测和HA联动

### track（HA视图）

**track**命令配置地址探测和HA联动。

**no track**命令用来删除地址探测和HA联动。

【命令】

**track** *track-name*

**no track** *track-name*

【视图】

HA配置视图

【参数】

*track-name*：要和HA联动的地址探测或者地址探测组名称，取值最大31个字符，且不能包含“%!"#$&`\*+,/:;<=>?\^'{}!”。

【使用指导】

当和HA联动的地址探测失败，表明网络中发生重大故障，需要启用备设备，主备设备会立刻切换。

需要注意的是，如果主设备和备设备的地址探测或者监控接口都发生故障，表明此时网络发生严重问题，此时主备切换也无法修复错误，所以主备不会发生切换。

【举例】

# 配置HA和地址探测m1联动。

host# configure terminal

host(config)# ha-config

host(ha-config)# track m1

# 安全策略

## 安全策略配置命令

### policy

policy命令用来配置安全策略。

no policy命令用来删除安全策略。

【命令】

policy *in-interface out-interface source-address dest-address service-name user-name application-name schedule-name* { audit| noaudit | deny } [ *id* ]

no policy *id*

【视图】

系统视图

【参数】

*in-interface*：安全策略匹配的源接口，设备上可用的接口如ge0，也可为any。

*out-interface*：安全策略匹配的目的接口，设备上可用的接口如ge0，也可为any。

*source-address*：安全策略匹配的源IP地址，可以引用某地址对象或者地址组，any表示源地址为任意地址。

*dest-address*：安全策略匹配的目的地址，可以引用某个地址对象或者地址组，any表示源地址为任意地址。

*service-name*：安全策略匹配的服务对象，可以引用服务对象或者服务组。

*user-name*：指定安全策略匹配的用户对象名称。

*application-name*：指定安全策略匹配的应用对象名称。

*schedule-name*：指定安全策略生效的时间对象名称。

*id*：安全策略的唯一标识。范围是1～65535，其中50001～65535是集中网关创建的策略。

audit：允许匹配的流量通过，并且审计匹配的流量。

noaudit：允许匹配的流量通过，对匹配的流量不进行审计。

deny：丢弃匹配的流量。

【使用指导】

出入接口、源目的ip地址、服务、应用、用户、时间等匹配条件除了any或者always外，需要配置具体的对象，才能被安全策略引用。

【举例】

# 创建一条服务是TCP，其余匹配条件为any，动作是免审计的安全策略。

host# configure termina

host(config)# policy any any any any TCP any any any always noaudit

## 安全策略修改命令

### application

**application**命令用来添加安全策略匹配的应用对象。

**no application**命令用来删除安全策略匹配的应用对象。

【命令】

**application** *name*

**no application** *name*

【视图】

策略配置节点视图

【参数】

*name*：应用对象或对象组名称。

【举例】

# 安全策略1添加abc应用对象。

host# configure termina

host(config)# policy 1

host(config-policy)# application abc

### dest-address

**dest-address**命令用来添加安全策略匹配的目的地址对象。

**no dest-address** 命令用来删除安全策略匹配的目的地址对象。

【命令】

**dest-address** *address-name*

**no dest-address** *address-name*

【视图】

策略配置节点视图

【参数】

*address-name*：目的地址对象或地址对象组名称。

【举例】

# 安全策略1添加目的地址对象abc。

host# configure termina

host(config)# address abc

host(config-address)# ip address 192.168.1.1

host(config)# policy 1

host(config-policy)# dest-address abc

### disable

**disable**命令用来去使能安全策略的状态，使其处于禁用模式。

【命令】

**disable**

【缺省情况】

缺省情况下，安全策略的状态为 enable。

【视图】

策略配置节点视图

【举例】

# 禁用安全策略1。

host# configure termina

host(config)#policy 1

host(config-policy)# disable

### enable

**enable**命令用来使能安全策略的状态，使其处于可用模式。

【命令】

**enable**

【缺省情况】

缺省情况下，安全策略的状态为 enable。

【视图】

策略配置节点视图

【举例】

# 使能策略1。

host# configure termina

host(config)#policy 1

host(config-policy)# enable

### in-interface

**in-interface**命令用来修改策略匹配的入接口。

【命令】

**in-interface** { *interface-name* | **any** }

【缺省情况】

无

【视图】

策略配置节点视图

【参数】

*interface-name*：安全策略匹配的入接口。

**any**：标识任意接口。

【举例】

# 修改策略1的入接口为ge0。

host# configure termina

host(config)# policy 1

host(config-policy)# in-interface ge0

### out-interface

**out-interface**命令用来修改策略匹配的出接口。

【命令】

**out-interface** { *interface-name* | **any** }

【视图】

策略配置节点视图

【参数】

*interface-name*：安全策略匹配的入接口。

**any**：标识任意接口。

【举例】

# 修改策略1的出接口为ge0。

host# configure termina

host(config)#policy 1

host(config-policy)# out-interface ge0

### schedule

**schedule**命令用来修改安全策略的生效时间。

【命令】

**schedule** *name*

【缺省情况】

缺省情况下，安全策略为永久生效。

【视图】

策略配置节点视图

【参数】

*name*：时间对象或对象组名称。

【举例】

# 修改安全策略1的生效时间，使其仅仅在9:00-18:00生效。

host# configure termina

host(config)# schedule-day worktime

host(config-schedule-day)# periodic start 9:00 end 18:00

host(config-schedule-day)# exit

host(config)# policy 1

host(config-policyt)# schedule worktime

### service

**service**命令用来添加安全策略匹配的服务类型对象。

**no service** 命令用来删除安全策略匹配的服务类型对象。

【命令】

**service** *service-name*

**no service** *service-name*

【视图】

策略配置节点视图

【参数】

*service -name*：服务类型对象或对象组名称。

【举例】

# 给安全策略1添加ICMP服务类型对象。

host# configure termina

host(config)#policy 1

host(config-policy)# service icmp

### source-address

**source-address**命令用来添加安全策略匹配的源地址对象。

**no source-address** 命令用来删除安全策略匹配的源地址对象。

【命令】

**source-address** *address-name*

**no source-address** *address-name*

【视图】

策略配置节点视图

【参数】

*address-name*：源地址对象或地址对象组名称。

【举例】

# 添加安全策略1的源地址对象abc。

host# configure termina

host(config)# address abc

host(config-address)# ip address 192.168.1.1

host(config)# policy 1

host(config-policy)# source-address abc

### timeout

**timeout** 命令用来修改安全策略的老化时间。

【命令】

**timeout** *time-range*

【缺省情况】

缺省情况下，按照各个协议设定的老化时间老化。

【视图】

策略配置节点视图

【参数】

*time-range*：匹配到该策略的流的老化时间（单位：秒），取值范围为0～1728000。

【举例】

# 修改安全策略1的老化时间为10s。

host# configure termina

host(config)# policy 1

host(config-policy)# timeout 10

### user

**user**命令用来添加安全策略匹配的用户对象。

**no user**命令用来删除安全策略匹配的用户对象。

【命令】

**user** *user-name*

**no user** *user-name*

【视图】

策略配置节点视图

【参数】

*user -name*：用户对象或对象组名称。

【举例】

# 给安全策略1添加abc用户对象。

host# configure termina

host(config)# policy 1

host(config-policy)# user abc

## 安全策略移动命令

### policy move

**policy move**命令用来将策略移到某条策略之后或者之前。

【命令】

**policy move** *id*{ **before** | **after** }*ref-id*

【视图】

系统视图

【参数】

*id*：被移动的安全策略的唯一标识。范围是1～65535，其中50001～65535是集中网关创建的策略。

**before**：将策略移到参考策略之前。

**after**：将策略移到参考策略之前。

*ref-id*：参考策略标识。范围是1～65535，其中50001～65535是集中网关创建的策略。

【举例】

# 将安全策略1移到安全策略2之后。

host# configure termina

host(config)# policy move 1 after 2

安全策略插入命令

policy insert

**policy insert**命令用来在某条策略之前插入一条新的策略。

【命令】

**policy insert***in-interface out-interface source-address dest-address service-name user-name application-name schedule-name* { **audit** | **noaudit** | **deny** } *id* **before** *ref-id*

【视图】

系统视图

【参数】

*in-interface*：安全策略匹配的源接口，设备上可用的接口如ge0，也可为any。

*out-interface*：安全策略的匹配的目的接口，设备上可用的接口如ge0，也可为any。

*source-address*：安全策略匹配的源IP地址，可以引用某地址对象或者地址组，any表示源地址为任意地址。

*dest-address*：安全策略匹配的目的地址，可以引用某个地址对象或者地址组，any表示源地址为任意地址。

*service-name*：安全策略匹配的服务对象，可以引用服务对象或者服务组。

*user-name*：指定安全策略匹配的用户对象名称。

*application-name*：指定安全策略匹配的应用对象名称。

*schedule-name*：指定安全策略生效的时间对象名称。

**audit**：允许匹配的流量通过，并且审计匹配的流量。

**noaudit**：允许匹配的流量通过，对匹配的流量不进行审计。

**deny**：丢弃匹配的流量。

*id*：安全策略的唯一标识。范围是1～65535，其中50001～65535是集中网关创建的策略。

*ref-id*：参考策略标识。范围是1～65535，其中50001～65535是集中网关创建的策略。

【使用指导】

出入接口、源目的ip地址、服务、应用、用户、时间等匹配条件除了any或者always外，需要配置具体的对象，才能被安全策略引用。

【举例】

# 在安全策略1之前插入一条新的ID为3的安全策略。

host# configure termina

host(config)# policy insert any any any any any any any alwalys deny 3 before 1

## 修改默认安全策略命令

### policy default-action

**policy default-action**命令用来修改安全策略的默认策略配置。

【命令】

**policy default-action** { **permit** | **deny** }

【缺省情况】

缺省情况下，默认策略的行为是允许。

【视图】

系统视图

【参数】

**permit**：允许匹配的流量通过。

**deny**：丢弃匹配的流量。

【举例】

# 修改默认策略的值为permit。

host# configure termina

host(config)# policy default-action permit

# 对象管理命令参考

## 地址对象命令

### address

**adresss**命令用来创建地址对象并进入相应的地址对象视图，如果指定的地址对象已经存在，则直接进入相应地址对象视图，不需要再创建地址对象。

**no address**命令用来删除已存在的地址对象。

【命令】

**address** *address-name*

**no address** *address-name*

【缺省情况】

缺省情况下，系统会创建any和private两个地址对象。

【视图】

系统视图

【参数】

*address-name*：对象的名称，取值最大31个字符，且不能包含“%!"#$&`\*+,/:;<=>?\^'{}!”。

【举例】

# 创建地址对象addr\_obj\_test。

host# configure terminal

host(config)# address addr\_obj\_test

【相关命令】

* show address

### address-group

**adresss-group**命令用来创建地址组对象并进入相应的地址组对象视图，如果指定的地址组对象已经存在，则直接进入相应地址组对象视图，不需要再创建地址组。

**no adresss-grou**命令用来删除已存在的地址组。

【命令】

**address-group** *group-name*

**no address-group** *group-name*

【视图】

系统视图

【参数】

*group-name*：地址组对象的名称

【举例】

# 创建名称为”addrgrp\_obj\_test”的地址对象组。

host# configure terminal

host(config)# address addr\_obj\_test

host(config)# address-group addrgrp\_obj\_test

【相关命令】

* show address-group

### exclude ip address

**exclude ip address**命令用来给已有的地址对象中添加单个排除地址。

**no exclude ip address**命令用来从已有的地址对象中删除单个排除地址。

【命令】

**exclude ip address** *ip-address*

**no exclude ip address** *ip-address*

【视图】

地址对象视图

【参数】

*ip-address*：需要在地址对象中排除的IP地址。

【举例】

# 地址对象”addr\_obj\_test”排除“192.168.1.100”的IP地址。

host# configure terminal

host(config)# address addr\_obj\_test

host(config-address)#excule ip address 192.168.1.100

【相关命令】

* show address

### excule ip range

**excule ip range** *ip-addr-min ip-addr-max*命令用来从地址对象中排除一个地址范围。

**no** **excule ip range** *ip-addr-min ip-addr-max*命令用来删除指定的排除地址范围。

【命令】

**excule** **ip subnet** *ip-addr-min ip-addr-max*

**no excule** **ip subnet** *p-addr-min ip-addr-max*

【视图】

地址对象视图

【参数】

*ip-addr-min*：起始IP地址。

*ip-addr-min*：结束IP地址。

【举例】

# 向地址对象”addr\_obj\_test”添加“192.168.30.1～192.168.30.100”的排除子网地址。

host# configure terminal

host(config)# address addr\_obj\_test

host(config-address)# exclude ip range 192.168.30.1 192.168.30.100

【相关命令】

* show address

### excule ip subnet

**excule** **ip subnet**命令用来给已有的地址对象中添加排除子网。

**excule** **no ip subnet**命令用来从已有的地址对象中删除排除子网。

【命令】

**excule** **ip subnet** *ip-address netmask-length*

**no excule** **ip subnet** *ip-address netmask-length*

【视图】

地址对象视图

【参数】

*ip-address*：IP地址。

*netmask-length*：子网掩码长度。

【举例】

# 向地址对象”addr\_obj\_test”添加“192.168.30.0/24”的排除子网地址。

host# configure terminal

host(config)# address addr\_obj\_test

host(config-address)# execule ip subnet 192.168.30.0/24

【相关命令】

* show address

### ip address

**ip address**命令用来在地址对象中添加一个地址。

**no ip address**命令用来从指定的地址对象中删除一个地址。

【命令】

**ip address** *ip-address*

**no ip address** *ip-address*

【视图】

地址对象视图

【参数】

*ip-address*：IP地址。

【举例】

# 给地址对象”addr\_obj\_test”添加“192.168.1.99”的IP地址。

host# configure terminal

host(config)# address addr\_obj\_test

host(config-address)# ip address 192.168.1.99

【相关命令】

* show address

### ip range

**ip range**命令用来向地址对象中添加一个地址范围。

**no ip range**命令用来从地址对象中删除一个地址范围。

【命令】

**ip range** *ip-addr-min ip-addr-max*

**no ip range** *ip-addr-min ip-addr-max*

【视图】

地址对象视图

【参数】

*ip-addr-min*：起始的IP地址。

*ip-addr-max*：结束的IP地址。

【举例】

# 向地址对象”addr\_obj\_test”添加“100.10.1.1～100.1.1.100”的地址范围。

host# configure terminal

host(config)# address addr\_obj\_test

host(config-address)# ip range 100.10.1.1 100.10.1.100

【相关命令】

* show address

### ip subnet

**ip subnet**命令用来给已有的地址对象中添加子网。

**no ip subnet**命令用来从已有的地址对象中删除子网。

【命令】

**ip subnet** *ip-address netmask-length*

**no ip subnet** *ip-address netmask-length*

【视图】

地址对象视图

【参数】

*ip-address*：IP地址。

*netmask-length*：子网掩码长度。

【举例】

# 向地址对象”addr\_obj\_test”添加“192.168.112.0/24”的子网地址。

host# configure terminal

host(config)# address addr\_obj\_test

host(config-address)# ip subnet 192.168.112.0/24

【相关命令】

* show address

### member

**member**命令用来向地址对象组中添加一个成员。

**no member**命令用来从地址对象组中删除一个指定的成员。

【命令】

**member** *addr-name*

**no member** *addr-name*

【视图】

地址组对象视图

【参数】

*addr-name*：地址对象或者是地址组对象的名称。

【使用指导】

地址组对象的成员即可以是一个地址对象，也可以是一个地址组对象。

【举例】

# 向刚创建的地址对象组”addrgrp\_obj\_test”添加名为“addr\_obj\_test”的地址对象。

host# configure terminal

host(config)# address-group addrgrp\_obj\_test

host(config-address-group)# member addr\_obj\_test

【相关命令】

* show address-group

### show address

**show address**命令显示设备的地址对象。

【命令】

**show address** [ *address-name* ]

【视图】

任意视图

【参数】

*address-name*：地址对象的名称。

【使用帮助】

如果没有指定*address-name*，**show address**命令显示所有的地址对象，如果指定*address-name*，**show address**命令会显示指定的地址对象。

【举例】

# 显示地址对象。

host# show address

Flags: e--Exclude

Name Ref Address

any 2 0.0.0.0/0

private 1 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16

addr\_obj\_test 0 192.168.1.1, 192.168.2.1-192.168.2.100, 192.168.3.1(e)

表 11-1 show address命令显示信息描述表

| 字段 | 描述 |
| --- | --- |
| Name | 地址对象的名称 |
| Ref | 被其它模块引用的次数 |
| Address | 包含的成员，有以下几种类型（带有e表示排除地址）：  A.B.C.D IP地址。  A.B.C.D/M 网络范围，包含主机号和网络号  A.B.C.D – A.B.C.D 网络地址的范围。 |

### show address-group

**show address-group**命令用来显示设备的地址对象。

【命令】

**show address-group** [ *address-group-name* ]

【视图】

任意视图

【参数】

*address-group-name*：地址组对象的名称。

【使用帮助】

如果没有指定*address-group-name*，**show address-group**命令显示所有的地址组，如果指定*address-group-name*，**show address-group**命令会显示指定的地址组。

【举例】

# 显示地址组对象。

host# show address-group

Flags: g--Group

Name Ref Members

addrgrp\_obj\_test 0 addr\_obj\_test, addr\_group(g)

addr\_group 1

表 11-2 show address-group命令显示信息描述表

| 字段 | 描述 |
| --- | --- |
| Name | 地址组的名称 |
| Ref | 被其它模块引用的次数 |
| Members | 地址组的成员，含有(g)标识的表示成员也是一个地址组对象 |

## 服务对象命令

### icmp type

**icmp type**命令用来向服务对象中添加一个ICMP条目。

**no icmp type**命令用来从服务对象中删除指定的ICMP条目。

【命令】

**icmp type** *icmp-type* **code** *code-min code-max*

**no icmp type** *icmp-type* **code** *code-min code-max*

【视图】

服务对象视图

【参数】

*icmp-type*：ICMP的type值，取值范围为0～255。

*code-min*：ICMP的code的起始值，取值范围为0～255。

*code-max*：ICMP的code的结束值，取值范围为0～255。

【举例】

# 向服务对象service\_obj\_test添加一个icmp条目。

host# configure terminal

host(config)#service service\_obj\_test

host(config-service)# icmp type 3 code 3 33

【相关命令】

* show service

### member

member命令用来向服务对象组中添加一个服务对象成员。

no member命令用来从服务对象组删除指定的服务对象成员。

【命令】

memberservice-name

no member serivce-name

【视图】

服务组对象视图

【参数】

*serivce-name*：服务对象或者是服务组的名称。

【使用指导】

被添加的服务对象可以是系统预定义的服务，也可以是用户自定义的服务。

【举例】

# 向服务对象组servicegrp\_obj\_test里添加服务对象service\_obj\_test

host(config)#config terminal

host(config)# service-group servicegrp\_obj\_test

host(config-service-group)# member service\_obj\_test

【相关命令】

* show service-group

### protocol

protocol命令用来向服务对象中添加一个IP协议类型。

no protocol命令用来从服务对象中删除如指定的IP协议类型。

【命令】

protocolprotocol-id

noprotocolprotocol-id

【视图】

服务对象视图

【参数】

*protocol-id*：IP协议号，取值范围为0～255。

【举例】

# 向服务对象service\_obj\_test添加IP协议号为233的其他协议。

host(config)#config terminal

host(config)#service service\_obj\_test

host(config-service)# protocol 233

【相关命令】

* show service

### service

**service**命令用来添加一个新的服务对象

**no service**命令用来删除一个已经存在的服务对象。

【命令】

**service** *serivce-name*

**no service** *serivce -name*

【视图】

系统视图

【参数】

*serivce-name*：对象的名称，取值最大31个字符，且不能包含“%!"#$&`\*+,/:;<=>?\^'{}!”

【举例】

# 添加名称为”service\_obj\_test”的服务对象。

host(config)#config terminal

host(config)#service service\_obj\_test

host(config)# service service\_obj\_test

【相关命令】

* show service

### service-group

service-group命令用来新建一个服务对象组。

no service-group命令用来删除指定的服务对象组。

【命令】

service-group group-name

no service-group group-name

【视图】

系统视图

【参数】

group-name：服务对象组的名称。

【举例】

# 创建名为servicegrp\_obj\_test的服务对象组。

host(config)#config terminal

host(config)# service-group servicegrp\_obj\_test

host(config-service-group)# show service-group

【相关命令】

* show service-group

### show service

**show service**命令用来删除显示设备中的服务。

【命令】

**show service** *service-name*

【视图】

任意视图

【使用帮助】

如果没有指定service-name，**show service**命令显示所有的服务对象，如果指定*serivce-name*，**show address**命令会显示指定的服务对象。

【举例】

# 显示所有的服务对象。

host# show service

Name Ref Service

any 1 Any

ah 0 PROTO(51)

aol 0 TCP(Dst: 5190-5194 Src: Any)

bgp 0 TCP(Dst: 179 Src: Any)

bootpc 0 UDP(Dst: 68 Src: Any)

bootps 0 UDP(Dst: 67 Src: Any)

daytime 0 TCP(Dst: 13 Src: Any), UDP(Dst: 13 Src: Any)

dhcp 0 UDP(Dst: 67-68 Src: Any)

dns 0 TCP(Dst: 53 Src: Any), UDP(Dst: 53 Src: Any)

discard 0 TCP(Dst: 9 Src: Any), UDP(Dst: 9 Src: Any)

esp 0 PROTO(50)

finger 0 TCP(Dst: 79 Src: Any)

ftp 0 TCP(Dst: 21 Src: Any)

gopher 0 TCP(Dst: 70 Src: Any)

gre 0 PROTO(47)

h323 0 TCP(Dst: 1720 Src: Any), TCP(Dst: 1503 Src: Any), UDP(Dst: 1719 Src: Any)

hostname 0 TCP(Dst: 101 Src: Any)

http 0 TCP(Dst: 80 Src: Any)

https 0 TCP(Dst: 443 Src: Any)

icmp 0 PROTO(1)

icmpv6 0 PROTO(58)

igmp 0 PROTO(2)

ike 0 UDP(Dst: 500 Src: Any), UDP(Dst: 4500 Src: Any)

imap 0 TCP(Dst: 143 Src: Any)

info\_address 0 ICMP(Type: 17 Code: 0)

info\_request 0 ICMP(Type: 15 Code: 0)

irc 0 TCP(Dst: 6660-6669 Src: Any)

int

host#

host# show service

Name Ref Service

any 1 Any

ah 0 PROTO(51)

aol 0 TCP(Dst: 5190-5194 Src: Any)

bgp 0 TCP(Dst: 179 Src: Any)

bootpc 0 UDP(Dst: 68 Src: Any)

bootps 0 UDP(Dst: 67 Src: Any)

daytime 0 TCP(Dst: 13 Src: Any), UDP(Dst: 13 Src: Any)

dhcp 0 UDP(Dst: 67-68 Src: Any)

dns 0 TCP(Dst: 53 Src: Any), UDP(Dst: 53 Src: Any)

discard 0 TCP(Dst: 9 Src: Any), UDP(Dst: 9 Src: Any)

esp 0 PROTO(50)

finger 0 TCP(Dst: 79 Src: Any)

ftp 0 TCP(Dst: 21 Src: Any)

gopher 0 TCP(Dst: 70 Src: Any)

gre 0 PROTO(47)

h323 0 TCP(Dst: 1720 Src: Any), TCP(Dst: 1503 Src: Any), UDP(Dst: 1719 Src: Any)

hostname 0 TCP(Dst: 101 Src: Any)

http 0 TCP(Dst: 80 Src: Any)

https 0 TCP(Dst: 443 Src: Any)

icmp 0 PROTO(1)

icmpv6 0 PROTO(58)

igmp 0 PROTO(2)

ike 0 UDP(Dst: 500 Src: Any), UDP(Dst: 4500 Src: Any)

imap 0 TCP(Dst: 143 Src: Any)

info\_address 0 ICMP(Type: 17 Code: 0)

info\_request 0 ICMP(Type: 15 Code: 0)

irc 0 TCP(Dst: 6660-6669 Src: Any)

internet-locator-service 0 TCP(Dst: 389 Src: Any)

l2tp 0 UDP(Dst: 1701 Src: Any)

ldap 0 TCP(Dst: 389 Src: Any)

msolap-ptp2 0 TCP(Dst: 2725 Src: Any)

ms-olap 0 TCP(Dst: 2393-2394 Src: Any)

ms-sql-s 0 TCP(Dst: 1433 Src: Any)

ms-sql-m 0 UDP(Dst: 1434 Src: Any)

mysql 0 TCP(Dst: 3306 Src: Any), UDP(Dst: 3306 Src: Any)

netmeeting 0 TCP(Dst: 1720 Src: Any)

netbios-ns 0 TCP(Dst: 137 Src: Any), UDP(Dst: 137 Src: Any)

netbios-dgm 0 TCP(Dst: 138 Src: Any), UDP(Dst: 138 Src: Any)

netbios-ssn 0 TCP(Dst: 139 Src: Any), UDP(Dst: 139 Src: Any)

nfs 0 TCP(Dst: 111 Src: Any), TCP(Dst: 2049 Src: Any), UDP(Dst: 111 Src: Any), ...

nicname 0 TCP(Dst: 43 Src: Any)

nntp 0 TCP(Dst: 119 Src: Any)

ntp 0 TCP(Dst: 123 Src: Any), UDP(Dst: 123 Src: Any)

onc-rpc 0 TCP(Dst: 111 Src: Any), UDP(Dst: 111 Src: Any)

ospf 0 PROTO(89)

pc-anywhere 0 TCP(Dst: 5631 Src: Any), UDP(Dst: 5632 Src: Any)

pim 0 PROTO(103)

ping 0 ICMP(Type: 8 Code: 0)

ping6 0 PROTO(58)

pop2 0 TCP(Dst: 109 Src: Any), UDP(Dst: 109 Src: Any)

pop3 0 TCP(Dst: 110 Src: Any), UDP(Dst: 110 Src: Any)

pptp 0 TCP(Dst: 1723 Src: Any), PROTO(47)

printer 0 TCP(Dst: 515 Src: Any)

quake 0 UDP(Dst: 26000 Src: Any), UDP(Dst: 27000 Src: Any), UDP(Dst: 27910 Src: Any), ...

radius 0 UDP(Dst: 1812 Src: Any)

radius-acct 0 TCP(Dst: 1813 Src: Any), UDP(Dst: 1813 Src: Any)

raudio 0 UDP(Dst: 7070 Src: Any)

rexec 0 TCP(Dst: 512 Src: Any)

rip 0 UDP(Dst: 520 Src: Any)

rlogin 0 TCP(Dst: 513 Src: Any), TCP(Dst: 513 Src: Any)

rsh 0 TCP(Dst: 514 Src: Any)

rtsp 0 TCP(Dst: 554 Src: Any), TCP(Dst: 7070 Src: Any), TCP(Dst: 8080 Src: Any), ...

samba 0 TCP(Dst: 139 Src: Any)

sccp 0 TCP(Dst: 2000 Src: Any)

sip 0 UDP(Dst: 5060 Src: Any)

sip-msnmessenger 0 TCP(Dst: 1863 Src: Any)

shell 0 TCP(Dst: 514 Src: Any)

smtp 0 TCP(Dst: 25 Src: Any)

smux 0 TCP(Dst: 199 Src: Any)

snmp 0 TCP(Dst: 161-162 Src: Any), UDP(Dst: 161-162 Src: Any)

socks 0 TCP(Dst: 1080 Src: Any), UDP(Dst: 1080 Src: Any)

squid 0 TCP(Dst: 3128 Src: Any), UDP(Dst: 3128 Src: Any)

ssh 0 TCP(Dst: 22 Src: Any)

syslog 0 UDP(Dst: 514 Src: Any)

talk 0 UDP(Dst: 517-518 Src: Any)

tcp 0 PROTO(6)

telnet 0 TCP(Dst: 23 Src: Any)

tftp 0 UDP(Dst: 69 Src: Any)

time 0 UDP(Dst: 37 Src: Any)

timestamp 0 ICMP(Type: 13 Code: 0)

tproxy 0 TCP(Dst: 8081 Src: Any), UDP(Dst: 8081 Src: Any)

udp 0 PROTO(17)

uucp 0 TCP(Dst: 540 Src: Any)

vdolive 0 TCP(Dst: 7000-7010 Src: Any)

wais 0 TCP(Dst: 210 Src: Any)

webcache 0 TCP(Dst: 8080 Src: Any), UDP(Dst: 8080 Src: Any)

winframe 0 TCP(Dst: 1494 Src: Any)

who 0 UDP(Dst: 513 Src: Any)

x-windows 0 TCP(Dst: 6000-6063 Src: Any)

abc 0 PROTO(0), PROTO(1), PROTO(6), ...

表 11-3 show service显示信息描述表

| 字段 | 描述 |
| --- | --- |
| Name | 服务对象的名称 |
| Ref | 被其它模块引用的次数 |
| Service | 服务对象包包含的成员，有四种成员  TCP成员  UDP成员  ICMP成员  PROTO，其它协议类型成员 |

### show service-group

**show service-group**命令用来显示设备中的服务组。

【命令】

**show service-group** [ *group-name* ]

【视图】

任意视图

【参数】

*group-name*：服务组的名称。

【使用帮助】

如果没有指定*group-name*，**show service-group**命令显示所有的服务组，如果指定*group-name*，**show service-group**命令会显示指定的服务组。

【举例】

# 显示系统中所有的服务组。

host# host# show service-group

Flags: g--Group

Name Ref Members

group-name 1 telnet, http

xxx 0 group-name(g)

表 11-4 show service-group显示信息描表

| 字段 | 描述 |
| --- | --- |
| Name | 服务组的名称 |
| Ref | 被其它模块引用的次数 |
| Members | 服务服的成员，如果成员含有(g)，表示此成员也是一个表示服务组 |

### tcp dst-port

**tcp dst-port**命令用来向服务对象中添加一个TCP端口范围。

**no tcp dst-port**命令用来从服务对象中删除指定的TCP端口范围。

【命令】

**tcp** **dst-port** *dst-port-min dst-port-max* **src-port** *src-port-min src-port-max*

**no tcp** **dst-port** *dst-port-min dst-port-max* **src-port** *src-port-min src-port-max*

【视图】

服务对象视图

【参数】

*dst-port-min*：最小目的端口号。

*dst-port-max*：最大目的端口号。

*src-port-min*：最小源端口号。

*src-port-min*：最大源端口号。

【举例】

# 向服务对象service\_obj\_test添加一个tcp端口范围。

host(config)#config terminal

host(config)#service service\_obj\_test

host(config-service)# tcp dst-port 1000 2000 src-port 3000 4000

【相关命令】

* show service

### udp dst-port

**udp dst-port**命令用来向服务对象中添加一个UDP端口范围。

**no udp dst-port**命令用来从服务对象中删除指定的UDP端口范围。

【命令】

**udp** **dst-port** *dst-port-min dst-port-max* **src-port** *src-port-min src-port-max*

**no udp** **dst-port** *dst-port-min dst-port-max* **src-port** *src-port-min src-port-max*

【视图】

服务对象视图

【参数】

*dst-port-min*：最小目的端口号，取值范围为0～65535。

*dst-port-max*：最大目的端口号，取值范围为0～65535。

*src-port-min*：最小源端口号，取值范围为0～65535。

*src-port-min*：最大源端口号，取值范围为0～65535。

【举例】

# 向服务对象service\_obj\_test添加一个udp端口范围。

host(config)#config terminal

host(config)#service service\_obj\_test

host(config-service)# tcp dst-port 1000 2000 src-port 3000 4000

【相关命令】

* show service

## 时间表命令

### day

day命令用来向周周期计划中增加一周的中的指定天。

no day命令用来从指定的周周期计划中删除一周中的指定天。

【命令】

**day** { **monday** | **tuesday** | **wednesday** | **thursday** | **friday** | **saturday** | **sunday** | **allday**} *schedule-day-name*

**no day** { **monday** | **tuesday** | **wednesday** | **thursday** | **friday** | **saturday** | **sunday** | **allday**} *schedule-day-name*

【视图】

周计划视图

【参数】

*schedule-day-name*：日周期计划的名称。

【使用指导】

配置周周期计划的时候，需要引用日周期计划，日周期计划。

【举例】

# 周计划sweek\_test添加周一到周日的周期计划，对应的日周期计划是always。

host(config)# configure terminal

host(config)# schedule-week sweek\_test

host(config-schedule-week)# day allday always

【相关命令】

* schedule-week
* schedule-day

### day start

day start命令用来向月周期计划中添加日。

no day start命令用来从指定的月周期计划中删除日。

【命令】

**day** **start** *start-day* **end** *end-day* *schedule-day-name*

**no day** **start** *start-day* **end** *end-day* *schedule-day-name*

【视图】

月计划视图

【参数】

*start-day*：月周期计划的开始日期，取值范围为1～31。

*end-day*：月周期计划的结束日期，取值范围为1～31。

*schedule-day-name*：日周期计划的名称。

【使用指导】

配置月周期计划的时候，需要引用日周期计划。

【举例】

# 月计划smonth\_test添加1～20日的周期计划，对应的日周期计划是always。

host(config)# configure terminal

host(config)# schedule-month smonth\_test

host(config-schedule-month)# day start 1 end 20 always

【相关命令】

* schedule-month
* schedule-day

### periodic

periodic命令用来新建时间范围。

no periodic命令用来删除指定的时间范围。

【命令】

**periodic start** start-time end end-time

**no periodic start** start-time end end-time

【视图】

日计划视图

【参数】

*start-time*：单次周期计划的开始时间。

*end-time*：单次周期计划的结束时间。

【举例】

# 为日周期计划sday\_test添加日周期时间为11:20到15:30的周期时间。

host(config)# configure terminal

host(config)# schedule-day sday\_test

host(config-schedule-day)# periodic start 11:20 end 15:30

【相关命令】

* schedule-day

### schedule-day

**schedule-day**命令用来创建日计划并进入相应的日计划视图，如果指定的日计划已经存在，则直接进入相日计划视图，不需要再创建日计划。

**no** **schedule-day**命令用来删除已存在的日计划。

【命令】

**schedule-day** *schedule-name*

no **schedule-day** *schedule-name*

【视图】

系统视图

【参数】

*schedule-name*：日周期计划的名称。

【使用指导】

周期计划分为日周期计划、周周期计划、月周期计划。日周期计划可以添加四个时间范围，而周周期计划、月周期计划都需要对日周期计划进行引用。

【举例】

# 创建名为”sday\_test”的日周期计划。

host(config)# configure terminal

host(config)# schedule-day sday\_test

【相关命令】

* show schedule-day
* periodic

### schedule-month

**schedule-month**命令用来创建月计划并进入相应的月计划视图，如果指定的月计划已经存在，则直接进入月计划视图，不需要再创建月计划。

**no** **schedule-month**命令用来删除已存在的月计划。

【命令】

**schedule-month** *schedule-name*

no **schedule-month** *schedule-name*

【视图】

系统视图

【参数】

*schedule-name*：月周期计划的名称。

【举例】

# 创建月计划month\_test。

host(config)# configure terminal

host(config)# schedule-month smonth\_test

【相关命令】

* show schedule-month

### schedule-once

**schedule-once**命令用来创建单次计划并进入相应的单次计划视图，如果指定的单次计划已经存在，则直接进入单次计划视图，不需要再创建单次计划。

**no** **schedule-once**命令用来删除已存在的单次计划。

【命令】

**schedule-once** *schedule-name*

no **schedule-once** *schedule-name*

【视图】

系统视图

【参数】

*schedule-name*：单次周期计划的名称。

【举例】

# 创建单次周期计划sonce\_test。

host(config)# configure terminal

host(config)# schedule-once sonce\_test

【相关命令】

* show schedule-once

### schedule-week

schedule-week命令用来创建月计划并进入相应的周计划视图，如果指定的月计划已经存在，则直接进入删除周计划视图，不需要再创建周计划。

no schedule-week命令用来删除已存在的周计划。

【命令】

schedule-week *schedule-name*

no schedule-week *schedule-name*

【视图】

系统视图

【参数】

*schedule-name*：周周期计划的名称

【举例】

# 创建名为”sweek\_test”的周周期计划。

host(config)# configure terminal

host(config)# schedule-week sweek\_test

【相关命令】

* show schedule-week

### show schedule-day

show schedule-day命令用来显示设备的日计划。

【命令】

show schedule-day [ *schedule-name* ]

【视图】

任意视图

【参数】

*schedule-name*：日计划的名称。

【使用帮助】

如果没有指定*schedule-name*，**show schedule-day**命令显示所有的日计划，如果指定*schedule-name*，**show schedule-day**命令只显示指定的日计划。

【举例】

# 显示设备的日计划。

host# show schedule-day

Name Ref Status Periodic-ranges

always 2 active 00:00-23:59

xxx 1 inactive

表 11-5 show schedule-day命令显示信息描述表

| 字段 | 描述 |
| --- | --- |
| Name | 时间对象的名称 |
| Ref | 被其它模块引用的次数 |
| Status | 时间表对象的激活状态：  active表示当时周期计划是激活状态  inactive表示当时周期计划是未激活状态 |
| Periodic-ranges | 日计划生效的时间范围 |

### show schedule-month

show schedule-month命令用来显示设备的月计划。

【命令】

show schedule-month [ *schedule-name* ]

【视图】

任意视图

【参数】

*schedule-name*：月计划的名称。

【使用帮助】

如果没有指定*schedule-name*，**show schedule-month**命令显示所有的月计划，如果指定*schedule-name*，**show schedule-month**命令只显示指定的月计划。

【举例】

# 显示设备的所有月计划。

host# show schedule-month

Name Ref Status Schedules

aaa 0 inactive

month 0 active [1]always, [2]always, [3]always, [4]always, ...

表 11-6 show schedule-day命令显示信息描述表

| 字段 | 描述 |
| --- | --- |
| Name | 时间对象的名称 |
| Ref | 被其它模块引用的次数 |
| Status | 时间表对象的激活状态：  active表示当时周期计划是激活状态  inactive表示当时周期计划是未激活状态 |
| Schedules | 周计划生效的时间范围，[]内为一月对应的日期，[]后面为生效的日周期对象时间范围 |

### show schedule-once

show schedule-once命令用来显示设备的单次计划。

【命令】

show schedule-once [ *schedule-name* ]

【视图】

任意视图

【参数】

*schedule-name*：单次计划的名称。

【使用帮助】

如果没有指定*schedule-name*，**show schedule-once**命令显示所有的单次计划，如果指定*schedule-name*，**show schedule-once**命令只显示指定的单次计划。

【举例】

# 显示设备的所有单次计划。

host(config)# show schedule-once

Flags: d--Day Schedule, w--Week Schedule, m--Month Schedule

Name Ref Status Start-date Start-time End-date End-time Members

schedule-test 0 active 2014-07-03 00:00 2014-07-03 23:59 always(d)

表 11-7 show schedule-day命令显示信息描述表

| 字段 | 描述 |
| --- | --- |
| Name | 时间对象的名称 |
| Ref | 被其它模块引用的次数 |
| Status | 时间表对象的激活状态：  active表示当时周期计划是激活状态  inactive表示当时周期计划是未激活状态 |
| Start-date | 开始日期 |
| Start-time | 开始时间 |
| Start-time | 结束日期 |
| End-time | 结束时间 |
| Members | 单次计划生效的日计划，限定单次计划生效的时间范围 |

### show schedule-week

show schedule-week命令用来显示设备的周计划。

【命令】

show schedule-week [ *schedule-name* ]

【视图】

任意视图

【参数】

*schedule-name*：周计划的名称。

【使用帮助】

如果没有指定*schedule-name*，**show schedule-week**命令显示所有的周计划，如果指定*schedule-name*，**show schedule-week**命令只显示指定的周计划。

【举例】

# 显示设备的所有周计划。

host# show schedule-week

Name Ref Status Schedules

abc 0 inactive

zhou 0 inactive [monday]xxx, [friday]always

表 11-8 show schedule-week命令显示信息描述表

| 字段 | 描述 |
| --- | --- |
| Name | 时间对象的名称 |
| Ref | 被其它模块引用的次数 |
| Status | 时间表对象的激活状态：  active表示当时周期计划是激活状态  inactive表示当时周期计划是未激活状态 |
| Schedules | 周计划生效的时间范围，[]内为一周对应的天，[]后面为生效的日周期对象时间范围 |

## 关键字命令

### content

**content**命令用来向关键字对象中添加关键字内容。

**no content**命令用来从关键字对象中删除指定关键字内容。

【命令】

**content** *keyword-content*

**no content** *keyword-content*

【视图】

关键字视图

【参数】

*keyword-content*：关键字的内容，最大长度为64。

【举例】

# 向关键字key1中添加关键字内容法轮功。

host# configure terminal

host(config)# keyword key1

host(config-keyword)# content 法轮功

【相关命令】

* show keyword

### description

**description**命令用来修改关键字对象的描述。

【命令】

**description** *desc*

【视图】

关键字视图

【参数】

*desc*：关键字对象的描述信息，最大长度为128，且不能包含“%!"#$&`\*+,/:;<=>?\^'{}!”。

【举例】

# 修改关键字key1的描述信息为“testkeyword”。

host# configure terminal

host(config)# keyword key1

host(config-keyword)# description testkeyword

【相关命令】

* show keyword

### keyword

**keyword**命令用来创建关键字对象并进入相应的关键字对象视图，如果指定的关键字对象已经存在，则直接进入相应关键字视图，不需要再创建关键字对象。

**no keyword**命令用来删除已存在的关键字对象。

【命令】

**keyword** *keyword-name*

no **keyword** *keyword-name*

【视图】

系统视图

【参数】

*keyword-name*：关键字的名称，最长31个字符，且不能包含“%!"#$&`\*+,/:;<=>?\^'{}!”。

【举例】

# 创建关键字对象key1。

host# configure terminal

host(config)# keyword key1

【相关命令】

* show keyword

### show keyword

**show keyword**命令用来显示设备的关键字对象，如果不指定*keyword-name*，显示所有的关键字对象，如果指定*keyword-name*，只显示指定的关键字对象。

【命令】

**show keyword** keyword-name

【视图】

任意视图

【参数】

*keyword-name*：关键字对象的名称。

【举例】

# 显示所有的关键字对象。

host# show keyword

==========================================

Keyword Name : key1

Description : 测试使用的关键字

5 items :

==========================================

表 11-9 show keyword命令显示信息描述表

| 字段 | 描述 |
| --- | --- |
| Keyword Name | 关键字的名称 |
| Description | 关键字的描述信息 |
| items | 关键字对象的内容的个数 |

# 应用控制

## 应用对象配置命令

### application

application命令用来进入应用对象视图。

【命令】

application application-name

【视图】

系统视图

【参数】

application-name：应用名称。

【使用指导】

命令行下只能使用应用的英文名称。

【举例】

# 进入应用QQ的视图。

host# configure terminal

host(config)# application QQ

【相关命令】

* show application

### application-group

application-group命令用来应用对象组并进入相应的应用对象组视图，如果指定的应用对象组已经存在，则直接进入相应的应用对象组视图，不需要再应用对象组。

no application-group命令用来删除指定的应用对象组**。**

【命令】

applicationgroup-name

no applicationgroup-name

【视图】

系统视图

【参数】

group-name：应用组名称，为1～32个字符的字符串，且不能包含“%!"#$&`\*+,/:;<=>?\^'{}!”。

【举例】

# 创建一个名为test的应用对象组。

host# configure terminal

host(config)# application-group test

【相关命令】

* show application-group

### description

description命令用来设置应用对象组的描述信息。

【命令】

description *desc*

【视图】

应用对象组视图

【参数】

desc：应用对象组的描述，为1～128个字符的字符串。

【缺省情况】

应用对象组默认描述为空。

【举例】

# 设置应用对象组test的描述。

host# configure terminal

host(config)# application-group test

host(config-application-group)# description This is a test group.

【相关命令】

* show application-group

### member application

member application命令用来添加应用对象组的应用对象成员。

no member application命令用来删除应用对象组的应用对象成员。

【命令】

member application *application-name*

no member application *application-name*

【视图】

应用对象组视图

【参数】

application-name：需要进行添加/删除的应用对象名。

【举例】

# 设置应用对象组test的描述。

host# configure terminal

host(config)# application-group test

host (config-application-group)# description This is a test group.

【相关命令】

* show application-group

### priority

priority命令用来修改应用的默认优先级。

【命令】

priority { high | medium | low }

【视图】

应用对象视图

【参数】

**high**：优先级为高。

**medium**：优先级为中。

**low**：优先级为低。

【缺省情况】

所有应用的默认优先级均为中。

【举例】

# 设置QQ的优先级为高。

host# configure terminal

host (config)# application QQ

host (config-application)# priority high

【相关命令】

* show application

### show application

show application命令用来显示应用对象信息。

【命令】

show application [ *application-name* ]

【视图】

用户视图

【参数】

application-name：应用对象名。

【使用指导】

如果不指定应用对象名，则显示所有应用对象的信息，此时不会显示每个应用所支持的行为。

【举例】

# 显示应用对象QQ的信息。

host# show application QQ

==========================================

Name : QQ

Description :

Category : IM\_Software

Popularity : 4

Risk : 3

Priority : high

8 actions : IM\_login IM\_receive\_file IM\_send\_file IM\_video IM\_send IM\_receive IM\_logout IM\_voice

==========================================

内容的详细解释见[表1-1](#_Hlk388804261)所示

表 12-1 show application命令显示信息描述表

| 字段 | 描述 |
| --- | --- |
| Name | 应用名称 |
| Description | 应用描述，目前暂未使用 |
| Category | 应用的分类 |
| Popularity | 应用的流行度 |
| Risk | 应用的风险等级 |
| Priority | 应用优先级 |
| actions | 应用具有的行为动作 |

### show application-category

show application-category命令用来显示应用对象类信息。

【命令】

show application-category [ *category-name* ]

【视图】

用户视图

【参数】

category-name：应用对象类名，为1～32个字符的字符串，且不能包含“%!"#$&`\*+,/:;<=>?\^'{}!”。

【使用指导】

如果不指定应用对象类名，则显示所有应用对象类的信息，此时不会显示每个应用类的具体成员。

【举例】

# 显示所有应用对象类。

host# show application-category

==================================================

Category name : IM\_Software

3 Actions : IM\_send

IM\_receive

IM\_login

78 Members :

==================================================

Category name : P2P\_Software

2 Actions : P2P\_download

P2P\_request

36 Members :

==================================================

Category name : Media\_Software

2 Actions : Media\_download

Media\_play

88 Members :

…………

表 12-2 show application-category显示信息描述表

| 字段 | 描述 |
| --- | --- |
| Category name | 应用分类的名称 |
| Actions | 应用分类的行为 |
| members | 应用分类的成员的数量 |

### show application-group

show application-group命令用来显示应用对象组信息。

【命令】

show application-group [ *group-name* ]

【视图】

用户视图

【参数】

group-name：应用对象组名。

【使用指导】

如果不指定应用对象组名，则显示所有应用对象组的信息，此时不会显示每个应用组的具体成员。

【举例】

# 显示所有应用对象。

host# show application-group

==========================================

Group name : byod

Description :

86 Members

==========================================

Group name : iOS

Description :

50 Members

==========================================

Group name : Android

Description :

40 Members

==========================================

Group name : speed\_limiter

Description :

112 Members

==========================================

Group name : bandwidth\_guarantee

Description :

163 Members

==========================================

Group name : test

Description : This is a test group.

0 Members

==========================================

表 12-3 show application-group显示信息描述表

| 字段 | 描述 |
| --- | --- |
| Group name | 应用组的名称 |
| Description | 应用组的描述信息 |
| Members | 应用组的成员的数量 |

### show application-summary

show application-summary命令用来显示应用对象统计信息。

【命令】

show application-summary

【视图】

用户视图

【举例】

# 显示应用对象统计信息。

host# show application-summary

==========================================

Total category : 18

Total application : 803

High priority application : 0

Medium priority application : 803

Low priority application : 0

表 12-4 show application-summary显示信息描述表

| 字段 | 描述 |
| --- | --- |
| Total category | 应用分类的数量 |
| Total application | 应用的数量 |
| High priority application | 优先级为高的应用的数量 |
| Medium priority application | 优先级为中的应用的数量 |
| Low priority application | 优先级为低的应用的数量 |

## 应用控制策略配置命令

### app-policy

app-policy命令用来新建一条应用控制策略。

no app-policy命令用来删除一条应用控制策略。

【命令】

app-policy *id* { application | category } *name* { behavior | any } { bhcontent | any } { keyword | integer } { include | exclude | equal | unequal | greater | less } { content | any } { accept | deny } { emerg | alert | crit | err | notice | info | ignore } *show* [ description]

no app-policy *id*

【视图】

策略视图

【参数】

id：应用控制策略ID，最小为1，最大为64。

application：应用控制策略的控制对象为单个应用。

category：应用控制策略的控制对象为单个应用类。

name：应用或应用类的名字。

behavior：应用或应用类的行为，any表示所有行为。

bhcontent：该行为的审计内容，any表示所有内容。

**keyword**：审计对象为关键字。

**integer**：审计对象为数字。

**include**：审计匹配条件为包含。

**exclude**：审计匹配条件为不包含。

**equal**：审计匹配条件为相等。

**unequal**：审计匹配条件为不相等。

**greater**：审计匹配条件为大于。

**less**：审计匹配条件为小于。

*content*：用于匹配的对象，any表示全部匹配。

accept：控制动作为放行。

deny：控制动作为阻断。

emerg：日志级别为紧急。

alert：日志级别为警告。

crit：日志级别为严重。

err：日志级别为错误。

notice：日志级别为通知。

info：日志级别为信息。

ignore：不记录日志。

*show*：显示策略描述。

*description*：描述内容。

【使用指导】

配置应用控制策略的安全策略的动作必须是审计。

【举例】

# 给id为1的策略增加应用控制，不允许在网络社区发帖。

host# configure terminal

host(config)# policy 1

host(config-policy)# app-policy 1 category Network\_Community Community\_topic any keyword include any deny warning BlockPost

### app-policy disable

app-policy disable命令禁用已定义的应用控制策略。

【命令】

app-policy disable *id*

**【缺省情况】**

缺省情况下，应用策略是启用的。

【视图】

策略视图

【参数】

*id*：需要禁用的应用策略的id，取值范围为1～64。

【举例】

# 禁用应用控制策略1。

host# configure terminal

host(config)# policy 1

host(config-policy)# app-policy disable 1

### app-policy enable

app-policy enable命令启用已定义的应用控制策略。

【命令】

app-policy enable *id*

**【缺省情况】**

缺省情况下，应用策略是启用的。

【视图】

策略视图

【参数】

*id*：需要启用的应用策略的id，取值范围为1～64。

【举例】

# 启用应用控制策略1。

host# configure terminal

host(config)# policy 1

host(config-policy)# app-policy enable 1

# 类与网站策略

## URL分类

### show url-category

show url-category命令用来显示URL分类的情况。

【命令】

show url-category { predefined | user-defined }

【视图】

用户视图

【参数】

predefined：显示预定义的URL分类。

user-defined：显示自定义的URL分类。

【举例】

# 显示所有预定义的URL分类。

host# show url-category predefined

Total Url category count: 54

==========================================

Name

--------------------------------

ad

adult

art

music

automobile

BBS

lottery

business

network

crime

…………

表 13-1 show url-category命令显示信息描述表

| 字段 | 描述 |
| --- | --- |
| Name | URL分类的名称 |

### url

url命令用来添加一条URL到自定义URL分类。

no url命令用来从自定义URL分类中删除指定的URL

【命令】

url *url*

no url *url*

【视图】

URL分类视图

【参数】

url：将要被添加或删除的URL，1～31个字符的字符串，可输入除“？”以外的可打印字符。

【举例】

# 为test自定义URL分类增加url：[www.baidu.com](http://www.baidu.com)。

host# configure terminal

host(config)# url-category test

host(config-url-category)# url www.baidu.com

【相关命令】

* show url-category

### url-category

url-category命令用来创建自定义URL分类，并进入URL分类视图。

no url-category命令用来删除自定义URL分类。

【命令】

url-category name

【视图】

系统视图

【参数】

name：自定义URL分类名称。

【举例】

# 创建名为test的自定义URL分类。

host# configure terminal

host(config)# url-category test

host(config-url-category)#

【相关命令】

* show url-category

## 网站策略配置命令

### website-policy

website-policy命令用来新建一条网站策略。

no website-policy命令用来删除一条网站策略。

【命令】

website-policy *id* { *url-category* | any } { accept | deny } { emerg | alert | crit | err | notice | info | ignore } *show*

【视图】

策略视图

【参数】

id：网站策略ID，最小为1，最大为64。

*url-category*：进行网站策略控制的分类，any表示所有分类。

accept：控制动作为放行。

deny：控制动作为阻断。

emerg：日志级别为紧急。

alert：日志级别为警告。

crit：日志级别为严重。

err：日志级别为错误。

notice：日志级别为通知。

info：日志级别为信息。

ignore：不记录日志。

*show*：策略描述。

【使用指导】

参数*url-category*可输入至多8个分类，用逗号进行分隔。

配置应用控制策略的安全策略的动作必须是审计。

【举例】

# 给id为1的ipv4策略增加网站策略，不允许访问博彩类、色情类网站。

host# configure terminal

host(config)# policy 1

host(config-policy)# website-policy 1 lottery,porn, deny alert

### website-policy disable

website-policy disable命令停用已定义的网站策略。

【命令】

website-policy disable *id*

【视图】

策略视图

【举例】

# 停用id为1 的ipv4策略的网站策略1。

host# configure terminal

host(config)# policy 1

host(config-policy)# website-policy disable 1

### website-policy enable

website-policy enable命令启用已定义的网站策略。

【命令】

website-policy enable *id*

【视图】

策略视图

【举例】

# 启用id为1 的ipv4策略的网站策略1。

host# configure terminal

host(config)# policy 1

host(config-policy)# website-policy enable 1

### website-policy malware

website-policy malware enable命令启用恶意URL过滤。

website-policy malware disable命令停用恶意URL过滤。

【命令】

website-policy malware { enable | disable }

【缺省情况】

缺省情况下，恶意URL过滤是禁用的。

【视图】

策略视图。

【举例】

# 启用启用id为1 的ipv4策略的恶意URL过滤。

host# configure terminal

host(config)# policy 1

host(config-policy)# website-policy malware enable

# 用户和用户认证

## 用户配置命令

### bind ip

**bind ip**命令用来绑定地址或地址范围。

**no bind ip**命令用来删除地址或地址范围绑定。

【命令】

**bind ip** { **address** *ip-address* **| range** *start\_ip end\_ip* }

**no bind ip** { **address** *ip-address* **| range** *start\_ip end\_ip* }

【视图】

用户配置视图

【参数】

*ip-address*：要绑定的地址。

*start-ip*：绑定地址范围的起始地址。

*end-ip*：绑定地址范围的结束地址。

【使用指导】

绑定IP地址可以配置多条，但是条目之间不能有冲突现象。

【举例】

# 将用户user1绑定到地址范围1.1.1.1-1.1.1.5。

host# configure terminal

host(config)# user user1

host(config-user)# bind ip range 1.1.1.1 1.1.1.5

【相关命令】

* show user

### bind ip exclude

**bind excludeip**命令用来创建绑定地址的排除地址。

**no bind exclude ip exclude**命令用来删除绑定地址的排除地址。

【命令】

**bind exclude ip** { **address** *ip-address*| **range** *start\_ip end\_ip* }

**no bind exclude ip** { **address** *ip-address*| **range** *start\_ip end\_ip* }

【视图】

用户配置视图

【参数】

*ip-address*：要排除的地址。

*start-ip*：排除地址范围的起始地址。

*end-ip*：排除地址范围的结束地址。

【使用指导】

排除IP地址可以配置多条，但是条目之间不能有冲突现象。

【举例】

# 将用户user1绑定到地址范围1.1.1.1-1.1.1.5，并且排除地址1.1.1.4。

host# configure terminal

host(config)# user user1

host(config-user)# bind ip range 1.1.1.1 1.1.1.5

host(config-user)# bind exclude ip address 1.1.1.4

【相关命令】

* show user

### clear user-recognition

**clear user-recognition**命令用来清除所有或者某个动态识别出的在线用户信息。

【命令】

**clear user-recognition** [ *name* ]

【视图】

用户视图

【参数】

*name*：要清除在线用户信息的用户名，为1～31个字符的字符串。

【举例】

# 清除所有动态识别出的在线用户信息。

host# clear user-recognition

### description

**description**命令用来设置本地用户描述。

**no description**命令用来清除本地用户描述

【命令】

**description** *text*

**no description**

【缺省情况】

缺省情况下，没有配置本地用户描述。

【视图】

用户配置视图

用户组配置视图

【参数】

*text*：用户描述信息，为1～127个字符的字符串，且不能包含“%!"#$&`\*+,/:;<=>?\^'{}!”。

【举例】

# 创建用户名为user1的用户，添加描述first user。

host# configure terminal

host(config)# user user1

host(config-user)# description first user

### enable

**enable**命令用来启用本地用户。

**no enable**命令用来禁用本地用户。

【命令】

**enable**

**no enable**

【缺省情况】

缺省情况下，用户创建后是启用状态。

【视图】

用户配置视图

【举例】

# 禁用用户名为user1的用户。

host# configure terminal

host(config)# user user1

host(config-user)# no enable

【相关命令】

* show user

### enable bind

**enable bind**命令用来配置用户为绑定用户

**no enable bind**命令用配置用户为非绑定用户。

【命令】

**enable bind**

**no enable bind**

【视图】

用户配置视图

【举例】

# 创建用户名为user1的用户并且设置为绑定用户。

host# configure terminal

host(config)# user user1

host(config-user)# enable bind

【相关命令】

* show user

### match user

**match user**命令用来测试一个用户是否属于一个用户组。

【命令】

**match user** *username*

【视图】

用户组配置视图

【参数】

*username*：要测试的用户名，为1～31个字符的字符串。

【使用指导】

某种情况下，可能用户组会套嵌多层用户组，这样不太好判断一个用户是否属于这个用户组。这个命令可以用来测试使用户是否属于这个用户组。

【举例】

# 测试用user1是否属于用户组group1。

host# configure terminal

host(config)# user-group group1

host(config-user-group)# match user user1

【相关命令】

* user-group
* member
* show user-group

### member

**member**命令用来将用户加入用户组。

**no member**命令用来将用户从用户组删除。

【命令】

**member** *name*

**no member** *name*

【视图】

用户组配置视图

【参数】

*name*：要加入组的用户名或用户组名，为1～31个字符的字符串，且不能包含“%!"#$&`\*+,/:;<=>?\^'{}!”。

【使用指导】

用户组成员可以是另外一个用户组。

配置用户组加入另外一个用户组时，不要发生循环套嵌。

【举例】

# 将用户user1加入用户组group1。

host# configure terminal

host(config)# user-group group1

host(config-user-group)# member user1

【相关命令】

* user-group
* match user
* show user-group

### show user

**show user**命令用来显示系统中配置的本地用户。

【命令】

**show user** [ *username* ]

【视图】

用户视图

【参数】

*username*：要显示的用户名，为1～31个字符的字符串，且不能包含“%!"#$&`\*+,/:;<=>?\^'{}!”。

【举例】

# 显示系统中配置的所有本地用户。

host# show user

Flags: E--Enabled, F--Frozen-Enabled, A--Authenticate-Need, B--Bind-Address

Name Ref Status Frozen-EndTime Account Bind-Address

any 0 E---

123 0 E-A- [SERVER GROUP]

A 0 E-A- [LOCAL]

user1 1 E---

user2 0 E--B 1.1.1.1-1.1.1.5, 1.1.1.4(e)

user3 0 E---

表 14-1 **r**命令显示信息描述表

| 字段 | 描述 | |
| --- | --- | --- |
| Name | 本地用户名 | |
| Ref | 用户引用计数 | |
| Status | 用户状态 | |
| E | 用户启用 |
| F | 用户被冻结 |
| A | 是认证用户 |
| B | 是绑定用户 |
| Frozen-EndTime | 冻结结束时间 | |
| Account | 用户认证类型 | |
| [LOCAL] | 用户是本地认证 | |
| [RADIUS] | 用户是RADIUS认证 | |
| [LDAP] | 用户是LDAP认证 | |
| [SERVER GROUP] | 用户是RADIUS或者LDAP组认证 | |
| Bind-Address | 绑定用户的绑定地址 | |
| (e) | 表示前边的地址是绑定地址中排除的部分 | |

# 显示用户名为user1的用户信息。

host# show user user1

Name: user1

Alias:

Description: first user

Reference count: 1

User Status: enabled

表 14-2 **show user**命令显示信息描述表

| 字段 | 描述 |
| --- | --- |
| Name | 本地用户命 |
| Alias | 用户别名 |
| Description | 用户描述 |
| Reference count | 引用计数 |
| User Status | 用户启用状态 |

### show user-group

**show user-group**命令用来显示用户组。

【命令】

**show user-group**[ *group-name* ]

【视图】

用户视图

【参数】

*group-name*：用户组名，为1～31个字符的字符串，且不能包含“%!"#$&`\*+,/:;<=>?\^'{}!”。

【举例】

# 显示系统所有用户组。

host# show user-group

Flags: g--Group

Name Ref Members

anonymous 0

mobile 0

group1 0 user1

表 14-3 show user-group命令显示信息描述表

| 字段 | 描述 |
| --- | --- |
| Name | 用户组名 |
| Ref Members | 引用计数 |
| Members | 用户组内用户成员 |

# 显示用户组group1。

host# show user-group group1

Name: group1

Description:

Reference count: 0

Member count: 1

Entry Members:

user1

表 14-4 **show user-group** *group-name*命令显示信息描述表

| 字段 | 描述 |
| --- | --- |
| Name | 用户组名 |
| Description | 用户组描述 |
| Reference count | 引用计数 |
| Member count | 用户组内成员个数 |
| Entry Members | 用户组内成员条目 |

### show user-param

**show user-param**命令用来显示用户识别属性。

【命令】

**show user-param**

【视图】

用户视图

【举例】

# 显示用户识别属性。

host# show user-param

Address Scope: private[Heuristic Mode]

Recognition threshold: 60000

Recognition minimum ttl: 120 seconds

Recognition maximum ttl: 1200 seconds

表 14-5 show user-param命令显示信息描述表

| 字段 | 描述 |
| --- | --- |
| Address Scope | 用户识别范围的地址对象名 |
| [ *mode* ] | 用户识别的方式 |
| Recognition threshold | 可识别用户的个数 |
| Recognition minimum ttl | 识别老化时间的最小值 |
| Recognition maximum ttl | 识别老化时间的最大值 |

### show user-recognition

**show user-recognition**命令用来显示本地已识别用户。

【命令】

**show user-recognition** [ **user name** *name* | **address** { **host** *host-ip |* **range** *start-ip end-ip* | **name** *address-name* } ]\*

【视图】

用户视图

【参数】

**user name**：只显示某个用户名的用户。

*name*：显示的用户名。

**address**：只显示地址为某种条件的用户。

**host**：只显示用户地址是某个地址的用户。

*host-ip*：用户地址。

**range**：只显示用户地址在某个地址范围内的用户。

*start-ip*：地址范围开始地址。

*end-ip*：地址范围结束地址。

**name**：只显示用户地址在某个地址对象范围内的用户。

*address-name*：地址对象名。

【举例】

# 显示本地已识别用户。

host# show user-recognition

Address Scope: private[Heuristic Mode]

Recognitions: 32

Name Identity IP MAC Status Online-StartTime Frozen-EndTime

192.168.1.56 anonymous 192.168.1.56 28:d2:44:38:43:0 2014/07/04 11:03

192.168.1.239 anonymous 192.168.1.239 00:23:ff:4b:6c:d1 2014/07/04 10:59

169.254.67.28 anonymous 169.254.67.28 c8:1f:66:f2:53:e6 2014/07/04 10:57

192.168.1.157 anonymous 192.168.1.157 7c:e9:d3:f5:13:d1 2014/07/04 10:50

表 14-6 show user-recognition命令显示信息描述表

| 字段 | 描述 | |
| --- | --- | --- |
| Address Scope | 用户识别范围的地址对象名 | |
| [ *mode* ] | 用户识别的方式 | |
| Recognitions | 已识别用户个数 | |
| Name | 识别的用户名 | |
| Identity | 识别用户类型 | |
| anonymous | 匿名用户 |
| static | 本地认证/静态绑定用户 |
| mobile | 移动用户 |
| IP | 用户登录地址 | |
| MAC | 用户登录mac地址 | |
| Status | 用户状态，是否被冻结 | |
| Online-StartTime | 用户登录的时间 | |
| Frozen-EndTime | 冻结结束时间 | |

### user

**user**命令用来创建本地用户。

**no user**命令用来删除本地用户。

【命令】

**user** *username*

**no user** *username*

【缺省情况】

缺省情况下，存在一个any用户。

【视图】

系统视图

【参数】

*username*：用户名，为1～31个字符的字符串，且不能包含“%!"#$&`\*+,/:;<=>?\^'{}!”。

【使用指导】

该命令执行完后进入用户配置节点。

【举例】

# 创建用户名为user1的用户。

host# configure terminal

host(config)# user user1

host(config-user)#

【相关命令】

* show user

### user-group

**user-group**命令用来创建本地用户组。

**no user-group**命令用来删除本地用户组。

【命令】

**user-group** *groupname*

**no user-group** *groupname*

【缺省情况】

缺省情况下，存在一个anonymous用户组。

【视图】

系统视图

【参数】

*groupname*：用户组名，为1～31个字符的字符串，且不能包含“%!"#$&`\*+,/:;<=>?\^'{}!”。

【使用指导】

该命令执行完后进入用户组配置节点。

【举例】

# 创建用户名为group1的用户。

host# configure terminal

host(config)# user-group group1

host(config-user-group)#

【相关命令】

* member
* match user
* show user-group

### user-param

**user-param recognition**命令用来修改用户识别属性。

**no user-param recognition**命令用来恢复用户识别属性。

【命令】

**user-param recognition scope** *address-object* { **heuristic** | **strict** }

**no user-param recognition scope** *address-object*

**user-param recognition threshold** *count*

【缺省情况】

缺省情况下，用户识别的范围是地址对象private，方式是启发式的，识别用户的个数是60000个。

【视图】

用户配置视图

【参数】

*address-object*：设置的用户识别的地址对象或者地址组对象名称，为1～31个字符的字符串。

**heuristic**：启发式识别，。

**strict**：严格识别。

*count*：识别用户上限，范围是5000～10000000。

【使用指导】

识别模式分为“启发模式”和“严格模式”两种。

“启发模式”指的是，优先将属于识别范围的IP地址识别为用户。

“严格模式”指的是，当一个IP地址属于识别范围时，一定会被识别为用户；反之当一个IP地址不属于识别范围时，一定不会识别为用户。

【举例】

# 将所有私有网络的识别模式改为严格模式。

host# configure terminal

host(config)# user-param recognition scope private strict

【相关命令】

* show user

## 用户认证配置命令

### authenticate

**authenticate**命令用来配置用户的认证方式。

【命令】

**authenticate**{ **local** *password* | **ldap** *ldap-server* | **radius** *radius-server* | **group** *group-name* }

【缺省情况】

缺省情况下，没有配置用户认证。

【视图】

用户配置视图

【参数】

**local**：启用本地认证。

*password*：本地认证的密码，为6～31个字符的字符串。

**ldap**：启用LDAP认证。

*ldap-server*：LDAP 的服务器，为1～31个字符的字符串。

**radius**：启用RADIUS认证。

*radius-server*：RADIUS的服务器，为1～31个字符的字符串。

**group**：使用LDAP或者RADIUS服务器组认证。

*group-name*：服务器组名称，为1-31个字符的字符串。

【使用指导】

认证方式要用**no enable authenticate**命令删除。

【举例】

# 配置用户user1使用本地认证，密码是123456。

host# configure terminal

host(config)# user user1

host(config-user)# enable authenticate

host(config-user)# authenticate local 123456

【相关命令】

* enable authenticate
* show user

### enable authenticate

**enable authenticate**命令用来启用用户认证。

**no enable authenticate**命令用来关闭用户认证并且删除认证方式。

【命令】

**enable authenticate**

**no enable authenticate**

【视图】

用户配置视图

【使用指导】

使用**no enable authenticate**会删除已经配置的认证方式。

【举例】

# 为用户user1启用本地认证。

host# configure terminal

host(config)# user user1

host(config-user)# enable authenticate

【相关命令】

* show user
* authenticate

### show user-policy

**show user-policy**命令用来显示用户策略。

【命令】

**show user-policy**

【视图】

用户视图

【举例】

# 显示用户策略。

host(config)# show user-policy

---------------------------------------------------------------------------------------

ID In-interface Out-interface Source-address Dest-address Schedul Action

----------------------------------------------------------------------------------------

1 any any any any always local-webauth

表 14-7 show user-policy命令显示信息描述表

| 字段 | 描述 |
| --- | --- |
| ID | 用户策略的ID号 |
| In-interface | 匹配流量入接口 |
| Out-interface | 匹配流量出接口 |
| Source-address | 匹配流量源地址 |
| Dest-address | 匹配流量目的地址 |
| Schedule | 匹配流量时间组 |
| Action | 匹配的流量的执行动作 |
| permit | 匹配用户的流量直接放行 |
| local-webauth | 用户必须通过WEB认证后，流量才可以通过 |
| portal-server-webauth | 用户必须通过portal认证后，流量才可以通过 |

### user-policy

**user-policy**命令用来创建用户策略。

**no user-policy**命令用来删除用户策略。

【命令】

**user-policy** { *if\_in*| **any** } { *if\_out*| **any** } {*sip* | **any** } { *dip* | **any** } { *schedule* | **always** } { **permit** | **local-webauth** | **portal-server-webauth** } [ *id* ] [ **head** | { **before** | **after** } [ *compare-id* ] ]

**no user-policy** *id*

【缺省情况】

缺省情况下，没有启用用户策略。

【视图】

系统视图

【参数】

*if\_in*：流量入接口。

**any**：任何接口。

*if\_out*：流量出接口。

**any**：任何接口：

*sip*：源地址匹配的地址对象或对象组。

**any**：任何源地址。

*dip* ：目的地址匹配的地址对象或对象组。

**any**：任何目的地址。

*schedule* ：配的时间对象。

**always**：任何时间。

**permit** ：允许放行，无需用户认证。

**local-webauth**：用户必须通过WEB认证后，流量才可以通过。

**portal-server-webauth**：用户必须通过portal认证后，流量才可以通过。

*id*：给流量指定的id号，范围是1～65535，缺省从1开始自动排列。

**head**：将用户策略的匹配顺序到放到最前面。

**before**：将用户策略的匹配顺序放到到某条策略之前。

**after**：将用户策略的匹配顺序放到到某条策略之后。

*compare-id*：**before**和**after**使用时的基准策略id，范围是1～65535。

*id*：要删除的流量id号，范围是1～65535，。

【使用指导】

用户策略的匹配时有顺序要求，一般按照显示的顺序从上到下匹配。

【举例】

# 创建配置所有通过设备的流量必须通过WEB认证。

host# configure terminal

host(config)# user-policy any any any any always local-webauth

【相关命令】

* show user-policy

### user-policy move

**user-policy move**命令用来调整用户策略的匹配顺序。

【命令】

**user-policy move** *id* {{ **head** *|* **tail**} | { **before** | **after** } *compare-id* }

【视图】

系统视图

【参数】

*id*：给要调整的用户策略id号，范围是1到65535，缺省从1开始自动排列。

**head**：将用户策略的匹配顺序到放到最前面。

**tail**：将用户策略的匹配顺序到放到最后面。

**before**：将用户策略的匹配顺序发到某条策略之前。

**after**：将用户策略的匹配顺序发到某条策略之后。

*compare-id*：**before**和**after**使用时的基准策略id，范围是1～65535。

【使用指导】

用户策略的匹配时有顺序的，一般按照显示的顺序从上到下匹配。

【举例】

# 将用户策略100调整到用户策略2之后。

host# configure terminal

host(config)# user-policy move 100 after 2

【相关命令】

* show user-policy

### user-webauth force-timeout

**user-webauth force-timeout**命令用来配置WEB强制重新认证时间。

**no user-webauth force-timeout**命令用来关闭WEB强制重新认证时间。

【命令】

**user-webauth force-timeout** *timeout*

**no no user-webauth force-timeout**

【缺省情况】

缺省情况下，不启用WEB强制重新认证。

【视图】

系统视图

【参数】

*timeout*：WEB强制重新认证时间，范围是10～144000，单位是分钟，缺省不启用。

【使用指导】

当用户登录以后，即使用户一直在线，在设定的时间长度之后，也必须重新登录。

【举例】

# 设置WEB强制重新认证时间为60分钟。

host# configure terminal

host(config)# user-webauth force-timeout 60

### user-webauth hello-url

**user-webauth hello-url** 命令用来配置WEB认证重定向URL。

**no user-webauth hello-url**命令用来关闭WEB认证重定向。

【命令】

**user-webauth hello-url** *url*

**no user-webauth hello-url**

【缺省情况】

缺省情况下，不启用WEB认证重定向。

【视图】

系统视图

【参数】

*url*：WEB认证重定向的URL地址，为1～127个字符的字符串。

【举例】

# 设置WEB认证重定向到www.abc.com。

host# configure terminal

host(config)# user-webauth hello-url www.abc.com

### user-webauth keepalive-timeout

**user-webauth keepalive-timeout**命令用来配置WEB心跳间隔时间。

**no user-webauth keepalive-timeout**命令用来恢复心跳间隔时间的默认配置。

【命令】

**user-webauth keepalive-timeout** *timeout*

**no user-webauth keepalive-timeout**

【缺省情况】

缺省情况下，心跳间隔时间是10分钟。

【视图】

系统视图

【参数】

*timeout*：WEB心跳间隔时间，范围是1到720，单位是分钟，缺省是10分钟。

【举例】

# 设置心跳间隔时间为30分钟。

host# configure terminal

host(config)# user-webauth keepalive-timeout 30

### user-webauth login-multi

**user-webauth login-multi**命令用来允许同一个用户名登录同时登录多次。

【命令】

**user-webauth login-multi number** [ *count* ]

【缺省情况】

缺省情况下，不允许同一个用户同时登录多次。

【视图】

系统视图

【参数】

*count*：允许同一个用户同时登录的次数，范围是2到1000次，如果不输入数字，缺省是无限制。

【举例】

# 设置WEB认证允许同一用户名在同时无限次登录。

host# configure terminal

host(config)# user-webauth login-multi number

### user-webauth login-single

**user-webauth login-single**命令用来限制用户同时只能登录一次。

【命令】

**user-webauth login-single mode** { **kick-old** | **forbid-new** }

【缺省情况】

缺省情况下，用户同时只能登录一次，缺省策略是踢出老用户。

【视图】

系统视图

【参数】

**kick-old**：新用户会踢出老用户。

**forbid-new**：禁止老用户登录。

【举例】

# 配置用户同时只能登录一次，新用户登录会踢出老用户。

host# configure terminal

host(config)# user-webauth login-single mode kick-old

## 配置认证服务器

### bindtype

**bindtype**命令用来配置LDAP服务器绑定类型。

【命令】

**bindtype** { **anonymous** | **simple** | **regular user** *name* **passwd** *password }*

【视图】

LDAP配置视图

【参数】

**anonymous**：绑定类型为匿名。

**simple**：绑定类型为简单。

**regular**：绑定类型为通用。

**user**：通用类型时的用户名。

*name*：用户名，为1～128个字符的字符串。

**passwd**：通用类型时的密码。

*password*：密码，为1～16个字符的字符串。

【举例】

# 配置LDAP服务器server2的绑定类型为通用，用户ldap1，密码123456。

host# configure terminal

host(config)# ldap server2

host(config-ldap)# bindtype regular user ldap1 passwd 123456

【相关命令】

* ldap
* cnid
* dn
* filter

### cnid

**cnid**命令用来配置通用名称。

【命令】

**cnid** *cnid*

【视图】

LDAP配置视图

【参数】

*cnid*：通用标识名，为1～4个字符的字符串。

【举例】

# 配置LDAP服务器server2的通用标识名为cn。

host# configure terminal

host(config)# ldap server2

host(config-ldap)# cnid cn

【相关命令】

* ldap
* bindtype
* dn
* filter

### dn

**dn**命令用来配置LDAP服务器区别名。

【命令】

**dn** *dn*

【视图】

LDAP配置视图

【参数】

*dn*：区别名，为1～128个字符的字符串。

【举例】

# 配置LDAP服务器server2的区别名为OU=users,OU=test, DC=com。

host# configure terminal

host(config)# ldap server2

host(config-ldap)# dn OU=users,OU=test,DC=com

【相关命令】

* ldap
* bindtype
* cnid
* filter

### filter

**filter**命令用来配置LDAP的过滤选项。

【命令】

**filter** *option*

【视图】

LDAP配置视图

【参数】

*option*：LDAP服务区的过滤选项，为1～19个字符的字符串。

【举例】

# 配置LDAP服务器server2的过滤选项为host。

host# configure terminal

host(config)# ldap server2

host(config-ldap)# **filter host**

【相关命令】

* ldap
* bindtype
* cnid
* dn

### ldap（LDAP配置视图）

**ldap**命令用来配置LDAP服务器地址。

【命令】

**ldap** *server-ip* [ *port* ]

【视图】

LDAP配置视图

【参数】

*server-ip*：LDAP服务器地址。

*port*：LDAP服务器端口，范围是1～65535，缺省389。

【举例】

# 配置LDAP服务器server2的地址为2.2.2.2。

host# configure terminal

host(config)# ldap server2

host(config-ldap)# ldap 2.2.2.2

【相关命令】

* ldap
* bindtype
* cnid
* dn
* filter

### ldap（系统视图）

**ldap**命令用来创建和管理LDAP服务器。

**no ldap**命令用来删除和管理LDAP服务器。

【命令】

**ldap** *name* [ **group** *groupname* ]

**no ldap** *name* [ **group** *groupname* ]

【缺省情况】

缺省情况下，没有配置LDAP服务器。

【视图】

系统视图

【参数】

*name*：LDAP服务器名称，为1～127个字符的字符串。

**group**将服务器加入到LDAP组中。

*groupname*：LDAP服务器要加入的服务器组名称，为1～19个字符的字符串。

【使用指导】

创建LDAP服务器后，会进入LDAP配置视图。

【举例】

# 创建名字为server2的LDAP服务器。

host# configure terminal

host(config)# ldap server2

host(config-ldap)#

【相关命令】

* ldap
* bindtype
* cnid
* dn
* filter

### radius-server

**radius-server**命令用来配置或管理RADIUS服务器。

**no radius-server**命令用来管理或删除RADIUS服务器。

【命令】

**radius-server** *name*  { *server-ip secret*[*port* ] | **group** *group-name* }

**no radius-server** *name* [ **group** *group-name* ]

【缺省情况】

缺省情况下，没有配置RADIUS服务器。

【视图】

用视图

【参数】

*name*：RADIUS服务器名字，为1～256个字符的字符串。

*server-ip*：服务器IP地址。

*secret*：服务器密码，为1～256个字符的字符串。

*port*：服务器的端口号，范围是1～65535，缺省是1812。

**group**：将服务器加入或删除RADIUS服务器组中。

*group-name*：服务器组名称，为1～256个字符的字符串。

【举例】

# 创建RADIUS服务器server1，IP地址1.1.1.1，密码123456。

host# configure terminal

host(config)# radius-server server1 1.1.1.1 123456

【相关命令】

* show radius-server

### server-group

**server-group**命令用来创建服务器组。

**no server-group**命令用来删除服务器组。

【命令】

**server-group** *name*{ **radius** | **ldap** } **firewall**

**no server-group** *name*

【缺省情况】

缺省情况下，没有配置服务组。

【视图】

系统视图

【参数】

*name*：服务器组名，为1～256个字符的字符串。

**radius**：服务器组为RADIUS服务器组。

**ldap**：服务器组为LDAP服务器组。

【举例】

# 创建名字为group2的LDAP服务器组。

host# configure terminal

host(config)# server-group group2 ldap firewall

【相关命令】

* radius-server
* ldap

### show radius-server

**show radius-server**命令用来显示系统中配置的服务器。

【命令】

**show radius-server** [ *servername* ]

【视图】

用户视图

【参数】

*servername*：要显示的服务器名字，为1～256个字符的字符串。

【举例】

host# show radius-server

# 显示系统内所有的RADIUS服务器。

Radius-Server Name Secret IP Address Port Reference Count

aaa \*\*\*\*\*\* 1.1.1.1 1812 1

12312 \*\*\*\*\* 2.2.2.2 1812 0

server1 \*\*\*\*\*\* 1.1.1.1 1812 0

Total radius-servers : 3

表 14-8 show radius-server命令显示信息描述表

| 字段 | 描述 |
| --- | --- |
| Radius-Server Name | RADIUS服务器名称 |
| Secret | 服务器密码，已经加密 |
| IP Address | 服务器地址 |
| Port | 服务器端口 |
| Reference Count | 引用计数 |
| Total radius-servers | 系统内RADIUS服务器个数 |

### show server-group

**show server-group**命令用来显示配置的服务器组。

【命令】

**show server-group** [ *groupname* ]

【视图】

用户视图

【参数】

*groupname*：要显示的服务组名称，为1-256个字符的字符串。

【举例】

# 显示系统所有的服务器组。

host(config)# show server-group

Group Name Type Mode Imprint\_Clean Access\_Security Rule Refer\_Count

bbbb firewall 1

dddd firewall 0

group2 firewall 0

Total groups : 3

表 14-9 show server-group命令显示信息描述表

| 字段 | 描述 |
| --- | --- |
| Group Name | 服务器组名称 |
| Type | 服务器组类型 |
| Refer\_Count | 引用计数 |
| Total groups | 系统内服务器组的个数 |

# 显示RADIUS服务器组bbbb和LDAP服务器组group2。

host(config)# show server-group bbbb

Group Name Type Mode Imprint\_Clean Access\_Security Rule Refer\_Count User List

bbbb firewall 1 123

1 user in group (bbbb)

Group Name Type Mode Refer\_Count Radius-server List

bbbb firewall 1 aaa

radius-server in group (bbbb)

host(config)# show server-group group2

Group Name Type Mode Imprint\_Clean Access\_Security Rule Refer\_Count User List

group2 firewall 0

0 user in group (group2)

Group Name Type Mode Refer\_Count Ldap-server List

group2 firewall 0 server2

1 ldap-server in group (group2

表 14-10 **show server-group**  *groupname* 命令显示信息描述表

| 字段 | 描述 |
| --- | --- |
| Group Name | 服务器组名称 |
| Type | 服务器组类型 |
| Refer\_Count | 引用计数 |
| Total groups | 服务器组的个数 |
| User List | 使用此服务器组认证的用户列表 |
| Radius-server List | 服务器组内RADIUS服务器列表 |
| Ldap-server | 服务器组内LDAP服务器列表 |

### user-portal-server

**user-portal-server**命令用来配置Portal认证的服务器IP地址。

**no user-portal-server**命令用来管理或删除Portal认证的服务器IP地址。

【命令】

**user-portal-server** {**server** *server-ip |* **radius** *server-name |* **timeout** *time-value*}

**no user-portal-server** {**server** *server-ip |* **radius** *server-name |* **timeout** *time-value*}

【缺省情况】

缺省情况下，没有配置Portal服务器。

【视图】

用户视图

【参数】

*server-ip*：Portal服务器IP地址。

*server*-*name*：RADIUS服务器的名称。

*time-out*：Portal认证用户的超时时间，范围是1到144000，单位是分钟，缺省是15分钟。

【举例】

# 配置Portal服务器的IP地址是192.168.10.1，radius服务器的名称是rad-server。

host# configure terminal

host(config)# user-portal-server server 192.168.10.1

host(config)# user-portal-server radius rad-server

# 流量管理

## 线路配置命令

### limit

**limit** 命令用来对线路流量进行限制。

【命令】

**limit** { **egress** | **ingress** | **both** }

【缺省情况】

缺省情况下，仅仅限制egress方向。

【视图】

线路配置节点视图

【参数】

**egress**：对下行流量进行流量管理。

**ingress**：对上行流量进行流量管理。

**both**：对上下行流量同时进行流量管理。

【使用指导】

线路限制上行（入）、下行（出）、或者上下行同时进行流量限制，缺省情况下，仅仅限制egress。

【举例】

# 对线路test的出方向进行流量限制。

host# configure terminal

host(config)# qos-profile line test

host(config-qos-test)# limit egress

### match interface

**match interface**命令用来绑定接口。

**no match interface** 命令用来取消绑定。

【命令】

**match interface** *interface-name*

**no match interface**

【视图】

线路配置节点视图

【参数】

*interface-name*：接口名称。

【使用指导】

线路必须和一个接口进行绑定，以便确定对哪个接口的流量进行控制。

取消绑定后，线路将不能进行流量管理。

【举例】

# 创建线路test，绑定ge0接口。

host# configure terminal

host(config)# qos-profile line test

host(config-qos-test)# match interface ge0

### maxbandwidth

**maxbandwidth**命令用来设置线路的最大带宽。

【命令】

**maxbandwidth** { **egress** | **ingress** }*bandwidth-range*

【缺省情况】

缺省情况下，最大带宽为1000000(Kbps)，即1Gbps。

【视图】

线路配置节点视图

【参数】

**egress**：指定下行流量的最大带宽。

**ingress**：指定上行流量的最大带宽。

*bandwidth-range*：最大带宽值，范围是8～1000000，单位Kbps。

【举例】

# 针对test线路配置上下行最大带宽分别为10Mbps。

host# configure terminal

host(config)# qos-profile line test

host(config-qos-test)# maxbandwidth egress 10000

host(config-qos-test)# maxbandwidth ingress 10000

### qos-profile line

**qos-profile line**命令用来创建线路，并进入线路节点视图，如果已经存在，则直接进入相应视图。

**no qos-profile line**命令用来删除线路。

【命令】

**qos-profile line** *line-name*

**no qos-profile line** *line-name*

【视图】

系统视图

【参数】

*line-name*：线路的名称，取值最大27个字符，且不能包含“%!"#$&`\*+,/:;<=>?\^'{}!”。

【举例】

# 创建一条线路，名称为test。

host# configure terminal

host(config)# qos-profile line test

## 管道配置命令

### bandwidth

**bandwidth line**命令用来设置管道的保障带宽。

【命令】

**bandwidth** { **egress** | **ingress** }*bandwidth-range*

【缺省情况】

缺省情况下，保障带宽为父节点保障带宽的20%。

【视图】

管道配置节点视图

【参数】

**egress**：指定下行流量。

**ingress**：指定上行流量。

*bandwidth-range*：管道的保证带宽。

【使用指导】

如果所有子节点的保障带宽超过了父节点的保障带宽，将依据配置值按比例进行分配，合理规划保障带宽，不超过父节点的保障带宽，否则可能起不到保障带宽的作用。

【举例】

# 配置管道channel0下行流量的保证带宽为10Mbps。

host# configure terminal

host(config)# qos-profile channel channel0

host(config-qos-channel0)# bandwidth egress 10000

### match

**match**命令用来设置管道的匹配规则。

【命令】

**match** { **address** | **application** | **service** | **user** }*name*

【视图】

管道配置节点视图

【参数】

**address**：地址或地址组对象。

**application**：应用对象。

**service**：服务对象。

**user**：用户或用户组对象。

*name*：对象的名称。

【使用指导】

相同类型的匹配，仅仅匹配一个就算匹配。

不同类型的匹配，必须两者都匹配，如果管道没有任何匹配规则，则该管道无法匹配。

如果配置管道下有子管道，则流量需要先匹配此管道的匹配规则，然后才会匹配子管道的规则。

【举例】

# 配置管道channel0匹配tcp服务。

host# configure terminal

host(config)# qos-profile channel channel0

host(config-qos-channel0)# match service tcp

### maxbandwidth

**maxbandwidth**命令用来设置管道的最大可用带宽。

【命令】

**maxbandwidth** { **egress** | **ingress** }*bandwidth-range*

【缺省情况】

缺省情况下，最大带宽为父节点的最大带宽。

【视图】

管道配置节点视图

【参数】

**egress**：指定下行流量。

**ingress**：指定上行流量。

*bandwidth-range*：管道的最大带宽。

【举例】

# 配置管道channel0下行流量的最大带宽为10Mbps。

host# configure terminal

host(config)# qos-profile channel channel0

host(config-qos-channel0)# maxbandwidth egress 10000

### move

**move**命令用来在相同级别的管道中，移动管道顺序。

【命令】

**move** { **bottom** | **top** |**up** | **down** }

【视图】

管道配置节点视图

【参数】

**bottom**：移动到底部，但是在缺省管道之前。

**top**：移动到顶部。

**up**：向上移动。

**donw**：向下移动。

【使用指导】

在相同级别的管道中，移动管道顺序。

管道匹配按照管道配置顺序进行匹配，如果某个管道的顺序不合理，可以移动管道顺序。

【举例】

# 把管道channel0移动到顶部。

host# configure terminal

host(config)# qos-profile channel channel0

host(config-qos-channel0)# move top

### perip

**perip**命令用来限制每个IP的最大流量。

【命令】

**perip** { **ingress** | **egress** }*bandwidth-range*

【缺省情况】

管道中没有IP流量限制。

【视图】

管道配置节点视图

【参数】

**egress**：指定下行流量。

**ingress**：指定上行流量。

*bandwidth-range*：每个IP每秒能够通过的流量，单位为Kbps。

【举例】

# 配置管道channel0中perip的流量为2Mbps。

host# configure terminal

host(config)# qos-profile channel channel0

host(config-qos-channel0)# perip egress 2000

### priority

**priority**命令用来修改管道的优先级。

【命令】

**priority** { **low** | **medium** | **high** }

【视图】

管道配置节点视图

【参数】

**low**：低优先级。

**medium**：中优先级。

**high**：高优先级。

【使用指导】

设置管道的优先级。优先级高的管道，就有更多可能借用上级节点的带宽。

【举例】

# 配置管道channel0的优先级为high。

host# configure terminal

host(config)# qos-profile channel channel0

host(config-qos-channel0)# priority high

### qos-profile channel

**qos-profile channe**命令用来创建管道，并进入管道节点视图，如果管道已经存在，则直接进入相应视图。

**no qos-profile channe**命令用来删除管道。

【命令】

**qos-profile channel** *channel-name* **parent** *parent-name*

**no qos-profile channel** *channel-name*

【视图】

系统视图

【参数】

*channel-name*：管道的名称。

*parent-name*：父管道或线路，首次创建线路的时候必填。

【使用指导】

首次创建管道的时候，需要填写父管道或者线路。

创建后，如果进入管道节点，则只需要填写管道名称。

父节点自动创建默认管道。

【举例】

# 创建管道channel0。

host# configure terminal

host(config)# qos-profile channel channel0 parent test

### schedule

**schedule**命令用来配置管道的生效时间。

【命令】

**schedule** *schedule-name*

【缺省情况】

缺省情况下，为永久生效。

【视图】

管道配置节点视图

【参数】

*schedule-name*：时间对象名称。

【举例】

# 配置管道channel0中perip的流量为2Mbps。

host# configure terminal

host(config)# schedule-day worktime

host(config-schedule-day)# periodic start 9:00 end 18:00

host(config)# qos-profile channel channel0

host(config-qos-channel0)# schedule worktime

## 白名单配置命令

### qos-profile white-list

**qos-profile white-list**命令用来配置流量限制白名单。

**no qos-profile white-list**命令用来删除流量限制白名单。

【命令】

**qos-profile white-list any any** *address-name***any** *user-name***any**

**no qos-profile white-list any any** *address-name* **any** *user-name* **any**

【视图】

系统视图

【参数】

*address-name*：地址对象名称。

*user-name*：用户对象名称。

【使用指导】

白名单可以直接将某些用户或地址排除在流量控制之外。

【举例】

# 配置地址对象为addr1的流量不进行流量管理。

host# configure terminal

host(config)# qos-profile white-list any any addr1 any any any

# 安全防护

## 异常报文攻击防护配置命令

### ip defend attack

**ip defend attack**命令用来配置异常报文攻击防护。

**no ip defend attack**命令用来删除异常报文攻击防护。

【命令】

**ip defend attack** { *winnuke | tear-drop | land-base | tcp-flag | smurf | ping-of-death | ip-option | ip\_spoof | jolt2*}

**no ip defend attack** { *winnuke | tear-drop | land-base | tcp-flag | smurf | ping-of-death | ip-option | ip\_spoof | jolt2*}

【视图】

系统视图

【参数】

*winnuke*：winnuke攻击。

*tear-drop*：tear-drop攻击。

*land-base*：land攻击。

*tcp-flag*：tcp flag攻击 。

*smurf*：smurf攻击。

*ping-of-death*：死亡之ping攻击。

*ip-option*：IP选项攻击。

*ip\_spoof*：ip地址欺骗。

*jolt2*：jolt2攻击。

【使用指导】

Ping-of-death： ping-of-death攻击是通过向目的主机发送长度超过65535的icmp报文，使目的主机发生处理异常而崩溃。配置了防ping-of-death攻击功能后，设备可以检测出ping-of-death攻击，丢弃攻击报文并根据配置输出告警日志信息。

Land-Base：land-base攻击通过向目的主机发送目的地址和源地址相同的报文，使目的主机消耗大量的系统资源，从而造成系统崩溃或死机。配置了防land-base攻击功能后，设备可以检测出land-base攻击，丢弃攻击报文并根据日志配置输出告警日志信息。

Tear-drop：tear-drop攻击通过向目的主机发送报文偏移重叠的分片报文，使目的主机发生处理异常而崩溃。配置了防tear-drop攻击功能后，设备可以检测出tear-drop攻击，并根据配置输出告警日志信息。因为正常报文传送也有可能出现报文重叠，因此设备不会丢弃该报文，而是采取裁减、重新组装报文的方式，发送出正常的报文。

Tcp flag：TCP 异常攻击防护功能开启后，默认情况下当安全网关发现受到TCP 异常攻击后，会丢弃攻击包，并根据配置输出告警日志。

winnuke：winnuke攻击通过向目的主机的139、138、137、113、53端口发送TCP紧急标识位URG为1的带外数据报文，使系统处理异常而崩溃。配置了防winnuke攻击功能后，可以检测出winnuke攻击报文，并根据配置输出告警日志信息。

Smurf：这种攻击方法结合使用了IP欺骗和ICMP回复方法使大量网络传输充斥目标系统，引起目标系统拒绝为正常系统进行服务。Smurf攻击通过使用将回复地址设置成受害网络的广播地址的ICMP应答请求(PING)数据包，来淹没受害主机，最终导致该网络的所有主机都对此ICMP应答请求做出答复，导致网络阻塞。

Ip-spoof：防护IP地址欺骗攻击，暂时用反向路由检测来实现，如果反向路由不存在或者反向路由查询结果是存在，但是该IP 为目的地址的数据包离开设备的接口和收到报文的接口不一致，则认为是攻击。

jolt2：jolt2攻击通过向目的主机发送报文偏移加上报文长度超过65535的报文，使目的主机处理异常而崩溃。

【举例】

# 配置tcp-flag安全防护。

host# configure termina

host(config)# ip defend attack tcp-flag

### ip defend attack log

**ip defend attack log**命令用来开启或关闭异常报文攻击防护日志。

【命令】

**ip defend attack log** { **enable** | **disable** }

【缺省情况】

缺省情况下，关闭异常报文攻击防护日志。

【视图】

系统视图

【参数】

**enable**：开启防护日志功能。

**disable**：关闭防护日志功能。

【举例】

# 开启安全防护日志功能。

host# configure termina

host(config)# ip defend attack log enable

## 扫描攻击防护配置命令

ip defend ip-sweep interface

**ip defend ip-sweep interface**命令用来配置IP扫描功能。

**no ip defend ip-sweep interface**命令用来删除IP扫描功能。

【命令】

**ip defend ip-sweep interface** *interface-name* **threshold** *threshold* [ **block-time** *time-value* ]

**no ip defend ip-sweep interface** *interface-name*

【视图】

系统视图

【参数】

*interface-name*：接口名称。

*threshold*：扫描阈值，单位(ms）。

*time-value*：阻断时长，单位（s）。

【使用指导】

IP地址扫描是指 一个源 IP 地址在规定的时间间隔 ( 缺省值为 10毫秒 ) 内将 10 个 ICMP报文发给不同的主机时，即进行了一次地址扫描。【举例】

# 在接口ge0上配置IP址扫描，阈值是10毫秒，且阻断200秒。

host# configure termina

host(config)# ip defend ip-sweep interface ge0 threshold 10 block-time 200

### ip defend port-scan interface

**ip defend port-scan interface**命令用来配置端口扫描。

**no ip defend port-scan interface**命令用来删除端口扫描。

【命令】

**ip defend port-scan interface** *interface-name* **threshold** *threshold* [ **block-time** *time-value* ]

**no ip defend port-scan interface** *interface-name*

【视图】

系统视图

【参数】

*interface-name*：接口名称。

*threshold*：扫描阈值，取值范围10～5000，单位(ms）。

*time-value*：阻断时长，取值范围1～600，单位（s）。

【使用指导】

端口扫描是指当一个源 IP 地址在规定的时间间隔内 (缺省值为 10毫秒 ) 将含有 TCP SYN 片段的 IP 报文或UDP报文发送给位于相同目标 IP 地址的 10 个不同端口时，即进行了一次端口扫描。

【举例】

# 在接口ge0上配置端口扫描，阈值是10毫秒，且阻断200秒。

host# configure termina

host(config)# ip defend port-scan interface ge0 threshold 10 block-time 200

### ip defend scan log

**ip defend scan log**命令用来开启或关闭扫描攻击防护日志。

【命令】

**ip defend attack log** { **enable** | **disable** }

【缺省情况】

缺省情况下，关闭扫描攻击防护日志。

【视图】

系统视图

【参数】

**enable**：开启防护扫描日志功能。

**disable**：关闭防护扫描日志功能。

【举例】

# 开启扫描攻击防护日志功能。

host# configure termina

host(config)# ip defend scan log enable

## flood攻击配置命令

### ip defend

**ip defend** 命令用来配置基于目的地址的Flood攻击。

**no ip defend** 命令用来删除基于目的地址的Flood攻击。

【命令】

**ip defend** { **synflood** | **udpflood** | **icmpflood** | **dnsflood** } **startip** *start-ip* **endip** *end-ip* **threshold** *threshold*

**no ip defend** { **synflood** | **udpflood** | **icmpflood** | **dnsflood** } **startip** *start-ip* **endip** *end-ip*

【视图】

系统视图

【参数】

**synflood**：synflood攻击。

**udpflood**：udpflood攻击。

**icmpflood**：icmpflood攻击。

**dnsflood**：dnsflood攻击。

*start-ip*：开始IP地址。

*end-ip*：结束IP地址。

*threshold*：阈值，取值范围1～100000，单位(连接数/秒)。

【举例】

# 对开始IP地址192.168.10.1和结束IP地址192.68.10.230网段配置防synflood攻击，阈值是100个连接每秒。

host# configure termina

host(config)# ip defend synflood startip 192.168.10.1 end-ip 192.168.10.230 threshold 100

ip defend flood log

**ip defend flood log**命令用来开启或关闭flood攻击防护日志。

【命令】

**ip defend flood log { enable | disable }**

【缺省情况】

缺省情况下，关闭flood攻击防护日志。

【视图】

系统视图

【参数】

**enable**：开启flood攻击日志功能。

**disable**：关闭flood攻击日志功能。

【举例】

# 开启flood攻击防护日志功能。

host# configure termina

host(config)# ip defend flood log enable

### ip defend { synflood | udpflood | icmpflood | dnsflood } interface

ip defend { synflood | udpflood | icmpflood | dnsflood } interface命令用来配置基于接口的Flood攻击。

no ip defend { synflood | udpflood | icmpflood | dnsflood } interface命令用来删除基于接口的Flood攻击。

【命令】

ip defend { synflood | udpflood | icmpflood | dnsflood } interface *interface-name* { source | destination } *threshold*

no ip defend { synflood | udpflood | icmpflood | dnsflood } interface *interface-name* { source | destination }

【视图】

系统视图

【参数】

synflood：synflood攻击。

udpflood：udpflood攻击。

icmpflood：icmpflood攻击。

dnsflood：dnsflood攻击。

*interface-name*：接口名称。

source：基于源地址的flood攻击。

destination：基于目的地址的flood攻击。

*threshold*：阈值，取值范围1～100000，单位(连接数/秒)。

【举例】

# 在ge0口配置源地址的synflood攻击，阈值是100个连接每秒。

host# configure termina

host(config)# ip defend synflood interface ge0 source threshold 100

## IPMAC绑定配置命令

### ipmac

**ipmac**命令用来配置IPMAC邦定功能。

**no ipmac**命令用来删除IPMAC邦定功能。

【命令】

**ipmac** *name ip-address mac-address* { **unique-ip** |**multi-ip** }

**no ipmac** *ip-address*

【视图】

系统视图

【参数】

**enable**：开启防护日志功能。

**disable**：关闭防护日志功能。

*name*：对象名称。

*ip-address*：IP地址。

*mac-address*：MAC地址。

**unique-ip**：绑定类型，指一个mac和一个ip地址唯一对应。

**multi-ip**：绑定类型，指一个mac地址和多个ip地址对应。

【举例】

# 配置IP地址192.168.1.1与MAC地址00:00:00:11:11:11的唯一绑定名称为abc。

host# configure termina

host(config)# ipmac abc 192.168.1.1 00:00:00:11:11:11 unique-ip

### ipmac log

**ipmac log**命令用来开启或关闭IPMAC绑定日志。

【命令】

**ipmac log** { **enable** | **disable** }

【缺省情况】

缺省情况下，关闭IPMAC绑定日志。

【视图】

系统视图

【参数】

**enable**：开启绑定日志功能。

**disable**：关闭绑定日志功能。

【举例】

# 开启IPMAC绑定日志功能。

host# configure termina

host(config)# ipmac log enable

## 防arp攻击配置命令

### anti-arp broadcast

**anti-arp broadcast**命令用来开启或关闭ARP主动保护发包功能。

【命令】

**anti-arp broadcast** { *enable | disable* }

【缺省情况】

缺省情况下，关闭ARP主动保护发包功能。

【视图】

系统视图

【参数】

**enable**：开启ARP主动保护发包功能。

**disable**：关闭ARP主动保护发包功能。

【举例】

# 开启ARP主动保护发包功能。

host# configure termina

host(config)# anti-arp broadcast enable

### anti-arp broadcast interface

**anti-arp broadcast interface** 命令用来来添加ARP主动列表。

**no anti-arp broadcast interface**命令用来删除ARP主动列表。

【命令】

**anti-arp broadcast interface** *interface-name* [**list** *ip-address mac-address* ]

**no anti-arp broadcast interface** *interface-nane* [ **list** *ip-address mac-address* ]

【视图】

系统视图

【参数】

*interface-name*：接口名称。

*ip-address*：IP地址。

*mac-address*：MAC地址。

【使用指导】

开启接口保护后，会根据主动保护开关和主动保护发包间隔发送接口对应的IP和MAC地址的免费ARP。

【举例】

# 在ge0端口上添加IP1.1.1.1和MAC地址00:0a:0b:ac:01:11的主动保护功能。

host# configure termina

host(config)# anti-arp broadcast interface ge0 list 1.1.1.1 00:0a:0b:ac:01:11

### anti-arp broadcast interval

**anti-arp broadcast interval** 命令用来设置主动保护发包间隔。

【命令】

**anti-arp broadcast interval** *threshold*

【视图】

系统视图

【参数】

*threshold*：发包间隔，取值范围1～10，单位(s)。

【举例】

# 设置ARP主动保护的发包间隔为5s。

host# configure termina

host(config)# anti-arp broadcast interval 5

### anti-arp flood

**anti-arp flood**命令用来开启或关闭ARP flood功能。

【命令】

**anti-arp flood** { *enable | disable* }

【缺省情况】

缺省情况下，关闭ARP flood功能。

【视图】

系统视图

【参数】

**enable**：开启ARP flood功能。

**disable**：关闭ARP flood学习功能。

【举例】

# 开启ARP flood功能。

host# configure termina

host(config)# anti-arp flood enable

### anti-arp flood block-time

**anti-arp flood block-time**命令用来设置ARP Flood的阻断时长。

**no anti-arp flood block-time**命令用来取消ARP Flood的阻断时长。

【命令】

**anti-arp flood block-time** *threshold*

**no anti-arp flood block-time**

【缺省情况】

缺省情况下，ARP Flood阻断时长为60s。

【视图】

系统视图

【参数】

*threshold*：阻断时长，取值范围1～65535，单位（s）。

【举例】

# 设置ARP Flood阻断时长500s。

host# configure termina

host(config)# anti-arp flood block-time 500

### anti-arp flood threshold

**anti-arp flood threshold**命令用来设置ARP Flood的阈值。

**no anti-arp flood threshold**命令用来取消ARP Flood的阈值。

【命令】

**anti-arp flood threshold** *threshold*

**no anti-arp flood threshold**

【视图】

系统视图

【参数】

*threshold*：1秒钟内接受到的ARP数据包数量，默认值是300。

【举例】

# 设置ARP Flood阈值为500。

host# configure termina

host(config)# anti-arp flood threshold 500

### anti-arp learning-arp

**anti-arp learning-arp**命令用来开启或关闭ARP学习功能。

【命令】

**anti-arp learning-arp** {**enable**|**disable** }

【缺省情况】

缺省情况下，关闭ARP学习功能。

【视图】

系统视图

【参数】

**enable**：开启ARP学习功能。

**disable**：关闭ARP学习功能。

【使用指导】

关闭了ARP学习后，任何报文只要不匹配IP-MAC绑定表，都将被丢弃，因此强烈建议在关闭此功能前一定要先绑定需要使用的IP-MAC。

【举例】

# 开启ARP主动学习功能。

host# configure termina

host(config)# anti-arp learning-arp enable

### anti-arp spoof

**anti-arp spoof**命令用来开启或关闭 ARP攻击防御功能。

【命令】

**anti-arp spoof** {**enable**|**disable** }

【缺省情况】

缺省情况下，关闭 ARP攻击防御功能。

【视图】

系统视图

【参数】

**enable**：开启ARP攻击防御功能。

**disable**：关闭ARP攻击防御功能。

【使用指导】

只有选择启用ARP防欺骗攻击后才能启用主动保护和ARP学习功能。

【举例】

# 开启ARP攻击防御功能。

host# configure termina

host(config)# anti-arp spoof enable

## 黑名单配置命令

### blist add

**blist add**命令用来黑名单配置。

【命令】

**blist add** *ip-address* **age** { **300** | **600** | **900** | **1800** | **3600** | **7200** | **14400** | **28800** | **86400** | **forever** }

【视图】

系统视图

【参数】

*ip-address*：主机IP地址。

**300**：老化时间为300秒。

**600**：老化时间为600秒。

**900**：老化时间为900秒。

**1800**：老化时间为1800秒。

**3600**：老化时间为3600秒。

**7200**：老化时间为7200秒。

**14400**：老化时间为14400秒。

**28800**：老化时间为28800秒。

**86400**：老化时间为86400秒。

**forever**：永久不老化。

【使用指导】

通过配置黑名单功能可以对来自指定IP地址的报文进行过滤，黑名单表项除了可以手工添加之外，还可以通过扫描攻击自动添加。

【举例】

# 将IP址1.1.1.1加入黑名单，加入时长设置为永久。

host# configure termina

host(config)# blist add A.B.C.D age forever

### show blist

**show blist**命令用来显示黑名单信息。

【命令】

**show blist**

【视图】

任意视图

【举例】

# 显示系统的黑名单信息。

host# show blist

IP address age leftTime reason

1.1.1.1 forever forever manual

表 16-1 show blist命令显示信息描述表

| 字段 | 描述 |
| --- | --- |
| IP address | 加入黑名单的IP地址 |
| age | 老化时间 |
| leftage | 剩余时间 |
| reason | 加入黑名单的方式：有manual和auto两种方式，manual代表认为加入，auto代表自动加入 |

# 会话限制

## 会话限制配置命令

### ip connection limit

**ip connection limi**t命令用来限制设备的会话连接数。

**no ip connection limit**命令用来取消设备的会话连接数限制。

【命令】

**ip connection limit** *user-name* **total** *limit-num* **per\_second** *limit-num*

**no ip connection limit** *user-name*

【缺省情况】

缺省情况下，未配置会话限制。

【视图】

系统视图

【参数】

*user-name*：用户对象名称。

*limit-num*：每一个IP能存在的总会话数，范围为0～10000000，0为不限制。

*limit-num*：每一个IP每秒能新建的会话数，范围为0～10000000，0为不限制。

【举例】

# 限制用户组any内的所有IP，会话连接数为10，每秒能新建的会话连接数为10。

* host# configure termina
* host(config)# ip connection limit any total 10 per\_second 10

### show ip connection limit config

**show ip connection limit config**命令用来查看配置了会话数限制的用户以及配置的值。

【命令】

**show ip connection limit config**

【视图】

任意视图

【举例】

# 显示配置的会话数限制。

host# show ip connection limit config

user-name limit-count second-count

any 10 10

表 17-1 show ip connection limit config命令显示信息描述表

| 字段 | 描述 |
| --- | --- |
| user-name | 用户对象名称 |
| limit-count | 设置的会话最大连接数 |
| second-count | 每秒新建会话连接数 |

### show ip connection statistics

**show ip connection statistics**命令用来查看当前的会话数统计。

【命令】

**show ip connection statistics** [ *ip-address* ]

【视图】

任意视图

【参数】

*ip-address*：指定的IP的会话数，如果不指定，则统计所有IP的会话数。

【举例】

# 显示会话统计。

host# show ip connection statistics

source-ip count

192.168.1.73 7

192.168.1.76 4

表 17-2 show ip connection statistics命令显示信息描述表

| 字段 | 描述 |
| --- | --- |
| source-ip | 统计的IP地址 |
| count | 当前的会话连接数 |

### show ip connection limit

**show ip connection limit**命令用来查看当前被限制的IP地址，以及这些IP地址被限制的情况。

【命令】

**show ip connection limit**

【视图】

任意视图

【举例】

# 显示设备上被限制的IP地址信息。

host# show ip connection limit

ip index limit-count second-index second-limit block-index

192.168.1.53 1 10 0 10 0

192.168.1.65 1 10 0 10 0

表 17-3 show ip connection limit命令显示信息描述表

| 字段 | 描述 |
| --- | --- |
| ip | 统计的IP地址 |
| index | 该IP现有的会话数 |
| limit-count | 该IP能存在的最大会话数 |
| second-index | 该IP当前新建的会话数 |
| second-limit | 该IP每秒能新建的最大会话数 |
| block-index | 该IP由于会话限制丢弃的会话数 |

# CA中心命令

## CA中心命令

### pki ca crl export tftp

**pki ca crl export tftp**命令用来通过TFTP协议将CRL文件导出至TFTP服务器。

【命令】

**pki ca crl export tftp** *ip-address*

【视图】

用户视图

【参数】

*ip-address*：TFTP服务器地址。

【举例】

# 导出CRL文件至TFT服务器。

host# pki ca crl export tftp 192.168.1.105

Upload file test\_ca.crl ....

Upload file(test\_ca.crl) success.

【相关命令】

* show pki ca crl

### pki ca crl generate

**pki ca crl generate**命令用来根据CA根证书生成CRL文件。

【命令】

**pki ca crl generate**

【视图】

用户视图

【使用指导】

设备上需要存在CA根证书。

当需要立即生成与CA根证书对应的CRL文件时，执行此命令。

【举例】

# 立即更新CRL文件。

host# pki ca crl generate

【相关命令】

* show pki ca crl

### pki ca crl update-period

**pki ca crl update-period**命令用来配置CRL文件自动更新的间隔时间。

【命令】

**pki ca crl update-period** *interval-time***<1-30>**

【缺省情况】

缺省情况下，CRL自动更新的间隔时间为30天。

【视图】

系统视图

【参数】

*interval-time*：CRL文件自动更新的间隔时间。取值范围为1～30天。默认为30天。

【使用指导】

当需要立即更新CRL文件时，请执行**pki ca crl generate**命令。

【举例】

# 配置CRL文件自动更新周期为10天。

host# configure terminal

host(config)# pki ca crl update-period 10

【相关命令】

* show pki ca crl

### pki ca root-certificate cert\_key import tftp

**pki ca root-certificate cert\_key import tftp**命令用来通过TFTP服务器导入证书密钥分离格式的CA根证书。

【命令】

**pki ca root-certificate cert\_key import tftp** *ip-address* *certificate* *keyfile* [ *password* ]

【缺省情况】

缺省情况下，没有配置CA根证书。

【视图】

用户视图

【参数】

*ip-address*：TFTP服务器IP地址。

*certificate*：导入的CA根证书的名称。名称最长不超过63个字符，名称中不能带“()”，支持“.cer”格式。

*keyfile*：导入的CA根证书的密钥文件名称。名称最长不超过63个字符，名称中不能带“()”，仅支持“.key”格式。

*password*：证书的保护密码。不超过63个字符。

【使用指导】

导入时，TFTP服务器上需要有相应的导入证书才可导入。

导入证书成功后，会删除原有的CA根证书。

【举例】

# 导入一个CA根证书。

host# pki ca root-certificate pkcs12 import tftp 192.168.1.2 test\_ca.cer test\_ca.key

This new CA certificate will replace the old one? Please enter "y/n" to confirm: y

Download file test\_ca.cer ....

Download file(test\_ca.cer) success.

Download file test\_ca.key ....

Download file(test\_ca.key) success.

【相关命令】

* show pki ca root-certificate

### pki ca root-certificate export tftp

**pki ca root-certificate export tftp**命令用来通过TFTP协议将CA根证书导出到TFTP服务器。

【命令】

**pki ca root-certificate export tftp** *ip-address*{ **pem** | **p12** }

【视图】

用户视图

【参数】

*ip-address*：TFTP服务器IP地址。

**pem**：导出证书为密钥证书分离格式。

**p12**：导出证书为单个文件格式。

【使用指导】

导出时需要TFTP服务器网络可达。

导出时需要设备上存在CA根证书。

【举例】

# 导出CA根证书至TFTP服务器。

host# pki ca root-certificate export tftp 192.168.1.10 p12

Upload file test\_ca.p12 ....

Upload file(test\_ca.p12) success.

【相关命令】

* show pki ca root-certificate

### pki ca root-certificate pkcs12 import tftp

**pki ca root-certificate pkcs12 import tftp**命令用来通过TFTP服务器导入PKCS12格式的CA根证书。

【命令】

**pki ca root-certificate pkcs12 import tftp** *ip-address**certificate*  [*password*]

【缺省情况】

缺省情况下，没有配置CA根证书。

【视图】

用户视图

【参数】

*ip-address：*TFTP服务器的IP地址。

*certificate：*导入的证书名称，名称最长不超过63个字符，名称中不能带“()”，支持“.p12”格式。

*password：*证书的保护密码。最多可输入63个字符。

【使用指导】

导入时，TFTP服务器上需要有相应的导入证书才可导入。

导入证书成功后，会删除原有的CA根证书。

【举例】

# 导入一个CA根证书。

host# pki ca root-certificate pkcs12 import tftp 192.168.1.2 test\_ca.p12 1

This new CA certificate will replace the old one? Please enter "y/n" to confirm: y

Download file test\_ca.p12 ....

Download file(test\_ca.p12) success.

【相关命令】

* show pki ca root-certificate

### show pki ca crl

**show pki ca crl**命令用来显示CRL文件的内容。

【命令】

**show pki ca crl**

【视图】

用户视图

【举例】

# 显示CRL文件内容。

host# show pki ca crl

Certificate Revocation List (CRL):

Version 2 (0x1)

Signature Algorithm: sha1WithRSAEncryption

Issuer: /C=CN/O=OR/ST=PRO/CN=test\_ca/L=LOCATION/OU=DE

Last Update: Jun 24 09:37:25 2014 GMT

Next Update: Jul 24 09:37:25 2014 GMT

CRL extensions:

X509v3 CRL Number:

1

X509v3 Authority Key Identifier:

DirName:/C=CN/O=OR/ST=PRO/CN=test\_ca/L=LOCATION/OU=DE

serial:D5:1E:36:4F:B1:E6:55:A8

Revoked Certificates:

Serial Number: 93094F4168DF73AC

Revocation Date: Jun 24 09:35:22 2014 GMT

CRL entry extensions:

X509v3 CRL Reason Code:

Key Compromise

Serial Number: D6A57BF1F6EA3873

Revocation Date: Jun 24 09:35:52 2014 GMT

CRL entry extensions:

X509v3 CRL Reason Code:

CA Compromise

Serial Number: D1FA7F2CB225F633

Revocation Date: Jun 24 09:37:25 2014 GMT

CRL entry extensions:

X509v3 CRL Reason Code:

Unspecified

Signature Algorithm: sha1WithRSAEncryption

ab:4c:26:83:fe:42:26:91:61:1d:8b:ee:b9:de:27:5a:84:f1:

0f:b0:bb:d2:e2:80:50:75:d1:20:7c:54:e0:de:59:76:cd:07:

44:49:b8:07:00:31:c3:7c:74:a1:b1:4c:b1:81:94:da:40:d1:

d4:60:ba:3d:2b:ee:96:dd:58:15:db:0c:cd:e7:d4:ff:19:ae:

73:77:82:10:20:0f:13:7b:ed:97:88:43:3a:06:a0:af:3c:67:

93:82:4d:1e:d9:71:02:3e:59:9d:04:01:3a:ac:ce:68:52:70:

7a:ca:da:cb:b1:5c:f3:9e:8a:af:de:b4:72:07:0b:9e:ef:8f:

8b:c9

### show pki ca root-certificate

**show pki ca root-certificate**命令用来显示CA根证书的内容。

【命令】

**show pki ca root-certificate**

【视图】

用户视图

【使用指导】

仅当CA根证书存在的情况下，才能显示出CA根证书的内容。

【举例】

# 显示CA根证书的内容。

host# show pki ca root-certificate

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 15356771495294948776 (0xd51e364fb1e655a8)

Signature Algorithm: sha1WithRSAEncryption

Issuer: C=CN, O=OR, ST=PRO, CN=test\_ca, L=LOCATION, OU=DE

Validity

Not Before: Jun 20 03:16:47 2014 GMT

Not After : Jul 10 03:16:47 2014 GMT

Subject: C=CN, O=OR, ST=PRO, CN=test\_ca, L=LOCATION, OU=DE

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (1024 bit)

Modulus:

00:c9:db:1e:45:66:2d:b5:6c:06:a0:79:62:4d:6c:

ce:92:4b:16:89:3b:5a:0a:62:b7:d6:7b:68:ab:f8:

ac:1c:3d:04:2f:0f:7f:fa:9a:69:4e:09:8f:9d:e2:

a1:35:67:44:58:c5:8d:14:fa:36:6f:c5:0f:b3:9b:

01:7e:1d:00:dc:44:ad:4a:34:16:1f:e9:af:1d:62:

6a:68:cb:e1:d9:30:e7:e2:0e:59:e7:ed:48:3d:83:

75:4e:12:df:90:35:0d:22:5c:7a:35:69:f7:33:ab:

39:58:68:ae:d7:71:55:65:36:53:f1:b4:09:3f:71:

c1:c0:66:0d:19:a2:e1:69:eb

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Basic Constraints: critical

CA:TRUE

X509v3 Key Usage: critical

Digital Signature, Certificate Sign, CRL Sign

Signature Algorithm: sha1WithRSAEncryption

2d:cb:0a:a8:d5:20:c7:f9:94:16:20:14:48:8d:26:40:ac:01:

8e:e1:42:f6:17:28:48:7a:56:d5:67:24:81:60:5e:e4:60:46:

13:64:5b:8b:f1:87:b1:f1:04:3e:63:7f:eb:79:61:43:91:1f:

06:0f:b5:e7:a5:d4:04:be:6a:93:46:70:90:c4:af:a5:61:67:

9d:1b:b1:39:e0:ca:17:58:3e:33:3b:48:71:80:dd:23:9b:94:

34:f7:6b:6b:60:ee:fd:cc:dc:61:63:c5:c1:52:37:95:05:b1:

d8:14:85:65:8a:71:61:f4:19:9f:66:fd:39:de:a5:a7:c0:d4:

88:d0

### show running-config pki

**show running-config pki**命令用来显示CA中心的配置。

【命令】

**show running-config pki**

【视图】

用户视图

【举例】

# 显示CA中心的配置。

host# show running-config pki

pki ca crl update-period 30

!

## 用户证书命令

### no pki ca user-certificate

**no pki ca user-certificate**命令用来删除设备上的用户证书。

【命令】

**no pki ca user-certificate** *certificate*

【视图】

用户视图

【参数】

*certificate*：需要被删除的证书名称。

【使用指导】

删除证书后，签发撤销记录中也将删除该证书的记录。

删除的证书必须是设备上存在的证书。

【举例】

# 删除一个证书。

host# no pki ca user-certificate test.cer

【相关命令】

* show pki ca user-certificate

### pki ca user-certificate copy

**pki ca user-certificate copy**命令用来将指定的用户证书拷贝到本地证书中的用户证书。

【命令】

**pki ca user-certificate copy** *certificate*

【视图】

用户视图

【参数】

*certificate*：用户证书的名称。

【使用指导】

拷贝的证书必须是设备上存在的证书。

【举例】

# 拷贝一个证书到本地证书中的用户证书。

host# pki ca user-certificate copy test.cer

### pki ca user-certificate export tftp

**pki ca user-certificate export tftp**命令用来通过TFTP协议导出用户证书。

【命令】

**pki ca user-certificate export tftp** *ip-address**certificate*{ **p12** | **pem** }

【视图】

用户视图

【参数】

*ip-address*：TFTP服务器的地址。

*certificate*：被导出的证书的名称。

**p12**：导出为PKCS12格式的证书。

**pem**：导出为PEM格式的证书。

【使用指导】

导出的证书仅为设备上存在的用户证书。

【举例】

# 导出一个用户证书。

host# pki ca user-certificate export tftp 192.168.1.105 test.cer p12

Upload file test.p12 ....

Upload file(test.p12) success.

【相关命令】

* show pki ca user-certificate

### pki ca user-certificate revoke

**pki ca user-certificate revoke**命令用来撤销已签发的用户证书。

【命令】

**pki ca user-certificate revoke** *certificate* **reason** { **Unspecified** | **KeyCompromise** | **CaCompromise** | **Affiliation Changed** }

【视图】

用户视图

【参数】

*certificate*：需要被撤销的用户证书的名称。

**Unspecified**：撤销原因为未指定。

**KeyCompromise**：撤销原因为私钥泄露。

**CaCompromise**：撤销原因为CA证书泄露。

**Affiliation Changed**：撤销原因为从属关系改变。

【使用指导】

能被撤销的用户证书，仅为已签发的用户证书。

撤消后，用户证书将不再为有效证书。

撤销的证书必须是设备上存在的证书。

【举例】

# 撤销一个用户证书。

host# pki ca user-certificate revoke test.cer reason KeyCompromise

【相关命令】

* show pki ca user-certificate

### pki ca user-certificate sign

**pki ca user-certificate sign**命令用来签发用户证书。

【命令】

**pki ca user-certificate sign** *certificate* **days** *days* **password** *password*

【缺省情况】

缺省情况下，没有用户证书请求，不能进行用户证书的签发。

【视图】

用户视图

【参数】

*certificate*：需要被签发的用户证书的名称。

*days*：被签发的用户证书的有效期。取值范围为1～65535天。

*password*：签发的用户证书的保护密码。最多可为63个字符。

【使用指导】

用户请求证书只可以在WEB页面中创建，命令行下仅可以进行签发。

被签发的用户请求证书，仅为已创建的用户请求证书。

【举例】

# 签发用户请求证书test.csr。

host# pki ca user-certificate sign test.csr days 10 password 1

【相关命令】

* show pki ca user-certificate

### show pki ca user-certificate

**show pki ca user-certificate**命令用来显示所有的用户证书或者指定用户证书的详细内容。

【命令】

**show pki ca user-certificate** [*certificate*]

【视图】

用户视图

【参数】

*certificate*：用户证书的名称。

【使用指导】

当指定某一存在的用户证书时，将显示该证书的详细内容。

当不指定用户证书时，将显示设备上所有的用户证书的简略信息。

【举例】

# 显示所有的用户证书。

host# show pki ca user-certificate

Name version location status reference subject

----------------------------------------------------------------------------------------

test.cer 3 Local Certificate 0 C=CN,CN=test

----------------------------------------------------------------------------------------

Total file: 1; Local certificate file: 1; Local certificate request file: 0

#显示一个用户证书的详细内容。

host# show pki ca user-certificate test.cer

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 12580604629034846311 (0xae9749415541c867)

Signature Algorithm: sha1WithRSAEncryption

Issuer: C=CN, O=OR, ST=PRO, CN=test\_ca, L=LOCATION, OU=DE

Validity

Not Before: Jul 5 03:00:03 2014 GMT

Not After : Jul 15 03:00:03 2014 GMT

Subject: C=CN, CN=test

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (1024 bit)

Modulus:

00:c2:27:5a:cd:42:40:ab:b1:bc:10:6c:10:6c:2b:

80:f1:75:11:43:c7:ee:3b:91:c3:7d:c7:ea:ca:96:

f8:4b:5d:5f:f2:ed:c3:24:23:40:a4:ee:e2:83:07:

11:db:6a:dd:a6:1d:a6:5a:5f:9c:ec:14:70:a9:63:

9a:ba:88:7e:54:98:c5:ca:5d:65:11:c1:f0:90:95:

f8:05:29:b2:c1:32:88:06:8f:76:1c:fc:f2:53:36:

a9:fe:13:08:c7:e8:dd:31:e9:00:cf:f2:32:fb:3b:

4c:9f:19:3d:61:5d:49:b9:3b:72:4c:9c:30:f9:e9:

82:16:27:25:29:87:e5:d6:3f

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Key Usage:

Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment

X509v3 Extended Key Usage:

TLS Web Server Authentication, TLS Web Client Authentication, E-mail Protection, Code Signing, Microsoft Server Gated Crypto, OCSP Signing, Time Stamping, dvcs

Signature Algorithm: sha1WithRSAEncryption

4a:f6:d4:fd:33:26:20:7c:79:da:19:2a:f6:58:bf:65:44:4a:

d2:50:59:be:52:0f:26:03:14:2e:e3:11:a7:21:9a:04:96:0a:

93:de:8b:54:a2:b8:b7:69:2f:60:ef:96:d1:7a:a3:4d:e0:4b:

46:f3:86:2b:8e:84:39:8d:96:9e:d6:68:21:04:b2:ad:90:2d:

08:ee:16:7d:85:eb:17:df:e0:f3:74:8e:74:0e:9b:9c:f0:14:

27:b0:ad:72:84:a6:de:ed:c0:a1:5d:45:a5:e2:38:ea:c9:ae:

de:18:0f:cd:bb:9f:5e:c5:e1:1b:e9:9a:4c:6e:4d:83:55:cf:

17:14

表 18-1 显示用户证书信息命令显示信息描述表

| 字段 | 描述 |
| --- | --- |
| Name | 用户证书的名称 |
| version | 证书版本信息 |
| location | 证书位置信息 |
| status | 证书状态，有Requset、Certificate、Revoked状态 |
| reference | 证书被引用次数 |
| subject | 主题信息 |
| Requset | 请求证书状态 |
| Certificate | 已签发的证书状态 |
| Revoked | 已撤销的证书状态 |

# 证书命令

## 本地证书命令

### no pki local certificate

**no pki local certificate**命令用来删除指定的用户证书。

【命令】

**no pki local certificate** *certificate*

【视图】

用户视图

【参数】

*certificate*：被删除的用户证书的名称。

【使用指导】

被删除的证书需要是在设备上存在的证书。

【举例】

# 删除一个用户证书。

host# no pki local certificate test.cer

【相关命令】

* show pki local certificate

### pki local certificate cert\_key import tftp

**pki local certificate cert\_key import tftp**命令用来通过TFTP协议导入证书密钥分离格式的用户证书。

【命令】

**pki local certificate cert\_key import tftp** *ip-address certificate keyfile*[*password*]

【缺省情况】

缺省情况下，没有配置任何用户证书。

【视图】

用户视图

【参数】

*ip-address*：TFTP服务器IP地址。

*certificate*：导入的CA根证书的名称。名称最长不超过63个字符，名称中不能带“()”，支持“.cer”格式。

*keyfile*：导入的CA根证书的密钥文件名称。名称最长不超过63个字符，名称中不能带“()”，仅支持“.key”格式。

*password*：证书的保护密码。不超过63个字符。

【使用指导】

导入时，TFTP服务器上需要有相应的导入证书才可导入。

【举例】

# 导入一个用户证书。

host# pki ca root-certificate pkcs12 import tftp 192.168.1.2 test.cer test.key

Download file test.cer ....

Download file(test.cer) success.

Download file test.key ....

Download file(test.key) success.

【相关命令】

* show pki local certificate

### pki local certificate export tftp

**pki local certificate export tftp**命令用来通过TFTP协议导出用户证书至TFTP服务器。

【命令】

**pki local certificate export tftp** *ip-address certificate*{ **p12** | **pem** }[*password*]

【视图】

用户视图

【参数】

*ip-address*：TFTP服务器IP地址。

*certificate*：导出证书的名称。

**pem**：导出证书为密钥证书分离格式。

**p12**：导出证书为单个文件格式。

*password*：导出证书为p12格式时的保护密码，与生成证书时的保护密码相同。

【使用指导】

导出时需要TFTP服务器网络可达。

导出时需要设备上存在相应的用户证书。

【举例】

# 导出用户证书至TFTP服务器。

host# pki local certificate export tftp 192.168.1.105 test.cer p12 1

Upload file test\_ca.p12 ....

Upload file(test\_ca.p12) success.

【相关命令】

* show pki local certificate

### pki local certificate pkcs12 import tftp

**pki local certificate pkcs12 import tftp**命令用来通过TFTP协议导入PKCS12格式的用户证书。

【命令】

**pki local certificate pkcs12 import tftp** *ip-address certificate*[ *password* ]

【缺省情况】

缺省情况下，没有配置任何用户证书。

【视图】

用户视图

【参数】

*ip-address：*TFTP服务器的IP地址。

*certificate：*导入的证书名称，名称最长不超过63个字符，名称中不能带“()”，支持“.p12”格式。

*password：*证书的保护密码。最多可输入63个字符。

【举例】

# 导入一个用户证书。

host# pki local certificate pkcs12 import tftp 192.168.1.105 test.p12 1

Download file test.p12 ....

Download file(test.p12) fail.

【相关命令】

* show pki local certificate

### show pki local certificate

**show pki local certificate**命令用来显示所有用户证书的概略信息，或者指定证书的详细信息。

【命令】

**show pki local certificate** [*certificate* ]

【视图】

用户视图

【参数】

*certificate*：要显示的用户证书的名称。

【举例】

# 显示所有用户证书的概略信息。

host# show pki local certificate

Name version location status reference subject

----------------------------------------------------------------------------------------

test.cer 3 Local Certificate 0 C=CN,CN=test

----------------------------------------------------------------------------------------

Total file: 1; Local certificate file: 1; Local certificate request file: 0

# 显示指定证书的详细内容。

host# show pki local certificate test.cer

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 11411664746016242959 (0x9e5e609ffa257d0f)

Signature Algorithm: sha1WithRSAEncryption

Issuer: C=CN, O=OR, ST=PRO, CN=test\_ca, L=LOCATION, OU=DE

Validity

Not Before: Jul 5 05:39:09 2014 GMT

Not After : Jul 15 05:39:09 2014 GMT

Subject: C=CN, CN=test

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (1024 bit)

Modulus:

00:bd:6c:aa:56:4f:ab:c6:62:d5:f8:77:9b:66:86:

71:30:11:6c:73:b6:96:54:d6:eb:d3:7f:87:97:10:

03:30:87:76:86:95:78:4b:25:a8:eb:34:49:8b:ab:

0d:f2:c1:19:7c:99:a4:55:5b:53:4e:ce:98:a9:90:

4a:89:8c:61:f0:7a:16:3a:0b:32:1d:c0:29:20:91:

94:e8:5f:eb:ab:89:17:ae:9b:c6:bf:6c:76:db:b6:

05:80:2a:d3:7b:3e:30:d4:f7:65:49:8a:c5:b8:02:

f9:b3:60:08:6a:41:a2:88:6a:6e:2c:d6:74:ca:82:

b1:44:12:2e:c5:94:b9:3e:a5

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Key Usage:

Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment

X509v3 Extended Key Usage:

TLS Web Server Authentication, TLS Web Client Authentication, E-mail Protection, Code Signing, Microsoft Server Gated Crypto, OCSP Signing, Time Stamping, dvcs

Signature Algorithm: sha1WithRSAEncryption

33:98:35:1e:93:6e:b5:d9:8d:8c:f8:0f:93:89:40:52:10:2a:

19:04:61:62:e9:27:27:40:e9:89:86:d1:08:68:01:39:35:5a:

c6:47:1d:4c:40:aa:3e:b8:97:d1:ce:06:24:f9:7b:10:f5:54:

fa:ce:06:28:a5:ed:1e:03:34:a1:1e:e7:a6:35:3d:35:ab:ca:

98:0a:5d:04:34:99:71:ec:97:2d:8b:58:05:42:66:05:8a:73:

30:ca:a9:3d:08:60:78:6f:99:a1:4e:b2:2b:10:85:f9:c3:23:

ed:47:be:48:06:85:74:dd:f6:63:48:5f:50:66:ec:d3:2a:bf:

3d:e7

表 19-1 show pki local certificate显示信息描述表

| 字段 | 描述 |
| --- | --- |
| Name | 用户证书的名称 |
| version | 证书版本信息 |
| location | 证书位置信息 |
| status | 证书状态，通常为Certificate状态 |
| reference | 证书被引用次数 |
| subject | 主题信息 |
| Certificate | 已签发的证书状态 |

## 本地CA证书命令

### no pki local ca

**no pki local ca**命令用来删除一个CA证书。

【命令】

**no pki local ca** *certificate*

【视图】

用户视图

【参数】

*certificate*：删除的证书名称。

【使用指导】

被删除的CA证书为在设备上存在的CA证书。

【举例】

# 删除一个CA证书。

host# no pki local ca test\_ca.cer

【相关命令】

* show pki local ca

### pki local ca export tftp

**pki local ca export tftp**命令用来通过TFTP协议导出一个CA证书至TFTP服务器。

【命令】

**pki local ca export tftp** *ip-address certificate*

【视图】

用户视图

【参数】

*ip-address*：TFTP服务器IP地址。

*certificate*：导出的证书名称。

【使用指导】

被导出的CA证书为在设备上存在的CA证书。

【举例】

# 导出一个CA证书至TFTP服务器。

host# pki local ca export tftp 192.168.1.105 test\_ca.cer

Upload file test\_ca.cer ....

Upload file(test\_ca.cer) success.

【相关命令】

* show pki local ca

### pki local ca import tftp

**pki local ca import tftp**命令用来通过TFTP协议向本地CA证书中导入CA证书。

【命令】

**pki local ca import tftp** *ip-address certificate*

【缺省情况】

缺省情况下，没有配置CA证书。

【视图】

用户视图

【参数】

*ip-address*：TFTP服务器IP地址。

*certificate*：导入的证书名称，名称最长不超过63个字符，名称中不能带“()”，支持“.cer”格式。

【使用指导】

导入时，TFTP服务器上需要有相应的导入证书才可导入。

【举例】

# 导入一个CA证书。

host# pki local ca import tftp 192.168.1.105 test\_ca.cer

Download file test\_ca.cer ....

Download file(test\_ca.cer) success.

【相关命令】

* show pki local ca

### show pki local ca

**show pki local ca**命令用来显示所有本地CA证书的概要信息或者某个证书的详细内容。

【命令】

**show pki local ca** [ *certificate*]

【视图】

用户视图

【参数】

*certificate*：要显示详细信息的证书名称。

【举例】

# 显示所有CA证书的概要信息。

host# show pki local ca

Name version reference subject

----------------------------------------------------------------------------------------

test\_ca.cer 3 0 C=CN,O=OR,ST=PRO,CN=test\_ca,L=LOCATION,OU=DE

----------------------------------------------------------------------------------------

Total CA certificate file: 1

# 显示指定CA证书的内容。

host# show pki ca root-certificate

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 15356771495294948776 (0xd51e364fb1e655a8)

Signature Algorithm: sha1WithRSAEncryption

Issuer: C=CN, O=OR, ST=PRO, CN=test\_ca, L=LOCATION, OU=DE

Validity

Not Before: Jun 20 03:16:47 2014 GMT

Not After : Jul 10 03:16:47 2014 GMT

Subject: C=CN, O=OR, ST=PRO, CN=test\_ca, L=LOCATION, OU=DE

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (1024 bit)

Modulus:

00:c9:db:1e:45:66:2d:b5:6c:06:a0:79:62:4d:6c:

ce:92:4b:16:89:3b:5a:0a:62:b7:d6:7b:68:ab:f8:

ac:1c:3d:04:2f:0f:7f:fa:9a:69:4e:09:8f:9d:e2:

a1:35:67:44:58:c5:8d:14:fa:36:6f:c5:0f:b3:9b:

01:7e:1d:00:dc:44:ad:4a:34:16:1f:e9:af:1d:62:

6a:68:cb:e1:d9:30:e7:e2:0e:59:e7:ed:48:3d:83:

75:4e:12:df:90:35:0d:22:5c:7a:35:69:f7:33:ab:

39:58:68:ae:d7:71:55:65:36:53:f1:b4:09:3f:71:

c1:c0:66:0d:19:a2:e1:69:eb

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Basic Constraints: critical

CA:TRUE

X509v3 Key Usage: critical

Digital Signature, Certificate Sign, CRL Sign

Signature Algorithm: sha1WithRSAEncryption

2d:cb:0a:a8:d5:20:c7:f9:94:16:20:14:48:8d:26:40:ac:01:

8e:e1:42:f6:17:28:48:7a:56:d5:67:24:81:60:5e:e4:60:46:

13:64:5b:8b:f1:87:b1:f1:04:3e:63:7f:eb:79:61:43:91:1f:

06:0f:b5:e7:a5:d4:04:be:6a:93:46:70:90:c4:af:a5:61:67:

9d:1b:b1:39:e0:ca:17:58:3e:33:3b:48:71:80:dd:23:9b:94:

34:f7:6b:6b:60:ee:fd:cc:dc:61:63:c5:c1:52:37:95:05:b1:

d8:14:85:65:8a:71:61:f4:19:9f:66:fd:39:de:a5:a7:c0:d4:

88:d0

表 19-2 show pki local ca显示信息描述表

| 字段 | 描述 |
| --- | --- |
| Name | 用户证书的名称 |
| version | 证书版本信息 |
| reference | 证书被引用次数 |
| subject | 主题信息 |

## 本地CRL命令

### no pki local crl

**no pki local crl**命令用来删除一个CRL证书。

【命令】

**no pki local crl** *certificate*

【视图】

用户视图

【参数】

*certificate*：要删除的CRL证书的名称。

【使用指导】

被删除的CRL证书必须在设备上存在。

【举例】

# 删除一个CRL证书。

host# no pki local crl test\_ca.crl

【相关命令】

* show pki local crl

### pki local crl export tftp

**pki local crl export tftp**命令用来通过TFTP协议导出CRL证书至TFTP服务器。

【命令】

**pki local crl export tftp** *ip-address certificate*

【视图】

用户视图

【参数】

*ip-address*：TFTP服务器IP地址。

*certificate*：导出的CRL证书名称。

【使用指导】

导出的CRL证书在设备上存在才可导出。

【举例】

# 导出一个CRL证书至TFTP服务器。

host# pki local crl export tftp 192.168.1.105 test\_ca.crl

Upload file test\_ca.crl ....

Upload file(test\_ca.crl) success.

【相关命令】

* show pki local crl

### pki local crl import tftp

**pki local crl import tftp**命令用来通过TFTP协议导入CRL证书。

【命令】

**pki local crl import tftp** *ip-address certificate*

【缺省情况】

缺省情况下，没有配置CRL证书。

【视图】

用户视图

【参数】

*ip-address*：TFTP服务器IP地址。

*certificate*：导入的CRL证书名称，名称最长不超过63个字符，名称中不能带“()”，支持“.crl”格式。

【使用指导】

导入时，TFTP服务器上需要有相应的导入证书才可导入。

【举例】

# 导入CRL证书。

host# pki local crl import tftp 192.168.1.105 test\_ca.crl

Download file test\_ca.crl ....

Download file(test\_ca.crl) success.

【相关命令】

* show pki local crl

### show pki local crl

**show pki local crl**命令用来显示所有CRL证书的概要息或者某个CRL证书的详细内容。

【命令】

**show pki local crl** [ *certificate* ]

【视图】

用户视图

【参数】

*certificate*：为要显示的CRL证书的名称。

【举例】

# 显示所有CRL证书的概要信息。

host# show pki local crl

Name version issuer

----------------------------------------------------------------------------------------

test\_ca.crl 2 C=CN,O=OR,ST=PRO,CN=test\_ca,L=LOCATION,OU=DE

----------------------------------------------------------------------------------------

Total CRL file: 1

# 显示指定CRL证书的详细信息。

host# show pki local crl test\_ca.crl

Certificate Revocation List (CRL):

Version 2 (0x1)

Signature Algorithm: sha1WithRSAEncryption

Issuer: /C=CN/O=OR/ST=PRO/CN=test\_ca/L=LOCATION/OU=DE

Last Update: Jul 5 03:18:47 2014 GMT

Next Update: Jul 15 03:18:47 2014 GMT

CRL extensions:

X509v3 CRL Number:

1

X509v3 Authority Key Identifier:

DirName:/C=CN/O=OR/ST=PRO/CN=test\_ca/L=LOCATION/OU=DE

serial:D5:1E:36:4F:B1:E6:55:A8

Revoked Certificates:

Serial Number: AE9749415541C867

Revocation Date: Jul 5 03:18:47 2014 GMT

CRL entry extensions:

X509v3 CRL Reason Code:

Key Compromise

Signature Algorithm: sha1WithRSAEncryption

90:3f:61:80:b4:da:6d:08:2f:bd:4b:2d:9a:01:c1:40:c5:e4:

67:5d:4e:b2:8c:37:e7:61:08:90:5a:1a:e5:ee:60:59:12:db:

92:20:15:d6:ed:ef:e7:8d:f7:2c:fc:50:e1:97:dd:e2:60:4b:

24:b3:c6:d7:81:b1:c2:68:61:f4:c0:2a:53:b8:2c:fe:cd:4c:

7e:3c:8e:b9:f4:c1:81:d4:87:cc:a9:72:45:37:67:11:b2:7a:

e1:be:46:9d:ca:53:d1:82:76:d7:2e:5a:54:24:38:b1:b5:82:

32:3c:63:e8:41:0d:14:ad:d3:71:e9:d0:8c:7e:b0:32:c3:fc:

f9:5d

表 19-3 show pki local crl显示信息描述表

| 字段 | 描述 |
| --- | --- |
| Name | 用户证书的名称 |
| version | 证书版本信息 |
| issuer | 签发者信息 |

## 自动获取CRL命令

### pki local crl auto-get

**pki local crl auto-get**命令用来添加一条自动获取CRL证书的配置。

**no pki local crl auto-get**命令用来删除一条自动获取CRL证书的配置。

【命令】

**pki local crl auto-get** *name**interval-time*{ **http-url** | **ldap-server** }*server*

**no pki local crl auto-get** *name*

【缺省情况】

缺省情况下，没有自动获取CRL文件的配置。

【视图】

系统视图

【参数】

*name*：自动获取CRL证书的配置名称。为1～31个字符的字符串，且不能包含“%!"#$&`\*+,/:;<=>?\^'{}!”。

*interval-time*：自动获取CRL证书的间隔时间。取值范围为1到720小时。

*server*：CRL证书服务器。

**http-url**：通过HTTP协议获取CRL证书。

**ldap-server**：从LDAP服务器获取CRL证书。

【使用指导】

自动获取到的CRL证书将以自动获取配置的名称命名。

【举例】

# 创建一条自动获取CRL证书的配置。

host(config)# pki local crl auto-get auto-crl 24 http-url http://192.168.1.1/ca.crl

【相关命令】

* show pki local crl auto-get
* show running-config pki

### show pki local crl auto-get

**show pki local crl auto-get**命令用来显示所有自动获取CRL证书的配置。

【命令】

**show pki local crl auto-get** [ *name* ]

【视图】

用户视图

【参数】

*name*：自动获取CRL证书的配置名称。

【举例】

# 显示所有CRL自动获取的配置。

host# show pki local crl auto-get

Name Period Type Server

----------------------------------------------------------------------------------------

auto-crl 24 http-url http://192.168.1.1/ca.crl

----------------------------------------------------------------------------------------

Total: 1

# 显示指定CRL自动获取配置。

host# show pki local crl auto-get auto-crl

pki local crl auto-get auto-crl 24 http-url <http://192.168.1.1/ca.crl>

表 19-4 显示CRL证书自动获取配置命令显示信息描述表

| 字段 | 描述 |
| --- | --- |
| Name | 自动获取CRL证书的配置名称 |
| Period | 自动获取的间隔时间 |
| Type | 自动获取的方式，有http-url、ldap两种 |
| Server | 自动获取的服务器信息 |
| http-url | 通过HTTP协议获取 |
| ldap | 通过LDAP服务器获取 |

【相关命令】

* show running-config pki

# SNMP命令

## SNMP命令

### community

**community**命令用来配置SNMP的读团体字。

**no community**命令用来删除SNMP的读团体字。

【命令】

**community** *name*

**no community**

【缺省情况】

缺省情况下，读团体字为“public”。

【视图】

snmp视图

【参数】

*name*：读团体字字符串。为1～31个字符的字符串，且不能包含“%!"#$&`\*+,/:;<=>?\^'{}!”。缺省值为“public”。

【使用指导】

当使用SNMP V1、V2C版本的get操作时，需要配置读团体字。

当执行删除操作后，读团体字的配置将恢复为缺省配置。

【举例】

# 配置读团体字。

host# configure terminal

host(config)# snmp

host(config-snmp)# community getinfo

【相关命令】

* show running-config snmp

### show snmpv3 usm-user

**show snmpv3 usm-user**命令用来显示已配置的USM用户信息。

【命令】

**show snmpv3 usm-user**

【视图】

用户视图

【举例】

# 显示USM用户信息。

host# show snmpv3 usm-user

usm-user authentication privacy

test MD5 DES

表 20-1 USM用户信息显示信息描述表

| 字段 | 描述 |
| --- | --- |
| usm-user | USM用户名称 |
| authentication | 认证方式，MD5或者SHA方式 |
| privacy | 加密方式，DES或者AES方式 |

### snmp

**snmp enable**命令用来开启SNMP。

**snmp disable**命令用来关闭SNMP。

【命令】

**snmp enable**

**snmp disable**

【缺省情况】

缺省情况下，未开启SNMP功能。

【视图】

snmp视图

【使用指导】

当需要用远端的SNMP管理软件监控设备时，需要开启SNMP。

【举例】

# 配置启用SNMP。

host# configure terminal

host(config)# snmp

host(config-snmp)# snmp enable

【相关命令】

* show running-config snmp

### snmpv3 usm-user

**snmpv3 usm-user**命令用来配置SNMP V3版本的USM用户。

**no snmpv3 usm-user**命令用来删除SNMP V3版本的USM用户。

【命令】

**snmpv3 usm-user** *name*

**snmpv3 usm-user** *name* **auth-mode** { **MD5** | **SHA** } *password*

**snmpv3 usm-user** *name* **auth-mode** { **MD5** | **SHA** }*password* **privacy** { **DES** | **AES** } *password*

**no snmpv3 usm-user** [name]

【缺省情况】

缺省情况下，未配置任何USM用户。

【视图】

snmp视图

【参数】

*name*：USM用户的名称。为1～31个字符的字符串，且不能包含“%!"#$&`\*+,/:;<=>?\^'{}!”。

**MD5**：使用MD5的认证方式。

**SHA**：使用SHA的认证方式。

*password*：认证密码或者加密密码。

**DES**：使用DES的加密方式。

**AES**：使用AES的加密方式。

【使用指导】

添加一个用户可以只配置用户名称，也可以只配置用户名称及认证模式，或者既配置认证模式，也配置加密方式。

SNMP管理软件使用V3版本认证时，相同的用户，需要使用相同的认证模式和加密方式。

【举例】

# 配置一个名为“test”的USM用户。

host# configure terminal

host(config)# snmp

host(config-snmp)# snmpv3 usm-user test auth-mode MD5 password1 privacy DES password2

【相关命令】

* show running-config snmp
* show snmpv3 usm-user

### syslocation

**syslocation**命令用来配置地理位置信息。

**no syslocation**命令用来删除地理位置信息。

【命令】

**syslocation** *name*

**no syslocation**

【缺省情况】

缺省情况下，未配置地理位置信息。

【视图】

snmp视图

【参数】

*name*：地理位置信息字符串。为1～31个字符的字符串，且不能包含“%!"#$&`\*+,/:;<=>?\^'{}!”。

【使用指导】

设备配置该命令后，可通过远端SNMP管理软件获取该设备的地理位置。

【举例】

# 配置syslocation。

host# configure terminal

host(config)# snmp

host(config-snmp)# syslocation beijing

【相关命令】

* show running-config snmp

### trap

**trap address**命令用来配置TRAP信息上报的服务器IP地址。

**no trap**命令用来删除TRAP信息上报的服务器IP地址。

【命令】

**trap address** *ip-address*

**no trap**

【缺省情况】

缺省情况下，未配置TRAP信息上报地址。

【视图】

snmp视图

【参数】

*ip-address*：TRAP信息上报的服务器IP地址。

【使用指导】

当需要获取设备的通知、告警等信息时，需要通过配置TRAP信息上报地址开启此功能。

【举例】

# 配置TRAP信息接收地址。

host# configure terminal

host(config)# snmp

host(config-snmp)# trap address 192.168.1.1

【相关命令】

* trap version { v1 | v2c\_notification | v2c\_inform }
* show running-config snmp

### trap version

**trap version**命令用来配置启用TRAP信息的某一版本。

**no trap version**命令用来关闭TRAP信息的某一版本。

【命令】

**trap version** { **v1** | **v2c\_notification** | **v2c\_inform** }

**no trap version** { **v1** | **v2c\_notification** | **v2c\_inform** }

【缺省情况】

缺省情况下，三个TRAP版本均默认开启。

【视图】

snmp视图

【参数】

**v1**：TRAP信息为V1版本。

**v2c\_notification**：TRAP信息为V2C Notification版本。

**v2c\_inform**：TRAP信息为V2C Inform版本。

【使用指导】

三个版本可同时有效，开启后，TRAP报文接收服务器将接收到与之对应的TRAP报文。

【举例】

# 配置TRAP报文版本。

host# configure terminal

host(config)# snmp

host(config-snmp)# trap version v1

host(config-snmp)# trap version v2c\_inform

host(config-snmp)# trap version v2c\_notification

【相关命令】

* **trap address** ip-address
* **show running-config snmp**

### version

【命令】

**version** { **v1** | **v2c** | **v3** }

**no version** { **v1** | **v2c** | **v3** }

【缺省情况】

缺省情况下，SNMP的三个版本均默认启用。

【视图】

snmp视图

【参数】

**v1**：SNMP的V1版本。

**v2c**：SNMP的V2C版本。

**v3**：SNMP的V3版本。

【使用指导】

当SNMP开启使用某一版本，SNMP对应的管理软件使用相应的版本，才可通信，获取和管理设备的信息。

【举例】

# 开启使用SNMP的三个版本。

host# configure terminal

host(config)# snmp

host(config-snmp)# version v1

host(config-snmp)# version v2c

host(config-snmp)# version v3

【相关命令】

* show running-config snmp

### write-community

**write-community**命令用来配置SNMP的写团体字。

**no write-community**命令用来删除SNMP的写团体字。

【命令】

**write-community** *name*

**no write-community**

【缺省情况】

缺省情况下，写团体字为“private”。

【视图】

snmp视图

【参数】

*name*：读团体字字符串。为1～31个字符的字符串，且不能包含“%!"#$&`\*+,/:;<=>?\^'{}!”。缺省值为“private”。

【使用指导】

当使用SNMP V1、V2C版本的set操作时，需要配置写团体字。

当执行删除操作后，写团体字的配置将恢复为缺省配置。

【举例】

# 配置写团体字。

host# configure terminal

host(config)# snmp

host(config-snmp)# write-community setinfo

【相关命令】

* show running-config snmp

# 日志命令参考

## 日志命令

### log facility

**log facility**命令用来设置日志的facility值。

【命令】

**log** { **system\_state** | **operate** | **mail** | **im** | **social\_log** | **search\_engine** | **command\_log** | **web\_access** | **malware\_app** | **other\_app** | **attack\_ipmac** | **attack\_scan** | **attack\_flood** | **attack\_abnormal\_pkt** } **facility** *facility-value*

【缺省情况】

缺省情况下，日志的facility值为0。

【视图】

系统视图

【参数】

**system\_state**：事件日志。

**operate**：操作日志。

**im**： IM聊天软件日志。

**social\_log**：社区日志。

**search\_engine**：搜索引擎日志。

**mail**：邮件日志。

**command\_log**：命令日志。

**other\_app**：其它应用日志。

**web\_access**：网站访问日志。

**malware\_app：**恶意网站日志。

**attack\_ipmac：**IP-MAC日志。

**attack\_scan：**扫描攻击防御日志。

**attack\_flood：**Flood攻击防御日志。

**attack\_abnormal\_pkt：**异常报文攻击日志。

*facility-value*：日志的facility值，取舍范围为0～65535。

【举例】

# 设置NAT日志的facility值为1024。

host# configure terminal

host(config)# log nat facility 1024

【相关命令】

* show log config

### log local

**log local**命令用来配置系统的日志是否记录在本地。

【命令】

**log** { **system\_state** | **operate** | **mail** | **im** | **social\_log** | **search\_engine | command\_log** | **web\_access** | **malware\_app** | **other\_app** | **attack\_ipmac** | **attack\_scan** | **attack\_flood** | **attack\_abnormal\_pkt** } **local** { **enable** | **disable** }

【缺省情况】

缺省情况下，本地不记录会话日志和NAT，其余类型的日志本地会记录。

【视图】

系统视图

【参数】

**system\_state**：事件日志。

**operate**：操作日志。

**im**：IM聊天软件日志。

**social\_log**：社区日志。

**search\_engine**：搜索引擎日志。

**mail**：邮件日志。

**command\_log**：命令日志。

**other\_app**：其它应用日志。

**web\_access**：网站访问日志。

**malware\_app：**恶意网站日志。

**attack\_ipmac：**IP-MAC日志。

**attack\_scan：**扫描攻击防御日志。

**attack\_flood：**Flood攻击防御日志。

**attack\_abnormal\_pkt：**异常报文攻击日志。

**enable**：记录日志在本地。

**disable**：不记录日志在本地。

【举例】

# 配置其它应用日志不记录在本地。

host# configure terminal

host(config)# log other\_app local disable

【相关命令】

* show log config

### log server addr

**log server addr**命令用来配置日志服务器的IP地址。

【命令】

**log server addr** *ip-address*

【视图】

系统视图

【参数】

*ip-address*：日志服务器的IP地址。

【举例】

# 配置日志服务器的地址为192.168.1.100。

host# configure terminal

host(config)# log server addr 192.168.1.10

【相关命令】

* local server enable
* local server port
* log server crypt
* show log config

### log server crypt

**log server crypt**命令用来启用日志内容的加密。

**no log server crypt**命令用来取消日志内容的加密。

【命令】

**log server crypt**

**no log server crypt**

【缺省情况】

缺省情况下，日志内容不加密。

【视图】

系统视图

【使用指导】

当启用日志内容加密之后，发送给日志服务器的日志内容会加密。只有外置数据中心可以解密日志的内容，保证日志在传输过程中的安全。

对于标准的日志服务器，不要使用日志加密选项，否则标准的日志服务器无法正确的解密日志。

【举例】

# 启用日志内容的加密。

host# configure terminal

host(config)# log server crypt

【相关命令】

* local server enable
* local server addr
* local server port
* show log config

### log server enable

**log server enable**命令用来启用远端日志服务器。

**log server disable**命令用来禁用远端日志服务器。

【命令】

**log server enable**

**log server disable**

【视图】

系统视图

【使用指导】

在使用**log server enable**命令启用日志服务器之前，确保之前已经使用**log server addr**命令配置了日志服务器地址。

【举例】

# 启用日志服务器。

host# configure terminal

host(config)# log server enable

【相关命令】

* local server addr
* local server port
* log server crypt
* show log config

### log server port

**log server port**命令用来配置日志服务器的端口。

【命令】

**log server port** *port-num*

【缺省情况】

缺省情况下，日志服务器的端口为514。

【视图】

系统视图

【参数】

*port-num*：日志服务器的UDP端口号。

【举例】

# 设置日志服务器的端口号为514。

host# configure terminal

host(config)# log server port 514

【相关命令】

* local server enable
* local server addr
* show log config

### log server second

**log server second**命令用来设置第二个日志服务器。

**no log server second**命令用来取消第二个日志服务器的配置。

【命令】

**log server second** { **addr** *ip-address |* **port** *port-num |* **crypt** }

**no log server second** { **addr** | **port** *|* **crypt** }

【缺省情况】

缺省情况下，第二日志服务器的端口是UDP 514，日志内容不加密。

【视图】

系统视图

【参数】

*ip-address*：第二个日志服务器的IP地址。

*port-num*：第二个日志服务器的端口号。

**crypt**：日志内容加密。

【使用指导】

如果一个日志服务器不够的用的话，可以使用**log server second**命令指定第二个日志服务器。

当启用日志内容加密之后，发送给日志服务器的日志内容会加密。只有外置数据中心可以解密日志的内容，保证日志在传输过程中的安全。

对于标准的日志服务器，不要使用日志加密选项，否则标准的日志服务器无法正确的解密日志。

【举例】

# 配置第二个日志服务器的地址为192.168.1.20，端口为514，日志内容不加密。

host# configure terminal

host(config)# log server second addr 192.168.1.20

host(config)# log server port 514

host(config)# no log server crypt

【相关命令】

* show log config

### log server third

**log server third**命令用来设置第三个日志服务器。

**no log server third**命令用来取消第三个日志服务器的配置。

【命令】

**log server third** { **addr** *ip-address |* **port** *port-num |* **crypt** }

**no log server third { addr** | **port** *|* **crypt** }

【缺省情况】

缺省情况下，第三日志服务器的端口是UDP 514，日志不加密。

【视图】

系统视图

【参数】

*ip-address*：第三个日志服务器的IP地址。

*port-num*：第三个日志服务器的端口号。

**crypt**：日志内容加密。

【使用指导】

如果二个日志服务器不够的用的话，可以使用**log server third**命令指定第三个日志服务器。

当启用日志内容的加密之后，发送给日志服务器的日志内容会进行加密。只有外置数据中心可以解密日志的内容，保证日志在传输过程中的安全。

对于标准的日志服务器，不要使用日志加密选项，否则标准的日志服务器无法正确的解密日志。

【举例】

# 配置第三个日志服务器的地址为192.168.1.20，端口为514，日志内容不加密。

host# configure terminal

host(config)# log server third addr 192.168.1.20

host(config)# log server port 514

host(config)# no log server crypt

【相关命令】

* show log config

### log server upto

**log server upto**命令用来过滤发送到日志服务器的日志的级别。

【命令】

**log server** { **system\_state** | **operate** | **mail** | **im** | **social\_log** | **search\_engine** | **command\_log** | **web\_access** | **malware\_app** | **other\_app** | **attack\_ipmac** | **attack\_scan** | **attack\_flood** | **attack\_abnormal\_pkt** } { **disable** | **enable** | **upto** { **alerts** | **critical** | **emergencies** | **errors** | **informational** | **notifications** | **warnings** } }

【缺省情况】

缺省情况下，对发送到远端的日志不做过滤，所有日志发送到远端日志服务器。

【视图】

系统视图

【参数】

**system\_state**：事件日志。

**operate**：操作日志。

**im**： IM聊天软件日志。

**social\_log**：社区日志。

**search\_engine**：搜索引擎日志。

**mail**：邮件日志。

**command\_log**：命令日志。

**other\_app**：其它应用日志。

**web\_access**：网站访问日志。

**malware\_app：**恶意网站日志。

**attack\_ipmac：**IP-MAC日志。

**attack\_scan：**扫描攻击防御日志。

**attack\_flood：**Flood攻击防御日志。

**attack\_abnormal\_pkt：**异常报文攻击日志。

**enable：**所有日志发送给远端服务器。

**disable：**所有日志不发送给远端服务器。

**alerts：**告警及以上级别的日志发送到日志服务器。

**critical：**严重及以上级别的日志发送到日志服务器。

**emergencies**：紧急及以上的级别的日志发送到日志服务器。

**errors**：错误及以上级别的日志发送到日志服务器。

**informational**：信息及以上级别的日志发送到日志服务器。

**notifications**：通知以及以上级别的日志发送到日志服务器。

**warnings**：警告及以及以上级别的日志发送到日志服务器**。**

【举例】

# 将警告以上级别的邮件日志发送到日志服务器。

host# configure terminal

host(config)# log mail server upto warnings

#将所有邮件日志发送到日志服务器。

host# configure terminal

host(config)# log mail server enable

# 将所有邮件日志不发送到日志服务器。

host# configure terminal

host(config)# log mail server disable

【相关命令】

* show log config

### log source addr

**log source addr**命令用来设置设备发送的日志的源地址。

**no log source addr**命令用来删除设备发送日志的源地址，系统会根据系统路由的配置情况，使用接口的IP地址做为syslog的源IP地址。

【命令】

**log source addr** *ip-address*

**no log source addr**

【视图】

系统视图

【参数】

*ip-address*：日志的源IP地址。

【使用指导】

如果没有特殊需求，建议不要配置日志的源IP，让系统自动选择。

【举例】

# 配置日志的源IP为192.168.1.10。

host# configure terminal

host(config)# log source addr 192.168.1.10

【相关命令】

* show log config

### show log config

**show log config**命令用来显示日志的配置。

【命令】

**show log config**

【视图】

任意视图

【举例】

# 显示日志的配置。

host# show log config

log traffic\_detail server enable

log traffic\_detail local enable

log traffic\_session server enable

log traffic\_session local enable

log traffic\_template server enable

log traffic\_template local enable

log web\_access server enable

log web\_access local enable

log malware\_app server enable

log malware\_app local enable

log im server enable

log im local enable

log social\_log server enable

log social\_log local enable

log search\_engine server enable

log search\_engine local enable

log mail server enable

log mail local enable

log command\_log server enable

log command\_log local enable

log other\_app server enable

log av server enable

log av local enable

log ips server enable

log ips local enable

log arp\_atk server enable

log arp\_atk local enable

log syn\_cookie\_atk server enable

log syn\_cookie\_atk local enable

log security\_ipmac server enable

log security\_ipmac local enable

log security\_scan server enable

log security\_scan local enable

log security\_flood server enable

log security\_flood local enable

log security\_abnormal\_pkt server enable

log security\_abnormal\_pkt local enable

log nat server enable

log nat local enable

log operate server enable

log operate local enable

log system\_state server enable

log system\_state local enable

log device\_health server enable

log device\_health local enable

log policy\_detail server enable

log policy\_detail local enable

log daemon server enable

log daemon local enable

log server addr 192.168.1.100

log server second addr 192.168.1.20

log server enable

log nat facility 1024

**show log config**命令显示日志模块的配置，具体的含义参见各个命令的介绍。

# HA

## HA配置命令

### auto\_sync

**auto\_sync**命令用来配置自动同步选项。

**no auto\_sync**命令用来关闭自动同步选项。

【命令】

**auto\_sync** { **config** | **session** | **lib** }

**no auto\_sync** { **config** | **session** | **lib** }

【缺省情况】

缺省情况下，未配置自动同步选项。

【视图】

HA配置视图

【参数】

**config**：自动同步设备配置。

**session**：自动同步设备运行相关信息，具体包括连接表，FDB表，用户信息，PKI证书等。

**lib**：自动同步特征库，具体包括病毒库，URL库，应用特征库，IPS库。

【使用指导】

需要注意的是：

HA的相关配置在配置同步时不会同步。

设备开始使用配置同步时，最好使用一台除了HA配置没有其他配置的设备，防止同步过来的配置和原有配置有冲突。

【举例】

# 配置自动同步配置，设备运行信息和特征库。

host# configure terminal

host(config)# ha-config

host(ha-config) #auto\_sync config

host(ha-config)# auto\_sync session

host(ha-config)# auto\_sync lib

### disable

**disable**命令用来关闭HA功能。

【命令】

**disable**

【缺省情况】

缺省情况下，未启用HA。

【视图】

HA配置视图

【举例】

# 关闭HA功能。

host# configure terminal

host(config)# ha-config

host(ha-config)# disable

### enable backup-master

**enable backup-master**命令用来启用HA主备模式。

【命令】

**enable backup-master**

【缺省情况】

缺省情况下，未启用HA。

【视图】

HA配置视图

【举例】

# 启用HA主备模式。

host# configure terminal

host(config)# ha-config

host(ha-config)# enable backup-master

### ha-config

**ha-config**命令用来进入HA配置视图。

【命令】

**ha-config**

【视图】

系统视图

【举例】

# 进入HA配置视图。

host# configure terminal

host(config)# ha-config

### hainterface

**hainterface** 命令用来配置HA接口。

**no hainterface**命令用来删除HA接口。

【命令】

**hainterface** *interface-name*

**no hainterface**

【缺省情况】

缺省情况下，未配置HA接口。

【视图】

HA配置视图

【参数】

*interface-name*：要配置的接口，必须是物理接口和聚合接口。接口不能和其他功能一起使用，比如不能加入桥，加入聚合，配置NAT。

【使用指导】

HA接口主要用于HA设备之间keepalive通讯和同步报文传输。

【举例】

# 配置ge2接口为HA接口。

host# configure terminal

host(config)# ha-config

host(ha-config)# hainterface ge2

### keepalive

**keepalive**用来配置HA心跳报文发送参数。

**no keepalive**用来还原HA心跳报文的缺省参数。

【命令】

**keepalive** *interval* **retry** *retry-count*

**no keepalive**

【缺省情况】

缺省情况下，HA心跳报文每50毫秒发送一次，重试次数是60次。

【视图】

HA配置视图

【参数】

*interval*：HA心跳报文的间隔时间，范围是20～1000，单位是毫秒，缺省值时50毫秒。

*retry-count*：心跳报文超时重试次数，范围是3～500次。如果设备在间隔时间乘以重试次数的时间内没有收到对端心跳报文，可以认定对端设备已经超时。

【使用指导】

主备设备的心跳间隔时间可以不一致。在不一致的情况下，设备发送心跳报文的间隔时间为两端间隔时间的最小值。

需要注意的是：

*interval*配置越短HA协商越稳定，但是会增加系统负担。

*retry-count*配置越少HA对故障相应越灵敏，但是会增加误报的几率。

用户最好根据自己的网络环境和需求确定*interval*和*retry-count*的值。

【举例】

# 配置HA心跳报文发送间隔时间为1秒，重试次数为3。

host# configure terminal

host(config)# ha-config

host(ha-config)# keepalive 1000 retry 3

### manage-ip

**manage-ip** 命令用来配置接口管理地址。

**no manage-ip**命令用来删除接口管理地址。

【命令】

**manage-ip** *address*

**no manage-ip**

【缺省情况】

缺省情况下，未配置接口管理地址。

【视图】

接口视图

【参数】

*address*：要配置的地址，格式为A.B.C.D/M。

【使用指导】

处于备状态的HA设备不会参与网络转发，因此无法通过接口配置的IP地址访问。为了解决这一问题，可以在设备上配置管理地址，用作备设备的网络管理。

要注意的是：

管理地址只能配置在物理接口，桥接口和VLAN子接口。

管理地址可以和接口主地址处于同一网段。

接口没有配置主地址也可以配置管理地址，但是如果接口的主地址是PPPOE或者DHCP地址，则无法配置管理地址。

管理员可以通过管理地址访问备设备的telnet 服务和web ui。但是备设备无法通过管理地址主动访问外部地址，除非应用制定了源地址为管理地址（比如说指定源地址的ping命令。）

【举例】

# 配置ge0的管理地址是192.168.1.18/24。

host# configure terminal

host(config)# interface ge0

host(config-ge0)# manage-ip 192.168.1.18/24

### monitor

**monitor**命令用来添加监控接口。

**no monitor**命令用来删除监控接口。

【命令】

**monitor** *interface-name*

**no monitor** *interface-name*

【缺省情况】

缺省情况下，未配置HA监控接口。

【视图】

HA配置视图

【参数】

*interface-name*：要配置成监控接口的接口名称。

【使用指导】

要配置成监控接口的接口，一般应是网络中重要的接口，比如通往internet的接口。如果此接口的状态发生改变，表明网络中发生重大故障，需要启用备设备，主备设备会立刻切换。

需要注意的是，如果主设备和备设备的地址探测或者监控接口都发生故障，表明此时网络发生严重错误，此时主备切换也无法修复错误，所以主备不会发生切换。

【举例】

# 配置ge0为监控接口。

host# configure terminal

host(config)# ha-config

host(ha-config)# monitor ge0

### preempt

**preempt** 命令用来配置抢占功能。

**no preempt**命令用来关闭抢占功能。

【命令】

**preempt**  { **master** | **backup** } [ *delay-time* ]

**no preempt**

【缺省情况】

缺省情况下，未配置HA抢占功能。

【视图】

HA配置视图

【参数】

**master**：表示设备希望抢占为主。

**backup**：表示设备希望抢占为备。

*delay-time*：抢占延时时间。范围是1到180，单位是秒，缺省抢占时间是3秒。当要抢占设备的监控接口全部正常后，开始计算时间。只有在这个时间内监控接口状态没有发生改变才实现状态切换。

【使用指导】

抢占模式必须在主设备和备设备上分别配置，一台设备配置为抢占主，一台配置为抢占备。否则HA无法协商。

主设备和备设备的抢占延时可以不同，如果抢占延时不同，实际抢占延时是主设备和备设备抢占延时的最大值。

【举例】

# 一台配置抢占为主，抢占延时为10s。

host# configure terminal

host(config)# ha-config

host(ha-config)# preempt master 10

### show ha state

**show ha state**命令用来查看HA状态。

【命令】

**show ha state**

【视图】

用户视图

【使用指导】

要注意的是：

如果没有配置自动同步特征库，或者对应特征库的license无效，不会显示特征库是否同步。

如果主备都没有配置抢占模式，不会显示抢占模式状态。

【举例】

# 显示HA状态。

host# show ha state

Keepalive send interval 50ms config interval 50ms

Preempt style master delay time 5s config delay time 3s

Local : Hostname=host Status=Master Monitor interface status=OK

app lib version : 20140227

Remote: Hostname=hostA Status=Backup Monitor interface status=OK

app lib version : 20140227

SYNC state:

System config different

表 22-1 show ha state显示信息描述表

| 字段 | 描述 |
| --- | --- |
| Keepalive send interval | 主备设备协商出的心跳报文发送间隔时间 |
| config interval | 设备配置的心跳报文间隔时间 |
| Preempt style | 设备配置的抢占模式 |
| delay time | 主备设备协商的抢占延时时间 |
| config delay time | 设备配置的抢占延时时间 |
| Local : | 本地设备的HA状态 |
| Remote: | HA邻居的HA状态 |
| Hostname | 设备的hostname |
| Status | 设备的HA状态 |
| interface status | 设备监控接口状态 |
| app lib version | 应用识别特征库版本 |
| url lib version | URL特征库版本 |
| ips lib version | 入侵防御系统特征库版本 |
| av lib version | 病毒特征库版本 |
| SYNC state | 同步状态 |
| System config | 系统配置同步状态 |
| App lib sync state | 应用识别特征库同步状态 |

### standby

**standby**命令用来使设备进入暂停模式。

**no standby**命令用来使设备退出暂停模式。

【命令】

**standby**

**no standby**

【视图】

HA配置视图

【使用指导】

进入暂停模式的设备不会响应邻居丢失，不再相应HA接口down从左，在没有手工切换HA状态的情况下将不再进行HA状态转换。

要注意的是：

在一台设备上配置standby，HA邻居也会进入暂停模式。

在一台设备上配置no standby，HA邻居也会退出暂停模式。

如果在standby状态下配置swap命令，将退出暂停模式，并且切换HA状态。

standby命令无法保存。

【举例】

# 配置HA设备进入暂停模式。

host# configure terminal

host(config)# ha-config

host(ha-config)# standby

### swap

**swap**命令用来手动切换HA主备状态。

【命令】

**swap**

【视图】

HA配置视图

【使用指导】

命令的功能是主设备主动从主状态切换成为备状态，并且通知对端设备从备状态变成主状态。

需要注意的是：

swap命令必须在主设备上配置。

配置了抢占模式的HA设备无法手动切换HA状态。

如果设备配置了暂停模式，使用swap命令后，HA设备将切换主备状态，并且退出暂停模式。

swap命令无法保存。

【举例】

# 手动切换HA的主备状态。

host#configure terminal

host(config)# ha-config

host(ha-config)# swap

### sync config

**sync config** 命令用来将主设备的配置手动同步给备设备并且重启备设备。

【命令】

**sync config**

【视图】

用户视图

【使用指导】

HA的相关配置在配置同步时不会同步。配置自动同步选项不会影响手动同步配置的效果。

【举例】

# 向备设备同步配置并重启备设备。

host# sync config

### sync lib

**sync lib**命令手动同步特征库。

【命令】

**sync lib** { **app** | **url** }

【视图】

用户视图

【参数】

**app**：应用识别特征库。

**url**：URL特征库。

【使用指导】

特征库自动同步选项不会影响手动同步效果。

【举例】

# 向备设备同步应用识别特征库。

host# sync lib app

# 接口状态同步组

## 接口状态同步组命令

### interface sync group

**interface sync group**命令用来创建接口状态同步组。

**no interface sync group**命令用来删除接口状态同步组。

【命令】

**interface sync group** *name interface*&<1-8>

**no interface sync group**

【缺省情况】

缺省情况下，没有配置接口状态同步组。

【视图】

系统视图

【参数】

*name*：接口状态同步组名称。

*interface*：组内成员，物理接口名称，最多可以配置8个。

【使用指导】

接口状态同步组，即是为加快链路状态变化的快速响应而出现的一种高可靠的功能。主要功能是将一个组内的多个接口状态保持同步，即组内的某一成员状态首先发生变化，则组内的其他成员也同时被置为与其一致的状态，只有当该成员状态恢复时，其他组内成员的状态才可以恢复。

组状态主要有3种：up，down和unknow。unknow状态为中间状态，为防止组内成员间的互相影响，所以当组状态为unknow时，需要下一 轮循环更新组状态。

组状态由以下方法确定：

当全部成员的链路状态都为up时，组状态为up。

当某一成员的链路状态为down时，组状态为down。

当上一条条件中的成员链路状态变为up时，将组内其它成员置位管理up，组状态置为unknow。

当组状态为unknow时，继续使用前两个条件确定状态。

需要注意的是设备支持的接口状态同步组的最大个数为16。

【举例】

# 配置个名为group1的接口状态同步组，组成员有ge0，ge1。

host# configure terminal

host(config)# interface sync group group1 ge0 ge1

# IPv6命令参考

## IPv6路由命令

### ipv6 route

**ipv6 route**命令用来添加IPv6路由。

**no ipv6 route**命令用来删除指定的IPv6路由。

【命令】

**ip route** *ipv6-address prefix-length* { *interface-name* | *next-hop-address* [ *interface-name*] }

**no ip route** *ipv6-address prefix-length* { *interface-name* | *next-hop-address* [ *interface-name*] }

【视图】

系统视图

【参数】

*ipv6-address*：IPv6地址。

*prefix-length*：IPv6前缀长度。

*next-hop-address*：下一跳IPv6地址。

*interface-name*：接口名称。

【使用指导】

在配置静态路由时，可以指定出接口（*interface-name*），也可指定下一跳地址（*nexthop-address*），具体采用哪种方法，需要根据实际情况而定：如果出接口类型为广播（如以太网接口、VLAN接口等），必须指定下一跳地址，也可以指定出接口，但如果下一跳地址为本地链路单播地址，则必须同时指定出接口；如果出接口类型为点到点类型（如隧道口等），则一般指定为出接口。

【举例】

# 配置IPv6静态路由，该路由的目的地址为1:1:2::/64，下一跳地址为1:1:3::1。

host# configure terminal

hostB(config)# ipv6 route 1:1:2::/64 1:1:3::1

【相关命令】

* show ipv6 route

### show ipv6 route

**show ipv6 route**命令用来显示IPv6路由。

【命令】

**show ipv6 route**

【视图】

任意视图

【举例】

# 显示所有IPv6路由。

host# show ipv6 route

Codes: C - connected, S - static

> - selected route, \* - FIB route

C>\* ::1/128 is directly connected, lo

S 1:1:2::/64 [1/0] via 1:1:3::1 inactive

C>\* fe80::/64 is directly connected, bvi0

表 24-1 show ipv6 route命令显示信息描述表

| 字段 | 描述 |
| --- | --- |
| S | 静态路由 |
| C | 直连路由 |
| > | 下发到内核用于转发的路由 |
| \* | 当前被选中的路由 |
| via X:X::X:X/M | 下一跳地址 |
| directly connected | 直连路由 |
| inactive | 下一跳不可达 |

【相关命令】

* show ipv6 route static

### show ipv6 route connected

**show ipv6 route** **connected**命令用来显示IPv6直连路由。

【命令】

**show ipv6 route connected**

【视图】

任意视图

【举例】

# 显示IPv6直连路由。

host# show ipv6 route connected

Codes: C - connected, S - static

> - selected route, \* - FIB route

C>\* ::1/128 is directly connected, lo

C>\* fe80::/64 is directly connected, bvi0

表 24-2 show ipv6 route connected命令显示信息描述表

| 字段 | 描述 |
| --- | --- |
| S | 静态路由 |
| C | 直连路由 |
| > | 下发到内核用于转发的路由 |
| \* | 当前被选中的路由 |
| directly connected | 直连路由 |

### show ipv6 route *ipv6-address*

**show ipv6 route** *ipv6-address*命令用来显示指定目的地址的IPv6路由信息。

【命令】

**show ipv6 route** *ipv6-address*

【视图】

任意视图

【参数】

*ipv6-address*：要显示路由信息的IPv6地址。

【举例】

# 显示3ffe:506::1的路由信息。

host# show ipv6 route 3ffe:506::1

Routing entry for ::/0

Known via "static", distance 1, metric 0

1:1:3::1 inactive

表 24-3 show ipv6 route*ipv6-address*命令显示信息描述表

| 字段 | 描述 |
| --- | --- |
| Routing entry for | 路由表条目 |
| via | 路由类型：  static表示静态路由  connect表示直连路由 |
| distance | 路由distance |
| metric | 路由metric |
| X:X::X:X/M inactive/active | Inactive表示路由不可达，active表示路由可达 |

### show ipv6 route *ipv6-prefix*

**show ipv6 route** *ipv6-preifx*命令用来显示通过指定前缀列表过滤的IPv6路由信息。

【命令】

**show ipv6 route** *ipv6-preifx*

【视图】

任意视图

【参数】

*ipv6-preifx*：指定需要显示路由信息的前缀列表。

【举例】

# 显示fe80::/64的路由信息。

host# show ipv6 route fe80::/64

Routing entry for fe80::/64

Known via "connected", distance 0, metric 1, best

\* directly connected, bvi0

表 24-4 show ipv6 route *ipv6-preifx*命令显示信息描述表

| 字段 | 描述 |
| --- | --- |
| Routing entry for | 路由表条目 |
| via | 路由类型:  static表示静态路由  connect表示直连路由 |
| distance | 路由distance |
| metric | 路由metric |
| X:X::X:X/M inactive/active | Inactive表示路由不可达，active表示路由可达 |

### show ipv6 route static

**show ipv6 route static**命令用来显示静态IPv6路由。

【命令】

**show ipv6 route static**

【视图】

任意视图

【举例】

# 显示IPv6静态路由。

host# show ipv6 route static

Codes: C - connected, S - static

> - selected route, \* - FIB route

S 1:1:2::/64 [1/0] via 1:1:3::1 inactive

表 24-5 show ipv6 route static命令显示信息描述表

| 字段 | 描述 |
| --- | --- |
| S | 静态路由 |
| C | 直连路由 |
| > | 下发到内核用于转发的路由 |
| \* | 当前被选中的路由 |
| via X:X::X:X/M | 下一跳地址 |
| directly connected | 直连路由 |
| inactive | 下一跳不可达 |

### show ipv6 route summary

**show ipv6 route summary**命令用来显示IPv6路由的汇总情况。

【命令】

**show ipv6 route summary**

【视图】

任意视图

【举例】

# 显示IPv6路由的汇总情况。

host# show ipv6 route summary

Route Source Routes FIB

connected 2 2

static 1 0

------

Totals 3 2

表 24-6 show ipv6 route summary命令显示信息描述表

| 字段 | 描述 |
| --- | --- |
| Route Source | 路由类型：  connected表示直连路由  static表示静态路由  Totals 表示合计 |
| Routes | 路由的条目数 |
| FIB | FIB的条目数 |

【相关命令】

* show ipv6 route

# IPv6邻居发现命令参考

## IPv6路由命令

### clear ipv6 neighbor

**clear ipv6 neighbor**命令用来清除设备上的IPv6邻居表项。

【命令】

**clear ipv6 neighbor**

【视图】

用户视图/系统视图

【举例】

# 清除IPv6邻居表项。

host# configure terminal

host(config)# clear ipv6 neighbor

### ipv6 nd dad attempts

**ipv6 nd dad attempts**命令用来设置地址重复性检测次数。

**no ipv6 nd dad attempts**命令用来恢复地址重复性检测次数的默认值。

【命令】

**ipv6 nd dad attempts** *times*

**no ipv6 nd dad attempts**

【缺省情况】

缺省情况下，地址重复性检测次数为1。

【视图】

接口视图

【参数】

*times*：地址重复性检测次数，取值范围为0～20。

【举例】

# 在接口ge1上设置地址重复性检测次数为3。

host# configure terminal

host(config)# interface ge1

host(config-ge1)# ipv6 nd dad attempts 3

【相关命令】

* show ipv6 nd nud-params

### ipv6 nd nud ns-retrans-interval

**ipv6 nd nud ns-retrans-interval**命令用来设置NS重传的时间间隔。

**no ipv6 nd nud ns-retrans-interval**命令用来恢复NS重传的时间间隔为默认值。

【命令】

**ipv6 nd nud ns-retrans-interval** *time*

**no ipv6 nd nud ns-retrans-interval**

【缺省情况】

缺省情况下，NS重传的时间间隔为1000毫秒。

【视图】

系统视图

【举例】

# 配置NS重传的时间间隔为2000毫秒。

host# configure terminal

host(config)# ipv6 nd nud ns-retrans-interval 2000

【相关命令】

* show ipv6 nd nud-params

### ipv6 nd nud reachable-time

**ipv6 nd nud reachable-time**命令用来设置邻居可达时间。

**no ipv6 nd nud reachable-time**命令用来恢复设置邻居可达时间到默认值。

【命令】

**ipv6 nd nud reachable-time** *time*

**no ipv6 nd nud reachable-time**

【缺省情况】

邻居可达时间默认为1000毫秒。

【视图】

接口视图

【参数】

*time*：地址重复性检测时发送NS的间隔，取舍范围为1～3600000，单位为毫秒。

【举例】

# 在接口ge1上设置地址重复性检测的间隔为2000毫秒。

host# configure terminal

host(config)# interface ge1

host(config-ge1)# ipv6 nd dad interval 2000

### ipv6 nd ra-interval

**ipv6 nd ra-interval**命令用来配置路由通告的发送间隔。

**no ipv6 nd ra-interval**命令用来恢复路由通告的发送间隔为默认值。

【命令】

**ipv6 nd ra-interval** *max-interval* [ *min-interval* ]

**no ipv6 nd ra-interval**

【缺省情况】

缺省情况下，最大发送间隔为600秒，最小间隔为198秒。

【视图】

接口视图

【参数】

*max-interval* ：路由通告的最大发送间隔，取值范围为4～1800，单位为秒。

*min-interval* ：路由通告的最小发送间隔，取值范围为3～1350，单位为秒。如果不指定最小间隔，则使用（最大间隔\*0.33）为默认的最小间隔，但如果最大发送间隔小于9秒，则最小间隔和最大间隔相等。

【举例】

# 配置路由通告的最大发送间隔为100秒，最小发送间隔为20秒。

host# configure terminal

host(config)# interface ge1

host(config-ge1)# ipv6 nd ra-interval 100 20

【相关命令】

* show ipv6 rtadv-conf

### ipv6 nd send-ra

**ipv6 nd send-ra**命令用来开启路由通告。

**no ipv6 nd send-ra**命令用来关闭路由通告。

【命令】

**ipv6 nd send-ra**

**no ipv6 nd send-ra**

【缺省情况】

缺省情况下，路由通告处于关闭状态。

【视图】

接口视图

【举例】

# 在接口ge1下开启路由通告。

host# configure terminal

host(config)# interface ge1

host(config-ge1)# ipv6 nd send-ra

【相关命令】

* show ipv6 rtadv-conf

### show ipv6 nd nud-params

**show ipv6 nd nud-params**命令用来显示邻居不可达检测的配置。

【命令】

**show ipv6 nd nud-params**

【视图】

任意视图

【举例】

# 显示邻居不可达检测的配置。

host# show ipv6 nd nud-params

NUD base reachable time: 30000(millisecond)

NUD current reachable time: 15550(millisecond)

gc statle time: 60000(millisecond)

NS retrans interval: 1000(millisecond)

表 25-1 show ipv6 nd nud-params命令显示信息描述表

| 字段 | 描述 |
| --- | --- |
| NUD base reachable time | 用户配置的邻居可达时间 |
| NUD current reachable time: | 设备当前实际使用的邻居可达时间 |
| gc stale time | 不可达邻居的超时时间 |
| NS retrans interval | NS报文重传间隔 |

### show ipv6 neighbor

**show ipv6** **neighbor**命令用来显示IPv6邻居表项。

【命令】

**show ipv6 neighbor**

【视图】

任意视图

【举例】

# 显示IPv6邻居表项。

host# show ipv6 neighbor

Codes: V - neighbor's HW address is valid S - static neighbor

----------------------------------------------------------------------------------------

IPv6 address HW address Device Flags State

----------------------------------------------------------------------------------------

2003:7856::3 28:d2:44:01:fc:3b ge0 V REACHABLE

表 25-2 show ipv6 neighbor命令显示信息描述表

| 字段 | 描述 |
| --- | --- |
| IPv6 address | IPv6地址 |
| HW address | MAC地址 |
| Device | 出接口 |
| Flags | 可能含有如下标志：  V表示邻居表项可用  S表示静态配置的邻居表项 |
| State | 邻居表项所处的状态：  REACHABLE，邻居可达  FAILED，邻居不可用  INCOMPLETE，邻居的MAC地址正在获取中 |

# IPv6隧道命令参考

## **IPv6隧道命令**

### interface tunnel

**interface tunnel**命令用来创建隧道并进入接口视图，如果指定的隧道已经存在，则直接进入隧道视图，不需要再创建隧道。

**no interface**命令用来删除已经存在的隧道接口。

【命令】

**interface****tunnel** *tunnel-id* **mode ipv6ip** { *manual* | *6to4* | *isatap* }

**no interface** *interface-name*

【视图】

系统视图

【参数】

*tunnel-id*：隧道id，取值范围是0到1023。

*manua*：IPv6手动隧道。

*6to4*：6to4隧道。

*isatap*：ISATAP 隧道。

*interface-name*：接口名称。

【举例】

# 创建一个IPv6手动隧道。

host(config)#interface tunnel 0 mode ipv6ip manual

【相关命令】

* show tunnel ipv6ip

### show tunnel

**show tunnel**命令用来查看指定的隧道的信息。

【命令】

show tunnel [ *tunnel-id* ]

【视图】

任意视图

【参数】

*tunnel-id*：隧道id，取舍范围为0～1023。

【举例】

# 查看tunnel0的隧道信息。

host#show tunnel 0

tunnel mode: manual(ipv6)

tunnel saddr: 192.168.1.134

tunnel daddr: 192.168.1.132

表 26-1 show tunnel命令显示信息描述表

| 字段 | 描述 |
| --- | --- |
| tunnel mode | 隧道的模式，可能是6to4、manual、isatap三种之一 |
| tunnel saddr | 隧道的源地址 |
| tunnel daddr | 隧道的目的地址 |

### show tunnel ipv6ip

**show tunnelipv6ip**命令用来查看所有IPv6隧道信息

【命令】

show tunnel ipv6ip

【视图】

任意视图

【举例】

# 查看所有IPv6隧道信息。

host# show tunnel ipv6ip

A:admin state;L:link state; U:up;D:down;

---------------------------------------------------------------------------

Interface Mode Source Destination A L

---------------------------------------------------------------------------

tunnel1 6to4 192.168.1.2 - U D

表 26-2 show tunnel ipv6ip命令显示信息描述表

| 字段 | 描述 |
| --- | --- |
| Interface | 隧道名称 |
| Mode | 模式，有三种模式：  6to4  manual  isatap |
| Source | 隧道的源地址或者源接口 |
| Destination | 隧道的目的地址 |
| A | 隧道的启用状态，D表示未启用，U表示已经启用 |
| L | 隧道的连接状态，D表示未连接，U表示已经连接 |

### tunnel destination

**tunnel destination**命令用来配置隧道的目的地址。

**tunnel destination**命令用来删除隧道的目的地址。

【命令】

**tunnel destination** *ip-address*

**no tunnel destination**

【视图】

接口视图

【参数】

*ip-address*：隧道目的地址。封装报文时，该地址将作为IPv4报头的目的地址。

【使用指导】

只有IPv6手动隧道才能配置隧道目的地址。

【举例】

# 配置隧道的目的地址为192.168.3.2。

host# configure terminal

host(config)#interface tunnel 0 mode ipv6ip manual

host(config-tunnel0)#tunnel destination 192.168.3.2

【相关命令】

* tunnel source
* show tunnel ipv6ip

### tunnel source

**tunnel source** 命令用来配置隧道的源地址或源接口。

**no tunnel source**命令用来删除隧道的源地址或源接口。

【命令】

**tunnel source** { *ip-address* | *inteface-name* }

**no tunnel source**

【视图】

接口视图

【参数说明】

*ip-address*：隧道源地址。封装报文时，该地址将作为IPv4报头的源地址。

*interface-name*：隧道源接口。封装报文时，将采用该接口的主IP地址作为IPv4报头的源地址。

【举例】

# 配置隧道的源地址为192.168.3.1。

host# configure terminal

host(config)#interface tunnel 0 mode ipv6ip manual

host(config-tunnel0)#tunnel source 192.168.3.1

【相关命令】

* tunnel destination
* show tunnel ipv6ip

# IPv6命令参考

## IPv6策略命令

### dest-address

**dest-address**命令用来增加策略的目的地址。

**no dest-address**命令用来删除策略的目的地址。

【命令】

**dest-address** *addr-name*

**no dest-address** *addr-name*

【视图】

IPv6策略视图

【参数】

*addr-name*：地址对象或者地址对象组的名称。

【使用指导】

策略上最多可以指定8个目的地址对象。

【举例】

# IPv6策略1添加目的地址对象abc。

host# configure terminal

host(config)#policy6 1

host(config-policy6)# dest-address aaa

【相关命令】

* show running-config ipv6-policy

### enable

**enable**命令用来启用IPv6策略。

**disable**命令用来禁用IPv6策略。

【命令】

**enable**

**disable**

【缺省情况】

缺省情况下，IPv6策略是启用的。

【视图】

IPv6策略视图

【举例】

# 禁用IPv6策略1。

host# configure terminal

host(config)#policy6 1

host(config-policy6)# disable

【相关命令】

* show running-config ipv6-policy

### in-interface

**in-interface**命令用来修改策略的源接口。

【命令】

**in-interface** { *interface-name* | **any** }

【视图】

IPv6策略视图

【参数】

*interface-name*：入接口的名称。

**any**：任意入接口。

【举例】

# 修改IPv6策略1的入接口为ge0。

host# configure terminal

host(config)#policy6 1

host(config-policy6)# in-interface ge0

【相关命令】

* show running-config ipv6-policy

### out-interface

**out- interface**命令用来修改IPv6策略的出接口。

【命令】

**out-interface** { *interface-name* | **any** }

【视图】

IPv6策略视图

【参数】

*interface-name*：出接口的名称。

**any**：任意出接口。

【举例】

# 修改IPv6策略1的出接口为ge1。

host# configure terminal

host(config)#policy6 1

host(config-policy6)# out-interface ge1

【相关命令】

* show running-config ipv6-policy

### policy6

**policy6**命令用来新建IPv6策略。

**no policy6**命令用来删除指定的IPv6策略。

【命令】

**policy6** *in-ineterface out-interface source-address destination-address service***anyany** *schedule* { **permit** | **deny** | **ipsec** } [ *id* ]

**no policy6** *id*

【视图】

系统视图

【参数】

*in-interface*：入接口。

*out-interface*：出接口。

*source-address*：源地址。

*destination-address*：目的地址。

*schedule*：时间表。

**permit：**行为是允许。

**deny：**行为是拒绝。

**ipsec：**行为是ipsec。

*id*：IPv6策略的id，取值范围为1～65535。

【使用指导】

如果添加一条IPv6策略，请执行以上命令，其中的出入接口、源目的ip地址、服务、应用、用户、时间等匹配条件除了any或者always外，需要配置具体的对象，才能被IPv6策略引用。

新添加的IPv6策略位于所有IPv6策略的最后面。

【举例】

# 创建一条服务是TCP，其余匹配条件为any，动作是允许通过的IPv6策略。

host# configure terminal

host(config)# policy6 any any any any TCP any any any always permit

【相关命令】

* show running-config ipv6-policy

### policy6 default-action

**policy6 default-action**命令用来设置设备IPv6策略的默认动作。

【命令】

**policy6 default-action** { **permit** | **deny** }

【缺省情况】

缺省情况下，IPv6策略的默认动作为允许。

【视图】

系统视图

【参数】

**permit**：IPv6策略的默认行为为允许。

**deny**：IPv6策略的默认行为为拒绝。

【举例】

# 将IPv6策略的默认行为改为拒绝。

host# configure terminal

host(config)# policy6 default-action deny

【相关命令】

* show running-config ipv6-policy

### policy6 insert

**policy6 insert**命令用来在指定的策略ID之前插入一条策略。

【命令】

**policy6** **insert** *in-ineterface out-interface source-address destination-address service* **any** **any** *schedule* { **permit** | **deny** | **ipsec** } *id* **before** *reference-policy-id*

【视图】

系统视图

【参数】

*in-interface*：入接口。

*out-interface*：出接口。

*source-address*：源地址对象。

*destination-address*：目的地址对象。

*service*：服务对象

*schedule*：时间表。

**permit：**行为是允许。

**deny：**行为是拒绝。

**ipsec：**行为是ipsec。

*id*：IPv6策略的id，取值范围为1到65535。

*id reference-policy-id*：被参照的IPv6策略id。

【举例】

# 创建ID是2服务是TCP，其余匹配条件为any，动作是允许的IPv6策略，位置在IPv6策略1的前面。

host# configure terminal

host(config)# policy6 insert any any any any tcp any any always permit 2 before 1

【相关命令】

* show running-config ipv6-policy

### policy6 move

**policy6 move**命令用来移动IPv6策略的位置。

【命令】

**policy6 move** *policy-id* { **before** | **after** } *reference-policy-id*

【视图】

系统视图

【参数】

*policy-id*：被移动的策略id。

**before**：把策略移动到参照的策略的前面。

**after**：把策略移动到参照的策略的后面。

*reference-policy-id*：被参照的策略id。

【举例】

# 将IPv6策略1移到IPv6策略2之后。

host# configure terminal

host(config)# policy6 move 1 after 2

【相关命令】

* show running-config ipv6-policy

### schedule

**schedule**命令用来设置IPv6策略生效的时间表。

【命令】

**schedule** *schedule-name*

【视图】

IPv6策略视图

【参数】

*schedule-name*：时间对象的名称。

【使用指导】

只有在时间对象处于active状态，IPv6策略才会生效。

【举例】

# 配置IPv6策略1，仅仅在9:00-18:00生效。

host# configure terminal

host(config)# schedule-day worktime

host(config-schedule-day)# periodic start 9:00 end 18:00

host(config-schedule-day)# exit

host(config)#policy6 1

host(config-policy6)# schedule worktime

【相关命令】

show running-config ipv6-policy

### service

**service**命令用来增加策略的服务。

**no service**命令用来删除策略的服务。

【命令】

**service** *service-name*

**no service** *service-name*

【视图】

IPv6策略视图

【参数】

*service-name*：服务对象的名称。

【使用指导】

策略上最多可以指定8个服务对象。

【举例】

# IPv6策略1添加目的服务对象icmp。

host# configure terminal

host(config)#policy6 1

host(config-policy6)# service icmp

【相关命令】

* show running-config ipv6-policy

### show running-config ipv6-policy

**show running-config ipv6**命令用来显示配置的IPv6策略。

【命令】

**show running-config ipv6**

【视图】

任意视图

【举例】

# 显示IPv6策略的配置。

host# show running-config ipv6-policy

policy6 any any any any any any any always permit 1

policy6 default-action deny

!

**show running-config ipv6**命令显示IPv6策略的配置，具体的含义参见各个命令的介绍。

【相关命令】

* show running-config ipv6-policy

### source-address

**source-address**命令用来增加策略的源地址。

**no source-address**命令用来删除策略的源地址。

【命令】

**source-address** *addr-name*

**no source-address** *addr-name*

【视图】

IPv6策略视图

【参数】

*addr-name*：地址对象的名称。

【使用指导】

策略上最多可以指定8个源地址对象。

【举例】

# IPv6策略1添加源地址对象abc。

host# configure terminal

host(config)#policy6 1

host(config-policy6)# source-address aaa

【相关命令】

* show **running**-config ipv6-policy