

山石网科应用交付系统命令行手册

Version 3.1



Copyright 2022 Hillstone Networks. All rights reserved.

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of those agreements. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Hillstone Networks.

Hillstone Networks

本文档禁止用于任何商业用途。

联系信息

北京

地址：北京市海淀区宝盛南路1号院20号楼5层

邮编：100192

联系我们：http://www.hillstonenet.com.cn/about/contact_Hillstone.html

苏州

地址：苏州高新区科技城景润路181号

邮编：215000

关于本手册

本手册介绍山石网科的应用交付系统 ADC的使用方法。

获得更多的文档资料，请访问：<https://docs.hillstonenet.com.cn>

针对本文档的反馈，请发送邮件到：TechDocs@hillstonenet.com

山石网科

<https://www.hillstonenet.com.cn>

TWNO: TW-CUG-ADC-3.1-CN-V1.0-9/16/2022

目 录

目 录	1
第1章 服务器负载均衡	1
SLB相关概念	2
负载均衡算法	2
配置虚拟服务器	4
配置虚拟服务器部署模式	8
配置虚拟服务器IP和端口	9
配置流量组	10
配置域名匹配规则	10
配置请求主机匹配SNI	12
启用默认虚拟服务器	12
配置自动源NAT	12
配置虚拟服务器IP地址是否允许被PING	13
配置数据库账号	14
开启/关闭事务保持功能	14
配置最大连接数	14
配置虚拟服务器的状态	15
指定缺省服务池	15
指定备份服务池	16
指定写服务池	16

指定读服务池	16
指定设备与客户端的交互方式	16
指定支持的客户端认证方式	17
指定服务器名称	17
指定虚拟服务器支持的功能	18
查看虚拟服务器的运行状态	18
配置最大连接数	19
配置连接失败动作	19
配置连接速率限制	20
配置防浪涌等待队列	20
配置超时连接动作	20
开启历史信息记录	21
记录日志	21
TOA类型	22
插入TOA	22
绑定SSL模板	23
绑定服务端SSL模板	23
绑定应用模板	23
绑定TCP模板	24
配置DNS服务器	24
配置IPv6的DNS查询	24
配置DNS有效时间	25

开启HTTP隧道模式	25
配置自动修改HTTP头部协议	25
指定脚本文件	26
指定四层内容交换规则	26
移动规则	27
指定七层内容交换规则	27
移动规则	28
指定内容改写规则	28
移动规则	28
指定SQL内容交换规则	29
移动规则	29
指定Web防护模板	30
配置主机改写	30
配置访问控制	31
移动规则	31
配置错误信息	31
导入页面	32
删除页面	32
查看页面	33
配置三角模式	33
配置UDP强制负载	33
配置UDP超时时间	33

反向路由	34
配置调度模式	34
镜像请求	35
配置入接口模式	35
配置虚拟服务器IP的路由发布	36
配置虚拟服务器外链改写	37
配置基于路径方式的外链改写	37
配置虚拟服务器外链探测	39
配置基于域名方式的外链改写	39
配置虚拟服务器的探测服务器功能	41
查看虚拟服务器信息	41
配置真实服务	42
创建真实服务	42
指定IP和端口	43
指定域名和端口	43
自动解析域名所有IP	44
配置最大连接数	44
配置连接速率限制	45
指定恢复时间	45
指定预热时间	45
配置真实服务的权重	46
配置真实服务的状态	46

绑定健康检查对象	47
开启历史信息记录	47
查看真实服务配置	47
查看真实服务的运行状态	47
配置服务池	48
创建服务池	48
添加真实服务	48
启用/禁用真实服务	49
指定真实服务恢复时间	49
指定真实服务预热时间	50
配置真实服务优先级调度功能	50
配置会话保持算法	51
基于Cookie的会话保持算法	51
基于Cookie哈希的会话保持算法	52
基于URL哈希的会话保持算法	53
基于首部的会话保持算法	54
基于插入Cookie的会话保持算法	55
基于改写Cookie的会话保持算法	57
基于HTTP版本的会话保持算法	58
基于请求方法的会话保持算法	58
基于目的IP的会话保持算法	59
基于源IP的会话保持算法	60

基于源IP与目的IP的会话保持算法	61
基于TOA的会话保持算法	62
基于TOA或源IP（TOA优先）的会话保持算法	63
基于真实源IP的会话保持算法	63
基于URL的会话保持算法	64
基于SSL ID的会话保持算法	65
基于SNI的会话保持算法	66
基于Call ID的会话保持算法	67
基于RDP的会话保持算法	67
基于RADIUS属性的会话保持算法	68
查看会话保持表	71
清空会话保持表	72
配置负载均衡算法	73
绑定健康检查对象	77
开启/关闭手动恢复功能	77
手动恢复运行状态	77
查看服务池配置	78
查看服务池的运行状态	78
服务池中真实服务的运行状态	79
配置SLB规则	79
配置四层内容交换规则	80
配置客户端源IP	80

配置客户端源端口	80
配置客户端目的IP	81
配置客户端目的端口	81
配置四层内容交换支持的协议	81
配置服务池	82
配置描述信息	82
查看四层内容交换规则	82
配置HTTP内容改写规则	82
配置文本编码方式	83
配置匹配操作符	84
配置匹配条件	84
配置匹配条件区分大小写	87
配置内容改写规则动作	87
配置动作为重定向	87
替换URL	87
指定协议（保持原有路径和查询）	88
改写URL	88
配置动作为消息体改写	89
配置动作为头部改写	89
配置动作为Cookie改写	90
配置动作为URL改写	91
配置动作为删除Cookie	91

配置动作为删除头部	91
配置动作为插入头部	92
配置动作为插入Cookie	92
配置动作为添加IP协议类型标识	93
配置动作为插入源IP	94
配置动作为插入真实源IP	94
配置描述信息	94
查看内容改写规则信息	95
HTTP内容改写_变量使用说明	95
配置HTTP内容交换规则	98
配置描述信息	99
配置文本编码方式	99
配置匹配操作符	99
配置服务池	100
配置匹配条件	100
配置匹配条件区分大小写	103
查看HTTP内容交换规则	103
SQL内容交换规则	103
配置匹配条件	104
配置服务池/真实服务器	104
配置失败动作	105
配置描述信息	105

查看SQL内容交换规则	105
配置访问控制规则	106
配置描述信息	106
配置文本编码方式	106
配置匹配操作符	107
配置匹配条件	107
配置匹配条件区分大小写	110
配置访问控制动作	110
配置时间表	111
查看访问控制规则	111
查看SLB规则状态	111
配置客户端SSL模板	112
创建SSL模板	112
配置握手超时时间	112
配置加密套件	113
启用服务器加密套件优先	113
调整加密套件顺序	113
配置SSL版本	114
配置证书链	114
配置基于SSL会话ID的会话复用功能	114
配置基于SSL会话票据的会话复用功能	115
配置0RTT功能	115

配置国密加密套件	115
调整国密加密套件顺序	116
配置国密签名证书链	117
配置国密加密证书链	117
SSL客户端验证	117
指定对客户端验证的方式	117
指定需验证的CA证书	118
自动CA证书通告	118
指定需通告的CA证书	118
配置验证证书最小密钥长度	118
配置客户端验证的证书最大深度	119
配置客户端验证规则	119
配置URL验证匹配规则	120
配置客户端证书的OCSP验证	121
清除OCSP缓存	122
配置OCSP Stapling	123
查看SSL模板配置	124
配置服务端SSL模板	124
创建服务端SSL模板	125
配置握手超时时间	125
启用SNI功能	125
配置加密套件	126

调整加密套件顺序	126
配置SSL版本	127
配置证书链	127
配置国密加密套件	127
调整国密加密套件顺序	128
配置国密签名证书链	128
配置国密加密证书链	129
查看SSL模板配置	129
SSL加速卡	129
SSL加速卡相关命令	129
查看加速卡统计数据	129
清除加速卡统计数据	131
测试加速卡功能	131
查看加速卡的驱动版本号	132
查看加速卡以及国密卡状态	132
切换SSL加速模式	133
配置应用模板	134
创建应用模板	134
HTTP 2.0协议	135
开启HTTP 2.0	135
配置空闲连接超时时间	135
配置最大并发流	135

配置接收窗口大小	135
配置数据帧大小	136
配置标题表大小	136
插入标题X-HTTP2	136
配置网页优化	136
配置网页的HTML优化	137
配置网页的图片优化	138
开启WebSocket	140
配置保活超时时间	140
配置连接超时时间	140
配置查询时间	141
配置MYSQL保活超时时间	141
配置读写超时时间	141
配置连接复用	142
配置读取超时时间	142
配置发送超时时间	143
开启X-Forward-For	143
开启X-Real-IP	143
配置缓冲区大小	143
配置首片缓冲区大小	144
配置最大请求体大小	144
配置最大请求头大小	144

启用/禁用代理缓冲功能	144
HTTP缓存	145
配置HTTP静态资源的内存缓存	145
配置HTTP静态资源的磁盘缓存	146
清除HTTP缓存	148
查看HTTP缓存统计信息	148
HTTP压缩	148
配置HTTP压缩	149
清除HTTP压缩	149
查看HTTP缓存信息	149
配置Cookie加密	149
配置客户端缓存大小	150
配置代理缓存大小	150
配置读写超时时间	150
查看应用模板信息	151
配置Web防护模板	151
创建Web防护模板	152
配置防护动作	153
配置基于虚拟服务器的检测规则	153
配置基于源IP的检测规则	154
配置客户端IP获取方式	154
配置基于URL的检测规则	154

移动基于URL检测规则的位置	155
查看Web防护模板	155
Web防护黑名单	156
查看或清除Web防护黑名单	156
Web防护信任名单	157
查看或清除Web防护信任名单	157
配置TCP模板	158
创建TCP模板	158
配置TCP单边加速	158
配置客户端侧单边加速	158
配置真实服务侧单边加速	159
查看TCP模板信息	159
其他命令	159
显示或清除会话信息	159
显示或清除会话保持表信息	161
延迟删除会话信息	161
启用/禁用延迟删除会话信息功能	161
查看延迟删除会话信息功能的启用状态	162
SSL透视镜模板	162
配置SSL透视镜模板	162
指定模式	162
配置信任域	162

配置匹配规则	163
配置解密协议	163
配置域名簿	163
配置解密SNI为空的流量	163
启用状态统计	164
开启日志开关	164
启用镜像解密监控	164
验证服务器证书	165
提醒信任域证书安装	165
信任域缓存表	166
查看信任域缓存表	166
清除信任域缓存表	166
白名单	167
添加白名单条目	167
删除白名单条目	167
查看白名单	167
状态统计	168
查看状态统计信息	168
清除状态统计信息	168
配置状态统计过期时间	168
健康检查	168
创建健康检查	169

DNS健康检查	171
FTP健康检查	174
SNMP-DCA健康检查	176
SNMP-DCA-BASE健康检查	179
HTTP/HTTPS健康检查	182
ICMP健康检查	185
IMAP健康检查	187
POP3健康检查	189
SMTP健康检查	191
TCP健康检查	193
TCP-ECHO健康检查	195
TCP-HALF-OPEN健康检查	197
UDP健康检查	199
Third-Party健康检查	201
RADIUS-AUTHENTICATION健康检查	203
RADIUS-ACCOUNTING健康检查	205
WebSocket健康检查	208
WebSocket-SSL健康检查	210
SIP-TCP健康检查	212
SIP-UDP健康检查	214
PASSIVE-HTTP健康检查	216
PASSIVE-TCP健康检查	217

MySQL健康检查	218
健康检查组	220
配置健康检查组操作符	221
配置健康检查组成员	221
第2章 全局负载均衡	223
DNS服务器	223
实现流程	223
DNS Server的部署场景	224
配置DNS服务器	225
配置DNS视图	226
创建DNS视图	226
启用DNS视图	226
配置源IP	226
配置目的IP	227
关联区域	228
关联智能DNS	228
递归查询	228
转发配置	228
配置转发目的地址	228
强制RD标志	229
配置默认DNS视图	229
关联智能DNS	229

关联区域	230
递归查询	230
转发配置	230
启用强制RD标志	231
清除DNS缓存	231
配置区域	231
创建区域	232
配置SOA资源	232
配置资源记录	233
配置A记录	233
配置AAAA记录	234
配置NS记录	234
配置CNAME记录	235
配置PTR记录	235
配置MX记录	236
配置TXT记录	236
配置SRV记录	237
启用资源记录	237
关联智能DNS	237
转发配置	238
转发目的地址	238
配置全局配置	238

配置DNS服务器监听地址	238
配置监听端口	239
发布监听地址路由	239
配置UDP会话超时	240
配置缓存	240
开启GSLB统计	240
开启GSLB日志	240
智能DNS	240
负载均衡算法	241
配置智能DNS	241
配置ISP	242
添加IP网段	242
配置地区	242
配置国家信息	243
配置省份信息	243
配置IP网段	243
配置ISP	243
配置服务器和服务池	244
创建服务器	244
服务器状态	244
服务器IP	244
服务器权重	244

指定健康检查	245
指定健康检查端口	245
引用地区	245
绑定接口	246
服务器优先级	246
启用服务器可用性验证	246
绑定数据中心	247
创建服务器池	247
服务器池状态	247
指定首选算法	247
指定备选算法	248
服务器池所属地区	249
服务器池权重	249
指定健康检查	249
指定健康检查端口	249
启用链路繁忙保护	250
配置服务器池成员	250
服务器成员运行状态	250
配置Smart DNS主机	251
DNS主机状态	251
配置域名	251
配置TTL	251

配置算法	252
配置保持算法	252
配置服务器池成员	252
配置默认服务器池	253
数据中心	253
应用场景举例	254
配置数据中心	254
创建本地数据中心	255
指定IP地址	255
指定联系人	255
指定地理位置	256
启用虚拟服务器发现	256
指定本地IP地址	256
指定本地设备	256
发现数据中心	257
查看数据中心	257
配置GSLB同步组	258
添加GSLB同步组成员	258
配置同步	258
查看GSLB同步组	258
注册SLB设备到数据中心	258
配置本地设备	259

手动发现虚拟服务器	259
查看本地设备	259
第3章 链路负载均衡	260
出站负载均衡	260
创建LLB Profile	260
配置负载均衡算法	261
配置带宽统计周期	265
开启综合考虑其它调度结果功能	265
配置链路负载均衡的优先级调度策略	266
配置主动探测	266
配置链路探测	267
开启链路探测	267
配置链路探测掩码/前缀	267
配置带宽利用率阈值	268
配置计算链路状态时各项权值	268
配置链路权重刷新时间	268
配置子网条目最大值	269
配置带宽探测方向	269
配置负载均衡的模式	269
配置会话保持方法	270
配置会话保持超时时间	270
配置链路繁忙保护	270

配置日志记录	271
添加描述信息	271
绑定LLB Profile	271
查看会话保持表	272
查看链路负载均衡信息	273
第4章 设备集群	274
集群基础概念	274
设备发现与认证	274
设备组	274
流量组	274
集群同步	275
配置集群	275
配置本地管理地址	276
设备发现与认证	276
配置本地设备	276
配置证书链	276
配置设备IP	276
配置主故障转移IP	277
配置次故障转移IP	277
配置主镜像IP	277
配置设备联系方式	277
配置设备地理位置	278

配置设备发现超时时间	278
配置设备在线超时时间	278
添加设备描述信息	278
发现设备	279
集群同步	279
配置设备组	280
配置同步范围	280
添加设备	281
配置心跳时间间隔	281
配置心跳阈值	281
配置流量组	282
配置故障转移顺序	282
配置负载系数	283
指定监测对象	283
启用抢占功能	284
配置抢占时间	284
启用数据对象同步	284
配置虚拟MAC	284
配置虚拟MAC前缀	285
配置非对称流量转发	285
启用非对称流量转发功能	285
查看集群配置	286

第5章 网络连接	287
安全域	287
配置安全域	288
显示域信息	288
创建安全域	288
指定描述信息	289
绑定二层域到VSwitch	289
绑定三层域到VRouter	289
配置安全域WAN属性	290
接口	290
查看接口信息	291
配置接口	292
绑定接口到域	294
配置接口描述信息	294
配置接口IP地址	294
配置接口IP地址的Local属性	295
配置接口IP地址所属流量组	295
配置接口浮动IP	296
配置接口二级IP地址	296
配置接口二级管理IP地址	296
配置接口所属ISP	297
配置接口的链路负载均衡优先级	297

配置接口的链路负载均衡权值	297
配置接口带宽	298
配置接口最大传输单元（MTU）	298
强制关闭接口	298
设置接口ARP超时时间	299
配置接口管理功能	299
配置FTP服务功能	300
关闭记录接口IP地址冲突日志功能（DAD模式ARP报文触发）	300
配置接口代理ARP功能	301
配置基于策略的接口镜像过滤功能	301
配置mirror Profile	302
指定流量镜像目的接口	302
指定流量镜像目的地址	303
指定策略规则引用mirror Profile	303
显示mirror Profile信息	303
配置接口逆向路由功能	304
配置接口备份功能	304
配置接口保持时间	305
配置接口保活功能	306
配置接口联动功能	306
配置接口Local属性	307
配置接口WAN属性	307

回环接口	307
创建回环接口	307
以太网接口	308
创建以太网子接口	308
进入以太网接口配置模式	308
配置以太网接口的速率	308
配置以太网接口的工作方式	309
克隆MAC地址	309
配置Combo口	310
VSwitch接口	310
创建VSwitch接口	310
集聚接口	311
创建集聚接口以及集聚子接口	311
添加接口到集聚接口	311
指定报文发送均衡方式	312
冗余接口	312
创建冗余接口以及冗余子接口	312
添加接口到冗余接口	313
指定主接口	313
开启或关闭ARP回环告警日志	313
隧道接口	314
创建隧道接口	314

绑定隧道	314
多隧道OSPF支持	315
配置借用IP地址功能 (IP Unnumbered)	315
查看隧道接口信息	315
PPPoE子接口	316
链路聚合	316
LACP动态协商聚合	316
聚合组成员接口状态	316
配置LACP动态协商聚合	317
启用/禁用LACP协议	317
指定LACP系统优先级	318
指定接口LACP优先级	318
指定LACP超时时间	318
指定最大活动链路数	319
指定最小活动链路数	319
指定报文发送均衡方式	319
查看聚合组信息	320
LLDP	320
LLDP工作模式	320
配置LLDP功能	321
开启/关闭全局LLDP功能	321
开启/关闭接口的LLDP功能	322

配置接口的LLDP工作模式	322
配置接口初始化延迟时间	322
配置LLDP报文发送间隔	323
配置LLDP报文发送延迟时间	323
配置TTL乘数	323
显示LLDP本地信息	324
显示接口的LLDP邻居信息	324
显示LLDP统计信息	324
显示LLDP报文收发信息	324
显示LLDP状态信息	324
DNS	325
配置DNS名字服务	325
设置域名	325
设置DNS域名服务器	326
配置DNS代理功能	326
配置DNS代理规则	327
创建DNS代理规则	327
配置DNS代理过滤条件	327
指定DNS入接口	327
指定DNS源地址	328
指定DNS目的地址	328
指定DNS 域名	329

配置DNS代理规则动作	329
配置DNS服务器调度算法	329
DNS服务器调度算法	330
配置DNS服务器	331
开启/关闭DNS64功能	332
配置DNS64服务器	332
配置DNS64前缀	332
配置描述信息	333
启用/禁用DNS代理规则	333
修改DNS代理规则的排列顺序	333
配置DNS代理服务器探测功能	334
开启/关闭DNS代理的UDP报文校验和功能	334
指定DNS代理响应报文的TTL	334
查看DNS代理规则信息	335
解析	335
设置DNS请求的响应超时时间	335
设置DNS请求重试次数	335
指定链路权值	336
指定DNS解析动态缓存的TTL	337
开启DNS解析日志功能	337
缓存	337
添加静态DNS映射条目	337

查看DNS映射条目	338
清除动态DNS映射条目	338
DNS Snooping	338
指定域名解析方式	339
指定精确域名最大映射IP数	340
指定转发响应报文延时时间	340
指定最大通配符域名数	340
指定DNS Snooping映射缓存TTL	341
查看DNS Snooping配置信息	341
查看DNS Snooping域名及IP映射信息	341
开启/关闭DNS功能	342
开启DNS解析日志功能	342
显示DNS配置信息	342
DHCP	342
配置DHCP客户端功能	343
配置DHCP方式获取IP地址	343
释放和重新获取IP地址	343
配置路由优先级（管理距离）和路由权值	344
配置DHCP服务器功能	344
DHCP地址池基本配置	345
IP地址配置	345
保留地址池配置	345

网关配置	345
网络掩码配置	346
DHCP租约配置	346
配置自动配置功能	346
为DHCP客户端配置DNS、WINS服务器和域名	346
为DHCP客户端配置SMTP、POP3和新闻服务器	347
配置中继代理IP地址	347
IP-MAC地址绑定	348
绑定地址池到接口	348
配置DHCP选项	348
配置Option 49	348
配置Option 60	349
验证客户端Option 60字段携带的VCI	349
设置DHCP服务器Option 60字段携带的VCI	349
配置Option 138	350
查看DHCP配置信息	350
配置DHCP中继代理功能	350
指定DHCP服务器的IP地址	351
开启接口的DHCP中继代理功能	351
DDNS	351
配置DDNS功能	352
配置DDNS服务名称	352

指定DDNS服务器类型	352
指定DDNS服务器名称和端口号	353
指定最小更新间隔	353
指定最大更新间隔	353
指定DDNS用户	354
绑定DDNS服务名称到接口	354
显示DDNS信息	354
PPPoE	355
配置PPPoE	355
配置PPPoE实例	355
指定访问集中器	356
指定验证方式	356
配置PPPoE连接方式	356
指定网络掩码	357
指定路由距离和权值	357
指定服务	357
指定静态IP	358
指定PPPoE用户信息	358
配置时间表功能	358
指定PPPoE服务器MAC地址	359
配置连接状态检测	359
配置接口使用PPPoE方式获得IP地址	360

绑定PPPoE实例到接口	360
手动连接或者断开PPPoE连接	360
显示PPPoE配置信息	360
虚拟交换机	361
VSwitch中的转发规则	361
查看MAC表信息	362
配置VSwitch	362
透明模式下的VLAN透传	363
透明模式下的ARP功能	364
配置NAT	364
创建SNAT规则	364
启用/禁用SNAT规则	367
修改SNAT规则排列顺序	367
开启/关闭扩展PAT端口池功能	368
删除SNAT规则	368
修改/删除SNAT描述信息	368
显示SNAT配置信息	369
查看监测失败的SNAT转换地址	369
创建DNAT规则	370
启用/禁用DNAT规则	372
修改DNAT规则排列顺序	372
修改/删除DNAT描述信息	372

删除DNAT规则	373
显示DNAT配置信息	373
DNS Rewrite	374
透明NAT	374
Full-cone NAT	374
显示Full-cone NAT配置信息	376
IP包数据处理选项	376
配置MSS值	376
TCP序列号检查	377
TCP三次握手超时时间检查	377
TCP连接终止老化时间配置	377
TCP SYN包检查	378
丢弃SYN包	379
IP分片包处理	379
逆向路由	380
应用层网关（ALG）	380
配置ALG功能	380
指定SIP代理模式	382
查看ALG SIP信息	382
第6章 路由	383
开启/关闭静态路由查询	383
开启/关闭会话重匹配路由	384

目的路由	385
添加IPv4目的路由条目	385
添加IPv6目的路由条目	386
查看IPv4/IPv6目的路由信息	387
目的接口路由	387
添加IPv4目的接口路由条目	387
添加IPv6目的接口路由条目	388
查看IPv4/IPv6目的接口路由信息	389
查看IPv6目的接口路由的FIB信息	389
源路由	390
添加IPv4源路由条目	390
添加IPv6源路由条目	391
查看IPv4/IPv6源路由条目信息	391
源接口路由	392
添加IPv4源接口路由条目	392
添加IPv6源接口路由条目	393
查看IPv4/IPv6源接口路由条目信息	394
IPv4 ISP路由	394
配置IPv4 ISP信息	394
添加IPv4子网条目	395
添加IPv4 ISP信息条目	395
配置IPv4 ISP路由	395

查看IPv4 ISP路由配置信息	396
上传IPv4 ISP配置文件	397
删除已上传的预定义IPv4 ISP配置文件	398
IPv6 ISP路由	398
配置IPv6 ISP信息	399
添加IPv6子网条目	399
添加IPv6 ISP信息条目	399
配置IPv6 ISP路由	400
查看IPv6 ISP信息	401
上传IPv6 ISP配置文件	401
删除已上传的预定义IPv6 ISP配置文件	402
策略路由	402
创建PBR策略	402
创建PBR规则	402
编辑PBR策略规则	404
启用/禁用PBR策略规则	406
修改规则排列顺序	406
配置目的路由优先查找	407
应用PBR策略	407
配置PBR策略全局匹配顺序	407
显示PBR策略全局匹配顺序	408
策略路由规则支持配置TTL	408

查看PBR策略规则信息	408
动态路由	408
RIP	409
基本配置	409
指定版本号	409
指定缺省度量	409
指定缺省距离	410
配置缺省信息发布	410
配置定时器	410
引入路由	411
配置被动接口	411
配置邻居	412
配置网络	412
配置距离	412
RIP数据库	413
配置接口的RIP功能	413
配置RIP报文认证	413
配置发送和接收的RIP版本号	413
配置水平分割	414
显示系统RIP信息	414
OSPF	414
OSPF协议配置	415

配置Router ID	416
配置接口的网络类型	417
配置区域的路由聚合	417
配置区域的缺省花费	418
配置区域的虚拟链路	418
配置stub区域	419
配置NSSA区域	420
配置OSPF的引用带宽	420
指定缺省度量	420
配置缺省信息发布	421
指定缺省距离	421
配置OSPF定时器	421
指定运行OSPF协议的接口网络	422
引入路由	422
配置路由映射表	423
匹配多条路由匹配规则	425
修改引入路由属性	426
配置路由访问控制列表	426
配置距离	428
配置被动接口	428
配置接口OSPF功能	428
配置接口的OSPF认证	429

指定接口的链路花费	429
配置接口定时器	429
指定接口路由器优先级	430
配置接口的网络类型	431
显示OSPF信息	431
OSPFv3	433
配置Router ID	434
配置区域的虚拟链路	435
指定缺省度量	435
配置缺省管理距离	435
配置缺省路由发布	436
指定接口区域及实例	436
配置引入路由	437
配置被动接口	437
配置OSPFv3接口定时器	438
指定接口路由器优先级	438
配置接口的链路花费	439
配置接口MTU匹配检查	439
关闭/开启OSPFv3协议	440
查看OSPFv3信息	440
IS-IS	441
IS-IS基本配置	443

指定路由器类型	443
使能接口IS-IS	443
配置接口IS-IS类型	444
配置网络类型为点对点类型	444
IS-IS路由信息配置	444
配置NET地址	444
配置管理距离	444
配置度量类型	445
配置接口度量值	445
引入路由	446
发布缺省路由	446
IS-IS网络优化	446
配置Hello报文发送时间间隔	446
配置Hello报文失效乘数	447
配置Hello报文填充功能	447
配置DIS选举优先级	447
配置被动接口	448
配置LSP生成时间间隔	448
配置LSP最大生存时间	448
配置LSP刷新时间	448
配置SPF计算时间间隔	449
配置过载标志位	449

配置主机名映射	449
IS-IS网络安全性	450
配置认证	450
配置接口认证模式	450
查看IS-IS信息	451
BGP	452
BGP协议配置	453
进入BGP配置模式	454
指定Router ID	454
创建聚合路由	455
添加静态BGP路由	455
配置定时器	455
指定BGP路由管理距离	456
指定缺省度量	456
创建BGP对等体组	457
添加BGP对等体到对等体组	457
配置BGP对等体	457
配置BGP MD5认证	458
激活BGP连接	458
配置缺省信息发布	458
配置描述信息	459
配置BGP对等体定时器	459

配置下一跳为自身	460
配置EBGP多跳	460
关闭对等体或者对等体组	460
重置BGP连接	461
配置AS路径访问控制列表	461
开启/关闭EBGP的multipath-relax功能	462
配置团体属性列表	462
引入路由	463
配置路由映射表	463
修改引入路由属性	465
配置基于AS路径访问控制列表的路由过滤	466
配置向对等体或者对等体组发送团体属性	467
配置基于路由映射表的路由过滤	467
等价负载均衡	467
查看BGP信息	468
等价多径路由（ECMP）	469
配置ECMP功能	469
配置ECMP选路方式	469
静态组播路由	469
开启/关闭组播路由功能	470
配置静态组播路由	470
配置IPv4静态组播路由	470

指定入接口/出接口	471
配置IPv6静态组播路由	471
指定入接口/出接口	472
显示组播路由信息	472
显示组播FIB信息	473
互联网组管理协议	474
IGMP Proxy	474
启用IGMP代理	474
配置接口的IGMP代理模式	475
查看IGMP Proxy信息	475
IGMP Snooping	476
启用IGMP Snooping	476
配置IGMP Snooping	476
未知组播丢弃	477
查看IGMP Snooping信息	477
协议无关组播（PIM）	477
PIM-SM基本原理	478
配置PIM-SM	479
PIM-SM的基本配置	479
开启/关闭PIM-SM功能	480
配置候选RP	480
配置候选BSR	480

配置静态RP	481
指定关闭RPT向SPT切换	481
配置接口的PIM-SM功能	483
开启/关闭接口的PIM-SM功能	483
配置DR优先级	483
指定接口的Hello报文发送间隔	484
指定发送IGMP通用查询报文间隔	484
指定IGMP通用查询超时时间	484
指定IGMP通用查询最大响应时间	485
显示PIM-SM信息	485
PIM-SSM	486
配置PIM-SSM	486
配置PIM-SSM组播组地址范围	487
配置IGMP报文过滤功能	487
BFD	488
BFD工作模式	488
BFD Echo功能	489
配置BFD基本功能	489
配置BFD检测模式	489
配置BFD会话参数	490
开启/关闭Echo功能	490
指定接收Echo报文时间间隔	491

配置Echo报文的源IP地址	491
配置BFD多跳检测	491
创建BFD多跳检测模板	492
指定BFD控制报文的加密认证方式	492
配置BFD多跳会话参数	493
配置BFD与路由协议联动	493
配置BFD与 静态路由联动	493
配置BFD与 OSPF联动	494
配置BFD与 BGP联动	494
显示BFD会话信息	495
第7章 用户认证	496
AAA简介	496
设备外部认证流程	497
配置AAA服务器	497
创建AAA服务器	497
配置本地服务器认证参数	498
配置密码控制	498
允许本地用户修改密码	499
配置密码过期时间及密码到期提醒功能	499
配置历史密码检查功能	499
配置密码复杂度	499
开启/关闭首次登录修改密码功能	500

配置角色映射规则	501
配置用户黑名单	501
配置备份认证服务器	501
配置防暴力破解功能	502
开启或关闭防暴力破解功能	502
配置尝试次数	502
配置锁定时间	503
查看锁定列表信息	503
解除用户/IP地址的锁定	503
配置RADIUS服务器认证参数	504
配置认证主服务器的IP地址或域名	504
配置备份服务器1的IP地址或域名	505
配置备份服务器2的IP地址或域名	505
配置RADIUS服务器端口号	505
配置RADIUS服务器的共享密钥秘密	506
配置重试次数	506
配置超时时间	506
指定角色映射规则	507
配置用户黑名单	507
配置备份认证服务器	507
添加字典文件	508
配置防暴力破解功能	509

开启或关闭防暴力破解功能	509
配置尝试次数	509
配置锁定时间	510
查看锁定列表信息	510
解除用户/IP地址的锁定	510
启用/禁用授权策略	511
添加授权策略到聚合策略	511
配置SM4国密加密算法	511
配置RADIUS服务器的计费功能	512
开启或关闭计费功能	512
配置计费主/备份服务器的IP地址或域名	512
配置计费服务器端口号	513
配置计费服务器的共享密钥	513
配置LDAP服务器认证参数	513
配置认证主服务器的IP地址或域名	514
配置备份服务器1的IP地址或域名	515
配置备份服务器2的IP地址或域名	515
配置服务器端口号	516
配置服务器认证或同步方法	516
指定Base-DN	516
指定登录DN	517
指定Authid属性值	517

指定登录密码	517
指定名称属性	518
指定用户组名称属性	518
指定Group-class	518
指定成员属性名	519
指定角色映射规则	519
配置用户黑名单	519
配置用户同步功能	520
启用/禁用用户同步功能	520
配置用户同步方式	520
配置用户过滤功能	521
配置同步的工作模式	522
配置备份认证服务器	522
配置防暴力破解功能	523
开启或关闭防暴力破解功能	523
配置尝试次数	524
配置锁定时间	524
查看锁定列表信息	524
解除用户/IP地址的锁定	524
配置Active-Directory服务器认证参数	525
配置认证主服务器的IP地址或域名	526
配置备份服务器1的IP地址或域名	526

配置备份服务器2的IP地址或域名	526
配置服务器端口号	527
配置服务器认证或同步方法	527
指定Base-DN	528
指定同步Base-DN	528
指定认证Base-DN	528
指定登录DN	529
指定sAMAccountName属性值	529
指定登录密码	529
指定角色映射规则	530
配置用户黑名单	530
配置服务器监控功能	530
开启/关闭服务器监控功能	530
指定监听端口及用户绑定信息删除超时时间	531
显示监控用户信息	531
踢出用户映射信息	531
配置用户同步功能	531
启用/禁用用户同步功能	532
配置用户同步方式	532
配置用户过滤功能	533
配置同步的工作模式	534
配置备份认证服务器	535

配置仅同步Base-DN下用户组	535
配置防暴力破解功能	536
开启或关闭防暴力破解功能	536
配置尝试次数	536
配置锁定时间	537
查看锁定列表信息	537
解除用户/IP地址的锁定	537
配置TACACS+服务器认证参数	537
配置认证主服务器的IP地址或域名	538
配置备份服务器1的IP地址或域名	538
配置备份服务器2的IP地址或域名	539
配置TACACS+服务器端口号	539
配置TACACS+服务器的共享密钥	539
指定系统管理员认证服务器	540
显示优先使用本地服务器认证启用状态	540
Radius动态授权	540
开启/关闭RADIUS动态授权功能	541
配置RADIUS动态授权服务器	541
配置动态授权端口号	541
查看RADIUS授权服务器配置信息	542
认证与授权的显示与调试	542
单点登录	542

SSO Radius单点登录	543
接收Radius计费报文	543
指定AAA服务器	543
指定设备接收Radius报文的端口号	543
配置Radius客户端	544
配置共享密钥	544
显示SSO Radius配置信息	544
查看用户映射信息	544
查看认证用户表	545
踢出用户映射信息	545
AD Scripting单点登录	545
进入AD Scripting配置模式	545
开启/关闭AD Scripting功能	545
指定AAA服务器	546
配置空闲超时时间	546
拒绝同名用户登录	546
显示AD Scripting配置信息	547
查看用户映射信息	547
查看认证用户表	547
踢出用户映射信息	547
AD Polling单点登录	547
创建AD Polling Profile	547

开启/关闭AD Polling功能	548
指定认证服务器	548
指定AAA服务器	548
指定账户	549
指定密码	549
指定AD Polling间隔	549
指定客户端探测间隔	549
指定强制超时时间	550
查看AD Polling配置	550
查看用户映射信息	550
查看认证用户表	550
踢出用户映射信息	551
SSO Monitor单点登录	551
创建SSO Monitor Profile	551
开启/关闭SSO Monitor功能	551
指定认证服务器	551
指定AAA服务器	552
指定端口	552
指定组织同步模式	552
指定重连超时时间	553
查看SSO Monitor配置	553
查看用户映射信息	553

查看认证用户表	553
踢出用户映射信息	554
TS Agent单点登录	554
创建TS Agent Profile	554
开启/关闭TS Agent功能	555
指定TS Agent服务器	555
指定TS Agent服务器端口	555
指定AAA服务器	555
指定断开超时时间	556
指定流量IP	556
查看TS Agent配置	556
查看TS Agent状态信息	557
查看TS Agent用户映射信息	557
查看认证用户表	557
踢出用户映射信息	557
单点登录配置举例	557
TS Agent单点登录配置举例	558
PKI	559
配置PKI	560
创建和删除PKI密钥对	560
配置PKI信任域	561
指定证书获得方法	562

指定密钥对	562
配置主题内容	562
配置证书撤销列表	563
配置在线证书状态协议	564
指定OCSP响应器	565
配置OCSP请求随机数	565
指定OCSP响应信息失效时间	565
导入CA证书	565
导入密钥	566
导入加密密钥对	566
生成证书服务请求	567
安装本地证书	567
下载证书撤销列表	567
导出和导入PKI信任域信息	567
导出PKI信任域信息	568
导入PKI信任域信息	568
证书链	569
创建证书链	569
导出证书链	569
导入证书链	570
显示证书链配置信息	571
重新自签名	572

显示PKI配置信息	572
第8章 对象	573
命名规则	573
地址簿	573
地址条目	574
配置地址簿	574
添加或者删除地址条目	574
指定地址条目的IP地址范围	575
指定排除地址条目成员	577
指定排除IPv4地址条目成员	577
重新命名地址条目	577
查看地址条目关联项	578
查看地址簿信息	578
服务簿	578
通过CLI查看服务信息	579
查看服务关联项	580
预定义服务（Predefined Services）	580
远程Shell（RSH）	581
Sun远程程序调用（Sun RPC）	581
微软远程过程调用（MS RPC）	581
修改预定义服务超时时间	581
预定义服务组	582

用户自定义服务	582
创建和删除自定义服务	582
为自定义服务添加和删除自定义服务条目	583
重命名自定义服务	584
服务组 (Service Group)	584
创建和删除服务组	585
为服务组添加和删除服务或者服务组	585
为服务或者服务组添加/删除描述信息	586
域名簿	586
添加或者删除域名条目	586
指定域名条目的域名范围	587
查看域名簿信息	587
时间表	587
创建时间表	587
指定绝对计划	588
指定周期计划	588
用户与角色	589
用户	590
配置静态绑定用户	591
配置认证用户	591
指定用户密码	592
指定用户有效期	592

配置用户描述信息	592
指定IKE ID	593
指定用户组	593
用户组	593
显示用户/用户组信息	594
角色	595
创建角色	595
配置角色映射规则	595
配置角色组合	596
显示角色信息	596
监测对象	597
ICMP报文监测	597
ICMPv6报文监测	598
HTTP报文监测	599
IPv6 HTTP报文监测	600
ARP报文监测	600
NDP报文监测	601
DNS报文监测	601
TCP报文监测	602
IPv6 TCP报文监测	603
接口链路状态监测	604
接口链路质量监测	604

接口流量监测	605
配置警戒值	606
监测对象警戒值	606
报文延时警戒值	606
接口流量警戒值	607
系统监控报警	608
第9章 流量管理	611
iQoS	611
管道与流控层级	611
管道	611
流控层级	613
配置iQoS	614
指定流控层级	614
启用/禁用流控层级/根管道/子管道	614
启用/禁用NAT IP匹配	615
创建根管道	615
创建子管道	616
配置流量匹配条件	617
配置流量白名单	619
配置根管道流量管理动作	621
配置子管道流量管理动作	622
配置根管道的流控模式	624

配置根管道时间表	625
配置子管道时间表	625
查看流控层级及管道的配置信息	625
配置阈值告警功能	626
开启/关闭阈值告警功能	626
指定告警阈值	626
显示阈值告警功能的启用状态	626
会话限制	626
会话限制配置	626
会话限制显示	628
第10章 安全策略	629
配置策略规则	630
进入策略配置模式	630
创建策略规则	630
编辑策略规则	632
启用/禁用策略规则	634
策略规则的日志管理	634
配置服务规则	635
指定缺省行为	636
修改规则排列顺序	637
规则冗余检测	637
查看策略规则信息	638

查看设备的当前策略配置信息	638
查看策略规则匹配次数	639
策略组	641
配置策略组	642
新建/删除策略组	642
启用/禁用策略组	642
添加/删除策略组描述信息	643
添加/删除策略规则成员	643
策略组重命名	643
查看策略组配置信息	644
策略助手	644
开启/关闭策略助手	644
查看开启策略助手的策略	644
聚合策略	645
创建聚合策略	645
添加聚合策略成员	646
移出聚合策略成员	647
删除聚合策略	647
调整优先级	647
启用/禁用聚合策略	648
添加/删除聚合策略描述信息	649
附表：ICMPv6 Type以及Code值对照表	649

第11章 威胁防护	653
攻击防护	653
常见网络攻击概述	653
ICMP Flood和UDP Flood攻击	653
ARP欺骗攻击	653
SYN Flood攻击	653
WinNuke攻击	654
IP地址欺骗 (IP Spoofing) 攻击	654
地址扫描与端口扫描攻击	654
Ping of Death攻击	654
Teardrop攻击防护	654
Smurf攻击	655
Fraggle攻击	655
Land攻击	655
IP Fragment攻击	655
IP Option攻击	655
Huge ICMP包攻击	655
TCP Flag异常攻击	656
DNS Query Flood攻击	656
TCP Split Handshake攻击	656
配置攻击防护功能	656
配置IP地址扫描攻击防护功能	657

配置端口扫描攻击防护功能	658
配置IP地址欺骗攻击防护功能	658
配置SYN Flood攻击防护功能	659
配置SYN-Proxy功能	660
配置ICMP Flood攻击防护功能	661
配置UDP Flood攻击防护功能	661
配置Huge ICMP包攻击防护功能	662
配置WinNuke攻击防护功能	662
配置Ping of Death攻击防护功能	662
配置Teardrop攻击防护功能	663
配置IP Option攻击防护功能	663
配置TCP异常攻击防护功能	663
配置Land攻击防护功能	664
配置IP 碎片攻击防护功能	664
配置Smurf和Fraggle攻击防护功能	665
配置ARP欺骗防护功能	665
配置DNS Query Flood攻击防护功能	666
配置DNS Reply Flood攻击防护功能	667
配置TCP Split Handshake攻击防护功能	668
配置攻击防护白名单	668
显示安全域的攻击防护配置和统计信息	669
第12章 VPN	670

IPSec协议	670
IPSec协议介绍	670
安全联盟 (Security Association)	671
SA建立方式	671
第一阶段SA	671
第二阶段SA	672
验证算法	673
加密算法	673
压缩算法	673
相关资料	674
IPSec VPN的应用	674
IPSec VPN	675
IPSec VPN基础概念	675
安全联盟	675
封装方式	675
协商方式	676
引用IPSec VPN	676
配置IKE VPN	676
配置P1提议	677
创建P1提议	677
指定认证方式	677
指定加密算法	678

指定验证算法	678
选择DH组	679
指定安全联盟的生命周期	680
配置P2提议	680
创建P2提议	680
指定协议类型	680
指定验证算法	681
指定加密算法	681
指定压缩算法	682
配置PFS功能	682
指定生命周期	683
配置ISAKMP网关	683
创建ISAKMP网关	683
绑定接口到ISAKMP网关	684
配置IKE协商模式	684
配置自定义IKE协商端口	684
指定对端的IP地址及类型	684
指定P1提议	685
配置预共享密钥	685
配置PKI信任域	685
配置对端证书的信任域	686
配置加密证书的信任域	686

配置协商协议标准	686
配置本端ID	687
配置对端ID	687
指定连接类型	688
开启NAT穿越功能	688
接受对端ID	688
配置自动生成路由功能	688
配置DPD功能	689
指定描述信息	689
配置隧道	689
创建IKE隧道	689
启用/禁用IPSec VPN隧道	690
指定IPSec协议的操作模式	690
指定ISAKMP网关	690
指定P2提议	690
指定第二阶段ID	690
配置IPsec VPN流量分流与限流	691
启用接受对端ID功能	691
配置自动连接功能	692
配置分片功能	692
配置防重放功能	692
开启/关闭VPN隧道状态通知功能	693

设置Commit位	693
指定描述信息	693
配置手工密钥VPN	694
创建手工密钥VPN	694
指定IPSec协议的操作模式	694
指定对端IP地址	695
指定安全参数索引	695
指定出接口	695
指定协议类型	696
指定加密算法	696
配置协议的加密密钥	696
指定验证算法	697
配置协议的验证密钥	697
指定压缩算法	698
配置IPSec-XAUTH地址池	698
启用XAUTH服务器	699
配置XAUTH地址池	699
创建XAUTH地址池	699
配置XAUTH地址池的IP地址范围	699
配置XAUTH地址池的保留地址	700
绑定地址池到XAUTH服务器	700
配置IP用户绑定和IP角色绑定规则	700

配置IP用户绑定规则	701
配置IP角色绑定规则	701
修改IP角色绑定规则排列顺序	701
配置推送到客户端的WINS/DNS服务器	702
强制断开客户端XAUTH连接	702
配置IPSec VPN监控	703
配置VPN监控	703
禁用或者启用VPN监控失败通知	703
查看VPN监控	704
配置举例	705
手工密钥VPN	705
组网需求	705
配置步骤	706
IKE VPN	709
组网需求	710
配置步骤	710
基于路由的VPN监控及冗余备份功能配置举例	716
组网需求	716
配置步骤	717
基于策略的VPN监控及冗余备份功能配置举例	724
组网需求	724
配置步骤	725

XAUTH	732
组网需求	732
配置步骤	733
配置PnPVPN	736
PnPVPN工作流程	736
PnPVPN链路冗余	737
PnPVPN服务器端配置	737
通过CLI配置PnPVPN服务器端	737
配置用户网络参数	737
配置隧道网络参数	738
配置ISAKMP网关对端通配符	739
配置PnPVPN客户端的隧道接口	739
通过WebUI配置服务器端	740
用户配置	740
IKE VPN配置	741
隧道接口配置	743
路由配置	744
策略配置	744
配置PnPVPN客户端	744
PnPVPN配置举例	745
组网需求	745
配置步骤	747

服务器端配置	747
客户端配置	751
IKEv2 VPN	752
配置P1提议	752
创建P1提议	752
指定验证算法	752
指定PRF算法	753
指定加密算法	753
选择DH组	754
指定的生命周期	754
配置IKEv2对等体	755
创建IKEv2对等体	755
绑定接口到对等体	755
指定对端的IP地址	755
配置认证方式	756
指定P1提议	756
配置本端ID	756
指定连接类型	756
创建IKEv2 Profile	757
配置对端ID	757
配置预共享密钥	757
配置被保护的数据流量信息	758

配置本端地址	758
配置对端地址	758
配置自动生成路由功能	758
配置P2提议	759
指定协议类型	759
指定验证算法	759
指定加密算法	760
配置PFS功能	760
指定生命周期	761
配置隧道	761
创建IKEv2隧道	761
指定IKEv2隧道的操作模式	761
指定IKEv2对等体	762
指定P2提议	762
配置自动连接功能	762
GRE协议	762
GRE协议介绍	762
GRE配置	762
配置GRE隧道	763
指定源地址	763
指定目的地址	764
指定出接口	764

指定IPSec VPN隧道	764
指定验证秘钥	764
绑定GRE隧道到隧道接口	765
显示GRE隧道配置信息	765
VXLAN	765
介绍	765
配置VXLAN静态隧道	766
显示VXLAN隧道配置信息	767
IPv6 6to4隧道配置	767
创建隧道	767
指定6to4子隧道最大数	768
指定隧道的出接口	768
绑定IPv6 6to4隧道到隧道接口	768
显示IPv6 6to4隧道配置信息	768
IPv6 4to6隧道配置	769
创建隧道	769
指定隧道的源地址/出接口	769
指定隧道的目的地址	770
绑定IPv6 4to6隧道到隧道接口	770
显示IPv6 4to6隧道配置信息	770
ISATAP隧道配置	770
创建ISATAP隧道	771

指定ISATAP子隧道最大数	771
指定ISATAP隧道的出接口	772
绑定ISATAP隧道到隧道接口	772
显示ISATAP隧道配置信息	772
第13章 监控	773
监控介绍	773
查看接口的统计信息	773
链路状态监控	774
开启/关闭接口的链路用户体验功能	774
开启/关闭接口的应用维度	774
指定描述信息	774
查看链路状态监控配置信息	775
查看链路用户体验统计信息	775
配置链路探测目的IP	775
查看链路探测监控配置信息	776
配置采样率	776
全局负载均衡监控	777
服务器负载均衡监控	777
开启/关闭服务器负载均衡统计	777
链路负载均衡	777
SSL透视镜监控	778
开启/关闭SSL透视镜统计	778

日志	778
日志的严重等级	779
日志信息输出目的地	779
日志信息格式	780
配置系统日志功能	780
开启和关闭日志功能	780
输出日志信息	781
输出流量日志信息	781
配置PBR日志主机名/用户名的显示状态	783
自定义不保存的日志类型	783
输出及过滤事件日志信息	783
配置接收事件日志信息的手机号码	785
输出威胁日志信息	785
输出Web防护日志信息	787
输出配置、操作、调试和网络日志信息	787
输出健康检查日志信息	788
配置日志信息的输出 格式	789
配置Syslog Server	789
配置GBK编码	790
指定场所	790
配置Email地址	790
配置SMTP实例	791

配置日志参数	792
关闭日志生成	792
配置日志级别	792
显示配置日志参数的日志条目	792
显示日志信息	793
导出日志信息	794
清除日志信息	794
日志分布式外发	795
第14章 高可靠性HA	797
HA基础概念	797
HA簇	797
HA组	797
HA Node	798
HA组接口和虚拟MAC	798
HA选举	798
HA同步	798
配置HA	799
配置HA组	799
指定优先级	799
指定Hello报文间隔	800
指定Hello报文警戒值	800
配置抢占模式	800

指定发送ARP包个数	801
手动发送免费ARP包	801
指定描述信息	801
指定监测对象	802
HA连接配置	802
指定HA连接接口	802
指定HA数据连接接口工作模式	803
指定HA连接接口IP地址	803
指定HA辅助链路接口	804
HA簇配置	804
配置HA虚MAC前缀	805
查看虚MAC前缀信息	805
接口管理IP配置	805
配置三层接口Down-Up功能	806
手动同步HA信息	806
启用/禁用HA会话自动同步	808
启用/禁用HA配置信息定时比较功能	808
手动切换HA设备的主备状态	808
备设备配置模式	809
指定vADC的HA心跳口MAC地址	809
配置vADC使用接口的真实MAC	809
配置通过二层单播方式进行HA协商通信	810

指定HA连接接口的最大传输单元（MTU）	810
配置Hello报文使用UDP协议	811
开启/关闭阿里云HAVIP	811
指定访问阿里云的密钥ID及密码	811
HA簇配置	812
显示HA配置	812
第15章 系统管理	814
配置主机名称	815
配置主机名称显示长度	815
查看主机名称显示长度	816
配置系统信息显示语言	816
配置管理员	816
配置默认用户登录操作	819
新建管理员角色	819
指定管理员角色的权限	819
指定管理员角色的描述信息	820
创建管理员	820
配置管理员角色	820
配置管理员密码	821
配置管理员密码策略	821
显示管理员密码策略信息	823
配置管理员访问方式	823

配置安全审计员可管理日志类型	824
配置管理员登录限制	824
配置管理员的最大数量	825
显示管理员角色的配置	825
显示管理员配置	825
配置可信主机	825
配置IPv6可信主机	826
显示可信主机配置	827
配置管理接口	827
配置Console管理接口	827
配置波特率	827
配置超时时间	827
配置Telnet管理接口	828
配置SSH管理接口	829
配置WebUI管理接口	830
显示管理接口配置	831
数据库修复	831
配置存储管理	832
开启/关闭存储管理功能	832
配置存储管理	832
自定义日志存储空间	833
开启/关闭存储空间告警	833

查看硬盘存储管理的配置信息	833
配置文件管理	834
配置设备配置信息	834
查看配置信息	834
回退起始配置信息	835
删除配置文件	835
保存配置信息	835
自动备份配置文件	836
查看自动备份配置文件信息	836
导出配置信息	836
导入配置信息	837
启用/禁用自动导入USB中配置文件功能	838
恢复出厂配置	839
切换接口工作模式	839
查看当前对象的配置信息	840
查看光模块状态信息	840
配置Banner功能	840
系统维护与调试	840
Ping命令	841
Traceroute命令	842
系统调试功能	843
配置系统重启	844

系统版本升级	845
启动系统介绍	845
Bootloader的工作模式	845
通过网络迅速升级系统（TFTP）	846
其它升级方式	848
通过FTP服务器获取系统文件	848
Sysloader菜单介绍	848
通过CLI升级系统	849
配置热补丁升级功能	849
备份与恢复配置	851
升级IP地理库	851
配置更新传输协议	852
升级域名地理库	853
配置更新传输协议	854
升级ISP信息库	854
配置更新传输协议	855
许可证管理	855
vADC许可证	856
vADC平台类许可证	857
vADC订阅类许可证	857
vADC功能服务类许可证	857
申请许可证	858

安装许可证	858
许可证命令	858
生成许可证请求	858
安装/卸载许可证	859
许可证校验	859
显示vADC与LMS的连接信息	860
许可证灌装介绍	860
许可证灌装操作	860
许可证安装	860
简单网络管理协议（SNMP）	861
山石网科设备的SNMP功能	862
SNMP版本	862
MIB信息库	863
Trap报文信息	863
配置SNMP	863
开启或者关闭SNMP代理功能	864
配置SNMP代理设备端口号	864
配置SNMP引擎ID	864
创建SNMPv3用户组	865
创建SNMPv3用户	865
配置管理主机地址	866
配置trap报文目标主机地址	866

配置管理员的标识及联系方法	867
配置山石网科设备位置	867
指定启用SNMP功能的VRouter	868
配置设备历史最大会话数功能	868
显示SNMP信息	868
网络时间协议（NTP）	869
手动配置时间	869
手动配置时区	869
配置夏令时	870
查看系统时间配置信息	872
配置NTP功能	872
开启/关闭NTP功能	872
配置NTP时钟服务器	872
配置最大调整时间	873
配置查询间隔	873
开启/关闭身份验证功能	874
配置NTP身份验证功能	874
查看NTP状态	874
查看NTP的调试信息	874
配置时间表功能	875
创建时间表	875
指定绝对计划	875

指定周期计划	876
HSCP协议	877
配置HSCP协议	877
短信发送参数	878
配置短信猫	878
认证短信发送参数	878
短信发送测试	879
显示短信猫配置信息	879
配置短信网关	879
指定短信网关默认协议类型	879
创建SP实例名称	880
指定VRouter	881
指定UMS/ALIYUNSMS/ACC协议	881
指定短信网关的地址和端口号	881
设置发送认证短信的号码	882
指定设备ID	882
指定用户名和密码	882
配置短信最大发送数量	883
指定企业编码	883
指定AccessKeyId	883
指定AccessKeySecret	884
发送测试短信	884

显示短信网关配置信息	884
HSM代理	884
配置HSM服务器管理参数	885
开启/关闭HSM代理功能	886
显示HSM代理配置	887
连接山石云平台	887
设备端配置	887
配置云平台服务器	888
启用山石云·景	888
启用云·景	889
开启数据上传	889
显示云平台服务器配置	889
Bypass	889
开启/关闭Bypass	890
开启强制Bypass	890
查看Bypass信息	891
配置举例	891
第16章 虚拟系统	893
配置VSYS	893
创建非根VSYS	894
配置非根VSYS的描述信息	894
创建VSYS Profile	895

配置QoS	895
设置资源配额	896
设置日志的缓存配额	898
启用/禁用CPU资源配额	898
查看VSYS的CPU资源占用	898
绑定Profile到VSYS	899
进入根VSYS	899
进入非根VSYS	899
配置共享属性	900
导入/导出物理接口	901
分配逻辑接口	901
绑定监测对象	901
监测指定VSYS状态	902
回退配置信息（非根VSYS）	902
退出配置回滚模式	903
配置退出配置回滚模式的动作	904
配置VSYS日志功能	904
配置跨VSYS转发功能	904
开启跨VSYS转发功能	905
配置Simple-Switch	905
创建Simple-Switch	905
绑定二层安全域到Simple-Switch	906

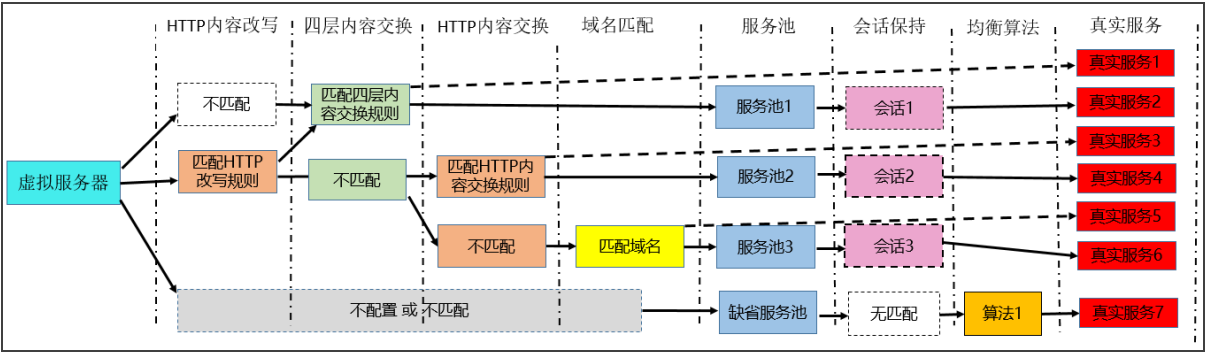
创建VWANIF接口	906
配置VPort接口	906
配置VWANIF接口	907
分配VWANIF接口	907
显示跨VSYS转发功能信息	907
显示VWANIF接口配置信息	907
显示VSYS信息	907
显示VSYS Profile信息	907
第17章 SLB脚本编程手册	909

第1章 服务器负载均衡

当应用访问量增加，单台服务器由于性能不足无法处理多个访问请求时，需要多台服务器来提供服务。服务器负载均衡（Server Load Balance）功能，将客户端的请求，按照特定的均衡算法分配到不同的服务器上，以达到快速响应的效果。

AX设备将多个真实服务的地址映射为一个虚拟服务器地址（Virtual IP）。当用户的访问到达AX设备后，虚拟服务器（Virtual Server）根据配置的SLB规则或均衡算法，转发用户的访问请求至适合的真实服务上。同时，设备对真实服务的运行状况进行监控，若发现异常，及时将访问请求转发到其它正常工作的真实服务上。

目前，AX设备支持四层负载均衡和七层负载均衡。以七层负载均衡为例，说明设备处理流程如下：



1. 客户端发起一个请求，该请求到达ADC设备后，根据设备上应用的配置，匹配到虚拟服务器。
2. 虚拟服务器根据SLB规则进行匹配，依次匹配内容改写规则、四层内容交换规则、HTTP内容交换规则。
3. 如匹配内容改写规则，设备将按规则的配置对报文内容改写，然后继续匹配四层内容交换规则。如不匹配内容改写规则，不进行报文改写直接匹配四层内容交换。
- 注意：如内容改写配置的为重定向改写规则，虚拟服务器将不会继续匹配四层内容交换规则，而是直接返回响应给客户端。
4. 如匹配四层内容交换，根据四层内容交换的配置，直接将用户请求分配到真实服务，或按照服务池配置分配到真实服务。如不匹配，继续匹配HTTP内容交换规则。
5. 如匹配HTTP内容交换规则，根据HTTP内容交换规则配置将用户请求分配到真实服务，或按照服务池配置分配真实服务。
6. 如匹配域名匹配规则，根据域名匹配规则配置将用户请求分配到真实服务，或按照服务池配置分配真实服务。

7. 如对SLB规则、域名匹配规则都不匹配，根据缺省服务池的会话保持表或者均衡算法选取真实服务，将请求分发到该真实服务上。
8. 虚拟服务器将真实服务的响应返回给客户端。



注意:

客户端请求进入服务池后，先匹配会话保持。如匹配到会话保持，设备直接分配一个真实服务，否则根据服务池配置的均衡算法，选出一个真实服务器。

SLB相关概念

服务器负载均衡功能主要包含以下概念：

- [真实服务](#)：在用户组网中真实服务器上部署的服务，负责处理客户端的请求。
- [服务池](#)：一组提供相同服务的真实服务的集合。
- [虚拟服务器](#)：处理SLB流程的起点。不同业务的流量匹配不同的虚拟服务器。根据虚拟服务器的配置，分配客户端请求至合理的服务器，再将服务器的处理响应发回到客户端。
- [负载均衡算法](#)：负责分配服务池请求的算法。根据负载均衡算法，虚拟服务器分配客户端的请求。
- [SLB规则](#)：包括交换规则（HTTP内容交换、SQL内容交换、四层内容交换）、改写规则（HTTP内容改写）、安全规则（访问控制、Web防护）。虚拟服务器通过SLB规则来分发客户端请求。
- [健康检查](#)：对真实服务的状态进行健康检查。如服务器工作异常，将被排除在可用来分配的服务器列表资源之外，以保证客户端请求被分发到可正常工作的服务器上。
- [会话保持](#)：保持会话的连续性和一致性，把客户端的前后访问请求都保持到一台服务器上进行处理，不分发至多个服务器。

负载均衡算法

系统支持多种负载均衡算法，包括：

算法	描述
轮询（Round Robin）	将客户端的请求轮流分配给每个真实服务。

加权轮询 (Weighted Round Robin)	根据真实服务的不同处理能力，分配不同的权重。设备根据真实服务的权重，按比例分发请求。权重大的真实服务，接收的请求多。
IP哈希 (Hash IP)	对客户端的源地址/目的地址/真实源IP地址进行哈希运算，根据运算的结果转发给一个真实服务进行处理。若服务列表不变，同一IP地址的客户端，每次都会分配到同一个真实服务。
加权IP哈希 (Weighted Hash IP)	在IP哈希算法的基础上，设备根据真实服务的权重，按比例分发请求。权重大的真实服务，接收的请求多。
IP端口哈希 (Hash IP Port)	对客户端的源地址/目的地址/真实源IP地址和端口进行哈希运算，根据运算的结果转发给一个真实服务进行处理。
加权IP端口哈希 (Weighted Hash IP Port)	在IP端口哈希算法的基础上，设备根据真实服务的权重，按比例分发请求。权重大的真实服务，接收的请求多。
一致IP哈希 (Consistence Hash IP)	对客户端的源地址/目的地址/真实源IP地址进行哈希运算，根据运算的结果转发给一个真实服务进行处理。若某个真实服务由于故障等原因无法提供服务，原来发送至该故障真实服务的请求，将被分配至其他可用的真实服务上；而原来发送至未故障的真实服务的请求（来自同一源IP或同一客户端），将继续被分配到原来的真实服务上。
最小连接 (Least Connection)	设备会记录每个真实服务或端口上的连接数。当产生新的连接时，设备将分配给当前连接数最少的真实服务。
加权最小连接 (Weighted Least Connection)	在最少连接数分发的基础上，根据真实服务的不同处理能力，为每个真实服务分配一个权重。各个真实服务用相应的权重表示其处理性能。当产生新的连接时，将最新的请求分配给当前连接数与权重的比值最小的真实服务上（计算方法：当前连接数除以权重）。
最快响应 (Fast Response Time)	设备会记录每个真实服务或端口上的连接数。当产生新的连接时，设备将其分配至当前处理响应最快的真实服务上。
优先权算法	根据真实服务的优先级来分配请求，将请求分配给优先级最高的真实服务。真实服务所配的优先级数值越小，其优先级越高。当有多个真实服务的优先级相同且最高时，将采用在这些真实服务之间轮询的方式分配资源。
动态比率算法	根据真实服务的不同处理能力，设备计算不同的动态权重。设备根据真实服务的动态权重，按比例分发请求。动态权重大的真实服务，接收的请求多。动态

	权重为0时，真实服务不参与分发请求。一般情况下，动态权重值是由SNMP类型的健康检查计算得出的结果；对于其他情况，如果真实服务可以提供服务时，动态权重值为1，否则为0。
最小带宽	设备会记录每个真实服务或端口上的上行与下行带宽总和。当产生新的连接时，设备将分配给带宽总和最小的真实服务。
加权最小带宽	在上行与下行带宽总和分发的基础上，根据真实服务的不同处理能力，为每个真实服务分配一个权重。各个真实服务用相应的权重表示其处理性能。当产生新的连接时，将最新的请求分配给当前带宽总和与权重的比值最小的真实服务上（计算方法：上行与下行带宽总和除以权重）。
随机	设备将客户端请求随机分配给一个可用的真实服务。
URL哈希 (Hash URL)	对客户端访问的URL地址进行哈希运算，根据运算的结果转发给一个真实服务进行处理。若服务列表不变，访问同一个URL地址的客户端，每次都会分配到同一个真实服务。

配置虚拟服务器

不同的协议支持配置的虚拟服务器类型不同。目前，系统支持的协议类型包括：HTTP、HTTPS、IMAP、POP3、SMTP、TCP、UDP、FTP、Any、快速HTTP、HTTP代理、SSL流代理、SIP-TCP、SIP-UDP、IP、RDP、SSL-OVER-TCP、RADIUS、MYSQL。如协议类型为HTTP，系统创建的即为HTTP协议类型的虚拟服务器。Any表示任意协议类型。

虚拟服务器类型不同，处理请求的方式也不同：

- 当虚拟服务器的类型为HTTP、HTTPS、IMAP、POP3、SMTP、TCP、UDP、FTP、快速HTTP、SIP-TCP、SIP-UDP、RDP、SSL-OVER-TCP、RADIUS时，设备将多个真实服务的地址映射为一个虚拟服务器的地址，并根据虚拟服务器中设置的SLB规则或均衡算法，将请求转发至适合的真实服务器。
- 当虚拟服务器的类型为HTTP、HTTPS时，系统支持为同一虚拟服务器配置多条域名匹配规则，当客户端对不同域名的业务发起访问时，系统会将客户端请求转发给各域名对应的真实服务，或按照域名对应的服务池配置分配真实服务；同时，系统可以根据客户端访问的域名，选择合适的SSL证书与真实服务建立SSL连接。对于HTTPS类型的虚拟服务器，系统还可以将待访问域名对应的SSL证书返回给客户端，由客户端进行认证，成功解密客户端的加密数据。

- 当虚拟服务器的类型为IP时，设备将匹配客户端请求中的目的地址，当目的地址与虚拟服务器IP匹配时，设备将根据虚拟服务器中设置的SLB规则或均衡算法，将请求转发至适合的真实服务，实现链路负载均衡。
- 当虚拟服务器的类型为HTTP代理、SSL流代理时，设备作为代理服务器，将用户的访问请求直接转发至目标服务器。HTTP代理类型的虚拟服务器只能转发HTTP请求，如需转发HTTPS请求，需开启HTTP隧道模式；SSL流代理类型的虚拟服务器可以直接转发HTTPS请求。
- 当虚拟服务器的类型为MYSQL时，设备将对MYSQL请求进行解析，将读/写操作分别发往读服务池/写服务池，或通过绑定SQL内容交换规则到虚拟服务器，将特定的请求转发至合适的服务池或真实服务器。

创建虚拟服务器，在全局配置模式下，使用以下命令：

```
slb virtual-server vs-name type {any | http | https | tcp | udp | fast-http | ssl-over-tcp | ssl-stream-proxy | http-proxy | sip-tcp | sip-udp | ip | rdp | imap | pop3 | smtp | radius | mysql}
```

- *vs-name* - 指定想要创建的虚拟服务器的名称并进入虚拟服务器配置模式。如果指定的名称已存在，则直接进入虚拟服务器配置模式。
- *any | http | https | tcp | udp | fast-http | ssl-over-tcp | ssl-stream-proxy | http-proxy | sip-tcp | sip-udp | ip | rdp | imap | pop3 | smtp | radius | mysql* - 指定虚拟服务器的协议类型。Any表示任意协议类型。

在全局配置模式下，使用`no slb virtual-server vs-name`删除该虚拟服务器的配置。

进入虚拟服务器配置模式后，可配置以下参数：

- [配置虚拟服务器部署模式](#)
- [虚拟服务器IP和端口](#)
- [配置流量组](#)
- [配置域名匹配规则](#)
- [配置默认虚拟服务器](#)
- [配置请求主机匹配SNI](#)
- [配置自动源NAT](#)
- [配置虚拟服务器IP地址是否允许被PING](#)

- [配置数据库账号](#)
- [配置虚拟服务器状态](#)
- [指定缺省服务池](#)
- [指定备份服务池](#)
- [指定写服务池](#)
- [指定读服务池](#)
- [指定设备与客户端的交互方式](#)
- [指定支持的客户端认证方式](#)
- [指定服务器名称](#)
- [指定虚拟服务器的支持功能](#)
- [查看虚拟服务器的运行状态](#)
- [配置最大连接数](#)
- [配置连接失败动作](#)
- [配置连接速率限制](#)
- [配置防浪涌等待队列长度](#)
- [配置超时连接动作](#)
- [开启历史信息记录](#)
- [记录日志](#)
- [TOA类型](#)
- [插入TOA](#)
- [绑定SSL模板](#)

- [绑定服务端SSL模板](#)
- [绑定应用模板](#)
- [绑定TCP模板](#)
- [配置DNS服务器](#)
- [配置IPv6的DNS查询](#)
- [配置DNS有效时间](#)
- [开启HTTP隧道模式](#)
- [配置自动修改HTTP头部协议](#)
- [指定脚本文件](#)
- [指定四层内容交换规则](#)
- [指定七层内容交换规则](#)
- [指定内容改写规则](#)
- [指定SQL内容交换规则](#)
- [指定Web防护模板](#)
- [配置主机改写](#)
- [配置访问控制](#)
- [配置错误信息](#)
- [配置三角模式](#)
- [配置UDP强制负载](#)
- [配置UDP超时时间](#)
- [配置逆向路由](#)

- [配置调度模式](#)
- [配置镜像请求](#)
- [配置入接口模式](#)
- [配置虚拟服务器IP的路由发布](#)
- [配置虚拟服务器外链改写](#)
- [配置虚拟服务器的探测服务器功能](#)
- [查看虚拟服务器信息](#)

配置虚拟服务器部署模式

当虚拟服务器类型为HTTPS或SSL-OVER-TCP时，可以指定其工作在透明或牵引模式。

指定后，ADC设备作为SSL代理，对客户端的加密流量进行解密（其中，HTTPS类型的虚拟服务器可以解密HTTPS流量，SSL-OVER-TCP类型的虚拟服务器可以解密HTTPS/SMTPS/POP3S/IMAPS流量），但不向客户端发送ARP报文，也不响应客户端的ARP请求，而是直接将客户端的ARP请求转发给真实服务器，再将真实服务器的响应返回给客户端。

同时，当虚拟服务器工作在透明或牵引模式时，仍然可以通过镜像流量的方式将解密后的客户端请求发送给其他安全设备，供其进行监控和分析；也可以对客户端流量执行用户所需的SLB规则或者其他相关配置，例如对请求报文进行最大连接数控制等。

在上述工作模式下，虚拟服务器的IP地址与真实服务器的IP地址一致，无需再为其配置服务池。

在创建HTTPS或SSL-OVER-TCP类型的虚拟服务器时，配置其部署模式，即在全局配置模式下，使用以下命令：

```
slb virtual-server vs-name type {https | ssl-over-tcp} [ deployment { load-balancing | transparent | routing } ]
```

- **deployment load-balancing** - 指定该虚拟服务器为负载均衡模式。指定后，设备将对命中的客户端流量执行负载均衡流程。默认情况下，HTTPS或SSL-OVER-TCP类型的虚拟服务器工作在此模式。
- **deployment transparent** - 指定该虚拟服务器为透明部署模式。指定后，该虚拟服务器工作在二层模式，网络中的交换机将命中虚拟服务器的客户端流量引流到ADC设备后，设备再对客户端的加密流量进行解密、转发等操作。

- **deployment routing** - 指定该虚拟服务器为牵引部署模式。指定后，该虚拟服务器工作在三层模式，网络中的路由器将命中的客户端流量引流到ADC设备后，再对客户端的加密流量进行解密、转发等操作。



注意:

- 不允许修改已创建好的虚拟服务器的部署模式。
- HTTPS或SSL-OVER-TCP类型的虚拟服务器处于不同的部署模式时，配置也将不同，请以实际为准。
- 部署在集群环境中的设备，不支持部署路由牵引模式以及透明模式。

配置虚拟服务器IP和端口

指定虚拟服务器的IP地址和端口号。用户可根据需要，添加多个虚拟服务器地址。在虚拟服务器配置模式下，使用以下命令配置虚拟服务器的IP地址和端口：

```
ip ip-address {port {port-number | any} | port range min-value max-value }
```

```
ip range min-value max-value port port-number
```

```
ipv6 ipv6-address {port {port-number | any} | port range min-value max-value }
```

```
ipv6 range min-value max-value port port-number
```

- **ip ip-address** - 指定虚拟服务器的IP地址。
- **ip ip-address netmask** - 指定IP类型虚拟服务器的IPv4网段。
- **ipv6 ipv6-address** - 指定虚拟服务器的IPv6地址。
- **ipv6 ipv6-prefix/length** - 指定IP类型虚拟服务器的IPv6网段。
- **ip range min-value max-value** - 指定虚拟服务器的IP范围。
- **ipv6 range min-value max-value** - 指定虚拟服务器的IPv6范围。
- **port {port-number | any}** - 指定虚拟服务器的端口号。**any**表示所有端口。
- **port-range min-value max-value** - 指定虚拟服务器的端口范围。

在虚拟服务器配置模式下，使用以下命令删除虚拟服务器的IP地址和端口：

```
no {ip ip-address | ip range min-value max-value} {port port-number}
```

在虚拟服务器配置模式下，使用以下命令删除虚拟服务器的IPv6地址和端口：

```
no {ipv6 ip-address | ip range min-value max-value} {port port-number}
```

配置流量组

指定虚拟服务器的IP地址和端口号后，可将IP地址对应的虚拟服务器绑定至指定的流量组。当客户端访问该虚拟服务器时，流量组的生效设备将发送ARP报文或NA（邻居通告）报文，将此次访问请求引流至自身，并对其进行处理。在虚拟服务器配置模式下，使用以下命令配置流量组：

```
{ip ip-address | ip range min-value max-value} {port port-number} [ traffic-group traffic-group-name]
```

- **traffic-group traffic-group-name** - 指定已创建好的流量组名称，将虚拟服务器的IPv4地址与流量组进行绑定。若不指定，默认加入系统预定义的default流量组。

```
{ipv6 ip-address | ip range min-value max-value} {port port-number} [ traffic-group traffic-group-name]
```

- **traffic-group traffic-group-name** - 指定已创建好的流量组名称，将虚拟服务器的IPv6地址与流量组进行绑定。若不指定，默认加入系统预定义的default流量组。

在虚拟服务器配置模式下，使用以下命令删除虚拟服务器的IP地址、端口和绑定的流量组：

```
no {ip ip-address | ip range min-value max-value} {port port-number}
```

在虚拟服务器配置模式下，使用以下命令删除虚拟服务器的IPv6地址、端口和绑定的流量组：

```
no {ipv6 ip-address | ip range min-value max-value} {port port-number}
```

配置域名匹配规则

当虚拟服务器的类型为HTTP或HTTPS时，系统支持配置域名匹配规则，当客户端请求命中该虚拟服务器时，系统将访问不同域名的请求调度到不同的服务池或直接分配给指定的真实服务。系统最多支持配置64条域名匹配规则。如不配置域名匹配规则，表示系统不进行域名匹配。

系统支持精确匹配、带通配符的域名匹配以及正则表达式匹配。在虚拟服务器配置模式下，使用以下命令创建域名匹配规则，并进入域名匹配规则配置模式：

```
domain-name domain-name type {accurate | regular | wildcard }
```

- **accurate** - 指定域名的名称，并指定域名匹配为精确匹配。*domain-name*由字母、数字、“-”和“.”组成，但是不能以“-”开始或结尾。
- **wildcard** - 指定域名的名称，并指定域名匹配为带通配符的域名匹配。*domain-name*由字母、数字、“-”和“.”组成，但是不能以“-”开始或结尾。通配符“*”可以放在域名开头或结尾，例如“*.example.com”，“www.example.*”。
- **regular** - 指定域名的名称，并指定域名匹配为正则表达式匹配。*domain-name*需满足PCRE规范，通配符“*”不可以放在开头。

执行上述命令后，进入域名匹配规则的配置模式。在域名匹配规则的配置模式下，使用以下命令配置域名匹配规则：

- **ssl-profile** *ssl-profile-name* - 仅HTTPS类型的虚拟服务器支持。指定客户端SSL模板，当客户端SSL请求中的SNI字段匹配上指定域名时，系统将使用该客户端SSL模板对客户端的数据进行解密。
- **server-ssl-profile** *server-ssl-profile-name* - 指定服务端SSL模板，对于HTTP类型的虚拟服务器，当客户端HTTP请求中的Host字段匹配上指定域名时，系统将使用该服务端SSL模板与相应真实服务建立SSL连接。对于HTTPS类型的虚拟服务器，系统将根据客户端请求中SNI字段与Host字段是否一致，来选择使用哪一个服务端SSL模板与相应真实服务建立SSL连接：
 - 若客户端请求中的SNI字段与Host字段一致，则使用SNI或Host字段匹配上的域名匹配规则中配置的服务端SSL模板。
 - 若不一致，则使用Host字段匹配上的域名匹配规则中配置的服务端SSL模板。
 - 若不一致，且Host字段没有匹配上任一域名规则，则使用虚拟服务器中配置的服务端SSL模板。
- **server-pool** *server-pool-name* [**real-server** *real-server-name*]
 - *server-pool-name* - 指定服务池。符合域名匹配规则的客户端请求，将被分配到指定的服务池。
 - **real-server** *real-server-name* - 根据需要，指定真实服务的名称。如配置该参数，设备将匹配的客户端请求直接分配给真实服务，不再进入到服务池中。如不指定该参数，客户端请求将在服务池内做负载均衡，由负载均衡算法决定分配至哪个真实服务。

在域名匹配规则下，使用**no {ssl-profile | server-ssl-profile | server-pool}**命令取消配置。



注意: 域名匹配优先级: 完全匹配 > 通配符在前的域名 > 通配符在后的域名 > 正则表达式。如所有域名都不匹配, 系统将选择与该虚拟服务器“IP:端口”相同、启用了“[默认虚拟服务器](#)”功能的虚拟服务器。

在虚拟服务器配置模式下, 使用 `no domain-name domain-name` 命令删除指定的域名匹配规则。

配置请求主机匹配SNI

仅HTTPS类型的虚拟服务器支持。该功能开启后, 只有当客户端请求中的SNI字段与Host字段一致时, 系统才继续处理该请求; 若不一致, 系统将阻断该客户端请求。

在虚拟服务器配置模式下, 使用以下命令启用或关闭请求主机匹配SNI功能:

- `request-host-match-sni enable` - 启用该功能。
- `no request-host-match-sni enable` - 关闭该功能。系统默认关闭该功能。

启用默认虚拟服务器

该功能启用后, 若存在IP地址和端口相同的HTTP/HTTPS虚拟服务器, 当客户端访问的域名与配置的所有域名均不匹配时, 优先选择该虚拟服务器下的[缺省服务池](#)。系统默认禁用该功能。

在虚拟服务器配置模式下, 使用以下命令启用或禁用默认虚拟服务器:

- 启用: `default-domain enable`
- 禁用: `no default-domain enable`

配置自动源NAT

系统支持开启自动源NAT功能。开启后, 系统将经过该虚拟服务器的源IP地址, 自动转换为出接口IP, 无需再配置SNAT转换。若同时配置了源NAT规则和自动源NAT, 自动源NAT的优先级较低。默认情况下, 该功能为关闭状态。开启自动源NAT, 在虚拟服务器配置模式下, 使用以下命令配置自动源NAT:

```
auto-snat [toa | eif-if | header [real-src-ip | x-forwarded-for | x-real-ip] header name | address-book | address  
address-entry [traffic-group traffic-group name]]
```

- **toa** - 若指定该参数，系统将经过该虚拟服务器的源IP地址，自动转换为TCP报文中TOA解析出来的源IP。
- **eif-ip** - 若指定该参数，系统将经过该虚拟服务器的源IP地址，自动转换为出接口IP，无需再配置SNAT转换。
- **header real-src-ip header name** - 若指定该参数，系统将经过该虚拟服务器的源IP地址，自动转换为真正发起请求的源IP。真正发起请求的源IP，获取方式的优先级依次为 X-Forwarded-For > X-Real-IP > 报文携带的源IP。当配置该选项时，系统优先在报文的 X-Forwarded-For 查找源IP，当找到时使用该源IP作为真正发起请求的源IP。当X-Forwarded-For 找不到时其次再查找 X-Real-IP，找到源IP即使用该源IP作为真正发起请求的源IP。当都查找不到时就使用报文自带的源IP作为真正发起请求的源IP。
- **header x-forwarded-for header name** - 若指定该参数，系统将经过该虚拟服务器的源IP地址，自动转换为HTTP/HTTPS报文头部中 X-Forwarded-For 解析出来的源IP。
- **header x-real-ip header name** - 若指定该参数，系统将经过该虚拟服务器的源IP地址，自动转换为HTTP/HTTPS报文头部中 X-Real-IP 解析出来的源IP。
- **address address-entry [traffic-group traffic-group name]** - 若指定该参数，系统将经过虚拟服务器的源IP地址，自动转换为地址簿中的地址条目。
 - *address-entry* - 指定配置好的地址簿名称。
 - *traffic-group name* - 指定配置好的流量组名称，将指定的地址簿绑定至该流量组。地址簿类型的自动源NAT规则，将随着与其绑定的流量组生效设备的切换而切换。即当地址簿绑定的流量组在另一台设备上生效时，该条自动源NAT规则也将在新的生效设备上生效。

使用**no address address-entry**命令删除指定的地址簿。

- **address-book** - 若指定该参数，系统将使用地址簿类型的自动源NAT规则。

在虚拟服务器配置模式下，使用**no auto-snat**命令关闭该功能。

配置虚拟服务器IP地址是否允许被PING

配置虚拟服务器IP地址是否允许被PING，以验证网络是否连通。

在虚拟服务器配置模式下，使用以下命令：

```
icmp-echo {disable | enable | selective}
```

- **disable** - 无论虚拟服务器是什么状态，其IP都不可以被PING。
- **enable** - 无论虚拟服务器是什么状态，其IP都可以被PING。默认情况下，开启该功能。
- **selective** - 与虚拟服务器状态一致。配置该参数后，系统将根据虚拟服务器的状态决定是否允许PING虚拟服务器IP。当虚拟服务器是禁用状态时，不允许PING虚拟服务器IP。当虚拟服务器是开启或维护状态时，可以启用PING功能。

配置数据库账号

当虚拟服务器的类型为MYSQL时，指定MYSQL数据库的账号。只有客户端使用配置的账号才能连接虚拟服务器。在虚拟服务器配置模式下，使用以下命令配置账号的用户名和密码：

user-name value password value

- **user-name value** - 指定数据库账号的用户名。
- **password value** - 指定数据库账号的密码。

在虚拟服务器配置模式下，使用**no user-name value**命令删除指定账号。

创建数据库账号后，进入数据库账号配置模式。在该模式下可以配置指定账号的事务保持功能和最大连接数。

开启/关闭事务保持功能

开启事务保持功能后，同一个事务的MYSQL请求会转发给同一个真实服务器。开启/关闭事务保持功能，在数据库账号配置模式下，使用以下命令：

- 开启：**transaction-persistent enable**
- 关闭：**no transaction-persistent enable**

配置最大连接数

配置一个账号可以支持的最大连接数，最大连接数的设置和虚拟服务器的性能有关，超出部分的连接将无法建立。在数据库账号配置模式下，使用以下命令：

max-connections value

- **value** - 指定最大连接数，取值范围为1至100000，默认值为200。最大连接数的设置和虚拟服务器的性能有关，超出部分的连接将无法建立。

在数据库账号配置模式下，使用**no max-connections**命令恢复默认值。

配置虚拟服务器的状态

配置虚拟服务器的状态。虚拟服务器实际的运行状态，请参见[查看虚拟服务器的运行状态](#)一节。配置状态包括以下三种：

- 启用 - 可以正常接收客户端的请求。
- 禁用 - 原有连接和保持表被删除；如有新的客户端请求，系统将显示连接超时。
- 维护 - 仅七层虚拟服务器支持“维护”状态。维护状态下，原有连接和保持表被删除；如有新的客户端请求，系统将返回错误消息页面，详见[错误](#)部分。

七层虚拟服务器的配置状态有启用、禁用、维护；四层虚拟服务器的配置状态有启用、禁用。

指定虚拟服务器的状态，在虚拟服务器配置模式下，使用以下命令：

```
status {disable | enable | maintain}
```

- **disable** - 指定虚拟服务器的状态为“禁用”。
- **enable** - 指定虚拟服务器的状态为“启用”。
- **maintain** - 指定虚拟服务器的状态为“维护”。

指定缺省服务池

指定虚拟服务器的缺省服务池。当客户端请求没有匹配到有效的四层或七层交换规则时，系统将在指定的缺省服务池中使用均衡算法分配真实服务。

指定缺省服务池，在虚拟服务器配置模式下，使用以下命令：

```
server-pool value
```

- **value** - 指定系统中已创建的服务池的名称。

在虚拟服务器配置模式下，使用**no server-pool**命令不配置缺省服务池。

指定备份服务池

当无法从缺省服务池中找到可用的真实服务时，系统将使用备份服务池的真实服务。指定备份服务池，在虚拟服务器配置模式下，使用以下命令：

backup-server-pool *value*

- *value* - 指定备份服务池的名称。

在虚拟服务器配置模式下，使用**no backup-server-pool**命令删除备份服务池。

指定写服务池

当虚拟服务器类型为MYSQL时，指定写服务池。设备将写操作的客户端请求发往写服务池。

指定写服务池，在虚拟服务器配置模式下，使用以下命令：

write-pool *value*

- *value* - 指定已有的MYSQL类型服务池的名称。

在虚拟服务器配置模式下，使用**no write-pool**命令删除写服务池。

指定读服务池

当虚拟服务器类型为MYSQL时，指定读服务池。设备将读操作的客户端请求发往读服务池。

指定读服务池，在虚拟服务器配置模式下，使用以下命令：

read-pool *value*

- *value* - 指定已有的MYSQL类型服务池的名称。

在虚拟服务器配置模式下，使用**no read-pool**命令删除读服务池。

指定设备与客户端的交互方式

当虚拟服务器类型为IMAP/POP3/SMTP时，需配置设备与客户端的交互方式。在虚拟服务器配置模式下，使用以下命令配置设备与客户端的交互方式：

mode {**plain-text** | **ssl** | **starttls** {**allow** | **require**}}

- **plain-text** - 指定设备将采用明文方式与客户端进行交互。默认情况下，采用该方式。
- **ssl** - 指定设备将采用SSL加密方式与客户端进行交互。
- **starttls** - 客户端请求到达后，设备先使用明文方式与客户端进行通信，协商是否使用STARTTLS协议。
 - **allow** - 指定该模式后，若客户端支持STARTTLS协议，设备将采用SSL加密方式与该客户端进行交互；若客户端不支持STARTTLS协议，设备将继续采用明文方式与客户端进行交互。
 - **require** - 指定该模式后，若客户端支持STARTTLS协议，设备将采用SSL加密方式与该客户端进行交互；若客户端不支持STARTTLS协议，设备接收到来自客户端的认证信息后，将返回错误提示。

在虚拟服务器配置模式下，使用**no mode**命令恢复设备与客户端交互的默认模式。

指定支持的客户端认证方式

当虚拟服务器类型为SMTP时，指定设备将支持的对客户端的认证方式。设备将支持的认证方式发送给客户端，客户端再从中选择一种进行认证。系统默认支持PLAIN和LOGIN两种认证方式。在虚拟服务器配置模式下，使用以下命令配置设备支持的客户端认证方式：

authentication {plain | login | cram-md5 | none}

- **plain** - 指定支持使用PLAIN认证方式。
- **login** - 指定支持使用LOGIN认证方式。
- **cram-md5** - 指定支持使用CRAM-MD5认证方式。
- **none** - 指定不对客户端进行认证。

在虚拟服务器配置模式下，使用**no authentication {plain | login | cram-md5 | none}**命令取消相应认证方式的配置。

指定服务器名称

当虚拟服务器类型为SMTP时，指定设备返回给客户端的服务器名称，可以为IP地址或域名。在虚拟服务器配置模式下，使用以下命令配置服务器名称：

server-name name

- **name** - 指定服务器名称。

在虚拟服务器配置模式下，使用**no server-name**命令取消服务器名称的配置。

指定虚拟服务器支持的功能

指定IMAP/POP3/SMTP类型的虚拟服务器需支持的功能命令，即当IMAP/POP3/SMTP类型的虚拟服务器收到来自客户端请求获取服务器功能列表的命令时，设备将指定的功能返回给客户端。POP3类型的虚拟服务器默认支持的功能为：TOP;USER;UIDL。IMAP类型的虚拟服务器默认支持的功能为：IMAP4;IMAP4rev1;UIDPLUS。若指定[交互模式](#)为“STARTTLS”，SMTP/IMAP类型的虚拟服务器将另外增加“STARTTLS”默认功能，POP3类型的虚拟服务器将另外增加“STLS”默认功能。

在虚拟服务器配置模式下，使用以下命令配置虚拟服务器的支持功能：

capabilities *string*

- *string* - 功能命令可配置多个，需以英文“;”间隔，如：TOP;USER。

在虚拟服务器配置模式下，使用**no capabilities**命令删除配置的虚拟服务器支持的功能命令。

查看虚拟服务器的运行状态

指定完虚拟服务器状态后，用户可在任何模式下，使用**show slb virtual-server server-name**，查看其实际的运行状态。虚拟服务器的运行状态，由服务池、备份服务池、SLB四/七层内容交换规则、以及虚拟服务器的配置状态共同决定，包含以下六种：

- **up**：表示虚拟服务器状态为“正常”。
当虚拟服务器配置了IP、配置状态为“启用”且所配置的服务池、备份服务池、四/七层内容交换规则至少有一个状态为“正常”时，该虚拟服务器的运行状态显示为正常。
- **off-line**：表示虚拟服务器状态为“离线”。
当虚拟服务器配置了IP、配置状态为“启用”且所配置的服务池、备份服务池、四/七层内容交换规则均为“离线”状态时，其运行状态显示为离线。或当虚拟服务器没有配置IP，或缺省服务池、备份服务池、四层/七层内容交换规则均未配置时，其运行状态显示为离线。
- **unknown**：表示虚拟服务器状态为“未知”。
当虚拟服务器配置了IP、配置状态为“启用”、其所配置的服务池、备份服务池、四/七层内容交换规则均不是“正常”状态且至少有一个状态为“未知”时，该虚拟服务器运行状态显示为未知。
- **disabled**：表示虚拟服务器状态为“禁用”。
当虚拟服务器状态配置为“禁用”时，其运行状态显示为“禁用”。

- **maintained**: 表示虚拟服务器状态为“维护”。
当虚拟服务器状态配置为“维护”时，其运行状态显示为“维护”。
- **manual-resume**: 表示虚拟服务器状态为“手动恢复”。
当虚拟服务器配置了IP、配置状态为“启用”且所配置的服务池为“手动恢复”状态时，其运行状态显示为“手动恢复”。

配置最大连接数

指定虚拟服务器允许的最大并发连接数。如虚拟服务器的现有连接数超过该值，新建连接将无法建立。在虚拟服务器配置模式下，使用以下命令配置最大连接数：

max-connection *value*

- *value* - 指定虚拟服务器允许的最大并发连接数。取值为0到10,000,000之间的整数。如取值为0，表示没有最大连接数限制。

在虚拟服务器配置模式下，使用**no max-connection**命令恢复默认值。

配置连接失败动作

当HTTP、HTTPS、HTTP代理类型的虚拟服务器现有连接数达到最大时，新建连接将无法建立，系统将按照配置执行以下连接失败动作：返回响应消息、返回响应页面、重定向到新页面。在虚拟服务器配置模式下，使用以下命令配置连接失败动作：

max-connection-action { **redirect** *url* | **response** { **page** *string* | **message** *string* } } [**status-code** { 301 | 302 | 303 | 307 | 308 }]

max-connection-action { **redirect** *url* [**status-code** { 301 | 302 | 303 | 307 | 308 }] | **response** { **page** *string* | **message** *string* } [**status-code** *code*] }

- **redirect** *url* - 指定重定向到的新页面的地址，以http://或https://开头。
- **page** *string* - 指定系统中预定义或自定义的响应页面。如需导入自定义的响应页面，请参见[导入页面](#)。系统支持上传HTM/HTML/JPG/PNG格式的文件，且小于128K。
- **message** *string* - 指定自定义响应消息内容，范围是1到255个字符。
- **status-code** *code* - 指定返回的状态码，默认值是503，范围是200到599。

在虚拟服务器配置模式下，使用**no max-connection-action**命令删除指定的连接失败动作。

配置连接速率限制

指定虚拟服务器允许的最大连接速率。若虚拟服务器的现有连接速率超过该值，新建连接将无法建立。取值为0到10,000,000之间的整数。如取值为0，表示没有最大连接速率限制。在虚拟服务器配置模式下，使用以下命令配置连接速率限制：

connection-rate-limit *value*

- *value* - 指定虚拟服务器允许的最大连接速率。取值为0到10,000,000之间的整数，默认值为0。如取值为0，表示没有最大连接数限制。

在虚拟服务器配置模式下，使用**no connection-rate-limit**命令恢复连接速率限制的默认值。

配置防浪涌等待队列

配置HTTP、HTTPS、HTTP代理类型虚拟服务器的[连接速率限制](#)后，可以指定防浪涌等待队列长度，即虚拟服务器繁忙时，系统自动将新连接放入等待队列，此队列允许存放的客户端连接个数的最大值。

当产生新的连接时，若等待队列中的已有连接个数没有达到最大值，新连接将依次进入队列；并且，系统将判断虚拟服务器当前的连接速率是否达到最大限制，如果没有达到，则立即放行等待队列中排在最前的连接。若等待队列中的已有连接个数达到最大值，系统将对新连接执行指定的[超时连接动作](#)。

在虚拟服务器配置模式下，使用以下命令配置防浪涌等待队列长度：

connection-queue-length *value*

- *value* - 指定虚拟服务器的防浪涌等待队列长度。取值为0到100000间的整数，默认值为0。如取值为0，表示没有等待队列，不进行防浪涌保护。

在虚拟服务器配置模式下，使用**no connection-queue-length**命令取消等待队列长度的配置。

例如：指定连接速率限制为1000个/秒，防浪涌等待队列长度为2000，超时连接动作为“阻断，并返回403提示页面”。客户端从0秒开始，以2500个/秒的速率发起连接。第1秒结束后，对于到达设备的2500个客户端连接，先达到的2000个连接进入等待队列，剩余的500个连接被阻断。在第1秒内，设备每隔1毫秒（1秒除以1000个/秒）将排在队列的前1000个连接放行（在第2秒内处理剩下的1000个连接），以此类推。

配置超时连接动作

当HTTP、HTTPS、HTTP代理类型的虚拟服务器现有连接速率达到连接速率限制值，且等待队列中的连接数达到最大值时，新建连接将无法建立，系统将按照配置执行以下超时连接失败动作：返回响应消息、返回响应页面、重定向到新页面。在虚拟服务器配置模式下，使用以下命令配置超时连接动作：

connection-rate-limit-action { **redirect url** [**status-code** {301 | 302 | 303 | 307 | 308}] | **response** { **page string** | **message string** } [**status-code code**]}

- **redirect url** - 指定重定向到的新页面的地址，以http://或https://开头。
- **page string** - 指定系统中预定义或自定义的响应页面。如需导入自定义的响应页面，请参见[导入页面](#)。系统支持上传HTM/HTML/JPG/PNG格式的文件，且小于128K。
- **message string** - 指定自定义响应消息内容，范围是1到255个字符。
- **status-code** - 指定返回的状态码。当指定动作为“重定向到新页面”时，默认状态码为302。

在虚拟服务器配置模式下，使用**no connection-rate-limit-action**命令恢复超时连接动作的默认值，即阻断。

开启历史信息记录

AX设备不仅可监控统计虚拟服务器“实时”数据，也可监控一段历史时间内的数据，如最近一小时、最近一天、最近一个月。开启“历史信息统计”后，设备将开始统计各个虚拟服务器监控项的历史数据，并根据选择（最近一小时/一天/一周/一月），显示该监控项在此时间段的数据。否则，该监控项历史数据显示为0。在虚拟服务器配置模式下，使用以下命令开启虚拟服务器的历史信息记录功能：

history-stats {**enable** | **disable**}

- **enable** - 开启虚拟服务器的历史信息记录功能。
- **disable** - 关闭虚拟服务器的历史信息记录功能。

记录日志

在虚拟服务器配置模式下，使用以下命令记录负载均衡日志：

log { **enable** | **using-src** | **using-toa** | **using-header** *header name* [**x-forwarded-for** | **x-real-ip** | **real-src-ip**] | **exclude** { **file-type** {**js** | **css** | **image** | **media**} | **method** {**get** | **put** | **post** | **head** | **delete**} } }

- **enable** - 启用记录负载均衡日志功能。
- **using-src** - 指定系统使用报文自带的源IP及源端口发送日志。
- **using-toa** - 指定系统使用由报文 TOA解析出来的源 IP（及源端口）发送日志，当解析失败时使用报文自身携带的源IP、源端口发送。

- **x-forwarded-for**- 指定系统使用由HTTP/HTTPS报文头部中 X-Forwarded-For 解析出来的源IP（及源端口）发送日志。当不存在时，使用报文自身携带的源IP、源端口发送。
- **x-real-ip**- 指定系统使用由HTTP/HTTPS报文头部中X-Real-IP 解析出来的源IP（及源端口）发送日志。当不存在时，使用报文自身携带的源IP、源端口发送。
- **real-src-ip**- 指定系统使用由HTTP/HTTPS报文头部中 X-Forwarded-For 或者X-Real-IP 解析出来的源IP（及源端口）发送日志。
- **exclude {file-type {js | css | image | media} | method {get | put | post | head | delete}}** - 当设备每秒产生的负载均衡日志数量过多，导致数据库无法保存时，用户可选择自定义不需要保存的日志。只有HTTP和HTTPS类型的虚拟服务器支持配置该功能。
 - 不记录方法 - 不保存method为get/put/head/post/delete类型的HTTP/HTTPS日志。
 - 不记录文件 - 不保存文件类型为css/js/image/media的HTTP/HTTPS日志。其中，image包括PNG/BMP/JPEG/GIF/JPE/JPG类型的图片；media包括FLV/SWF/MP4/MP3/AVI类型。

TOA类型

配置发报文时所需要的TOA类型，在虚拟服务器配置模式下，使用以下命令：

```
toa type { ipv4 value | ipv6 value }
```

- **ipv4 value** - 指定发送报文为IPv4类型，取值范围为2至255。
- **ipv6 value** - 指定发送报文为IPv6类型，取值范围为2至255。

该值用于插入TOA、记录日志、自动源NAT以及会话保持。

插入TOA

在虚拟服务器配置模式下，使用以下命令插入TOA：

```
insert-toa tcp-flags [ FIN | RST | ACK | SYN | PSH | URG | ALL ]
```

- **FIN** - 指定对含有FIN标志位的TCP报文插入TOA。
- **RST** - 指定对含有RST标志位的TCP报文插入TOA。
- **ACK** - 指定对含有ACK标志位的TCP报文插入TOA。

- **SYN** - 指定对含有SYN标志位的TCP报文插入TOA。
- **PSH** - 指定对含有PSH标志位的TCP报文插入TOA。
- **URG** - 指定对含有URG标志位的TCP报文插入TOA。
- **ALL** - 指定对含有所有标志位的TCP报文插入TOA。

绑定SSL模板

仅当虚拟服务器的协议类型为HTTPS或SSL-OVER-TCP时，此配置生效。为HTTPS或SSL-OVER-TCP虚拟服务器绑定SSL模板后，当客户端与设备间通过SSL/TLS加密方式进行交互时，系统将对客户端与ADC设备间的数据进行解密。绑定SSL模板，在虚拟服务器配置模式下，使用以下命令：

ssl-profile *ssl-profile-name*

- *ssl-profile-name* - 指定系统中已创建的SSL模板的名称。

在虚拟服务器配置模式下，使用**no ssl-profile**命令删除绑定的SSL模板。

绑定服务端SSL模板

仅当虚拟服务器的协议类型为HTTPS或HTTP时，此配置生效。为HTTPS或HTTP类型的虚拟服务器绑定服务端SSL模板后，系统将对ADC设备与真实服务间的数据进行加密。绑定服务端SSL模板，在虚拟服务器配置模式下，使用以下命令：

server-ssl-profile *server-ssl-profile-name*

- *server-ssl-profile-name* - 指定系统中已创建的服务端SSL模板的名称。

在虚拟服务器配置模式下，使用**no server-ssl-profile**命令删除绑定的服务端SSL模板。

绑定应用模板

当虚拟服务器的类型为HTTP、HTTPS、HTTP代理、SSL流代理、快速HTTP、MYSQL时，系统支持绑定应用模板。绑定应用模板，在虚拟服务器配置模式下，使用以下命令：

app-profile *app-profile-name*

- *app-profile-name* - 指定系统中已创建的应用模板的名称。

在虚拟服务器配置模式下，使用**no app-profile**命令删除绑定的应用模板。

绑定TCP模板

当虚拟服务器的类型为HTTP、HTTPS、HTTP代理、TCP、SSL-OVER-TCP、SSL流代理、SMTP、IMAP或POP3时，系统支持绑定TCP模板，实现TCP通信加速。绑定TCP模板，在虚拟服务器配置模式下，使用以下命令：

```
tcp-profile tcp-profile-name
```

- *tcp-profile-name* - 指定系统中已创建的TCP模板的名称。

在虚拟服务器配置模式下，使用**no tcp-profile**命令删除绑定的TCP模板。

配置DNS服务器

当虚拟服务器的类型为HTTP代理、SSL流代理时，系统支持自定义DNS服务器。默认情况下，使用系统中已配置的DNS服务器。

使用系统DNS服务器，在虚拟服务器配置模式下，使用以下命令：

```
dns server using-system
```

使用**no dns server using-system**命令取消使用系统DNS服务器。

自定义DNS服务器，在虚拟服务器配置模式下，使用以下命令。

```
dns server {ipv4 | ipv6} ip-address
```

- *ip-address*: 指定虚拟服务器的DNS服务器地址，包括IPv4地址和IPv6地址。最多可配置6个自定义DNS服务器。

使用**dns server {ipv4 | ipv6}**命令取消对DNS服务器地址的指定。

配置IPv6的DNS查询

当虚拟服务器的类型为HTTP代理、SSL流代理时，系统支持开启发送查询IPv6地址的DNS请求。发送查询IPv6地址的DNS请求，在虚拟服务器配置模式下，使用以下命令：

```
dns ipv6-query
```

使用**no dns ipv6-query**命令关闭对IPv6地址的查询。

配置DNS有效时间

当虚拟服务器的类型为HTTP代理、SSL流代理时，系统支持配置DNS响应报文在设备上缓存的有效时间。指定DNS响应的有效时间，在虚拟服务器配置模式下，使用以下命令：

```
dns valid-time time
```

- *time*: 当客户端请求目标服务器后，系统会将目标服务器返回给客户端的DNS响应报文进行缓存。超出缓存有效时间后，系统将重新发起DNS请求。范围为0-3600秒。默认值为0，0表示使用响应报文中的有效时间（TTL）作为缓存时间。由于响应报文中的有效时间较短，建议修改有效时间，避免频繁发起DNS请求。

在虚拟服务器配置模式下，使用**no dns valid-time**命令取消对DNS有效时间的指定。

开启HTTP隧道模式

当虚拟服务器的类型为HTTP代理时，设备为代理服务器且仅可以转发HTTP协议的报文。如需转发HTTPS协议的报文，需要开启HTTP隧道模式。开启后，设备将在客户端和目标服务器之间建立隧道连接，通过隧道转发HTTPS报文。开启或者关闭HTTP隧道模式，在虚拟服务器配置模式下，使用以下命令：

```
http-tunnel {enable | disable}
```

配置自动修改HTTP头部协议

当虚拟服务器类型为HTTPS时，开启自动修改HTTP头部协议功能。启用后，在HTTPS类型的虚拟服务器[绑定SSL模板](#)的情况下，当真实服务返回响应报文时，系统按照以下原则自动修改报文中的Location/Refresh字段：

- 当"http://Host" 位于Location字段的起始位置，并且Host字段与客户端原始请求中的Host字段一致时，系统自动将"http" 修改为"https"。
- 当"http://Host" 位于Refresh字段的第7个字符位置，并且Host字段与客户端原始请求中的Host字段一致时，系统自动将"http" 修改为"https"。

在HTTPS类型的虚拟服务器配置模式下，使用以下命令，配置自动修改HTTPS头部协议：

```
auto-rewrite-headers-scheme enable
```

- **enable** - 启用自动修改HTTPS头部协议功能。默认情况下，启用该功能。

在虚拟服务器配置模式下，使用**no auto-rewrite-headers-scheme**命令关闭该功能。

指定脚本文件

当虚拟服务器类型为TCP、HTTP、HTTPS、SSL-OVER-TCP或RADIUS时，系统支持引用脚本文件：

- 实现基于消息的负载均衡。例如：引用系统预定义脚本文件“8583-async.lua”，可以实现基于银联8583协议、采用异步处理方式的`消息负载均衡`。
- 实现基于ALPN的负载均衡，即当客户端SSL请求中携带ALPN字段时，系统将根据ALPN字段中的相关协议信息，将客户端请求分配至适合的真实服务上。
- 实现基于TCP Payload的负载均衡，即系统根据客户端请求报文中Payload携带的相关协议信息，将客户端请求分配至适合的真实服务上。
- 对于HTTP和HTTPS类型的虚拟服务器，系统提供预定义的脚本文件“external-link-domain-http.lua”和“external-link-domain-https.lua”供用户参考，实现[基于域名方式的外链改写](#)。
- 对于RADIUS类型的虚拟服务器，系统提供预定义的脚本文件“radius_attribute_persist.lua”供用户参考，实现RADIUS负载均衡的同时，实现基于指定RADIUS属性的会话保持。
- 对于HTTP类型和部署在负载均衡或路由牵引模式的HTTPS类型的虚拟服务器，用户可以通过编写脚本文件，实现对客户端请求进行基于应用层数据或IP地址、端口等的SNAT转换。例如，可以将访问指定域名的客户端请求的源IP地址转换为配置好的地址簿中的地址。同时，系统也支持通过编写脚本，将属于不同流量组的访问请求的客户端源IP地址转换成不同地址簿中的地址。

注意：若同时配置了自动源NAT、源NAT规则和编写脚本进行SNAT，则生效的优先级为：源NAT规则 > 脚本中定义的SNAT > 自动源NAT。

为实现基于ALPN、TCP Payload的负载均衡，系统提供预定义脚本文件“tcp_payload_and_ssl.lua”供用户参考。自定义脚本文件的详细信息，请参照[SLB脚本编程手册](#)章节。在虚拟服务器配置模式下，使用以下命令引用脚本文件：

script *filename*

- *filename* - 指定系统内已有的脚本文件名称。

在虚拟服务器配置模式下，使用**no script**命令删除引用的脚本文件。

指定四层内容交换规则

指定虚拟服务器的四层内容交换规则，在虚拟服务器配置模式下，使用以下命令：

l4-content-switch *l4-name* [**after** *name1* | **before** *name2* | **top**]

- *l4-name* - 指定已创建的四层内容交换规则的名称。
- **after name1 | before name2 | top** - 指定该四层内容交换规则在规则列表的位置。如绑定多条四层内容交换规则，系统按规则列表中的先后顺序进行匹配，且匹配到一条规则后，不再继续匹配其他规则。如不配置该参数，默认指定的规则为列表中最后一条规则。**after name1**: 移动该规则至name1之后；**before name2**: 移动该规则至name2之前；**top**: 移动该规则至列表顶部。

在虚拟服务器配置模式下，使用**no l4-content-switch l4-name**删除指定的规则。

移动规则

用户可根据需要，对已创建的规则的位置进行移动，以调整规则匹配的优先级。在虚拟服务器配置模式下，使用以下命令移动规则：

```
move l4-content-switch l4-name {after name1 | before name2 | top}
```

- *l4-name* - 指定已创建的四层内容交换规则的名称。
- **after name1 | before name2 | top** - 指定该四层内容交换规则在规则列表的位置。如绑定多条四层内容交换规则，系统按规则列表中的先后顺序进行匹配，且匹配到一条规则后，不再继续匹配其他规则。如不配置该参数，默认指定的规则为列表中最后一条规则。**after name1**: 移动该规则至name1之后；**before name2**: 移动该规则至name2之前；**top**: 移动该规则至列表顶部。

指定七层内容交换规则

指定虚拟服务器的七层内容交换规则，在虚拟服务器配置模式下，使用以下命令：

```
l7-content-switch l7-name [after name1 | before name2 | top]
```

- *l7-name* - 指定已创建的七层内容交换规则的名称。
- **after name1 | before name2 | top** - 指定该七层内容交换规则在规则列表的位置。如绑定多条七层内容交换规则，系统按规则列表中的先后顺序进行匹配，且匹配到一条规则后，不再继续匹配其他规则。如不配置该参数，默认指定的规则为列表中最后一条规则。**after name1**: 移动该规则至name1之后；**before name2**: 移动该规则至name2之前；**top**: 移动该规则至列表顶部。

在虚拟服务器配置模式下，使用**no l7-content-switch l7-name**删除指定的规则。

移动规则

用户可根据需要，对已创建的规则位置进行移动，以调整规则匹配的优先级。在虚拟服务器配置模式下，使用以下命令移动规则：

```
move l7-content-switch l7-name {after name1 | before name2 | top}
```

- *l7-name* - 指定已创建的七层内容交换规则的名称。
- **after** *name1* | **before** *name2* | **top** - 指定该七层内容交换规则在规则列表的位置。如绑定多条七层内容交换规则，系统按规则列表中的先后顺序进行匹配，且匹配到一条规则后，不再继续匹配其他规则。如不配置该参数，默认指定的规则为列表中最后一条规则。**after** *name1*：移动该规则至*name1*之后；**before** *name2*：移动该规则至*name2*之前；**top**：移动该规则至列表顶部。

指定内容改写规则

仅HTTP和HTTPS类型的协议支持内容改写功能。指定内容改写规则，在虚拟服务器配置模式下，使用以下命令：

```
content-rewrite name [after name1 | before name2 | top]
```

- *name* - 指定已创建的内容改写规则名称。
- **after** *name1* | **before** *name2* | **top** - 指定该内容改写规则在规则列表的位置。如绑定多条内容改写规则，系统按规则列表中的先后顺序进行匹配。且所有内容改写规则均需匹配，即匹配到一条规则后，继续匹配其他所有规则。**after** *name1*：移动该规则至*name1*之后；**before** *name2*：移动该规则至*name2*之前；**top**：移动该规则至列表顶部。

在虚拟服务器配置模式下，使用**no content-rewrite** *name*删除指定的规则。

移动规则

用户可根据需要，对已创建的规则位置进行移动，以调整规则匹配的优先级。在虚拟服务器配置模式下，使用以下命令移动规则：

```
move content-rewrite name {after name1 | before name2 | top}
```

- *name* - 指定已创建的内容改写规则的名称。
- **after name1 | before name2 | top** - 指定该内容改写规则在规则列表的位置。如绑定多条内容改写规则，系统按规则列表中的先后顺序进行匹配。且所有内容改写规则均需匹配，即匹配到一条规则后，继续匹配其他所有规则。**after name1**: 移动该规则至name1之后；**before name2**: 移动该规则至name2之前；**top**: 移动该规则至列表顶部。

指定SQL内容交换规则

仅MYSQL类型的协议支持SQL内容交换规则。如绑定多条SQL内容交换规则，系统按规则列表中的先后顺序进行匹配，且匹配到一条规则后，不再继续匹配其他规则。指定SQL内容交换规则，在虚拟服务器配置模式下，使用以下命令：

```
sql-content-switch name [after name1 | before name1 | top]
```

- *name* - 指定已创建的SQL内容交换规则名称。
- **after name1 | before name1 | top** - 指定该SQL内容交换规则在规则列表的位置。如不配置该参数，默认指定的规则为列表中最后一条规则。**after name1**: 移动该规则至name1之后；**before name1**: 移动该规则至name1之前；**top**: 移动该规则至列表顶部。

在虚拟服务器配置模式下，使用**no content-rewrite name**删除指定的规则。

移动规则

用户可根据需要，移动虚拟服务器中SQL内容交换规则的位置，以调整规则匹配的优先级。在虚拟服务器配置模式下，使用以下命令移动规则：

```
move sql-content-switch name {after name1 | before name1 | top}
```

- *name* - 指定虚拟服务器中SQL内容交换规则的名称。
- **after name1 | before name1 | top** - 指定该SQL内容交换规则在规则列表的位置。如绑定多条SQL内容交换规则，系统按规则列表中的先后顺序进行匹配，且匹配到一条规则后，不再继续匹配其他规则。**after name1**: 移动该规则至name1之后；**before name1**: 移动该规则至name1之前；**top**: 移动该规则至列表顶部。

指定Web防护模板

仅HTTP和HTTPS类型的协议支持[Web防护](#)功能。指定Web防护模板，在虚拟服务器配置模式下，使用以下命令：

```
web-protect-profile profile-name
```

- *profile-name* - 指定已创建的Web防护模板的名称。

在虚拟服务器配置模式下，使用**no web-protect-profile**命令删除指定的模板。

配置主机改写

仅HTTP和HTTPS类型的协议支持主机改写功能。在虚拟服务器配置模式下，使用以下命令配置主机改写：

```
host-rewrite {auto | force [domain domain-name] | original value target value}
```

- **auto** - 当Host字段为“IP地址：端口”类型时，系统将按照以下规则分别对Host/Referer/Location字段进行改写：
 - 将Host字段改写为“真实服务IP地址：端口”；
 - 将Referer字段中首个“IP地址：端口”改写为“真实服务IP地址：端口”；
 - 将Location字段中首个“真实服务IP地址：端口”改写为原始的Host字段。
- **force** - 无论Host字段是什么类型，系统都将按照强制改写规则对Host/Referer/Location字段进行改写。
 - **domain** *domain-name* - 指定需匹配的域名。配置后，只有当Host字段匹配上指定域名时，系统才将按照强制改写规则进行改写。

强制改写规则为：

- 将Host字段改写为“真实服务IP地址：端口”；
- 将Referer字段中首个与Host字段匹配的内容改写为“真实服务IP地址：端口”；
- 将Location字段中首个“真实服务IP地址：端口”改写为原始的Host字段。
- **original** *value1* **target** *value2* - 指定Host/Referer字段中的原始内容与改写内容，*value1*表示原始内容，*value2*表示改写内容。系统将改写Host/Referer字段中的“原始内容”为“改写内容”，将Location字段中首个“改写内容”改写为“原始内容”。

在虚拟服务器配置模式下，使用**no host-rewrite**命令关闭主机改写功能。

配置访问控制

仅HTTP和HTTPS类型的协议支持访问控制功能。指定访问控制规则，在虚拟服务器配置模式下，使用以下命令：

```
acl name [after name1 | before name2 | top]
```

- *name* - 指定已创建的访问控制规则名称。
- **after** *name1* | **before** *name2* | **top** - 指定该访问控制规则在规则列表的位置。如绑定多条访问控制规则，系统按规则列表中的先后顺序进行匹配。且所有访问控制规则均需匹配，即匹配到一条规则后，继续匹配其他所有规则。**after** *name1*：移动该规则至*name1*之后；**before** *name2*：移动该规则至*name2*之前；**top**：移动该规则至列表顶部。

在虚拟服务器配置模式下，使用**no acl *name***删除指定的规则。

移动规则

用户可根据需要，对已创建的规则位置进行移动，以调整规则匹配的优先级。在虚拟服务器配置模式下，使用以下命令移动规则：

```
move acl name { after name1 | before name2 | top }
```

- *name* - 指定已创建的访问控制规则的名称。
- **after** *name1* | **before** *name2* | **top** - 指定该访问控制规则在规则列表的位置。如绑定多条访问控制规则，系统按规则列表中的先后顺序进行匹配。且所有访问控制规则均需匹配，即匹配到一条规则后，继续匹配其他所有规则。**after** *name1*：移动该规则至*name1*之后；**before** *name2*：移动该规则至*name2*之前；**top**：移动该规则至列表顶部。

配置错误信息

当七层虚拟服务器的状态为“离线”或“维护”，或者所有真实服务均不可用时，虚拟服务器收到客户端请求后，会提示错误，包括：回复错误消息，返回错误页面，或重定向到新页面。

配置错误，在虚拟服务器配置模式下，使用以下命令：

```
error-message { page value [code number] | redirect value | string }
```

- **page value** [**code number**] - 指定系统中的错误页面，包含预定义页面和自定义页面。如需导入自定义的错误页面，请参见[导入页面](#)。系统支持上传HTM/HTML/JPG/PNG格式的文件，且小于128K。
- **redirect value** - 输入重定向到的新页面的地址，以http://或https://开头。
- **string** - 自定义错误消息。系统默认发送错误信息“Service Unavailable”和错误码“503”。

在虚拟服务器配置模式下，使用 **no error-message** 恢复默认值。

导入页面

系统中预定义14个页面，包含200-zh.html、200-cn.html、301-zh.html、301-cn.html、302-zh.html、302-cn.html、403-zh.html、403-cn.html、404-zh.html、404-cn.html、50x-zh.html、50x-cn.html、maintain-zh.html和maintain-cn.html页面。其中，名字中包含-cn的为英文页面，包含-zh的为中文页面。预定义的页面不可删除。用户也可根据需要，导入页面。

导入页面，在执行模式下，使用以下命令：

```
import error-page from {ftp | tftp} server IP_address [user username password password | vrouter vr-name] file-name
```

- **{ftp | tftp}** - 指定上传的方式，通过FTP上传或TFTP上传。
- **server IP_address** - 指定FTP服务器或TFTP服务器的IP地址。
- **user username password password** - 指定服务器的用户名和密码。
- **vrouter vr-name** - 指定所属VRouter的名称。
- **file-name** - 指定导入文件的名称，支持HTM/HTML/JPG/PNG格式的文件，且小于128K。

删除页面

删除页面，在执行模式下，使用以下命令：

```
delete error-page file file-name
```

- **file-name** - 指定需删除页面的名称。

查看页面

查看系统中的页面，在任何模式下，使用以下命令：

```
show error-page
```

配置三角模式

三角模式，即DSR模式。在三角部署模式下，客户端发送给真实服务的请求报文会经过设备处理，然后转发给真实服务，但真实服务返回的响应报文将不再经过设备，而是直接发送给客户端。仅TCP/UDP/Any协议支持该配置。开启或关闭三角模式，在虚拟服务器配置模式下，使用以下命令：

- **direct-server-return enable** - 开启三角模式。
- **direct-server-return disable** - 关闭三角模式。系统默认关闭三角模式。

配置UDP强制负载

仅UDP类型的协议支持UDP强制负载功能。开启该功能后，当客户端发起请求，设备根据UDP数据包分配服务器，将UDP四层负载均衡转化为七层负载均衡，实现相同五元组的客户端请求分配到不同的服务器。配置该功能后，虚拟服务器与其服务池中的真实服务成员均不可配置“端口Any”，并且ALG功能将失效。启用或关闭UDP强制负载功能，在虚拟服务器配置模式下，使用以下命令：

- **datagram enable** - 开启UDP强制负载功能。
- **datagram disable** - 关闭UDP强制负载功能。系统默认关闭该功能。

配置UDP超时时间

对于开启UDP强制负载功能的UDP类型虚拟服务器、RADIUS类型的虚拟服务器，用户可以配置超时时间，超过该时间，设备将断开与真实服务的UDP连接。

在虚拟服务器配置模式下，使用以下命令配置超时时间：

datagram-timeout time - 指定设备与真实服务建立UDP连接的超时时间。取值范围为1至60秒，默认值为5秒。

使用**no datagram-timeout**命令恢复默认值。

逆向路由

逆向路由是指用于转发反向数据的路由，反向是相对于初始化数据流方向。启用或关闭逆向路由，在虚拟服务器配置模式下使用以下命令：

reverse-route [**force** | **prefer**]

- **force** – 开启逆向路由。如果能找到逆向路由，则使用逆向路由转发反向数据。如果找不到逆向路由，则丢弃数据包。
- **prefer** – 优先使用逆向路由。如果能够找到逆向路由就使用逆向路由转发反向数据；如果找不到逆向路由则按原路径返回。

关闭逆向路由，在全局配置模式下使用命令 **no reverse-route**。关闭后，反向数据流到达设备后不进行逆向路由检查，原路返回。

配置调度模式

当虚拟服务器类型为HTTP或HTTPS时，指定设备对客户端请求的调度模式。在客户端发起访问时使用HTTP 1.1协议的情况下，设备可以继续使用HTTP 1.1协议连接到真实服务，在一个TCP连接上进行最大次数的请求/应答，即采用长连接机制；也可以使用HTTP 1.0连接到真实服务，在每次请求/应答后，关闭TCP连接，即采用短连接机制。

配置对客户端请求的调度模式，在虚拟服务器配置模式下，使用以下命令：

schedule-by {**each-request** | **first-request**}

- **each-request** - 指定设备连接至真实服务时，采用短连接机制，即当客户端发起的HTTP连接中包含多个请求时，系统将按照[七层负载均衡处理流程](#)，逐个处理每个请求。如在配置了HTTP内容改写的情况下，系统将对每一个请求进行内容改写规则的匹配。默认情况下，选择该调度模式。
- **first-request** - 指定设备连接至真实服务时，采用长连接机制，即当客户端发起的HTTP连接中包含多个请求时，系统将只对第一个请求执行[七层负载均衡处理流程](#)，后续请求都将被转发至与第一个请求一致的真实服务上。如在配置了HTTP内容改写的情况下，系统将只对第一个请求进行内容改写规则的匹配。



注意：若指定HTTP/HTTPS类型虚拟服务器的调度模式为“首请求”，部分功能将失效，如缓存、压缩等。

镜像请求

当客户端访问HTTP/HTTPS类型的虚拟服务器时，系统将镜像真实的客户端请求，发送至指定的服务器。在不影响客户端访问的情况下，服务器可以利用镜像的客户端请求，进行相关测试。每个虚拟服务器最多支持添加8个服务器接收客户端请求的镜像。



注意: 当HTTPS类型的虚拟服务器工作在透明部署或牵引部署模式时，不支持该功能。

在虚拟服务器配置模式下，使用以下命令配置镜像请求的功能：

mirror-request {enable | request-body enable | target {ip | ipv6} address port num [percent value]}

- **enable** - 开启镜像请求功能。

使用**no mirror-request enable**命令关闭镜像请求功能。

- **request-body enable** - 开启镜像客户端请求时携带请求体内容的功能。默认开启该项。使用**no mirror-request request-body enable**命令关闭镜像客户端请求时携带请求体内容。

- **target {ip | ipv6} address port num [percent value]**

- **address** - 指定接收客户端请求镜像的服务器IPv4或IPv6地址。
- **num** - 指定接收客户端请求镜像的服务器的端口号。取值范围是1到65535。
- **value** - 指定镜像原始客户端请求数目的百分比，系统将按照指定的百分比镜像原始请求，并发送至相应的服务器。取值范围是1%到100%，默认值是100%，表示系统将镜像全部的客户端请求至指定的服务器。

使用**no mirror-request target {ip | ipv6} address port num**命令删除接收客户端请求镜像的服务器配置。

配置入接口模式

客户端请求到达设备，匹配到虚拟服务器后，设备将按照配置对流量的入接口进行匹配，并对该流量执行指定的动作。

在虚拟服务器配置模式下，使用以下命令配置入接口模式：

ingress-if status {specify-disabled | specify-enabled}

- **specify-disabled** - 指定该模式后，系统将阻断从指定入接口进入的流量。
- **specify-enabled** - 指定该模式后，系统将放行从指定入接口进入的流量。

ingress-if interface *intef-name*

- *intef-name* - 指定需匹配的接口名称。用户可以根据需要，添加多个接口，每个虚拟服务器最多可配置64个。

在虚拟服务器配置模式下，使用**no ingress-if interface** *intef-name*命令删除指定的接口。

在虚拟服务器配置模式下，使用**no ingress-if status**命令恢复入接口匹配的默认模式，即放行从所有接口进入的流量。



注意:

- 当指定入接口时，需指定为三层接口，即系统仅对从三层接口进入的流量执行相应的动作。
- 对于VSYS，此处需指定属于相应VSYS的接口。
- 当入接口指定为逻辑接口时，逻辑接口下包含的所有物理接口都将作为生效配置。例如：集聚接口aggregate1包含了物理接口ethernet0/1、ethernet0/2，配置虚拟服务器的“入接口匹配”为“阻断指定接口：aggregate1”，那么无论是从接口ethernet0/1，还是从接口ethernet0/2进入的流量，该虚拟服务器都将进行阻断。

配置虚拟服务器IP的路由发布

虚拟路由器IP的路由发布，即将该虚拟服务器的IP地址发布给ADC设备所在网络中的动态路由，供网络中的动态路由协议进行路由计算。然后，根据计算结果，选择最优的路由路径将客户端请求转发至正常运行的ADC设备。

例如，网络中部署有两台ADC设备，且配置了相同的虚拟服务器IP地址，对外提供服务。当ADC设备将虚拟服务器的IP地址发布给网络中的动态路由后，若两台ADC设备均正常运行，根据动态路由协议的路由计算结果，客户端请求将被转发给距离其最近的ADC设备；若其中一台ADC设备发生故障，根据动态路由表项，客户端请求仍然可以被转发给另外一台正常运行的ADC设备。

该功能需和动态路由的“引入路由”功能一起使用才可以生效，例如OSPF的[引入路由](#)。

在虚拟服务器配置模式下，使用以下命令配置虚拟服务器IP的路由发布：

route-advertisement {**enable** | **disable** | **selective**}

- **enable** - 开启该功能，无论虚拟服务器是什么状态，系统都将发布该虚拟服务器IP给网络中的动态路由。
- **disable** - 关闭该功能，无论虚拟服务器是什么状态，系统都不发布该虚拟服务器IP给网络中的动态路由。默认情况下，关闭该功能。
- **selective** - 配置该参数后，系统将根据虚拟服务器的运行状态决定是否发布虚拟服务器IP给网络中的动态路由。当虚拟服务器是“正常”或“未知”状态时，发布该虚拟服务器IP给网络中的动态路由。当虚拟服务器是“禁用/维护/离线”运行状态时，系统将不发布。

配置虚拟服务器外链改写

仅HTTP/HTTPS/HTTP代理类型的虚拟服务器支持外链改写功能。在客户端升级为IPv6的场景中，当真实服务返回给客户端的响应中包含IPv4的外链链接时，系统将对包含IPv4外链的响应体进行改写，然后返回给客户端。设备将作为代理访问外链网站并返回响应给客户端，从而解决客户端升级为IPv6后，IPv4外链网站无法访问的问题。

HTTP/HTTPS类型的虚拟服务器支持基于路径和域名两种外链改写方式，HTTP代理类型的虚拟服务器仅支持基于路径方式的外链改写。

配置外链改写之前，需先启用虚拟服务器的外链改写功能，在虚拟服务器配置模式下，使用以下命令：

external-link-rewrite enable

在虚拟服务器配置模式下，使用**no external-link-rewrite enable**命令关闭外链改写功能。

配置基于路径方式的外链改写

配置该功能后，系统将按照改写路径的方式，对响应页面中的外链进行改写。

在虚拟服务器配置模式下，使用以下命令配置基于路径方式的虚拟服务器外链探测：

external-link-rewrite {**type** **path** | **multi-level enable** | **ip-family-detect** {**enable** | **url** *url*} | **content-rewrite enable** | **scheme** {**virtual-server-type** | **https** | **http**} | **location-prefix** *prefix* | **host** *host-name* [**scheme** {**http** | **https**}]}

- **type path** - 指定按照改写路径的方式对外链进行改写。该方式为默认方式。
使用**no external-link-rewrite type**命令恢复外链改写的默认方式。

- **multi-level enable** - 开启多级外链的改写功能。当客户端通过设备改写后的外链进行访问时，若响应体中仍存在IPv4外链，则会继续改写。

使用**no external-link-rewrite multi-level enable**命令关闭多级外链的改写功能。

- **ip-family-detect {enable | url url}** - 配置客户端的单双栈探测功能。
 - **enable** - 开启客户端的单双栈探测功能。启用后，客户端将向探测网站发送探测请求，根据网站返回的响应，客户端再次发起访问请求时，将携带标识其是单栈还是双栈的Cookie。当客户端再次发起访问的请求达到设备时，若请求携带的Cookie表示客户端为单栈，即只可以访问IPv6地址，后续系统将为其执行外链改写流程；若请求携带的Cookie表示客户端为双栈，即可以访问IPv6和IPv4地址，后续系统将不会为其执行外链改写流程。

使用**no ip-family-detect enable**命令关闭单双栈探测功能。

- **url url** - 指定探测网站的IPv4网址。

使用**no ip-family-detect url**命令取消探测URL的配置。

说明：若使用该功能，指定的探测网站必须支持跨域访问，客户端的单双栈探测才能成功。因此，用户可以根据客户端提供的自身可达的IPv4地址和端口号，另外配置一个虚拟服务器，开启该虚拟服务器的[探测服务器](#)功能，将该虚拟服务器作为探测服务器，进行客户端的单双栈探测。

- **content-rewrite enable** - 开启外链的内容改写功能。当HTTP/HTTPS/HTTP代理类型的虚拟服务器指定[内容改写规则](#)时，设备从外链网站获取响应后，将匹配虚拟服务器设置的内容改写规则，并将改写后的响应返回给客户端。

使用**no external-link-rewrite content-rewrite enable**命令关闭外链的内容改写功能。

- **scheme {virtual-server-type | https | http}** - 指定客户端访问外链时使用的虚拟服务器类型。
 - **virtual-server-type** - 使用与原虚拟服务器类型一致的虚拟服务器访问外链链接。该项为默认值。
 - **https** - 使用HTTPS类型的虚拟服务器访问外链链接。
 - **http** - 使用HTTP类型的虚拟服务器访问外链链接。

使用**no external-link-rewrite scheme**命令恢复默认值**virtual-server-type**。

- **location-prefix prefix** - 指定外链改写后的链接前缀，范围是1到63个字符。

使用**no external-link-rewrite location-prefix**命令恢复默认值“proxy”。

- **host** - 指定需改写的外链链接。
 - *host-name* - 指定外链链接的域名。系统将对匹配上指定域名的外链链接进行改写。
 - **scheme http** - 将外链链接改写为HTTP类型。
 - **scheme https** - 将外链链接改写为HTTPS类型。

使用 **no external-link-rewrite host host-name** 命令删除指定的外链链接。

基于路径方式的外链改写，举例如下：指定 **host scheme** 为 **https**，*host-name* 为 “www.baidu.com”，指定 *prefix* 为 “ax_proxy”，指定访问外链时使用的 **scheme** 为 “HTTP”，当客户端申请访问 “http://[2000::8]:9999/index.com” 的虚拟服务器，真实服务返回给客户端的响应中包含IPv4外链，且外链链接域名中包含 “www.baidu.com” 时，系统将该链接改写为 “http://[2000::8]:9999/ax_proxy.https.www.baidu.com/index.html”。

配置虚拟服务器外链探测

若用户选择基于路径方式的外链改写，可以使用外链探测功能。启用外链探测功能后，当客户端升级为IPv6，访问虚拟服务器，真实服务返回响应给客户端时，系统将自动探测该响应中包含的IPv4外链链接。

在虚拟服务器配置模式下，使用以下命令配置虚拟服务器外链探测：

```
external-link-detect {enable | mode {all | href-only}}
```

- **enable** - 开启虚拟服务器外链探测功能。
- **mode{all | href-only}** - 指定外链探测的发现模式，系统支持“全部URL”和“仅超链接”。“全部URL”表示以“http://”、“https://”和“//”开始的外链，“仅超链接”表示以href=“http://”、href=“https://”和href=“//”开始的外链。

使用**no external-link-detect mode**命令恢复默认值**all**。

在虚拟服务器配置模式下，使用**no external-link-detect enable**命令关闭外链探测功能。

配置基于域名方式的外链改写

用户还需为该虚拟服务器引用外链改写相关的[脚本](#)文件，系统才能按照改写域名的方式，对响应页面中的外链进行改写。用户可以在脚本中配置外链改写的白名单等参数。系统提供预定义脚本文件 “external-link-domain-http.lua” 和 “external-link-domain-https.lua” 供用户参考，用户可以根据需要对预定义脚本编辑后进行引用。自定义脚本文件的详细信息，请参照[SLB脚本编程手册](#)章节。

在虚拟服务器配置模式下，使用以下命令配置基于域名方式的虚拟服务器外链探测：

```
external-link-rewrite { type domain | ip-family-detect {enable | url url} | scheme {virtual-server-type | https | http} |  
location-prefix prefix | domain-name domain-name}
```

- **type domain** - 指定按照改写域名的方式对外链进行改写。

使用**no external-link-rewrite type**命令恢复外链改写的默认方式，即基于路径方式的外链改写。

- **ip-family-detect {enable | url url}**

- **enable** - 开启客户端的单双栈探测功能。启用后，客户端将向探测网站发送探测请求，根据网站返回的响应，客户端再次发起访问请求时，将携带标识其是单栈还是双栈的Cookie。当客户端再次发起访问的请求达到设备时，若请求携带的Cookie表示客户端为单栈，即只可以访问IPv6地址，后续系统将其执行外链改写流程；若请求携带的Cookie表示客户端为双栈，即可以访问IPv6和IPv4地址，后续系统将不会为其执行外链改写流程。

使用**no ip-family-detect enable**命令关闭单双栈探测功能。

- **url url** - 指定用来探测的IPv4网址。

使用**no ip-family-detect url**命令取消探测URL的配置。

说明：若使用该功能，指定的探测网站必须支持跨域访问，客户端的单双栈探测才能成功。因此，用户可以根据客户端提供自身可达的IPv4地址和端口号，另外配置一个虚拟服务器，开启该虚拟服务器的[探测服务器](#)功能，将该虚拟服务器作为探测服务器，进行客户端的单双栈探测。

- **scheme {virtual-server-type | https | http}**

- **virtual-server-type** - 使用与原虚拟服务器类型一致的虚拟服务器访问外链链接。该项为默认值。
- **https** - 使用HTTPS类型的虚拟服务器访问外链链接。
- **http** - 使用HTTP类型的虚拟服务器访问外链链接。

- **location-prefix prefix** - 指定外链改写后的链接前缀，范围是1到63个字符。

使用**no external-link-rewrite location-prefix**恢复默认值“proxy”。

- **domain-name domain-name** - 指定虚拟服务器的域名。配置后，若客户端使用HTTP类型的虚拟服务器访问外链链接，系统将外链链接中的域名改写为以下格式：外链原始域名.prefix.domain-name；若客户端使用HTTPS类型的虚拟服务器访问外链链接，系统将外链链接中的域名改写为以下格式：外链原始域名-prefix-

domain-name，同时将外链原始域名中的“.”改写为“-”。

使用`no domain-name`命令取消该配置。

基于域名方式的外链改写，举例如下：指定 **scheme** 为 **https**，**prefix** 为“proxy”，**domain-name** 为“www.ax.com”。当客户端申请访问该虚拟服务器，真实服务返回给客户端的响应中包含IPv4外链“http://www.baidu.com”时，系统将该链接改写为“https://www-baidu-com-proxy-www.ax.com/?proxy_scheme=http&proxy_port=80”。

指定 **scheme** 为 **http**，**prefix** 为“proxy”，**domain-name** 为“www.ax.com”。当客户端申请访问该虚拟服务器，真实服务返回给客户端的响应中包含IPv4外链“https://www.baidu.com”时，系统将该链接改写为“http://www.baidu.com.proxy.www.ax.com/?proxy_scheme=https&proxy_port=443”。

配置虚拟服务器的探测服务器功能

当系统在另一虚拟服务器上启用了外链改写的[单双栈探测](#)功能时，用户可以启用该虚拟服务器作为探测服务器的功能。

在虚拟服务器配置模式下，使用以下命令启用探测服务器功能：

```
detect-server {enable | path path-name}
```

- **enable** - 启用该虚拟服务器作为探测服务器的功能。
- **path path-name** - 指定探测服务器URL地址的路径部分。例如，HTTP类型的虚拟服务器VS1上启用了外链改写的单双栈探测功能，指定探测服务器的URL地址为“http://10.10.10.12:80/a/b.html”，其中“10.10.10.12”为客户端可达的地址。那么用户需再配置一个HTTP类型的虚拟服务器VS2，VS2的IP地址和端口号为“10.10.10.12:80”，然后在VS2上启用探测服务器功能，输入的探测服务器的URL路径为“a/b.html”。

在虚拟服务器配置模式下，使用`no detect-server {enable | path}`命令取消配置。

查看虚拟服务器信息

在任何模式下，使用以下命令查看虚拟服务器信息，包含协议类型、虚拟服务器状态、缺省服务池配置、SLB规则配置等：

```
show slb virtual-server [name]
```

- **name** - 指定虚拟服务器的名称。

配置真实服务

真实服务，即在用户组网中真实服务器上部署的服务，负责处理客户端的请求。

系统支持配置真实服务的IP地址和域名，同时支持IPv4和IPv6的IP类型和域名类型。

当配置域名时，系统在创建真实服务（即父真实服务）的同时，会将域名解析出的IP地址，自动创建出对应的子真实服务（通常被命名为“--子真实服务IP地址@父真实服务名称”），用户可选择解析所有IP还是首个IP来创建子真实服务。当域名解析出的IP发生变化时，系统将自动更新子真实服务。对于不存在的IP，其对应的子真实服务将会自动被删除，对于新解析出IP，系统将会自动新建子真实服务，从而避免因真实服务的IP变化而造成的频繁更改配置的不便。



注意: 当真实服务配置为域名时，设备将使用系统中的DNS服务器对域名进行解析，所以需用户提前配置DNS服务器。

创建真实服务

在全局配置模式下，使用以下命令创建真实服务：

```
slb real-server server-name
```

- *server-name* - 指定真实服务的名称并进入真实服务配置模式。如果指定的名称已存在，则直接进入真实服务配置模式。

在全局配置模式下，使用`no slb real-server server-name`命令删除真实服务。

进入虚拟服务器配置模式后，可配置以下参数：

- [指定IP和端口](#)
- [指定域名和端口](#)
- [自动解析域名所有IP](#)
- [配置最大连接数](#)
- [配置连接速率限制](#)
- [指定恢复时间](#)
- [指定预热时间](#)

- [配置真实服务的权重](#)
- [配置真实服务的状态](#)
- [绑定健康检查对象](#)
- [开启历史信息记录](#)

指定IP和端口

在真实服务配置模式下，使用以下命令指定真实服务的IP地址和端口号：

```
{ ip | ipv6 } ip-address port number
```

- *ip-address* - 指定真实服务的IPv4或IPv6地址。
- *number* - 指定真实服务监听客户端请求的端口号。取值范围为1至65535。

使用`no { ip | ipv6 }`删除真实服务的IP的配置。

指定域名和端口

指定真实服务的域名和端口，在真实服务配置模式下，使用以下命令指定真实服务的域名和端口号：

```
domain-name name port number [ ipv4 | ipv6 ]
```

- *name* - 指定真实服务的域名名称。长度为1-254字符。
- *number* - 指定真实服务监听客户端请求的端口号。取值范围为1至65535。
- *ipv4 | ipv6* - 指定真实服务的域名类型，IPv4或IPv6。若为IPv4，则对所配置域名解析A记录（即将域名指向一个IPv4地址），并根据解析结果生成子真实服务；若为IPv6，则对所配置域名解析AAAA记录（即将域名指向一个IPv6地址），并根据解析结果生成子真实服务。

使用`no domain-name`删除真实服务域名的配置。



注意:

- 新建真实服务时，真实服务的IP和域名不能同时设置，同时注意真实服务名称不能包含



“@” 符号。

- 当配置真实服务的域名时，若父真实服务状态为禁用时，系统依然会解析并创建子真实服务。
- 子真实服务有单独的运行状态、健康检查状态，其他属性和父真实服务相同，比如健康检查、端口、权重、优先级等。
- 子真实服务不支持编辑和删除。
- 四七内容交换规则不可以指定父真实服务。
- 父真实服务不会生成健康检查实例，子真实服务会生成健康检查实例。

自动解析域名所有IP

用户可选择是将解析到的“所有IP”还是“首个IP”，来创建子真实服务。当开启自动解析域名所有IP时，系统将解析到的每个IP新建一个子真实服务，每个父真实服务最多支持新建16个子真实服务。关闭时，系统会将解析到的第一个IP新建一个子真实服务，作为域名的子真实服务。

开启自动解析域名所有IP，在真实服务配置模式下，使用以下命令：

```
auto-populate all-ip
```

关闭自动解析域名所有IP，在真实服务配置模式下，使用以下命令：

```
no auto-populate all-ip
```

配置最大连接数

最大连接数的设置和真实服务的性能有关。如真实服务的现有连接数超过该值，超出部分的连接将被分配给其他可用的真实服务；如所有真实服务的现有连接数均超过其设定的最大值，新连接将无法建立。在真实服务配置模式下，使用以下命令配置最大连接数：

```
max-connection number
```

- *number* - 指定真实服务允许的最大并发连接数。取值为0到10,000,000之间的整数，默认值为0。如取值为0，表示没有最大连接数限制。

在真实服务配置模式下，使用 **no max-connection** 命令恢复默认值。

配置连接速率限制

指定真实服务允许的最大连接速率。若真实服务的现有连接速率超过该值，新建连接将被分配至其他可用的真实服务；若所有真实服务的现有连接速率均超过其设定的最大值，新连接将无法建立。

connection-rate-limit *value*

- *value* - 指定真实服务允许的最大连接速率。取值为0到10,000,000之间的整数，默认值为0。如取值为0，表示没有最大连接速率限制。

在虚拟服务器配置模式下，使用**no connection-rate-limit**恢复最大连接速率的默认值。

指定恢复时间

指定真实服务的恢复时间。配置健康检查后，真实服务的健康检查状态由Down变为Up时，真实服务立即进入恢复阶段。在恢复时间内，真实服务不接收客户端的请求。恢复时间结束后，真实服务进入预热阶段。

在真实服务配置模式下，使用以下命令配置恢复时间：

recovery-time *value*

- *value* - 指定真实服务的恢复时间。恢复时间可根据服务器的性能设置，取值范围为0至3600秒，默认为0，即真实服务不需要恢复时间，直接进入预热阶段。

在真实服务配置模式下，使用**no recovery-time**命令恢复默认值。

指定预热时间

指定真实服务的预热时间。在指定的预热时间内，真实服务对客户端进行部分响应；到预热阶段结束后，真实服务对客户端请求全响应，直至达到最大连接数或连接速率限制。

在真实服务配置模式下，使用以下命令配置恢复时间：

warmup-time *value*

- *value* - 指定真实服务的预热时间。预热时间可根据服务器的性能进行设置，取值范围为0至3600秒，默认为0。如取值为0，表示系统不需要预热时间，在恢复时间后立即响应客户端的请求，直至达到最大连接数或连接速率限制。

在真实服务配置模式下，使用**no warmup-time**命令恢复默认值。

配置真实服务的权重

指定真实服务的权重。给真实服务分配不同的权重，使其接收相应权重比例的服务请求。如：给配置低、负载高的机器，分配较低的权重，使其负载降低。在真实服务配置模式下，使用以下命令配置真实服务的权重：

weight value

- **value** - 指定真实服务的权重值。取值范围为1至255，默认值为1。

在真实服务配置模式下，使用**no weight**命令恢复默认值。

配置真实服务的状态

配置真实服务的状态。真实服务的实际运行状态，请参见[查看真实服务的运行状态](#)。配置状态包括以下四种：

- **enable** 启用 - 当真实服务为启用状态时，可以正常接收客户端的请求。
- **disable** 禁用 - 当真实服务为禁用状态时，原有的连接被删除不可继续使用，也不再接收客户端新的连接请求。
- **disable keep-persistence** 平滑退出（等待保持表老化） - 当真实服务为此状态时，原有连接和会话保持可继续使用。保持表等待老化，新的客户端请求若匹配保持表，可转发到真实服务。系统不再接收不匹配保持表的新建连接请求，以确保正在运行的业务不中断。
- **disable no-persistence** 平滑退出（清空保持表） - 当真实服务为此状态时，原有的连接可以继续使用，系统将立即删除保持表，并不再接收新的请求。

指定真实服务的状态，在真实服务配置模式下，使用以下命令：

status {disable | enable | disable keep-persistence | disable no-persistence}

- **disable** - 指定真实服务的状态为“禁用”。
- **enable** - 指定真实服务的状态为“启用”。
- **disable keep-persistence** - 指定真实服务的状态为“平滑退出（等待保持表老化）”。
- **disable no-persistence** - 指定真实服务的状态为“平滑退出（清空保持表）”。

绑定健康检查对象

健康检查用于检查各种服务的可用状态。设备可配置各种检查方法，对协议进行健康检查，例如TCP，UDP，HTTP，HTTPS等。绑定已创建的健康检查，在真实服务配置模式下，使用以下命令：

```
health-check name [group group-name]
```

- *name* - 指定已创建的健康检查的名字。
- **group** *group-name* - 指定已创建的健康检查组的名字。

在真实服务配置模式下，使用**no health-check**命令解除绑定的健康检查对象。

开启历史信息记录

AX设备不仅可监控统计真实服务“实时”数据，也可监控一段历史时间内的数据，如最近一小时、最近一天、最近一个月。开启“历史信息统计”后，设备将开始统计各个真实服务监控项的历史数据，并根据选择（最近一小时/一天/一周/一月），显示该监控项在此时间段的数据。否则，该监控项历史数据显示为0。在真实服务配置模式下，使用以下命令开启真实服务的历史信息记录功能：

```
history-stats {enable | disable}
```

- **enable** - 开启真实服务的历史信息记录功能。
- **disable** - 关闭真实服务的历史信息记录功能。

查看真实服务配置

在任何模式下，使用以下命令查看系统中已配置的真实服务：

```
show slb real-server name
```

- *name* - 指定真实服务的名称。

查看真实服务的运行状态

配置真实服务状态后，可在任何模式下，使用**show slb real-server server-name**查看其实际的运行状态。包含以下三种：

- **up**: 表示真实服务状态为“正常”。当真实服务状态被指定为“启用”且该真实服务配置了IP时，其运行状态显示为“启用”。
- **down**: 表示真实服务状态为“禁用”。当真实服务状态配置为“禁用”时，其状态显示为“禁用”。当真实服务状态被指定为“启用”且该真实服务没有配置IP时，其运行状态显示为“禁用”。
- **wait-down**: 表示真实服务状态为“禁用中”。当真实服务状态被指定为“平滑退出（清空保持表）”或“平滑退出（等待保持表老化）”时，原有的连接还未关闭或保持表还未老化时，真实服务的运行状态为“禁用中”。当原有连接正常关闭或保持表老化后，运行状态显示为“禁用”。

配置服务池

一组提供相同服务的真实服务的集合称之为服务池。负载均衡即针对服务池中的多个真实服务使用不同的均衡算法进行均衡。

创建服务池

在全局配置模式下，使用以下命令创建服务池：

```
slb server-pool pool-name type {any | http | https | tcp | udp | fast-http | ftp | ssl-over-tcp | sip-tcp | sip-udp | ip | rdp | imap | pop3 | smtp | radius | mysql}
```

- *pool-name* - 指定服务池的名称并进入服务池配置模式。如果指定的名称已存在，则直接进入服务池配置模式。
- *type {any | http | https | tcp | udp | fast-http | ftp | ssl-over-tcp | sip-tcp | sip-udp | ip | rdp | imap | pop3 | smtp | radius | mysql}* - 指定协议的类型。如：指定的协议类型为HTTP，该服务池将分发HTTP类型的请求。



注意: 根据协议类型的不同，四层和七层的服务池选项配置也将不同，请以实际为准。

在全局配置模式下，使用`no slb server-pool pool-name`命令删除指定的服务池。

添加真实服务

添加真实服务到服务池，在服务池配置模式下，使用以下命令：

```
real-server server-name
```


- **server-name** - 指定真实服务的名称。系统将该真实服务添加到服务池中。一个服务池可以添加多个真实服务。

在服务池配置模式下，使用**no real-server server-name**命令从服务池中删除该真实服务。

启用/禁用真实服务

为了使用户能够指定真实服务在不同服务池中的状态，设备支持在服务池下启用/禁用真实服务。默认情况下，该真实服务状态与首次配置时保持一致。

启用/禁用服务池中真实服务，在服务池配置模式下，使用以下命令：

```
real-server server-name [ status { enable | disable no-persistence | disable keep-persistence } ]
```

- **enable** - 指定真实服务的状态为“启用”。
- **disable no-persistence** - 指定真实服务的状态为“平滑退出（清空保持表）”，清除该服务池下此真实服务的所有会话保持表后，此真实服务变为禁用状态。
- **disable keep-persistence** - 指定真实服务的状态为“平滑退出（等待保持表老化）”，该服务池下此真实服务的所有会话保持表还未老化时，真实服务为禁用中状态；所有会话保持表老化后，真实服务变为禁用状态。

指定真实服务恢复时间

指定真实服务的恢复时间。配置健康检查后，真实服务的健康检查状态由Down变为Up时，真实服务立即进入恢复阶段。在恢复时间内，真实服务不接收客户端的请求。恢复时间结束后，真实服务进入预热阶段。

在服务池配置模式下，使用以下命令配置恢复时间：

```
recovery-time value
```

- **value** - 指定真实服务的恢复时间。恢复时间可根据服务器的性能设置，取值范围为0至3600秒，默认为0秒。如取值为0，表示真实服务不需要恢复时间，直接进入预热阶段。

在服务池配置模式下，使用**no recovery-time**命令恢复默认值。



注意：若服务池中的真实服务成员自身配置了恢复时间，则生效的优先级为：真实服务的恢复时间 > 服务池的恢复时间。

指定真实服务预热时间

指定真实服务的预热时间。在指定的预热时间内，真实服务对客户端进行部分响应；到预热阶段结束后，真实服务对客户端请求全响应，直至达到最大连接数或连接速率限制。

在服务池配置模式下，使用以下命令配置预热时间：

warmup-time *value*

- *value* - 指定真实服务的预热时间。预热时间可根据服务器的性能进行设置，取值范围为0至3600秒，默认为0秒。如取值为0，表示系统不需要预热时间，在恢复时间后立即响应客户端的请求，直至达到最大连接数或连接速率限制。

在服务池配置模式下，使用**no warmup-time**命令恢复默认值。



注意：若服务池中的真实服务成员自身配置了预热时间，则生效的优先级为：真实服务的预热时间 > 服务池的预热时间。

配置真实服务优先级调度功能

启用优先级调度策略，并指定真实服务的最小活跃数。最小活跃数，即当前系统中参与服务池均衡调度的真实服务的最少数。

在服务池配置模式下，使用以下命令配置真实服务的最小活跃数：

- **min-active-real-server** *value* - 开启真实服务的优先级调度功能，并指定真实服务的最小活跃数目。

在服务池配置模式下，使用**no min-active-real-server**命令关闭真实服务的优先级调度功能。

如系统中有100个真实服务，最小活跃数为20，那么根据真实服务优先级排序，最高优先级的可用真实服务优先加入调度；如果参与调度的真实服务数小于20，次优先级的可用真实服务加入调度。以此类推，直到参与调度的真实服务数大于等于20或者所有的可用真实服务都参与调度为止。若有参与调度的真实服务不可用，导致实际参与调度的真实服务数小于20，会继续从未参与调度的真实服务中选择优先级最高的真实服务加入调度，直到满足条件。当高优先级的真实服务由不可用恢复为可用时，已经加入调度的低优先级的真实服务也有可能重新变为不可调度。

举例说明，服务池中配置了不同优先级的真实服务：真实服务RS1、RS2、RS3、RS4、RS5的优先级依次为10、10、30、50、50；

- 若最小活跃数指定为2，只有2个真实服务参与调度，即RS1、RS2。若RS1或RS2中有一个不可用，RS3将参与调度；若RS1和RS2均不可用，因为RS4和RS5优先级相同，所以RS3、RS4和RS5将参与调度。
- 若最小活跃数指定为4，5个真实服务参与调度，即RS1、RS2、RS3、RS4和RS5。
- 若最小活跃数指定为8，则全部真实服务参与调度，即RS1、RS2、RS3、RS4、RS5。

配置会话保持算法

为保持会话的连续性和一致性，设备支持会话保持功能。通过配置会话保持算法，设备将携带此会话保持算法特征的客户端请求，都保持到一台服务器上进行处理，不分发至多个服务器，始终分发至第一次访问的服务器上，实现会话保持。基于不同的应用，配置不同的会话保持算法。

用户可以根据需要，同时配置会话保持的默认算法和备份保持算法。配置后，当客户端请求进入到服务池时，匹配会话保持的流程如下：

1. 如客户端请求匹配到了由默认保持算法产生的会话保持条目，系统将直接根据该会话保持为客户端请求分配真实服务；如不匹配，继续匹配备份保持算法产生的会话保持条目。
2. 如匹配到了备份保持算法产生的会话保持条目，系统也将直接为客户端请求分配真实服务。
3. 如对所有的会话保持条目均不匹配，则根据该服务池配置的均衡算法为客户端请求选择真实服务。同时，由默认保持算法和备份保持算法产生的相应会话保持条目，将被记录在会话保持表。



注意：

- 当服务池类型为快速HTTP时，或者，当RADIUS类型的服务池配置的默认保持算法为“RADIUS”、RDP类型的服务池配置的默认保持算法为“RDP”时，不支持配置备份保持算法。
- 配置备份会话保持算法之前，需先为服务池配置默认会话保持算法。

基于Cookie的会话保持算法

配置基于Cookie的会话保持算法，在服务池配置模式下，使用以下命令：

```
[persistence | fallback-persistence] cookie cookie-name
```

- **persistence** - 指定默认保持算法为基于Cookie的会话保持算法。
- **fallback-persistence** - 指定备份保持算法为基于Cookie的会话保持算法。
- **cookie-name** - 指定HTTP Cookie的名称。配置后，系统将从客户端请求中获取指定的HTTP Cookie数值。携带此Cookie数值的请求，将被分配至与第一次访问相同的服务器上。执行该命令后，系统进入基于Cookie的会话保持算法配置模式。

在基于Cookie的会话保持算法配置模式下，使用以下命令配置相关参数：

- **encryption password *password*** - 开启Cookie加密并配置AES加密密码。开启后，系统针对服务器响应中Set-Cookie中指定的Cookie数值进行加密，当客户端再次发起请求携带指定的Cookie时，系统对该指定的Cookie值解密，若解密成功，则继续将请求分配至与第一次访问相同的服务器上；若解密失败，则不会进行会话保持。使用**no encryption**关闭Cookie加密功能。
- **accept-plaintext** - 开启明文兼顾模式。开启后，系统将对解密失败的Cookie数值，将当作明文形式继续进行会话保持。使用**no accept-plaintext**关闭明文兼顾模式。
- **match-across virtual-server** - 开启跨虚拟服务器共享功能。开启后，基于该Cookie的会话保持表将共享给其他虚拟服务器。使用 **no match-across** 命令关闭跨虚拟服务器共享功能。
- **override-limit enable** - 开启忽略连接限制功能，即忽略真实服务“最大连接数”和“连接速率限制”的功能。系统默认关闭该功能。开启后，当系统基于Cookie的会话保持算法将客户端请求分配至某真实服务时，即使该真实服务当前的连接数或连接速率已达到其指定的最大值，系统仍将此次客户端请求分配给它。使用**no override-limit**命令关闭忽略连接限制的功能。
- **timeout *time*** - 指定会话的超时时间。超过指定的时间值，设备将清除该客户端的会话信息。使用**no timeout**命令恢复会话超时时间的默认值300秒。

在服务池配置模式下，使用**no {persistence | fallback-persistence}**命令删除会话保持算法。

基于Cookie哈希的会话保持算法

配置基于Cookie哈希的会话保持算法，在服务池配置模式下，使用以下命令：

```
[persistence | fallback-persistence] hash-cookie cookie-name
```

- **persistence** - 指定默认保持算法为基于Cookie哈希的会话保持算法。
- **fallback-persistence** - 指定备份保持算法为基于Cookie哈希的会话保持算法。
- **cookie-name** - 指定HTTP Cookie的名称。配置后，系统将从客户端请求中获取指定的HTTP Cookie数值。携带此Cookie数值的请求，将被分配至与第一次访问相同的服务器上。执行该命令后，系统进入基于Cookie哈希的会话保持算法配置模式。

在基于Cookie哈希的会话保持算法配置模式下，使用以下命令配置相关参数：

- **encryption password *password*** - 开启Cookie加密并配置AES加密密码。开启后，系统针对服务器响应中Set-Cookie中指定的Cookie数值进行加密，当客户端再次发起请求携带指定的Cookie时，系统对该指定的Cookie值解密，若解密成功，则继续将请求分配至与第一次访问相同的服务器上；若解密失败，则不会进行会话保持。使用**no encryption**关闭Cookie加密功能。
- **accept-plaintext** - 开启明文兼顾模式。开启后，系统将对解密失败的Cookie数值，将当作明文形式继续进行会话保持。使用**no accept-plaintext**关闭明文兼顾模式。
- **match-across virtual-server** - 开启跨虚拟服务器共享功能。开启后，基于该Cookie哈希的会话保持表将共享给其他虚拟服务器。使用 **no match-across** 命令关闭跨虚拟服务器共享功能。
- **override-limit enable** - 开启忽略连接限制功能，即忽略真实服务“最大连接数”和“连接速率限制”的功能。系统默认关闭该功能。开启后，当系统基于Cookie哈希的会话保持算法将客户端请求分配至某真实服务时，即使该真实服务当前的连接数或连接速率已达到其指定的最大值，系统仍将此次客户端请求分配给它。使用**no override-limit**命令关闭忽略连接限制的功能。
- **timeout *time*** - 指定会话的超时时间。超过指定的时间值，设备将清除该客户端的会话信息。使用**no timeout**命令恢复会话超时时间的默认值300秒。

在服务池配置模式下，使用**no {persistence | fallback-persistence}**命令删除会话保持算法。

基于URL哈希的会话保持算法

配置基于URL哈希的会话保持算法，在服务池配置模式下，使用以下命令：

```
[persistence | fallback-persistence] hash-url
```

- **persistence** - 指定默认保持算法为基于URL哈希的会话保持算法。
- **fallback-persistence** - 指定备份保持算法为基于URL哈希的会话保持算法。
- **hash-url** - 指定基于URL哈希的会话保持算法。配置后，系统将从客户端请求中的HTTP URL路径中获取字符串进行哈希。携带同一字符串的请求，将被分配至与第一次访问相同的服务器上。执行该命令后，系统进入基于URL哈希的会话保持算法配置模式。

在基于URL哈希的会话保持算法配置模式下，使用以下命令配置相关参数：

- **param param-name** - 指定URL参数值。配置后，系统将从客户端请求中的该URL参数值中获取字符串。携带同一字符串的请求，将被分配至与第一次访问相同的服务器上。使用**no param**命令删除该配置。
- **subrange value1 value2** - 指定URL路径或URL参数值字符串的起始位置和结束位置。使用 **no subrange**命令删除该配置。
- **match-across virtual-server** - 开启跨虚拟服务器共享功能。开启后，基于该URL的会话保持表将共享给其他虚拟服务器。使用 **no match-across**命令关闭跨虚拟服务器共享功能。
- **override-limit enable**- 开启忽略连接限制功能，即忽略真实服务“最大连接数”和“连接速率限制”的功能。系统默认关闭该功能。开启后，当系统基于URL哈希的会话保持算法将客户端请求分配至某真实服务时，即使该真实服务当前的连接数或连接速率已达到其指定的最大值，系统仍将此次客户端请求分配给它。使用**no override-limit**命令关闭忽略连接限制的功能。
- **timeout time**- - 指定会话的超时时间。超过指定的时间值，设备将清除该客户端的会话信息。使用**no timeout**命令恢复会话超时时间的默认值300秒。

在服务池配置模式下，使用**no {persistence | fallback-persistence}**命令删除会话保持算法。

基于首部的会话保持算法

配置基于首部的会话保持算法，在服务池配置模式下，使用以下命令：

[persistence | fallback-persistence] header header-name

- **persistence** - 指定默认保持算法为基于首部的会话保持算法。
- **fallback-persistence** - 指定备份保持算法为基于首部的会话保持算法。

- **header-name** - 指定头部名称。配置后，系统将从客户端请求中的HTTP header获取字符串。携带此字符串的请求，将被分配至与第一次访问相同的服务器上。执行该命令后，系统进入基于首部的会话保持算法配置模式。

在基于首部的会话保持算法配置模式下，使用以下命令配置相关参数：

- **subrange value1 value2** - 指定header字符串的起始位置和结束位置。使用 **no subrange**命令删除该配置。
- **match-across virtual-server** - 开启跨虚拟服务器共享功能。开启后，基于该首部的会话保持表将共享给其他虚拟服务器。使用 **no match-across**命令关闭跨虚拟服务器共享功能。
- **override-limit enable** - 开启忽略连接限制功能，即忽略真实服务“最大连接数”和“连接速率限制”的功能。系统默认关闭该功能。开启后，当系统基于首部的会话保持算法将客户端请求分配至某真实服务时，即使该真实服务当前的连接数或连接速率已达到其指定的最大值，系统仍将此次客户端请求分配给它。使用**no override-limit**命令关闭忽略连接限制的功能。
- **timeout time** - 指定会话的超时时间。超过指定的时间值，设备将清除该客户端的会话信息。使用**no timeout**命令恢复会话超时时间的默认值300秒。

在服务池配置模式下，使用**no {persistence | fallback-persistence}**命令删除会话保持算法。

基于插入Cookie的会话保持算法

配置基于插入Cookie的会话保持算法，在服务池配置模式下，使用以下命令：

[persistence | fallback-persistence] insert-cookie cookie-name

- **persistence** - 指定默认保持算法为基于插入Cookie的会话保持算法。
- **fallback-persistence** - 指定备份保持算法为基于插入Cookie的会话保持算法。
- **cookie-name** - 指定HTTP Cookie的名称。配置后，经过设备的HTTP请求，设备主动在响应报文中插入一条该Cookie。若不指定Cookie名称，系统将使用当前地址池的ID（例如“SLBServerPool3”）作为默认的Cookie插入到请求中。携带此Cookie值的请求，将被分配至与第一次访问相同的服务器上。执行该命令后，系统进入基于插入Cookie的会话保持算法配置模式。

在基于插入Cookie的会话保持算法配置模式下，使用以下命令配置相关参数：

- **domain** *domain-name* - 指定需匹配的域名称，匹配成功的客户端请求将被插入Cookie并进行会话保持。使用 **no domain** 命令删除域名的配置。
- **path** *path-name* - 指定需匹配的URL路径，匹配成功的客户端请求将被插入Cookie并进行会话保持。使用 **no path** 命令删除域名的配置。
- **expire { session-Cookie | expire-time }**
 - **session-Cookie** - 开启会话Cookie。开启后，插入的Cookie将不会存放在客户端磁盘上，当浏览器关闭时，Cookie 将从此永久丢失。只要不关闭浏览器，会话可一直保持，不受Cookie超时时间限制。若不开启，插入的 Cookie 会存放在客户端磁盘中。浏览器关闭时，会话信息不会清除，只有当Cookie超时后，才会从客户端磁盘中删除。
 - **expire-time** - 关闭会话Cookie并指定Cookie的超时时间。取值范围为1 - 31536000秒，默认为300秒。超过指定的时间后，Cookie信息将被从客户端磁盘中清除，客户端发送报文也将不再携带该Cookie值，设备也将不再按照插入的Cookie进行会话保持。使用 **no expire** 命令恢复Cookie超时时间的默认值300秒。
- **http-only** - 开启Cookie的HTTP Only属性。开启后，插入的Cookie只对浏览器可见，JS脚本无法获取。使用 **no http-only** 命令关闭Cookie的HTTP Only属性。
- **secure** - 开启Cookie的Secure属性。开启后，客户端浏览器只能通过HTTPS连接发送插入的Cookie。使用 **no secure** 命令关闭Cookie的Secure属性
- **nopass-to-server** - 开启不传递到真实服务功能。开启后，插入的Cookie将不会被透传到真实服务上。使用 **no nopass-to-server** 关闭该功能。
- **encryption password** *password* - 开启Cookie加密并配置AES加密密码。开启后，系统会将插入的Cookie进行加密，当客户端再次发起访问请求时，系统会重新对Cookie数值进行解密，若解密成功，则继续将请求分配至与第一次访问相同的服务器上；若解密失败，则不会进行会话保持。使用 **no encryption** 关闭Cookie加密功能。
- **accept-plaintext** - 开启明文兼顾模式。开启后，系统将对解密失败的Cookie数值，将当作明文形式继续进行会话保持。使用 **no accept-plaintext** 命令关闭明文兼顾模式。
- **override-limit enable** - 开启忽略连接限制功能，即忽略真实服务“最大连接数”和“连接速率限制”的功能。系统默认关闭该功能。开启后，当系统基于插入Cookie的会话保持算法将客户端请求分配至某真实服

务时，即使该真实服务当前的连接数或连接速率已达到其指定的最大值，系统仍将此次客户端请求分配给它。使用**no override-limit**命令关闭忽略连接限制的功能。

在服务池配置模式下，使用**no {persistence | fallback-persistence}**命令删除会话保持算法。

基于改写Cookie的会话保持算法

配置基于改写Cookie的会话保持算法，在服务池配置模式下，使用以下命令：

```
[persistence | fallback-persistence] rewrite-cookie cookie-name
```

- **persistence** - 指定默认保持算法为基于改写Cookie的会话保持算法。
- **fallback-persistence** - 指定备份保持算法为基于改写Cookie的会话保持算法。
- **cookie-name** - 指定需匹配的 Cookie 名称。配置后，经过设备的HTTP请求，设备将主动对响应报文中指定 Cookie 名称对应的Value值进行改写。携带此Cookie值的请求，将被分配至与第一次访问相同的服务器上。响应报文中指定Cookie名称对应的Value值将被设备改写为如下格式：“0000.虚拟服务器的ID.服务池的ID.真实服务的ID.时间戳.原Value值”。并且，客户端请求携带改写后的Cookie值到达设备时，设备将对Cookie值进行还原，然后转发客户端请求至分配到的服务器上。

在基于改写Cookie的会话保持算法配置模式下，使用以下命令配置相关参数：

- **http-only** - 开启Cookie的HTTP Only属性。开启后，改写后的Cookie只对浏览器可见，JS脚本无法获取。使用**no http-only**命令关闭Cookie的HTTP Only属性。
- **secure** - 开启Cookie的Secure属性。开启后，客户端浏览器只能通过HTTPS连接发送改写后的Cookie。使用**no secure**命令关闭Cookie的Secure属性。
- **encryption password password** - 开启Cookie加密并配置AES加密密码。开启后，系统会将插入的Cookie进行加密，当客户端再次发起访问请求时，系统会重新对Cookie数值进行解密，若解密成功，则继续将请求分配至与第一次访问相同的服务器上；若解密失败，则不会进行会话保持。使用**no encryption**关闭Cookie加密功能。
- **accept-plaintext** - 开启明文兼顾模式。开启后，系统将对解密失败的Cookie数值，将当作明文形式继续进行会话保持。使用**no accept-plaintext**命令关闭明文兼顾模式。

- **override-limit enable**- 开启忽略连接限制功能，即忽略真实服务“最大连接数”和“连接速率限制”的功能。系统默认关闭该功能。开启后，当系统改写Cookie的会话保持算法将客户端请求分配至某真实服务时，即使该真实服务当前的连接数或连接速率已达到其指定的最大值，系统仍将此次客户端请求分配给它。使用**no override-limit**命令关闭忽略连接限制的功能。

在服务池配置模式下，使用**no {persistence | fallback-persistence}**命令删除会话保持算法。

基于HTTP版本的会话保持算法

配置基于HTTP版本的会话保持算法，在服务池配置模式下，使用以下命令：

[persistence | fallback-persistence | http-version

- **persistence** - 指定默认保持算法为基于HTTP版本的会话保持算法。
- **fallback-persistence** - 指定备份保持算法为基于HTTP版本的会话保持算法。
- **http-version** - 指定基于HTTP版本的会话保持算法。配置后，系统将从客户端请求中获取HTTP版本信息，携带此信息的请求，将被分配至与第一次访问相同的服务器上。执行该命令后，系统进入基于HTTP版本的会话保持算法配置模式。

在基于HTTP版本的会话保持算法配置模式下，使用以下命令配置相关参数：

- **match-across virtual-server** - 开启跨虚拟服务器共享功能。开启后，基于该HTTP版本的会话保持表将共享给其他虚拟服务器。使用 **no match-across** 命令关闭跨虚拟服务器共享功能。
- **override-limit enable**- 开启忽略连接限制功能，即忽略真实服务“最大连接数”和“连接速率限制”的功能。系统默认关闭该功能。开启后，当系统基于HTTP版本的会话保持算法将客户端请求分配至某真实服务时，即使该真实服务当前的连接数或连接速率已达到其指定的最大值，系统仍将此次客户端请求分配给它。使用**no override-limit**命令关闭忽略连接限制的功能。
- **timeout time** - 指定会话的超时时间。超过指定的时间值，设备将清除该客户端的会话信息。使用**no timeout**命令恢复会话超时时间的默认值300秒。

在服务池配置模式下，使用**no {persistence | fallback-persistence}**命令删除会话保持算法。

基于请求方法的会话保持算法

配置基于请求方法的会话保持算法，在服务池配置模式下，使用以下命令：

[**persistence** | **fallback-persistence** | **request-method**

- **persistence** - 指定默认保持算法为基于请求方法的会话保持算法。
- **fallback-persistence** - 指定备份保持算法为基于请求方法的会话保持算法。
- **request-method** - 指定基于请求方法的会话保持算法。配置后，系统将从客户端请求中获取HTTP请求方法，携带此信息的请求，将被分配至与第一次访问相同的服务器上。执行该命令后，系统进入基于请求方法的会话保持算法配置模式。

在基于请求方法的会话保持算法配置模式下，使用以下命令配置相关参数：

- **match-across virtual-server** - 开启跨虚拟服务器共享功能。开启后，基于该HTTP请求方法的会话保持表将共享给其他虚拟服务器。使用 **no match-across** 命令关闭跨虚拟服务器共享功能。
- **override-limit enable** - 开启忽略连接限制功能，即忽略真实服务“最大连接数”和“连接速率限制”的功能。系统默认关闭该功能。开启后，当系统基于请求方法的会话保持算法将客户端请求分配至某真实服务时，即使该真实服务当前的连接数或连接速率已达到其指定的最大值，系统仍将此次客户端请求分配给它。使用 **no override-limit** 命令关闭忽略连接限制的功能。
- **timeout time** - 指定会话的超时时间。超过指定的时间值，设备将清除该客户端的会话信息。使用 **no timeout** 命令恢复会话超时时间的默认值300秒。

在服务池配置模式下，使用 **no {persistence | fallback-persistence}** 命令删除会话保持算法。

基于目的IP的会话保持算法

配置基于目的IP的会话保持算法，在服务池配置模式下，使用以下命令：

[**persistence** | **fallback-persistence** | **dst-ip**

- **persistence** - 指定默认保持算法为基于目的IP的会话保持算法。
- **fallback-persistence** - 指定备份保持算法为基于目的IP的会话保持算法。
- **dst-ip** - 指定基于目的IP的会话保持算法。配置后，系统会将访问同一个目的 IP 地址的客户端请求（包含后续的所有连接请求）都发送至同一个真实服务上。支持IPv4和IPv6地址。执行该命令后，系统进入基于目的IP的会话保持算法配置模式。

在基于目的IP的会话保持算法配置模式下，使用以下命令配置相关参数：

- **granularity-ipv4 value** - 指定IPv4地址的粒度，即该IPv4地址的子网掩码，取值范围为1至32，默认值为32。使用 **no granularity-ipv4**命令恢复IPv4地址子网掩码的默认值。
- **granularity-ipv6 value** - 指定IPv6地址的粒度，即该IPv6地址的前缀长度，取值范围为1至128，默认值为128。使用 **no granularity-ipv6**命令恢复IPv6地址前缀长度的默认值。
- **match-across virtual-server** - 开启跨虚拟服务器共享功能。开启后，基于该目的IP的会话保持表将共享给其他虚拟服务器。使用 **no match-across**命令关闭跨虚拟服务器共享功能。
- **override-limit enable**- 开启忽略连接限制功能，即忽略真实服务“最大连接数”和“连接速率限制”的功能。系统默认关闭该功能。开启后，当系统基于目的IP的会话保持算法将客户端请求分配至某真实服务时，即使该真实服务当前的连接数或连接速率已达到其指定的最大值，系统仍将此次客户端请求分配给它。使用**no override-limit**命令关闭忽略连接限制的功能。
- **timeout time** - 指定会话的超时时间。超过指定的时间值，设备将清除该目的IP的会话信息。使用**no timeout**命令恢复会话超时时间的默认值300秒。

在服务池配置模式下，使用**no {persistence | fallback-persistence}**命令删除会话保持算法。

基于源IP的会话保持算法

配置基于源IP的会话保持算法，在服务池配置模式下，使用以下命令：

[persistence | fallback-persistence | src-ip

- **persistence** - 指定默认保持算法为基于源IP的会话保持算法。
- **fallback-persistence** - 指定备份保持算法为基于源IP的会话保持算法。
- **src-ip** - 指定基于源IP的会话保持算法。配置后，系统会将来自同一个源 IP 地址的客户端请求（包含后续的所有连接请求）都发送至同一个真实服务上。支持IPv4和IPv6地址。执行该命令后，系统进入基于源IP的会话保持算法配置模式。

在基于源IP的会话保持算法配置模式下，使用以下命令配置相关参数：

- **granularity-ipv4 value** - 指定IPv4地址的粒度，即该IPv4地址的子网掩码，取值范围为1至32，默认值为32。使用 **no granularity-ipv4**命令恢复IPv4地址子网掩码的默认值。

- **granularity-ipv6 value** - 指定IPv6地址的粒度，即该IPv6地址的前缀长度，取值范围为1至128，默认值为128。使用 **no granularity-ipv6** 命令恢复IPv6地址前缀长度的默认值。
- **match-across virtual-server** - 开启跨虚拟服务器共享功能。开启后，基于该源IP的会话保持表将共享给其他虚拟服务器。使用 **no match-across** 命令关闭跨虚拟服务器共享功能。
- **override-limit enable** - 开启忽略连接限制功能，即忽略真实服务“最大连接数”和“连接速率限制”的功能。系统默认关闭该功能。开启后，当系统基于源IP的会话保持算法将客户端请求分配至某真实服务时，即使该真实服务当前的连接数或连接速率已达到其指定的最大值，系统仍将此次客户端请求分配给它。使用 **no override-limit** 命令关闭忽略连接限制的功能。
- **timeout time** - 指定会话的超时时间。超过指定的时间值，设备将清除该客户端的会话信息。使用 **no timeout** 命令恢复会话超时时间的默认值300秒。

在服务池配置模式下，使用 **no {persistence | fallback-persistence}** 命令删除会话保持算法。

基于源IP与目的IP的会话保持算法

配置基于源IP与目的IP的会话保持算法，在服务池配置模式下，使用以下命令：

[persistence | fallback-persistence] src-dst-ip

- **persistence** - 指定默认保持算法为基于源IP与目的IP的会话保持算法。
- **fallback-persistence** - 指定备份保持算法为基于源IP与目的IP的会话保持算法。
- **src-dst-ip** - 指定基于源IP与目的IP的会话保持算法。配置后，系统会将来自同一个客户端且目的地址相同的客户端请求（包含后续的所有连接请求）都发送至同一个真实服务上。执行该命令后，系统进入基于源IP与目的IP的会话保持算法配置模式。

在基于源IP与目的IP的会话保持算法配置模式下，使用以下命令配置相关参数：

- **match-across virtual-server** - 开启跨虚拟服务器共享功能。开启后，基于该源IP与目的IP的会话保持表将共享给其他虚拟服务器。使用 **no match-across** 命令关闭跨虚拟服务器共享功能。
- **override-limit enable** - 开启忽略连接限制功能，即忽略真实服务“最大连接数”和“连接速率限制”的功能。系统默认关闭该功能。开启后，当系统基于源IP与目的IP的会话保持算法将客户端请求分配至某真实

服务时，即使该真实服务当前的连接数或连接速率已达到其指定的最大值，系统仍将此次客户端请求分配给它。使用**no override-limit**命令关闭忽略连接限制的功能。

- **timeout time** - 指定会话的超时时间。超过指定的时间值，设备将清除该客户端的会话信息。使用**no timeout**命令恢复会话超时时间的默认值300秒。

在服务池配置模式下，使用**no {persistence | fallback-persistence}**命令删除会话保持算法。

基于TOA的会话保持算法

配置基于TOA的会话保持算法，在服务池配置模式下，使用以下命令：

[persistence | fallback-persistence] toa

- **persistence** - 指定默认保持算法为基于TOA的会话保持算法。
- **fallback-persistence** - 指定备份保持算法为基于TOA的会话保持算法。
- **toa** - 指定基于TOA的会话保持算法。配置后，系统会将从客户端TCP请求中获取TOA信息，携带此TOA值的请求，将被分配至与第一次访问相同的服务器上。执行该命令后，系统进入基于TOA的会话保持算法配置模式。

在基于TOA的会话保持算法配置模式下，使用以下命令配置相关参数：

- **granularity-ipv4 value** - 指定IPv4地址的粒度，即该IPv4地址的子网掩码，取值范围为1至32，默认值为32。使用 **no granularity-ipv4**命令恢复IPv4地址子网掩码的默认值。
- **granularity-ipv6 value** - 指定IPv6地址的粒度，即该IPv6地址的前缀长度，取值范围为1至128，默认值为128。使用 **no granularity-ipv6**命令恢复IPv6地址前缀长度的默认值。
- **override-limit enable** - 开启忽略连接限制功能，即忽略真实服务“最大连接数”和“连接速率限制”的功能。系统默认关闭该功能。开启后，当系统基于TOA的会话保持算法将客户端请求分配至某真实服务时，即使该真实服务当前的连接数或连接速率已达到其指定的最大值，系统仍将此次客户端请求分配给它。使用**no override-limit**命令关闭忽略连接限制的功能。
- **timeout time** - 指定会话的超时时间。超过指定的时间值，设备将清除该客户端的会话信息。使用**no timeout**命令恢复会话超时时间的默认值300秒。

在服务池配置模式下，使用**no {persistence | fallback-persistence}**命令删除会话保持算法。

基于TOA或源IP（TOA优先）的会话保持算法

配置基于TOA或源IP（TOA优先）的会话保持算法，在服务池配置模式下，使用以下命令：

```
[persistence | fallback-persistence] toa-or-src-ip
```

- **persistence** - 指定默认保持算法为基于TOA或源IP（TOA优先）的会话保持算法。
- **fallback-persistence** - 指定备份保持算法为基于TOA或源IP（TOA优先）的会话保持算法。
- **toa-or-src-ip** - 指定基于TOA或源IP（TOA优先）的会话保持算法。配置后，系统会从客户端TCP请求中获取TOA或源IP，优先级为TOA优先。携带此值的请求，将被分配至与第一次访问相同的服务器上。执行该命令后，系统进入基于TOA或源IP（TOA优先）的会话保持算法配置模式。

在基于TOA或源IP（TOA优先）的会话保持算法配置模式下，使用以下命令配置相关参数：

- **granularity-ipv4 value** - 指定IPv4地址的粒度，即该IPv4地址的子网掩码，取值范围为1至32，默认值为32。使用 **no granularity-ipv4** 命令恢复IPv4地址子网掩码的默认值。
- **granularity-ipv6 value** - 指定IPv6地址的粒度，即该IPv6地址的前缀长度，取值范围为1至128，默认值为128。使用 **no granularity-ipv6** 命令恢复IPv6地址前缀长度的默认值。
- **override-limit enable** - 开启忽略连接限制功能，即忽略真实服务“最大连接数”和“连接速率限制”的功能。系统默认关闭该功能。开启后，当系统基于TOA或源IP（TOA优先）的会话保持算法将客户端请求分配至某真实服务时，即使该真实服务当前的连接数或连接速率已达到其指定的最大值，系统仍将此次客户端请求分配给它。使用 **no override-limit** 命令关闭忽略连接限制的功能。
- **timeout time** - 指定会话的超时时间。超过指定的时间值，设备将清除该客户端的会话信息。使用 **no timeout** 命令恢复会话超时时间的默认值300秒。

在服务池配置模式下，使用 **no {persistence | fallback-persistence}** 命令删除会话保持算法。

基于真实源IP的会话保持算法

配置基于真实源IP的会话保持算法，在服务池配置模式下，使用以下命令：

```
[persistence | fallback-persistence] real-src-ip
```


- **persistence** - 指定默认保持算法为基于真实源IP的会话保持算法。
- **fallback-persistence** - 指定备份保持算法为基于真实源IP的会话保持算法。
- **real-src-ip** - 指定基于真实源IP的会话保持算法。配置后，系统会将从客户端请求中获取真实源IP值，携带此源IP值的请求，将被分配至与第一次访问相同的服务器上。真实源IP获取方式的优先级依次为X-Forwarded-For > X-Real-IP > 报文携带的源IP。当配置该选项时，系统优先在报文的X-Forwarded-For查找源IP，当找到时使用该源IP作为真正发起请求的源IP。当X-Forwarded-For找不到时其次再查找X-Real-IP，找到源IP即使用该源IP作为真正发起请求的源IP。当都查找不到时就使用报文自带的源IP作为真正发起请求的源IP。执行该命令后，系统进入基于真实源IP的会话保持算法配置模式。

在基于真实源IP的会话保持算法配置模式下，使用以下命令配置相关参数：

- **granularity-ipv4 value** - 指定IPv4地址的粒度，即该IPv4地址的子网掩码，取值范围为1至32，默认值为32。使用 **no granularity-ipv4**命令恢复IPv4地址子网掩码的默认值。
- **granularity-ipv6 value** - 指定IPv6地址的粒度，即该IPv6地址的前缀长度，取值范围为1至128，默认值为128。使用 **no granularity-ipv6**命令恢复IPv6地址前缀长度的默认值。
- **match-across virtual-server** - 开启跨虚拟服务器共享功能。开启后，基于该源IP的会话保持表将共享给其他虚拟服务器。使用 **no match-across**命令关闭跨虚拟服务器共享功能。
- **override-limit enable** - 开启忽略连接限制功能，即忽略真实服务“最大连接数”和“连接速率限制”的功能。系统默认关闭该功能。开启后，当系统基于真实源IP的会话保持算法将客户端请求分配至某真实服务时，即使该真实服务当前的连接数或连接速率已达到其指定的最大值，系统仍将此次客户端请求分配给它。使用**no override-limit**命令关闭忽略连接限制的功能。
- **timeout time** - 指定会话的超时时间。超过指定的时间值，设备将清除该客户端的会话信息。使用**no timeout**命令恢复会话超时时间的默认值300秒。

在服务池配置模式下，使用**no {persistence | fallback-persistence}**命令删除会话保持算法。

基于URL的会话保持算法

配置基于URL的会话保持算法，在服务池配置模式下，使用以下命令：

[persistence | fallback-persistence] url

- **persistence** - 指定默认保持算法为基于URL的会话保持算法。
- **fallback-persistence** - 指定备份保持算法为基于URL的会话保持算法。
- **url** - 指定基于URL的会话保持算法。配置后，系统将从客户端请求中的HTTP URL路径中获取字符串。携带同一字符串的请求，将被分配至与第一次访问相同的服务器上。执行该命令后，系统进入基于URL的会话保持算法配置模式。

在基于URL的会话保持算法配置模式下，使用以下命令配置相关参数：

- **param** *param-name* - 指定URL参数值。配置后，系统将从客户端请求中的该URL参数值中获取字符串。携带同一字符串的请求，将被分配至与第一次访问相同的服务器上。使用 **no param** 命令删除该配置。
- **subrange** *value1 value2* - 指定URL路径或URL参数值字符串的起始位置和结束位置。使用 **no subrange** 命令删除该配置。
- **match-across virtual-server** - 开启跨虚拟服务器共享功能。开启后，基于该URL的会话保持表将共享给其他虚拟服务器。使用 **no match-across** 命令关闭跨虚拟服务器共享功能。
- **override-limit enable** - 开启忽略连接限制功能，即忽略真实服务“最大连接数”和“连接速率限制”的功能。系统默认关闭该功能。开启后，当系统基于URL的会话保持算法将客户端请求分配至某真实服务时，即使该真实服务当前的连接数或连接速率已达到其指定的最大值，系统仍将此次客户端请求分配给它。使用 **no override-limit** 命令关闭忽略连接限制的功能。
- **timeout** *time* - 指定会话的超时时间。超过指定的时间值，设备将清除该客户端的会话信息。使用 **no timeout** 命令恢复会话超时时间的默认值300秒。

在服务池配置模式下，使用 **no {persistence | fallback-persistence}** 命令删除会话保持算法。

基于SSL ID的会话保持算法

配置基于SSL ID的会话保持算法，在服务池配置模式下，使用以下命令：

[persistence | fallback-persistence | ssl-id

- **persistence** - 指定默认保持算法为基于SSL ID的会话保持算法。
- **fallback-persistence** - 指定备份保持算法为基于SSL ID的会话保持算法。

- **ssl-id** - 指定基于SSL ID的会话保持算法。配置后，当客户端发起HTTPS请求时，设备将与客户端协商得到此次请求的SSL ID。携带此SSL ID的请求，将被分配至与第一次访问相同的服务器上。执行该命令后，系统进入基于SSL ID的会话保持算法配置模式。

在SSL ID的会话保持算法配置模式下，使用以下命令配置会话的超时时间：

- **override-limit enable** - 开启忽略连接限制功能，即忽略真实服务“最大连接数”和“连接速率限制”的功能。系统默认关闭该功能。开启后，当系统基于SSL ID的会话保持算法将客户端请求分配至某真实服务时，即使该真实服务当前的连接数或连接速率已达到其指定的最大值，系统仍将此次客户端请求分配给它。使用**no override-limit**命令关闭忽略连接限制的功能。
- **timeout time** - 指定会话的超时时间。超过指定的时间值，设备将清除该客户端的会话信息。使用**no timeout**命令恢复会话超时时间的默认值300秒。

在服务池配置模式下，使用**no {persistence | fallback-persistence}**命令删除会话保持算法。

说明：配置基于SSL ID的会话保持算法，需开启“客户端SSL模板”中“SSL连接复用”或“SSL无状态连接复用”功能，详细信息请参阅配置[客户端SSL模板](#)章节。

基于SNI的会话保持算法

配置基于SNI的会话保持算法，在服务池配置模式下，使用以下命令：

[persistence | fallback-persistence] sni

- **persistence** - 指定默认保持算法为基于SNI的会话保持算法。
- **fallback-persistence** - 指定备份保持算法为基于SNI的会话保持算法。
- **sni** - 指定基于SNI的会话保持算法。配置后，当客户端发起HTTPS请求时，设备将从客户端SSL握手请求中获取SNI信息。携带此SNI的请求，将被分配至与第一次访问相同的服务器上。执行该命令后，系统进入基于SNI的会话保持算法配置模式。

在SNI的会话保持算法配置模式下，使用以下命令配置会话的超时时间：

- **override-limit enable** - 开启忽略连接限制功能，即忽略真实服务“最大连接数”和“连接速率限制”的功能。系统默认关闭该功能。开启后，当系统基于SNI的会话保持算法将客户端请求分配至某真实服务时，即使该真实服务当前的连接数或连接速率已达到其指定的最大值，系统仍将此次客户端请求分配给它。使用**no override-limit**命令关闭忽略连接限制的功能。

- **timeout time** - 指定会话的超时时间。超过指定的时间值，设备将清除该客户端的会话信息。使用**no timeout**命令恢复会话超时时间的默认值300秒。

在服务池配置模式下，使用**no {persistence | fallback-persistence}**命令删除会话保持算法。

基于Call ID的会话保持算法

配置基于Call ID的会话保持算法，在服务池配置模式下，使用以下命令：

[persistence | fallback-persistence] call-id

- **persistence** - 指定默认保持算法为基于Call ID的会话保持算法。
- **fallback-persistence** - 指定备份保持算法为基于Call ID的会话保持算法。
- **call-id** - 指定基于Call ID的会话保持算法。配置后，系统将从客户端SIP请求中获取call-id，携带此call-id值的请求，将被分配至与第一次访问相同的服务器上。执行该命令后，系统进入基于Call ID的会话保持算法配置模式。

在基于Call ID的会话保持算法配置模式下，使用以下命令配置相关参数：

- **match-across virtual-server** - 开启跨虚拟服务器共享功能。开启后，基于该Call ID的会话保持表将共享给其他虚拟服务器。使用**no match-across**命令关闭跨虚拟服务器共享功能。
- **override-limit enable** - 开启忽略连接限制功能，即忽略真实服务“最大连接数”和“连接速率限制”的功能。系统默认关闭该功能。开启后，当系统基于Call ID的会话保持算法将客户端请求分配至某真实服务时，即使该真实服务当前的连接数或连接速率已达到其指定的最大值，系统仍将此次客户端请求分配给它。使用**no override-limit**命令关闭忽略连接限制的功能。
- **timeout time** - 指定会话的超时时间。超过指定的时间值，设备将清除该客户端的会话信息。使用**no timeout**命令恢复会话超时时间的默认值300秒。

在服务池配置模式下，使用**no {persistence | fallback-persistence}**命令删除会话保持算法。

基于RDP的会话保持算法

从客户端请求中的RDP Cookie获取远程连接的用户名信息或访问的真实服务器地址，携带相同用户名信息的请求，将被分配至与第一次访问相同的服务器上；携带真实服务器地址的请求，将被直接转发至该服务器上。配置基于RDP的会话保持算法，在服务池配置模式下，使用以下命令：

persistence rdp

- **persistence** - 指定默认保持算法为基于RDP的会话保持算法。
- **rdp** - 指定基于RDP的会话保持算法。配置后，当客户端发起远程连接请求时，系统从客户端请求中获取RDP Cookie。当Cookie字段为msthash时，使用Cookie中的用户名信息，携带此用户名信息的请求，将被分配至与第一次访问相同的服务器上；当Cookie字段为msts时，用户需开启Session Broker功能，系统才可以从Cookie中获取真实服务器的IP地址和端口号，然后将客户端请求转发至该服务器上。执行该命令后，系统进入基于RDP的会话保持算法配置模式。

在基于RDP的会话保持算法配置模式下，使用以下命令配置相关参数：

- **match-across virtual-server** - 开启跨虚拟服务器共享功能。开启后，基于该RDP的会话保持表将共享给其他虚拟服务器。使用 **no match-across** 命令关闭跨虚拟服务器共享功能。
- **secondary-match-content src-ip** - 指定客户端请求次匹配的会话保持算法为 **src-ip**，即基于源IP的会话保持算法。当系统根据 **rdp** 会话保持算法，没有为客户端请求分配真实服务器时，系统将按照 **src-ip** 会话保持算法，为客户端请求分配真实服务器。使用 **no secondary-match-content** 命令删除该配置。
- **session-broker enable** - 开启Session Broker功能。开启后，当客户端请求中的Cookie字段为msts时，系统可以从该Cookie中解析出真实服务器的地址和端口号，然后将客户端请求转发至该服务器。使用 **no session-broker** 命令关闭Session Broker功能。
- **override-limit enable** - 开启忽略连接限制功能，即忽略真实服务“最大连接数”和“连接速率限制”的功能。系统默认关闭该功能。开启后，当系统基于RDP的会话保持算法将客户端请求分配至某真实服务时，即使该真实服务当前的连接数或连接速率已达到其指定的最大值，系统仍将此次客户端请求分配给它。使用 **no override-limit** 命令关闭忽略连接限制的功能。
- **timeout time** - 指定会话的超时时间。超过指定的时间值，设备将清除该客户端的会话信息。使用 **no timeout** 命令恢复会话超时时间的默认值300秒。

在服务池配置模式下，使用 **no persistence** 命令删除会话保持算法。

基于RADIUS属性的会话保持算法

当客户端的RADIUS请求报文中携带了用户指定的任一RADIUS属性时，系统认为该RADIUS请求匹配上了基于RADIUS属性的会话保持；携带相同RADIUS属性的客户端请求，将被分配至与第一次访问相同的服务器。

上。系统最多支持同时配置4个RADIUS属性。

配置基于RADIUS属性的会话保持算法，在RADIUS类型的服务池配置模式下，使用以下命令：

persistence radius-avp

- **persistence** - 指定默认保持算法为基于RADIUS属性的会话保持算法。
- **radius-avp** - 指定基于RADIUS属性的会话保持算法。执行该命令后，系统进入基于RADIUS属性的会话保持算法配置模式。

在基于RADIUS属性的会话保持算法配置模式下，使用以下命令配置相关参数：

- **attribute [id id] {Vendor-Specific vendor-id vendor-id vendor-type vendor-type | User-Name | User-Password | CHAP-Password | NAS-IP-Address | NAS-Port | Service-Type | Framed-Protocol | Framed-IP-Address | Framed-IP-Netmask | Framed-Routing | Filter-Id | Framed-MTU | Framed-Compression | Login-IP-Host | Login-Service | Login-TCP-Port | Reply-Message | Callback-Number | Callback-Id | Framed-Route | Framed-IPX-Network | State | Class | Session-Timeout | Idle-Timeout | Termination-Action | Called-Station-Id | Calling-Station-Id | NAS-Identifier | Proxy-State | Login-LAT-Service | Login-LAT-Node | Login-LAT-Group | Framed-AppleTalk-Link | Framed-AppleTalk-Network | Framed-AppleTalk-Zone | Acct-Status-Type | Acct-Delay-Time | Acct-Input-Octets | Acct-Output-Octets | Acct-Session-Id | Acct-Authentic | Acct-Session-Time | Acct-Input-Packets | Acct-Output-Packets | Acct-Terminate-Cause | Acct-Multi-Session-Id | Acct-Link-Count | CHAP-Challenge | NAS-Port-Type | Port-Limit | Login-LAT-Port | NAS-IPv6-Address | Framed-Interface-Id | Framed-IPv6-Prefix | Login-IPv6-Host | Framed-IPv6-Route | Framed-IPv6-Pool | type-num}**
 - **id id** - 指定基于该RADIUS属性的会话保持算法的ID。若不配置，系统将自动为其分配ID。取值范围是1到4，即系统最多支持同时配置4个RADIUS属性。使用**no attribute id id**命令删除基于指定的RADIUS属性的会话保持算法。
 - **Vendor-Specific vendor-id vendor-id vendor-type vendor-type | User-Name | User-Password | CHAP-Password | NAS-IP-Address | NAS-Port | Service-Type | Framed-Protocol | Framed-IP-Address | Framed-IP-Netmask | Framed-Routing | Filter-Id | Framed-MTU | Framed-Compression | Login-IP-Host | Login-Service | Login-TCP-Port | Reply-Message | Callback-Number | Callback-Id | Framed-Route | Framed-IPX-Network | State | Class | Session-Timeout | Idle-Timeout | Termination-Action | Called-Station-Id | Calling-Station-Id | NAS-Identifier | Proxy-State | Login-LAT-Service | Login-LAT-Node | Login-LAT-**

Group | Framed-AppleTalk-Link | Framed-AppleTalk-Network | Framed-AppleTalk-Zone | Acct-Status-Type | Acct-Delay-Time | Acct-Input-Octets | Acct-Output-Octets | Acct-Session-Id | Acct-Authentic | Acct-Session-Time | Acct-Input-Packets | Acct-Output-Packets | Acct-Terminate-Cause | Acct-Multi-Session-Id | Acct-Link-Count | CHAP-Challenge | NAS-Port-Type | Port-Limit | Login-LAT-Port | NAS-IPv6-Address | Framed-Interface-Id | Framed-IPv6-Prefix | Login-IPv6-Host | Framed-IPv6-Route | Framed-IPv6-Pool | *type-num* - 指定RADIUS属性。对于需要匹配的RADIUS属性，用户可以直接输入上述属性名，也可以输入上述属性名对应的属性号 *type-num*。如需匹配的RADIUS属性为“User-Name”时，既可以输入属性名“User-Name”，也可以输入属性名User-Name对应的属性号“1”。

重复上述命令，指定多个RADIUS属性，客户端请求中携带任一指定的RADIUS属性，即符合会话保持条件。

- **move id *id1* {after *id2* | before *id2* | bottom | top}** - 指定ID为*id1*的基于RADIUS属性的会话保持算法的位置。客户端的RADIUS请求流量进入设备后，设备对基于RADIUS属性的会话保持算法进行顺序查找，然后按照查找到的相匹配的第一个RADIUS属性对客户端请求进行会话保持。设备不是将基于RADIUS属性的会话保持算法的ID作为匹配的顺序，而是按照该会话保持算法列表中的显示顺序进行匹配。
 - **after *id2*** - 指定基于某一RADIUS属性的会话保持算法*id1*位于基于另一RADIUS属性的会话保持算法*id2*之后。
 - **before *id2*** - 指定基于某一RADIUS属性的会话保持算法*id1*位于基于另一RADIUS属性的会话保持算法*id2*之前。
 - **bottom** - 指定基于某一RADIUS属性的会话保持算法*id1*位于所有会话保持算法之后。
 - **top** - 指定基于某一RADIUS属性的会话保持算法*id1*位于所有会话保持算法之前。
- **match-across virtual-server** - 开启跨虚拟服务器共享功能。开启后，基于该RADIUS属性的会话保持表将共享给其他虚拟服务器。使用 **no match-across** 命令关闭跨虚拟服务器共享功能。
- **override-limit enable** - 开启忽略连接限制功能，即忽略真实服务“最大连接数”和“连接速率限制”的功能。系统默认关闭该功能。开启后，当系统基于RADIUS属性的会话保持算法将客户端请求分配至某真实服务时，即使该真实服务当前的连接数或连接速率已达到其指定的最大值，系统仍将此次客户端请求分配给它。使用 **no override-limit enable** 命令关闭忽略连接限制的功能。

- **timeout** *time* - 指定会话的超时时间。超过指定的时间值，设备将清除该客户端的会话信息。使用**no timeout** 命令恢复会话超时时间的默认值300秒。



注意: 客户端请求进入服务池后，先匹配会话保持。如匹配到会话保持，设备直接分配一个真实服务器，否则根据服务池配置的均衡算法，选出一个真实服务器。

查看会话保持表

查看会话保持表,在任意模式下,使用以下命令:

```
show slb persistence [ virtual-server vs-name ] [ method method-name ] [ real-server rs-name ] [ server-pool pool-name ]
```

- *vs-name* - 指定虚拟服务器的名称。
- *method-name* - 指定会话保持算法的名称。
- *rs-name* - 指定真实服务名称。
- *pool-name* - 指定服务池的名称。

当查看基于RADIUS属性的会话保持算法的保持表时，需使用以下命令查看具体某一RADIUS属性的会话保持表：

```
show slb persistence method radius-avp attribute { Vendor-Specific [ vendor-id vendor-id ] [ vendor-type vendor-type ] |
User-Name | User-Password | CHAP-Password | NAS-IP-Address | NAS-Port | Service-Type | Framed-Protocol |
Framed-IP-Address | Framed-IP-Netmask | Framed-Routing | Filter-Id | Framed-MTU | Framed-Compression |
Login-IP-Host | Login-Service | Login-TCP-Port | Reply-Message | Callback-Number | Callback-Id | Framed-
Route | Framed-IPX-Network | State | Class | Session-Timeout | Idle-Timeout | Termination-Action | Called-Sta-
tion-Id | Calling-Station-Id | NAS-Identifier | Proxy-State | Login-LAT-Service | Login-LAT-Node | Login-LAT-
Group | Framed-AppleTalk-Link | Framed-AppleTalk-Network | Framed-AppleTalk-Zone | Acct-Status-Type |
Acct-Delay-Time | Acct-Input-Octets | Acct-Output-Octets | Acct-Session-Id | Acct-Authentic | Acct-Session-
Time | Acct-Input-Packets | Acct-Output-Packets | Acct-Terminate-Cause | Acct-Multi-Session-Id | Acct-Link-
Count | CHAP-Challenge | NAS-Port-Type | Port-Limit | Login-LAT-Port | NAS-IPv6-Address | Framed-Inter-
face-Id | Framed-IPv6-Prefix | Login-IPv6-Host | Framed-IPv6-Route | Framed-IPv6-Pool | type-num } [ avp-value ]
```

- **attribute** {*attribute*} - 指定RADIUS属性，查看该指定的RADIUS属性的会话保持表。对于需要查看会话保持表的RADIUS属性，用户可以直接输入上述属性名，也可以输入上述属性名对应的属性号 *type-num*。如需查看的RADIUS属性为“User-Name”时，既可以输入属性名“User-Name”，也可以输入属性名User-Name对应的属性号“1”。
- **avp-value** - 指定需查看的RADIUS属性后，用户可以根据需要，继续指定RADIUS属性的Value值需匹配的内容。指定后，系统将在相应RADIUS属性的所有会话保持表中，再按照指定的内容对此RADIUS属性的Value值进行模糊匹配，展现出满足条件的会话保持表。

清空会话保持表

清空会话保持表,在任意模式下,使用以下命令:

```
clear slb persistence [ virtual-server vs-name ] [ method method-name ] [ real-server rs-name ] [ server-pool pool-name ]
```

- *vs-name* - 指定虚拟服务器的名称。
- *method-name* - 指定会话保持算法的名称。
- *rs-name* - 指定真实服务名称。
- *pool-name* - 指定服务池的名称。

当清空基于RADIUS属性的会话保持算法的保持表时，需使用以下命令清空具体某一RADIUS属性的会话保持表：

```
clear slb persistence method radius-avp attribute { Vendor-Specific [vendor-id vendor-id] [ vendor-type vendor-type ] | User-Name | User-Password | CHAP-Password | NAS-IP-Address | NAS-Port | Service-Type | Framed-Protocol | Framed-IP-Address | Framed-IP-Netmask | Framed-Routing | Filter-Id | Framed-MTU | Framed-Compression | Login-IP-Host | Login-Service | Login-TCP-Port | Reply-Message | Callback-Number | Callback-Id | Framed-Route | Framed-IPX-Network | State | Class | Session-Timeout | Idle-Timeout | Termination-Action | Called-Station-Id | Calling-Station-Id | NAS-Identifier | Proxy-State | Login-LAT-Service | Login-LAT-Node | Login-LAT-Group | Framed-AppleTalk-Link | Framed-AppleTalk-Network | Framed-AppleTalk-Zone | Acct-Status-Type | Acct-Delay-Time | Acct-Input-Octets | Acct-Output-Octets | Acct-Session-Id | Acct-Authentic | Acct-Session-Time | Acct-Input-Packets | Acct-Output-Packets | Acct-Terminate-Cause | Acct-Multi-Session-Id | Acct-Link-Count | CHAP-Challenge | NAS-Port-Type | Port-Limit | Login-LAT-Port | NAS-IPv6-Address | Framed-Interface-Id | Framed-IPv6-Prefix | Login-IPv6-Host | Framed-IPv6-Route | Framed-IPv6-Pool | type-num } [ avp-value ]
```


- **attribute {attribute}** - 指定RADIUS属性，清空该指定的RADIUS属性的会话保持表。对于需要清空会话保持表的RADIUS属性，用户可以直接输入上述属性名，也可以输入上述属性名对应的属性号 *type-num*。如需清空的RADIUS属性为“User-Name”时，既可以输入属性名“User-Name”，也可以输入属性名User-Name对应的属性号“1”。
- **avp-value** - 指定需清空的RADIUS属性后，用户可以根据需要，继续指定RADIUS属性的Value值需匹配的内容。指定后，系统将在相应RADIUS属性的所有会话保持表中，再按照指定的内容对此RADIUS属性的Value值进行模糊匹配，清空满足条件的会话保持表。

配置负载均衡算法

指定负载均衡算法。配置该参数后，系统将对服务池内的请求，按照指定的算法进行分配。

系统支持多种负载均衡算法，包括：

算法	描述
轮询（Round Robin）	将客户端的请求轮流分配给每个真实服务。
加权轮询（Weighted Round Robin）	根据真实服务的不同处理能力，分配不同的权重。设备根据真实服务的权重，按比例分发请求。权重大的真实服务，接收的请求多。
IP哈希（Hash IP）	对客户端的源地址/目的地址/真实源IP地址进行哈希运算，根据运算的结果转发给一个真实服务进行处理。若服务列表不变，同一IP地址的客户端，每次都会分配到同一个真实服务。
加权IP哈希（Weighted Hash IP）	在IP哈希算法的基础上，设备根据真实服务的权重，按比例分发请求。权重大的真实服务，接收的请求多。
IP端口哈希（Hash IP Port）	对客户端的源地址/目的地址/真实源IP地址和端口进行哈希运算，根据运算的结果转发给一个真实服务进行处理。
加权IP端口哈希（Weighted Hash IP Port）	在IP端口哈希算法的基础上，设备根据真实服务的权重，按比例分发请求。权重大的真实服务，接收的请求多。
一致IP哈希（Consistence Hash IP）	对客户端的源地址/目的地址/真实源IP地址进行哈希运算，根据运算的结果转发给一个真实服务进行处理。若某个真实服务由于故障等原因无法提供服务，原来发送至该故障真实服务的请求，将被分配至其他可用的真实服务上；而原

	来发送至未故障的真实服务的请求（来自同一源IP或同一客户端），将继续被分配到原来的真实服务上。
最小连接（Least Connection）	设备会记录每个真实服务或端口上的连接数。当产生新的连接时，设备将分配给当前连接数最少的真实服务。
加权最小连接（Weighted Least Connection）	在最少连接数分发的基础上，根据真实服务的不同处理能力，为每个真实服务分配一个权重。各个真实服务用相应的权重表示其处理性能。当产生新的连接时，将最新的请求分配给当前连接数与权重的比值最小的真实服务上（计算方法：当前连接数除以权重）。
最快响应（Fast Response Time）	设备会记录每个真实服务或端口上的连接数。当产生新的连接时，设备将其分配至当前处理响应最快的真实服务上。
优先权算法	根据真实服务的优先级来分配请求，将请求分配给优先级最高的真实服务。真实服务所配的优先级数值越小，其优先级越高。当有多个真实服务的优先级相同且最高时，将采用在这些真实服务之间轮询的方式分配资源。
动态比率算法	根据真实服务的不同处理能力，设备计算不同的动态权重。设备根据真实服务的动态权重，按比例分发请求。动态权重大的真实服务，接收的请求多。动态权重为0时，真实服务不参与分发请求。一般情况下，动态权重值是由SNMP类型的健康检查计算得出的结果；对于其他情况，如果真实服务可以提供服务时，动态权重值为1，否则为0。
最小带宽	设备会记录每个真实服务或端口上的上行带宽、下行带宽或上行与下行带宽总和。当产生新的连接时，设备将分配给带宽或带宽总和最小的真实服务。
加权最小带宽	在上行与下行带宽总和分发的基础上，根据真实服务的不同处理能力，为每个真实服务分配一个权重。各个真实服务用相应的权重表示其处理性能。当产生新的连接时，将最新的请求分配给当前带宽（总和）与权重的比值最小的真实服务上（计算方法：上行带宽、下行带宽或上行与下行带宽总和除以权重）。
随机	设备将客户端请求随机分配给一个可用的真实服务。
URL哈希（Hash URL）	对客户端访问的URL地址进行哈希运算，根据运算的结果转发给一个真实服务进行处理。若服务列表不变，访问同一个URL地址的客户端，每次都会分配到同一个真实服务。

在服务池配置模式下，使用以下命令指定负载均衡算法：

```
balance method { {consistence-hash-ip | hash-ip | weighted-hash-ip | hash-ip-port | weighted-hash-ip-port } [dst-ip | real-src-ip | src-ip] [value] | {round-robin | weighted-round-robin } [comprehensive] | {least-bandwidth |
```

`weighted-least-bandwidth` } [`stream-direction` {`bidirection` | `downstream` | `upstream`}] [`bandwidth-statistics-period`*value*] | `dynamic-ratio` | `priority` [*value*] | `fastest-response` | `least-connection` | `weighted-least-connection` | `random` | `hash-url` | [`fail-action` {`drop` | `reselect` | `reselect-after-retry` *retry-time* | `retry` *retry-time*}]

- **consistence-hash-ip** - 指定负载均衡算法为一致IP哈希。
- **hash-ip** - 指定负载均衡算法为IP哈希。
- **weighted-hash-ip** - 指定负载均衡算法为加权IP哈希
- **hash-ip-port** - 指定负载均衡算法为IP端口哈希。
- **weighted-hash-ip-port** - 指定负载均衡算法为加权IP端口哈希。
- [**dst-ip** | **real-src-ip** | **src-ip**] [*value*] - 当算法为一致IP哈希、IP哈希、加权IP哈希、IP端口哈希、加权IP端口哈希时，系统支持指定从客户端请求中获取哪一种类型的IP地址以及相应IP地址值中的前多少位用于哈希计算。若不配置，系统默认从客户端请求的源IP地址值中前128位为用于哈希计算。仅当服务池类型为HTTP、HTTPS、快速HTTP时该配置生效。
 - **dst-ip** - 指定从客户端请求中获取目的IP地址值用于哈希计算。
 - **real-src-ip** - 指定从客户端请求中获取真实源IP地址值用于哈希计算。
 - **src-ip** - 指定从客户端请求中获取源IP地址值用于哈希计算。
 - *value* - 指定从客户端请求中获取目的IP地址/真实源IP地址/源IP地址值中的前多少位用于哈希计算。取值范围为0至128，默认值为128，如取值为0，表示不进行负载均衡。
- **round-robin** - 指定负载均衡算法为轮询。
- **weighted-round-robin** - 指定负载均衡算法为加权轮询。
- **comprehensive** - 当服务池的均衡算法指定为“轮询”、“加权轮询”时，开启“综合考虑其它调度结果”功能。开启该功能后，系统将综合考虑可编程脚本、七层内容交换规则、四层内容交换规则、会话保持和负载均衡算法对真实服务的调度结果，进行负载均衡。系统会根据各真实服务正在处理客户端请求的情况，判断其当前的处理能力，当设备接收新的客户端请求时，优先将请求轮流分配给当前处理能力较大的真实服务。

- `{least-bandwidth | weighted-least-bandwidth} [stream-direction {bidirection | downstream | upstream}] [bandwidth-statistics-period value]` - 当虚拟服务器类型为IP时，指定均衡算法为最小带宽或加权最小带宽算法。指定后，用户还可以配置用来计算带宽的流量方向以及计算带宽的统计周期。
 - `least-bandwidth` - 指定均衡算法为最小带宽。
 - `weighted-least-bandwidth` - 指定均衡算法为加权最小带宽。
 - `bidirection` - 指定系统计算数据流的入和出两个方向上带宽之和，进行负载均衡。该方向为默认方向。
 - `downstream` - 指定系统计算数据流的入方向上的带宽，进行负载均衡。
 - `upstream` - 指定系统计算数据流的出方向上的带宽，进行负载均衡。
 - `bandwidth-statistics-period value` - 指定带宽统计周期。取值范围为1到300秒，默认值为120秒。
- `dynamic-ratio` - 指定负载均衡算法为动态比率算法。
- `priority [value]` - 指定负载均衡算法为优先权算法。优先级数值越小，其优先级越高。
- `fastest-response` - 指定负载均衡算法为最快响应算法。
- `least-connection` - 指定负载均衡算法为最小连接算法。
- `weighted-least-connection` - 指定负载均衡算法为加权最小连接算法。
- `random` - 指定负载均衡算法为随机算法。
- `hash-url` - 指定负载均衡算法为URL哈希。
- `[fail-action {drop | reselect | reselect-after-retry retry-time | retry retry-time}]` - 配置好负载均衡算法后，指定失败动作，即客户端发起请求后，若真实服务没有响应，系统将执行该指定动作。
 - `drop` - 指定失败动作为“丢弃”，即丢弃该客户端请求，不进行响应。
 - `reselect` - 指定失败动作为“重选”，即重新选择一个真实服务。
 - `reselect-after-retry retry-time` - 指定失败动作为“重试后重选”，即系统将重新尝试对真实服务发起连接，按指定次数进行尝试。如失败，重新选择一个真实服务。

- **retry** *retry-time* - 指定失败动作为“重试”，即系统重新尝试对真实服务发起连接，按指定次数进行尝试。

在服务池配置模式下，使用**no balance**命令删除负载均衡算法。

绑定健康检查对象

健康检查用于检查各种服务的可用状态。设备可配置各种检查方法，对协议进行健康检查，例如TCP，UDP，HTTP，HTTPS等。绑定已创建的健康检查或健康检查组，在服务池配置模式下，使用以下命令：

health-check *name* [**group** *group-name*]

- **health-check** *name* - 绑定已创建的健康检查，并指定健康检查的名字。
- **health-check** **group** *group-name* - 绑定已创建的健康检查组，并指定健康检查组的名字。

在服务池配置模式下，使用**no health-check** 命令解除绑定的健康检查或健康检查组。

开启/关闭手动恢复功能

默认情况下，手动恢复功能是关闭的。在开启手动恢复功能后，当健康检查状态从“不可用”变为“可用”时，服务池运行状态将显示为“手动恢复”状态，不可用状态的真实服务需要通过执行手动恢复运行状态命令后，才可以恢复为可用状态。在服务池配置模式下，使用以下命令：

- 开启：**manual-resume enable**
- 关闭：**no manual-resume enable**



注意：

- 当服务池运行状态为“手动恢复”状态时，所配置的虚拟服务器、备份服务池、SLB四/七层内容交换规则状态均随之改变为“手动恢复”状态。
- 关于手动恢复运行状态的命令行介绍，参见[手动恢复运行状态](#)部分。

手动恢复运行状态

在执行手动恢复运行状态命令后，服务池的运行状态、服务池中真实服务的运行状态将按照当前健康检查状态进行改变：

- 当前健康检查状态为“可用”时，服务池运行状态、服务池中真实服务的运行状态将从“手动恢复”变为“正常”。
- 当前健康检查状态为“不可用”时，服务池运行状态、服务池中真实服务的运行状态将从“手动恢复”变为“离线”。

手动恢复服务池以及服务池中真实服务的运行状态，在服务池配置模式下，使用以下命令：

```
exec slb server-pool pool-name [real-server server-name] resume
```

- *pool-name* - 指定需要手动恢复运行状态的服务池名称。
- **real-server** *server-name* - 指定需要手动恢复的服务池中真实服务的名称。如不指定该参数，在手动恢复服务池运行状态后，服务池中的所有真实服务状态将会随之一同恢复。

查看服务池配置

在任何模式下，使用以下命令查看系统中已配置的服务池：

```
show slb server-pool pool-name
```

- *pool-name* - 指定服务池的名称。

查看服务池的运行状态

用户可在任何模式下，使用**show slb server-pool** *pool-name*命令，查看系统中每个服务池的实际运行状态。服务池状态由[池中真实服务的运行状态](#)决定，包含以下四种：

- **up**：表示服务池状态为“正常”。当服务池中至少有一个真实服务的运行状态为“正常”时，该服务池状态即为正常。
- **off-line**：表示服务池状态为“离线”当服务池中真实服务的运行状态均为“离线”或“禁用”时，该服务池状态即为离线。
- **unknown**：表示服务池状态为“未知”。当服务池中真实服务的运行状态均不是“正常”、且至少有一个为“未知”或“禁用中”时，该服务池状态为未知。
- **manual-resume**：表示服务池状态为“手动恢复”。当服务池开启了手动恢复功能且健康检查状态从“不可用”变为“可用”状态时，该服务池状态为“手动恢复”。

服务池中真实服务的运行状态

服务池状态由池中真实服务的运行状态决定，其与真实服务的运行状态（参见[查看真实服务状态](#)一节）不同。池中真实服务的运行状态，与其配置状态和健康检查状态相关，包含正常（up）、未知（unknown）、禁用（disabled）、离线（off-line）、禁用中（wait-down）、手动恢复（manual-resume）：

- 当真实服务配置状态为“启用”时：
 - 若未配置健康检查，服务池中真实服务的状态为“未知”；
 - 若健康检查结果为“可用”时，服务池中真实服务的状态为“正常”；
 - 若健康检查结果为“不可用”时，服务池中真实服务的状态为“离线”；
 - 若健康检查结果为从“不可用”变为“可用”状态，并且服务池开启了手动恢复功能时，服务池中真实服务的状态为“手动恢复”。
- 当真实服务配置状态为“禁用”时，无论真实服务或其所在服务池是否配置健康检查，均不产生该真实服务的健康检查实例，此时服务池中该真实服务的状态为“禁用”。
- 当真实服务配置状态为“平滑退出（清空保持表）”时，无论真实服务或其所在服务池是否配置健康检查，均不产生该真实服务的健康检查实例，此时服务池中该真实服务的状态为分两个阶段：
 - 该真实服务相关的所有会话关闭之前为“禁用中”。
 - 该真实服务相关的所有会话全部关闭后为“禁用”。
- 当真实服务配置状态为“平滑退出（等待保持表老化）”时，无论真实服务或其所在服务池是否配置健康检查，均不产生该真实服务的健康检查实例，此时服务池中该真实服务的状态为分两个阶段：
 - 该真实服务相关的所有会话关闭以及所有保持表老化之前为“禁用中”。
 - 该真实服务相关的所有会话全部关闭以及所有保持表老化后为“禁用”。

配置SLB规则

虚拟服务器通过SLB规则来分发客户端请求。SLB规则包含[HTTP内容改写规则](#)、[四层内容交换规则](#)、[HTTP内容交换规则](#)、[SQL内容交换规则](#)和[访问控制规则](#)。

配置四层内容交换规则

一个虚拟服务器中可配置多条四层内容交换规则。系统按四层内容交换列表中显示的先后顺序进行匹配。在全局配置模式下，使用以下命令创建四层内容交换规则：

```
slb l4-content-switch name
```

- *name* - 指定想要创建的规则的名称。如果指定的名称已存在，则直接进入四层内容交换规则模式。

在全局配置模式下，使用以下命令删除四层内容交换规则：

```
no slb l4-content-switch name
```

配置客户端源IP

在四层内容交换规则模式下，使用以下命令配置客户端源IP：

```
src-ip {ip-address | range min-value max-value}
```

- *ip-address* - 指定客户端的源IP地址。
- **range** *min-value max-value* - 指定客户端的源IP地址范围。

在四层内容交换规则模式下，使用以下命令删除源IP：

```
no src-ip
```

配置客户端源端口

在四层内容交换规则模式下，使用以下命令配置客户端源端口：

```
src-port {port-number | range min-value max-value}
```

- *port-number* - 指定客户端的源端口。
- **range** *min-value max-value* - 指定客户端的源端口范围。

在四层内容交换规则模式下，使用以下命令删除源端口：

```
no src-port
```


配置客户端目的IP

在四层内容交换规则模式下，使用以下命令配置客户端目的IP：

```
dst-ip {ip-address | range min-value max-value}
```

- *ip-address* - 指定客户端的目的IP地址。
- **range** *min-value max-value* - 指定客户端的目的IP地址范围。

在四层内容交换规则模式下，使用以下命令删除目的IP地址：

```
no dst-ip
```

配置客户端目的端口

在四层内容交换规则模式下，使用以下命令配置客户端目的端口：

```
dst-port {port-number | range min-value max-value}
```

- *port-number* - 指定客户端的目的端口。
- **range** *min-value max-value* - 指定客户端的目的端口范围。

在四层内容交换规则模式下，使用以下命令删除目的端口：

```
no dst-port
```

配置四层内容交换支持的协议

在四层内容交换规则模式下，使用以下命令配置四层内容交换支持的协议：

```
protocol {tcp | udp}
```

- **tcp** - 指定四层内容交换支持的协议为TCP。
- **udp** - 指定四层内容交换支持的协议为UDP。

在四层内容交换规则模式下，使用**no protocol** 命令删除四层内容交换支持的协议。

配置服务池

符合匹配条件的客户端请求，将被分配到指定的服务池。在四层内容交换规则模式下，使用以下命令配置服务池：

```
server-pool pool-name [real-server rs-name]
```

- *pool-name* - 指定服务池的名称。
- *rs-name* - 根据需要，指定真实服务。如配置该参数，设备将匹配的客户端请求直接分配给真实服务，不再进入到服务池中。如不指定该参数，客户端请求将在服务池内做负载均衡，由负载均衡算法决定分配至哪个真实服务。

在四层内容交换规则模式下，使用以下命令删除服务池配置：

```
no server-pool
```

配置描述信息

在四层内容交换规则模式下，使用以下命令配置描述信息：

```
description description
```

- *description* - 添加该规则的描述信息。

在四层内容交换规则模式下，使用 **no description** 命令删除描述信息。

查看四层内容交换规则

查看四层内容交换规则的配置信息，在任何模式下，使用以下命令：

```
show slb l4-content-switch name
```

- *name* - 指定四层内容交换规则的名称。

配置HTTP内容改写规则

系统支持对 HTTP 内容进行改写，可以对客户端请求的内容进行改写，也可以对服务器响应的内容进行改写。一条内容改写规则，可以配置 16 个匹配条件。当配置多个匹配条件时，各条件间关系为“与”，即多个条件同时满足才能匹配。

在全局配置模式下，使用以下命令创建内容改写规则：

```
slb content-rewrite name {type {request | response}}
```

- **name** - 指定想要创建的规则的名称。如果指定的名称已存在，则直接进入内容改写规则模式。
- **request** - 配置内容改写规则的方向为请求方向，即改写客户端请求的内容。
- **response** - 配置内容改写规则的方向为响应方向，即改写真实服务返回的响应。

在全局配置模式下，使用以下命令删除内容改写规则：

```
no slb content-rewrite name
```

内容改写规则的配置包含：

- [配置文本编码方式](#)
- [配置匹配操作符](#)
- [配置匹配条件](#)
- [配置匹配条件区分大小写](#)
- [配置系统动作](#)
- [配置描述信息](#)
- [查看内容改写规则信息](#)

配置文本编码方式

在内容改写规则模式下，使用以下命令配置文本编码方式：

```
charset {gb18030 | gb2312 | gbk | utf8}
```

- **gb18030** - 指定以GB18030方式对输入字符串编码。
- **gb2312** - 指定以GB2312方式对输入字符串编码。
- **gbk** - 指定以GBK方式对输入字符串编码。
- **utf8** - 指定UTF8方式对输入字符串编码。

配置匹配操作符

在内容改写规则模式下，使用以下命令配置匹配操作符：

match operation {and | or}

- **and**- 指定匹配条件的操作符为“与”，表示所有匹配条件都需满足。
- **or**- 指定匹配条件的操作符为“或”，表示只满足一个匹配条件即可。

配置匹配条件

当客户端请求满足此处配置的匹配条件时，设备将请求转发至服务池或真实服务。当类型为响应方向的规则时，匹配条件可以匹配请求方向或响应方向的对象内容；当类型为请求方向的规则时，匹配条件只能匹配请求方向的对象内容。

在内容改写规则模式下，使用以下命令配置匹配条件：

match [id id] url {contain string | end-with string | equal string | not-contain string | not-end-with string | not-equal string | regex-match string | not-start-with string | not-regex-match string | start-with string}

match [id id] {header header-name | cookie cookie-name | ssl-tls {cipher-name | tlsext-sni}} {contain string | end-with string | equal string | exist | not-contain string | not-end-with string | not-equal string | not-exist | not-regex-match string | not-start-with string | regex-match string | start-with string}

match [id id] ssl-tls protocol {equal {TLSv1 | TLSv1.1 | TLSv1.2 | TLSv1.3 | SSLv2 | SSLv3} | not-equal {TLSv1 | TLSv1.1 | TLSv1.2 | TLSv1.3 | SSLv2 | SSLv3}}

match [id id] ssl-tls client-verify-result-code {equal number | not-equal number}

match [id id] client-ip-family http {equal { ipv4 | ipv6 | any} | not-equal { ipv4 | ipv6 | any}}

match [id id] http-version {equal { 0.9 | 1.0 | 1.1 | 2.0} | not-equal {0.9 | 1.0 | 1.1 | 2.0}}

match [id id] {dst-ip | dst-port | src-ip | real-src-ip} {equal IP-address | not-equal IP-address | in-range from-IP-address to-IP-address | not-in-range from-IP-address to-IP-address}

match [id id] request-method {equal string [GET | POST | HEAD | PUT | DELETE | OPTIONS | CONNECT] | not-equal string [GET | POST | HEAD | PUT | DELETE | OPTIONS | CONNECT]}

match [id id] x509-cert {cert {exist | not-exist}}

```
match [id id] x509-cert {issuer-dn | issuer-dn-commonName | issuer-dn-countryName | issuer-dn-emailAddress |  
issuer-dn-localityName | issuer-dn-organizationalUnit | issuer-dn-organizationName | issuer-dn-stateOrProvince |  
subject-dn | subject-dn-commonName | subject-dn-countryName | subject-dn-emailAddress | subject-dn-loc-  
alityName | subject-dn-organizationalUnit | subject-dn-organizationName | subject-dn-stateOrProvince} {contain  
string | end-with string | equal string | exist | not-contain string | not-end-with string | not-equal string | not-exist |  
not-regex-match string | not-start-with string | regex-match string | start-with string}  
  
match [id id] x509-cert version {equal{1 | 2 | 3} | not-equal{1 | 2 | 3}}
```

- **id** *id* - 指定匹配条件的ID，范围为1至16。如果不指定ID，系统将自动生成匹配条件的ID。一个规则中最多指定16个匹配条件。当配置多个匹配条件时，各条件间关系为“与”，即多个条件同时满足才能匹配。
- **url** - 指定客户端请求为URL。
- **header** *header-name* - 指定客户端请求的Header名称。
- **cookie** *cookie-name* - 指定客户端请求的Cookie名称。
- **client-ip-family** - 指定客户端请求的IP协议类型标识。
- **http-version** - 指定客户端请求的HTTP版本。
- **real-src-ip** - 指定客户端请求的真实源IP地址。
- **src-ip** - 指定客户端请求的源IP地址。
- **dst-ip** - 指定客户端请求的目的IP地址。
- **dst-port** - 指定客户端请求的目的端口。
- **request-method** - 指定客户端的请求方法。
- **cert** - 指定匹配项为X509证书。
- **issuer-dn** - 指定匹配项为X509签发者。
- **issuer-dn-commonName** - 指定匹配项为X509证书的签发者名称。
- **issuer-dn-countryName** - 指定匹配项为X509证书签发者的国家。
- **issuer-dn-emailAddress** - 指定匹配项为X509证书签发者的电子邮件。

- **issuer-dn-localityName** - 指定匹配项为X509证书签发者的城市。
- **issuer-dn-organizationalUnit** - 指定匹配项为X509证书签发者的部门。
- **issuer-dn-organizationName** - 指定匹配项为X509证书签发者的公司或机构。
- **issuer-dn-stateOrProvince** - 指定匹配项为X509证书签发者的州或省份。
- **subject-dn** - 指定匹配项为X509证书的主题。
- **subject-dn-commonName** - 指定匹配项为X509证书的主题名称。
- **subject-dn-countryName** - 指定匹配项为X509证书主题的国家。
- **subject-dn-emailAddress** - 指定匹配项为X509证书主题的电子邮件。
- **subject-dn-localityName** - 指定匹配项为X509证书主题的城市。
- **subject-dn-organizationName** - 指定匹配项为X509证书主题的公司或机构。
- **subject-dn-organizationalUnit** - 指定匹配项为X509证书主题的部门。
- **subject-dn-stateOrProvince** - 指定匹配项为X509证书主题的州或省份。
- **version** - 指定匹配项为X509证书版本。
- **contain *string*** - 当客户端请求包含指定字符时，满足匹配条件。
- **not-contain *string*** - 当客户端请求中不包含指定字符时，满足匹配条件。
- **equal *string*** - 当客户端请求等于指定字符时，满足匹配条件。
- **end-with** - 当客户端请求以指定字符结尾时，满足匹配条件。
- **not-end-with** - 当客户端请求不以指定字符结尾时，满足匹配条件。
- **start-with** - 当客户端请求以指定字符开始时，满足匹配条件。
- **not-start-with** - 当客户端请求不以指定字符开始时，满足匹配条件。
- **not-equal *string*** - 当客户端请求不等于指定字符时，满足匹配条件。

- **regex-match** *string* - 当客户端请求符合正则表达式，满足匹配条件。
- **not-regex-match** *string* - 当客户端请求不符合正则表达式，满足匹配条件。
- **exist** *string* - 当客户端请求存在指定字符时，满足匹配条件。
- **not-exist** *string* - 当客户端请求不存在指定字符时，满足匹配条件。
- **in-range** - 当客户端请求的IP地址在指定区间时，满足匹配条件。
- **not-in-range** - 当客户端请求的IP地址不在指定区间时，满足匹配条件。

配置匹配条件区分大小写

用户可根据需要，配置匹配条件区分大小写。配置后，系统将按照字母大小写区分匹配条件。在内容改写规则模式下，使用以下命令进行配置：

- 配置匹配条件区分大小写：**match case-sensitive**
- 配置匹配条件不区分大小写：**match case-insensitive**

配置内容改写规则动作

对符合匹配条件的HTTP内容，指定系统所采取的动作，包括重定向、URL改写、Cookie改写、消息体改写、头部改写、删除Cookie、删除头部、插入头部、插入Cookie。

配置动作为重定向

对符合匹配条件的HTTP内容，配置系统所采取的动作作为重定向。此选项仅当内容改写规则的方向为请求方向，即**request**方向时可配置。

替换URL

指定重定向的类型为“替换URL”，系统将HTTP内容重定向到指定的URL地址，同时返回指定的状态码。在内容改写规则模式下，使用以下命令配置替换URL：

```
action redirect [using-variables] new_url [status-code {301 | 302 | 307}]
```

- **using-variables** - 开启使用变量功能。开启后，系统识别改写内容中配置的的预定义变量，将其替换为对应的信息，并发送至真实服务器。
- **new_url** - 指定重定向的URL地址，系统将HTTP内容重定向到指定的新URL地址。
- **status-code {301 | 302 | 307}** - 配置设备返回给客户端的状态码。

在内容改写规则模式下，使用**no action**命令删除该配置。

指定协议（保持原有路径和查询）

指定重定向的类型为“指定协议（保持原有路径和查询）”，即用户可根据需要，修改原来的协议和端口，在HTTP/HTTPS重定向时保持原来的网址。在内容改写规则模式下，使用以下命令配置指定协议（保持原有路径和查询）：

action redirect keep-path-and-query protocol {http | https} [port number] [status-code {301 | 302 | 307}]

- **http** - 将当前协议改为 HTTP 协议。
- **https** - 将当前协议改为 HTTPS 协议。
- **port number** - 指定重定向到的目的端口号。
- **status-code {301 | 302 | 307}** - 配置重定向的设备状态码。

在内容改写规则模式下，使用**no action**命令删除该配置。

改写URL

指定重定向的类型为“改写URL”后，需指定URL改写的原始内容及改写后的内容，系统将按照配置，将URL的原始内容替换为改写后的内容。用户可根据需要，在内容改写规则模式下，使用以下命令配置改写URL：

action redirect replace-url original original-value target [using-variables] target-value [status-code {301 | 302 | 307}]

- **original-value** - 指定URL的原始内容。
- **target-value** - 指定改写后的内容。
- **using-variables** - 开启使用变量功能。开启后，系统识别改写内容中配置的的预定义变量，将其替换为对应的信息，并发送至真实服务器。
- **status-code {301 | 302 | 307}** - 配置重定向的设备状态码。

在内容改写规则模式下，使用`no action`命令删除该配置。

配置动作为消息体改写

对符合匹配条件的HTTP内容，配置系统所采取的动作作为消息体改写。配置后，系统将按照配置，将消息体的原始内容替换为改写后的内容。如是响应方向的消息体改写，仅支持对文本类的Body进行改写。

在内容改写规则模式下，使用以下命令配置系统动作为消息体改写：

action replace-body [*subrange value1 value2*] [*original value*] **target** [*using-variables*] *value*

- **subrange value1 value2** - 指定消息体的取值范围。
- **original value** - 指定消息体的原始内容。
- **using-variables** - 开启使用变量功能。开启后，系统识别改写内容中配置的的预定义变量，将其替换为对应的信息，并发送至真实服务器。
- **target value** - 指定改写后的内容。系统支持开启 **using-variables** 功能，即使用预定义变量对内容进行改写，需以“`${}`”的形式添加变量，支持的字符包含字母、数字、“.”和“_”。变量说明，请参阅《[HTTP内容改写_变量使用说明](#)》。

在内容改写规则模式下，使用`no action`命令删除该配置。

配置动作为头部改写

对符合匹配条件的HTTP内容，配置系统所采取的动作作为头部改写。配置后，系统将按照配置，将头部的原始内容替换为改写后的内容。

在内容改写规则模式下，使用以下命令配置系统动作为头部改写：

action replace-header *header-name* [*subrange value1 value2*] [*original value*] **target** [*using-variables*] *value*

- *header-name* - 输入头部的名称。
- **subrange value1 value2** - 指定header的取值范围。
- **original value** - 指定头部的原始内容。
- **using-variables** - 开启使用变量功能。开启后，系统识别改写内容中配置的的预定义变量，将其替换为对应的信息，并发送至真实服务器。

- **target value** -指定改写后的内容。系统支持开启 **using-variables** 功能，即使用预定义变量对内容进行改写，需以“**\${}**”的形式添加变量，支持的字符包含字母、数字、“.”和“_”。变量说明，请参阅《[HTTP内容改写_变量使用说明](#)》。

在内容改写规则模式下，使用**no action**命令删除该配置。

配置动作为Cookie改写

对符合匹配条件的HTTP内容，配置系统所采取的动作作为Cookie改写。配置后，系统将按照配置，将Cookie的原始内容替换为改写后的内容。

在内容改写规则模式下，使用以下命令配置系统动作为Cookie改写：

```
aciton replace-cookie cookie-name [ subrange value1 value2] [original value] [http-only] [secure] target [using-variables] value
```

- **cookie-name** - 输入Cookie的名称。
- **subrange value1 value2** - 指定Cookie的取值范围。
- **original value** - 指定Cookie的原始内容。
- **http-only** - 开启Cookie的HTTP Only属性。开启后，插入的Cookie只对浏览器可见，JS脚本无法获取。此选项仅当内容改写规则的方向为“**response 响应**”时生效。
- **secure** - 开启Cookie的Secure属性。开启后，客户端浏览器只能通过HTTPS连接发送插入的Cookie。此选项仅当内容改写规则的方向为“**response 响应**”时生效。
- **using-variables** - 开启使用变量功能。开启后，系统识别改写内容中配置的的预定义变量，将其替换为对应的信息，并发送至真实服务器。
- **target value** - 指定改写后的内容。系统支持开启 **using-variables** 功能，即使用预定义变量对内容进行改写，需以“**\${}**”的形式添加变量，支持的字符包含字母、数字、“.”和“_”。变量说明，请参阅《[HTTP内容改写_变量使用说明](#)》。

在内容改写规则模式下，使用**no action**命令删除该配置。

配置动作为URL改写

对符合匹配条件的HTTP内容，配置系统所采取的动作作为URL改写。配置后，系统将按照配置，将Cookie的原始内容替换为改写后的内容。

在内容改写规则模式下，使用以下命令配置系统动作为URL改写：

```
action replace-url subrange value1 value2 [original value] target [using-variables] value
```

- **subrange** *value1 value2* - 指定URL改写的地址范围。
- **original** *value* - 指定URL的原始内容。
- **using-variables** - 开启使用变量功能。开启后，系统识别改写内容中配置的的预定义变量，将其替换为对应的信息，并发送至真实服务器。
- **target** *value* - 指定改写后的内容。系统支持开启 **using-variables** 功能，即使用预定义变量对内容进行改写，需以“`${}`”的形式添加变量，支持的字符包含字母、数字、“.”和“_”。变量说明，请参阅《[HTTP内容改写_变量使用说明](#)》。

在内容改写规则模式下，使用**no action**命令删除该配置。

配置动作为删除Cookie

对符合匹配条件的HTTP内容，配置系统所采取的动作作为删除Cookie。配置后，系统将删除指定的Cookie。

在内容改写规则模式下，使用以下命令配置系统动作为删除Cookie：

```
action delete-cookie cookie-name
```

- *cookie-name* - 指定Cookie的名称。

在内容改写规则模式下，使用**no action**命令删除该配置。

配置动作为删除头部

对符合匹配条件的HTTP内容，系统所采取的动作作为删除头部。配置后，系统将删除指定的头部。

在内容改写规则模式下，使用以下命令配置系统动作为删除头部：

```
action delete-header header-name
```

- *header-name* - 指定头部的名称。

在内容改写规则模式下，使用**no action**命令删除该配置。

配置动作为插入头部

对符合匹配条件的HTTP内容，系统所采取的动作作为插入头部。配置后，系统将指定的头部字段插入到请求或者响应消息中。

在内容改写规则模式下，使用以下命令配置系统动作为插入头部：

```
action insert-header header-name [using-variables] value
```

- *header-name* - 指定头部的名称。
- **using-variables** - 开启使用变量功能。开启后，系统识别插入内容中配置的的预定义变量，将其替换为对应的信息，并发送至真实服务器。
- *value* - 指定插入的头部内容。系统支持开启 **using-variables** 功能，即使用预定义变量对内容进行改写，需以“`${}`”的形式添加变量，支持的字符包含字母、数字、“.”和“_”。变量说明，请参阅《[HTTP内容改写_变量使用说明](#)》。

在内容改写规则模式下，使用**no action**命令删除该配置。

配置动作为插入Cookie

对符合匹配条件的HTTP内容，系统所采取的动作作为插入Cookie。配置后，系统将指定的Cookie字段插入到请求或者响应消息中。

在内容改写规则模式下，使用以下命令配置系统动作为插入Cookie：

```
action insert-cookie cookie-name [using-variables] value [http-only] [secure] [domain domain-name path path-name]  
[expires expire-time]
```

- *cookie-name* - 指定Cookie的名称。
- **using-variables** - 开启使用变量功能。开启后，系统识别改写内容中配置的的预定义变量，将其替换为对应的信息，并发送至真实服务器。
- *value* - 指定改写后的内容。系统支持开启**using-variables**功能，即使用预定义变量对内容进行改写，需以“`${}`”的形式添加变量，支持的字符包含字母、数字、“.”和“_”。变量说明，请参阅《[HTTP内容改写_变量使用说明](#)》。
- **http-only** - 开启Cookie的HTTP Only属性。开启后，插入的Cookie只对浏览器可见，JS脚本无法获取。此选项仅当内容改写规则的方向为“**response 响应**”时可配置。

- **secure** - 开启Cookie的Secure属性。开启后，客户端浏览器只能通过HTTPS连接发送插入的Cookie。此选项仅当内容改写规则的方向为“**response** 响应”时可配置。
- **domain** *domain-name* - 指定需匹配的域名称，匹配成功的客户端请求对应的响应报文将被插入Cookie。此选项仅当内容改写规则的方向为“**response** 响应”时可配置。
- **path** *path-name* - 指定需匹配的URL路径，匹配成功的客户端请求对应的响应报文将被插入Cookie。此选项仅当内容改写规则的方向为“**response** 响应”时可配置。
- **expires** *expire-time* - 指定Cookie的超时时间。取值范围为300 - 31536000秒，默认为300秒。超过指定的时间后，Cookie信息将被从客户端磁盘中清除，客户端发送报文也将不再携带该Cookie值。

在内容改写规则模式下，使用**no action**命令删除该配置。

配置动作为添加IP协议类型标识

对符合匹配条件的HTTP内容，系统所采取的动作作为添加IP协议类型标识，即支持修改HTTP响应中的IPv4文本内容/IPv6文本内容、文本位置、文字大小、字体颜色、背景颜色。此选项仅当匹配条件的方向为“**response** 响应”时生效。

在内容改写规则模式下，使用以下命令进入添加IP协议类型标识配置模式：

action add-ip-family-prompt

在内容改写规则模式下，使用**no action**命令删除该配置。

在添加IP协议类型标识配置模式下，使用以下命令在指定网页上添加IP协议类型标识：

- 背景颜色：**bg-color** {**white** | **black** | **red** | **yellow** | **green** | **blue** | **orange** | **purple** | **cyan** | **pink**}
- 字体颜色：**font-color** {**white** | **black** | **red** | **yellow** | **green** | **blue** | **orange** | **purple** | **cyan** | **pink**}
- 字体大小：**font-size** *size*，取值范围10至20，单位pt。
- IPv4文本内容：**ipv4-content** *content*
- IPv6文本内容：**ipv6-content** *content*
- 文本位置：**position** {**top** | **bottom**}



注意: 在虚拟服务器中引用HTTP内容改写规则时，动作为“添加IP协议类型标识”的规则仅支持引用一条。

配置动作为插入源IP

对符合匹配条件的HTTP内容，系统所采取的动作作为插入源IP。配置后，系统将客户端的源IP地址插入到请求消息中指定的首部字段中。

在内容改写规则模式下，使用以下命令配置系统动作为插入源IP地址：

action insert-src-ip *header-name*

- *header-name* - 指定需被插入源IP地址的首部名称。

在内容改写规则模式下，使用**no action**命令删除该配置。

配置动作为插入真实源IP

对符合匹配条件的HTTP内容，系统所采取的动作作为插入真实源IP。配置后，系统将客户端的真实源IP地址插入到请求消息中指定的首部字段中。

在内容改写规则模式下，使用以下命令配置系统动作为插入真实源IP地址：

action insert-real-src-ip *header-name*

- *header-name* - 指定需被插入真实源IP地址的首部名称。

在内容改写规则模式下，使用**no action**命令删除该配置。

配置描述信息

在内容改写规则模式下，使用以下命令配置描述信息：

description *description*

- *description* - 添加该规则的描述信息。

在内容改写规则模式下，使用**no description**命令删除描述信息。

查看内容改写规则信息

查看内容改写规则的配置信息，在任何模式下，使用以下命令：

```
show slb content-rewrite name
```

- *name* - 指定内容改写规则的名称。

HTTP内容改写_变量使用说明

下表为HTTP内容改写的变量使用说明。

变量使用说明。

变量	说明
\${X509.version}	客户端证书的版本。
\${X509.serial_num}	客户端证书的序列号。
\${X509.signature_algorithm}	客户端证书的签名算法。
\${X509.not_valid_before}	客户端证书的有效时间（在此之前无效）。
\${X509.not_valid_after}	客户端证书的有效时间（在此之后无效）。
\${X509.public_key_algorithm}	客户端证书的公钥算法。
\${X509.public_key_type}	客户端证书的公钥类型。
\${X509.public_key_bits}	客户端证书的公钥长度。
\${X509.md5}	客户端证书的MD5散列。
\${X509.fingerprint}	客户端证书的指纹（经SHA-1散列）。
\${X509.whole}	实际的客户端证书本身（PEM格式）。
\${X509.der_whole}	实际的客户端证书本身（DER格式，经Base64编码）。
\${X509.subject_dn}	客户端证书主题(各部分以','作为分隔符)。
\${X509.subject_dn_r}	客户端证书主题的逆序(各部分以','作为分隔符)。
\${X509.subject_dn_cn}	客户端证书主题的名称。
\${X509.subject_dn_e}	客户端证书主题的电子邮件。

变量	说明
\${X509.subject_dn_o}	客户端证书主题的公司/机构。
\${X509.subject_dn_ou}	客户端证书主题的部门。
\${X509.subject_dn_c}	客户端证书主题的国家。
\${X509.subject_dn_st}	客户端证书主题的州/省份。
\${X509.subject_dn_l}	客户端证书主题的城市。
\${X509.issuer_dn}	客户端证书签发者，各部分以','作为分隔符。
\${X509.issuer_dn_r}	客户端证书签发者的逆序，各部分以','作为分隔符。
\${X509.issuer_dn_cn}	客户端证书签发者的名称。
\${X509.issuer_dn_e}	客户端证书签发者的电子邮件。
\${X509.issuer_dn_o}	客户端证书签发者的公司/机构。
\${X509.issuer_dn_ou}	客户端证书签发者的部门。
\${X509.issuer_dn_c}	客户端证书签发者的国家。
\${X509.issuer_dn_st}	客户端证书签发者的州/省份。
\${X509.issuer_dn_l}	客户端证书签发者的城市。
\${SSL.version}	SSL/TLS协议版本。
\${SSL.cipher_id}	SSL/TLS协议的协商算法ID。
\${SSL.cipher_name}	SSL/TLS协议的协商算法名称。
\${SSL.client_verify_result_code}	对客户端证书的认证错误码。
\${SSL.client_verify_result_string}	对客户端证书验证的结果。
\${SSL.session_id}	SSL/TLS的session ID。
\${SSL.tlsextn_sni}	TLS协议拓展字段中的SNI字段。
\${HTTP.args}	HTTP协议请求行中的参数。
\${HTTP.content_length}	HTTP协议请求头中的Content_Length字段。
\${HTTP.content_type}	HTTP协议请求头中的Content_Type字段。
\${HTTP.cookie_name}	HTTP协议Cookie中指定的 <code>name</code> 字段， <code>name</code> 为指定字段的名称。

变量	说明
\${HTTP.host}	HTTP协议请求中的Host字段名，获取方式的优先级依次为：请求行中的主机名>请求头中的主机名>处理请求的服务器名。
\${HTTP.http_name}	HTTP协议请求头中指定的name字段，name为指定字段的名称。
\${HTTP.cookie}	HTTP协议请求头中的Cookie字段。
\${HTTP.header_host}	HTTP协议请求头中的Host字段。
\${HTTP.referer}	HTTP协议请求头中的Referer字段。
\${HTTP.user_agent}	HTTP协议请求头中的User-Agent字段。
\${HTTP.via}	HTTP协议请求头中的Via字段。
\${HTTP.x_forwarded_for}	HTTP协议请求头中的X_Forwarded_For字段。
\${HTTP.with_args}	HTTP协议请求行中若带参数，则为"?"；若不带参数，则为空字符串。
\${HTTP.remote_user}	HTTP协议请求中经Basic Authentication验证的用户名。
\${HTTP.request_line}	HTTP协议请求行完整的原始数据。
\${HTTP.request_method}	HTTP协议请求行中的Method字段，如"GET"和"POST"。
\${HTTP.request_uri_with_args}	HTTP协议请求行中完整的URL字段（带参数）。
\${HTTP.scheme}	HTTP协议请求行中的URL Scheme字段，如"http"和"https"。
\${HTTP.protocol}	HTTP协议请求行中的协议字段，如"HTTP/1.0"、"HTTP/1.1"和"HTTP/2.0"。
\${HTTP.uri}	HTTP协议请求行中URL字段的未编码或解码后的URL地址。
\${HTTP.version}	HTTP协议请求行中的HTTP_Version字段，如"0.9"、"1.0"、"1.1"和"2.0"。

变量	说明
<code>\${HTTP.request_time}</code>	HTTP请求发送至设备的时间。
<code>\${IP.real_remote_addr}</code>	HTTP协议请求头中的真实源IP地址，获取方式的优先级依次为：X_ForWARDED_For > X_Real_IP > 报文携带的源IP。
<code>\${IP.remote_addr}</code>	客户端的IP地址。
<code>\${IP.vs_addr}</code>	客户端请求虚拟服务器的IP地址。
<code>\${IP.rs_addr}</code>	设备返回给客户端真实服务的IP地址。
<code>\${IP.client_addr_family}</code>	客户端IP地址的类型。
<code>\${IP.server_addr_family}</code>	真实服务IP地址的类型。
<code>\${IP.snat_addr}</code>	客户端请求源IP地址经设备自动源NAT转换后，从设备流出的源IP地址。
<code>\${TCP.real_remote_port}</code>	TCP连接中客户端的端口号，获取方式的优先级依次为：X_ForWARDED_For > X_Real_IP > 报文携带的源IP。
<code>\${TCP.remote_port}</code>	当前TCP连接的源端口号。
<code>\${TCP.rcv_space}</code>	当前TCP连接的接收缓存大小。
<code>\${TCP.rtt}</code>	当前TCP连接的往返时延，单位为微秒。
<code>\${TCP.snd_cwnd}</code>	当前TCP连接的拥塞控制窗口值。
<code>\${TCP.trrvar}</code>	当前TCP连接的平均往返时延，单位为微秒。
<code>\${TCP.vs_port}</code>	TCP连接中虚拟服务器的端口号。
<code>\${TCP.rs_port}</code>	TCP连接中真实服务的端口号。
<code>\${TCP.snat_port}</code>	TCP连接中流量经设备自动源NAT转换后，从设备流出的源端口号。

配置HTTP内容交换规则

对于访问同一个虚拟服务器的客户端请求，设备可配置HTTP内容交换规则，根据请求的来源属性和内容属性，决定将请求转发到哪个服务池或者真实服务。一条HTTP内容交换规则，可以配置 16 个匹配条件。当配

置多个匹配条件时，各条件间关系为“与”，即多个条件同时满足才能匹配。若配置多条HTTP内容交换规则，系统将按照规则列表的顺序进行匹配。目前，仅 HTTP和HTTPS 类型的虚拟服务器支持该功能。

在全局配置模式下，使用以下命令创建HTTP内容交换规则：

```
slb l7-content-switch name
```

- *name* - 指定想要创建的规则的名称。如果指定的名称已存在，则直接进入HTTP内容交换规则模式。

在全局配置模式下，使用以下命令删除HTTP内容交换规则：

```
no slb l7-content-switch name
```

配置描述信息

在HTTP内容交换规则模式下，使用以下命令配置描述信息：

```
description description
```

- *description* - 添加该规则的描述信息。

在HTTP内容交换规则模式下，使用**no description** 命令删除描述信息。

配置文本编码方式

在HTTP内容交换规则模式下，使用以下命令配置文本编码方式：

```
charset {gb18030 | gb2312 | gbk | utf8}
```

- **gb18030** - 指定以GB18030方式对输入字符串编码。
- **gb2312** - 指定以GB2312方式对输入字符串编码。
- **gbk** - 指定以GBK方式对输入字符串编码。
- **utf8** - 指定UTF8方式对输入字符串编码。

配置匹配操作符

在HTTP内容交换规则模式下，使用以下命令配置匹配操作符：

```
match operation {and | or}
```

- **and** - 指定匹配条件的操作符为“与”，表示所有匹配条件都需满足。
- **or** - 指定匹配条件的操作符为“或”，表示只满足一个匹配条件即可。

配置服务池

符合匹配条件的客户端请求，将被分配到指定的服务池。在HTTP内容交换规则模式下，使用以下命令配置服务池：

```
server-pool pool-name [real-server rs-name]
```

- *pool-name* - 指定服务池的名称。
- *rs-name* - 根据需要，指定真实服务。如配置该参数，设备将匹配的客户端请求直接分配给真实服务，不再进入到服务池中。如不指定该参数，客户端请求将在服务池内做负载均衡，由负载均衡算法决定分配至哪个真实服务。

在HTTP内容交换规则模式下，使用以下命令删除服务池配置：

```
no server-pool
```

配置匹配条件

当客户端请求满足此处配置的匹配条件时，设备将请求转发至服务池或真实服务。在HTTP内容交换规则模式下，使用以下命令配置匹配条件：

```
match [id id] url {contain string | end-with string | equal string | not-contain string | not-end-with string | not-equal string | regex-match string | not-start-with string | not-regex-match string | start-with string}
```

```
match [id id] {header header-name | cookie cookie-name | ssl-tls {cipher-name | tlsext-sni}} {contain string | end-with string | equal string | exist | not-contain string | not-end-with string | not-equal string | not-exist | not-regex-match string | not-start-with string | regex-match string | start-with string}
```

```
match [id id] ssl-tls protocol {equal {TLSv1 | TLSv1.1 | TLSv1.2 | TLSv1.3 | SSLv2 | SSLv3} | not-equal {TLSv1 | TLSv1.1 | TLSv1.2 | TLSv1.3 | SSLv2 | SSLv3}}
```

```
match [id id] ssl-tls client-verify-result-code {equal number | not-equal number}
```

```
match [id id] ip-family http {equal { ipv4 | ipv6 | any} | not-equal { ipv4 | ipv6 | any}}
```

```
match [id id] http-version {equal { 0.9 | 1.0 | 1.1 | 2.0} | not-equal {0.9 | 1.0 | 1.1 | 2.0}}
```

`match [id id] {dst-ip | dst-port | src-ip | real-src-ip} {equal IP-address | not-equal IP-address | in-range from-IP-address to-IP-address | not-in-range from-IP-address to-IP-address}`

`match [id id] request-method {equal string [GET | POST | HEAD | PUT | DELETE | OPTIONS | CONNECT] | not-equal string [GET | POST | HEAD | PUT | DELETE | OPTIONS | CONNECT]}`

`match [id id] x509-cert {cert {exist | not-exist}}`

`match [id id] x509-cert {issuer-dn | issuer-dn-commonName | issuer-dn-countryName | issuer-dn-emailAddress | issuer-dn-localityName | issuer-dn-organizationalUnit | issuer-dn-organizationName | issuer-dn-stateOrProvince | subject-dn | subject-dn-commonName | subject-dn-countryName | subject-dn-emailAddress | subject-dn-localityName | subject-dn-organizationalUnit | subject-dn-organizationName | subject-dn-stateOrProvince} {contain string | end-with string | equal string | exist | not-contain string | not-end-with string | not-equal string | not-exist | not-regex-match string | not-start-with string | regex-match string | start-with string}`

`match [id id] x509-cert version {equal {1 | 2 | 3} | not-equal {1 | 2 | 3}}`

- **id id** - 指定匹配条件的ID，范围为1至16。如果不指定ID，系统将自动生成匹配条件的ID。一个规则中最多指定16个匹配条件。当配置多个匹配条件时，各条件间关系为“与”，即多个条件同时满足才能匹配。
- **url** - 指定客户端请求为URL。
- **header header-name** - 指定客户端请求的Header名称。
- **cookie cookie-name** - 指定客户端请求的Cookie名称。
- **ip-family** - 指定客户端请求的IP协议类型标识。
- **http-version** - 指定客户端请求的HTTP版本。
- **real-src-ip** - 指定客户端请求的真实源IP地址。
- **src-ip** - 指定客户端请求的源IP地址。
- **dst-ip** - 指定客户端请求的目的IP地址。
- **dst-port** - 指定客户端请求的目的端口。
- **request-method** - 指定客户端的请求方法。
- **cert** - 指定匹配项为X509证书。

- **issuer-dn** - 指定匹配项为X509签发者。
- **issuer-dn-commonName** - 指定匹配项为X509证书的签发者名称。
- **issuer-dn-countryName** - 指定匹配项为X509证书签发者的国家。
- **issuer-dn-emailAddress** - 指定匹配项为X509证书签发者的电子邮件。
- **issuer-dn-localityName** - 指定匹配项为X509证书签发者的城市。
- **issuer-dn-organizationalUnit** - 指定匹配项为X509证书签发者的部门。
- **issuer-dn-organizationName** - 指定匹配项为X509证书签发者的公司或机构。
- **issuer-dn-stateOrProvince** - 指定匹配项为X509证书签发者的州或省份。
- **subject-dn** - 指定匹配项为X509证书的主题。
- **subject-dn-commonName** - 指定匹配项为X509证书的主题名称。
- **subject-dn-countryName** - 指定匹配项为X509证书主题的国家。
- **subject-dn-emailAddress** - 指定匹配项为X509证书主题的电子邮件。
- **subject-dn-localityName** - 指定匹配项为X509证书主题的城市。
- **subject-dn-organizationName** - 指定匹配项为X509证书主题的公司或机构。
- **subject-dn-organizationalUnit** - 指定匹配项为X509证书主题的部门。
- **subject-dn-stateOrProvince** - 指定匹配项为X509证书主题的州或省份。
- **version** - 指定匹配项为X509证书版本。
- **contain *string*** - 当客户端请求包含指定字符时，满足匹配条件。
- **not-contain *string*** - 当客户端请求中不包含指定字符时，满足匹配条件。
- **equal *string*** - 当客户端请求等于指定字符时，满足匹配条件。
- **end-with** - 当客户端请求以指定字符结尾时，满足匹配条件。

- **not-end-with** - 当客户端请求不以指定字符结尾时，满足匹配条件。
- **start-with** - 当客户端请求以指定字符开始时，满足匹配条件。
- **not-start-with** - 当客户端请求不以指定字符开始时，满足匹配条件。
- **not-equal string** - 当客户端请求不等于指定字符时，满足匹配条件。
- **regex-match string** - 当客户端请求符合正则表达式，满足匹配条件。
- **not-regex-match string** - 当客户端请求不符合正则表达式，满足匹配条件。
- **exist string** - 当客户端请求存在指定字符时，满足匹配条件。
- **not-exist string** - 当客户端请求不存在指定字符时，满足匹配条件。
- **in-range** - 当客户端请求的IP地址在指定区间时，满足匹配条件。
- **not-in-range** - 当客户端请求的IP地址不在指定区间时，满足匹配条件。

配置匹配条件区分大小写

用户可根据需要，配置匹配条件区分大小写。配置后，系统将按照字母大小写区分匹配条件。在HTTP内容交换规则模式下，使用以下命令进行配置：

- 配置匹配条件区分大小写：**match case-sensitive**
- 配置匹配条件不区分大小写：**match case-insensitive**

查看HTTP内容交换规则

查看HTTP内容交换规则的配置信息，在任何模式下，使用以下命令：

```
show slb l7-content-switch name
```

- *name* - 指定HTTP内容交换规则的名称。

SQL内容交换规则

对于访问同一个虚拟服务器的客户端请求，用户可配置SQL内容交换规则，然后系统将根据请求的来源属性和内容属性，决定将请求转发到哪个服务池或者真实服务。当配置多个匹配条件时，各条件间关系为

“与”，即多个条件同时满足才能匹配。若配置多条SQL内容交换规则，系统将按照规则列表的顺序进行匹配。仅 MYSQL类型的虚拟服务器支持该功能。

在全局配置模式下，使用以下命令创建SQL内容交换规则：

```
slb sql-content-switch name
```

- *name* - 指定想要创建的规则的名称。如果指定的名称已存在，则直接进入SQL内容交换规则模式。

在全局配置模式下，使用以下命令删除指定的SQL内容交换规则：

```
no slb sql-content-switch name
```

配置匹配条件

当MYSQL请求满足此处配置的匹配条件时，设备将请求转发至服务池或真实服务。在SQL内容交换规则模式下，使用以下命令配置匹配条件：

- 配置源IP： **src-ip** *ip_address*
- 配置目的IP： **dst-ip** *ip_address*
- 配置目的端口： **dst-port** *port*（端口范围为1至65535。）
- 配置数据库名： **database-name** *name*（指定请求访问的数据库名。）
- 配置数据库账号： **user-name** *name*（指定虚拟服务器中创建的数据库账号。）
- 配置是否匹配字符串： **pattern {match | not-match} value**（字符串范围为1至255字符，支持正则表达式。）
 - **match** *value* - 匹配指定的字符串则表示符合匹配条件。
 - **not-match** *value* - 不匹配指定的字符串则表示符合匹配条件。

配置服务池/真实服务器

符合匹配条件的MYSQL请求，将被分配到指定的服务池或真实服务器。在SQL内容交换规则模式下，使用以下命令：

```
server-pool pool-name [real-server rs-name]
```

- *pool-name* - 指定服务池的名称。

- **rs-name** - 根据需要，指定真实服务。如配置该参数，设备将匹配的MYSQL请求直接分配给真实服务，不再进入到服务池中。如不指定该参数，MYSQL请求将在服务池内做负载均衡，由负载均衡算法决定分配至哪个真实服务。

在SQL内容交换规则模式下，使用以下命令删除配置：

```
no server-pool
```

配置失败动作

若请求不符合SQL内容交换规则的匹配条件，系统将会丢弃该请求或者继续匹配下一条SQL内容交换规则。指定失败动作，在SQL内容交换规则模式下，使用以下命令：

```
fail-action {drop | match-next}
```

- **drop** - 指定失败动作为丢弃该请求。
- **match-next** - 指定失败动作为继续匹配下一条SQL内容交换规则。该动作为默认动作。

配置描述信息

在SQL内容交换规则模式下，使用以下命令配置描述信息：

```
description description
```

- **description** - 添加该规则的描述信息。

在SQL内容交换规则模式下，使用**no description**命令删除描述信息。



注意：系统内置两条SQL内容交换规则，实现MYSQL读写操作的分离。若系统中不存在自定义的SQL内容交换规则，或所有内容交换规则均匹配失败且失败动作为“匹配下一条”时，将使用系统内置的SQL内容交换规则。此时，当虚拟服务器中配置了[读/写服务池](#)后，根据内置的SQL内容交换规则，将读/写请求分离并分别分配到读/写服务池，实现读写操作分离。

查看SQL内容交换规则

查看SQL内容交换规则的配置信息，在任何模式下，使用以下命令：

```
show slb sql-content-switch name
```

- *name* - 指定SQL内容交换规则的名称。

配置访问控制规则

通过创建访问控制规则，系统对满足匹配策略的流量进行允许、拒绝、重定向或返回指定页面的操作。配置后，需将访问控制规则绑定到虚拟服务器上，以使其生效。当前版本仅 HTTP、HTTPS 和HTTP代理类型的虚拟服务器支持绑定访问控制规则。

在全局配置模式下，使用以下命令创建访问控制规则：

```
slb acl acl-rule
```

- *acl-rule* - 指定访问控制规则的名称，并进入访问控制配置模式。如果指定的名称已存在，则直接进入访问控制配置模式。

在全局配置模式下，使用以下命令删除访问控制配置：

```
no slb acl acl-rule
```

配置描述信息

在访问控制配置模式下，使用以下命令添加描述信息：

```
description description
```

- *description* - 添加该规则的描述信息。

在配置访问控制模式下，使用**no description** 命令删除描述信息。

配置文本编码方式

在访问控制配置模式下，使用以下命令配置文本编码方式：

```
charset {gb18030 | gb2312 | gbk | utf8}
```

- *gb18030* - 指定以GB18030方式对输入字符串编码。
- *gb2312* - 指定以GB2312方式对输入字符串编码。
- *gbk* - 指定以GBK方式对输入字符串编码。
- *utf8* - 指定以UTF8方式对输入字符串编码。

配置匹配操作符

在访问控制配置模式下，使用以下命令配置匹配操作符：

match operation {and | or}

- **and** - 指定匹配条件的操作符为“与”，表示所有匹配条件都需满足。
- **or** - 指定匹配条件的操作符为“或”，表示只满足一个匹配条件即可。

配置匹配条件

当客户端请求满足此处配置的匹配条件时，设备将执行指定的动作，以对满足匹配条件的请求实现访问控制。在访问控制配置模式下，使用以下命令配置匹配条件：

match [id id] url {contain string | end-with string | equal string | not-contain string | not-end-with string | not-equal string | regex-match string | not-start-with string | not-regex-match string | start-with string}

match [id id] {header header-name | cookie cookie-name | ssl-tls {cipher-name | tlsext-sni}} {contain string | end-with string | equal string | exist | not-contain string | not-end-with string | not-equal string | not-exist | not-regex-match string | not-start-with string | regex-match string | start-with string}

match [id id] ssl-tls protocol {equal {TLSv1 | TLSv1.1 | TLSv1.2 | TLSv1.3 | SSLv2 | SSLv3} | not-equal {TLSv1 | TLSv1.1 | TLSv1.2 | TLSv1.3 | SSLv2 | SSLv3}}

match [id id] ssl-tls client-verify-result-code {equal number | not-equal number}

match [id id] ip-family http {equal { ipv4 | ipv6 | any } | not-equal { ipv4 | ipv6 | any } }

match [id id] http-version {equal { 0.9 | 1.0 | 1.1 | 2.0 } | not-equal { 0.9 | 1.0 | 1.1 | 2.0 } }

match [id id] {dst-ip | dst-port | src-ip | real-src-ip} {equal IP-address | not-equal IP-address | in-range from-IP-address to-IP-address | not-in-range from-IP-address to-IP-address}

match [id id] request-method {equal string [GET | POST | HEAD | PUT | DELETE | OPTIONS | CONNECT] | not-equal string [GET | POST | HEAD | PUT | DELETE | OPTIONS | CONNECT]}

match [id id] x509-cert {cert {exist | not-exist}}

match [id id] x509-cert {issuer-dn | issuer-dn-commonName | issuer-dn-countryName | issuer-dn-emailAddress | issuer-dn-localityName | issuer-dn-organizationalUnit | issuer-dn-organizationName | issuer-dn-stateOrProvince | subject-dn | subject-dn-commonName | subject-dn-countryName | subject-dn-emailAddress | subject-dn-

localityName | subject-dn-organizationalUnit | subject-dn-organizationName | subject-dn-stateOrProvince} {contain *string* | end-with *string* | equal *string* | exist | not-contain *string* | not-end-with *string* | not-equal *string* | not-exist | not-regex-match *string* | not-start-with *string* | regex-match *string* | start-with *string*}

match [id *id*] x509-cert version {equal {1 | 2 | 3} | not-equal {1 | 2 | 3}}

- **id** *id* - 指定匹配条件的ID，范围为1至16。如果不指定ID，系统将自动生成匹配条件的ID。一个规则中最多指定16个匹配条件。当配置多个匹配条件时，各条件间关系为“与”，即多个条件同时满足才能匹配。
- **url** - 指定客户端请求为URL。
- **header** *header-name* - 指定客户端请求的Header名称。
- **cookie** *cookie-name* - 指定客户端请求的Cookie名称。
- **ip-family** - 指定客户端请求的IP协议类型标识。
- **http-version** - 指定客户端请求的HTTP版本。
- **real-src-ip** - 指定客户端请求的真实源IP地址。
- **src-ip** - 指定客户端请求的源IP地址。
- **dst-ip** - 指定客户端请求的目的IP地址。
- **dst-port** - 指定客户端请求的目的端口。
- **request-method** - 指定客户端的请求方法。
- **cert** - 指定匹配项为X509证书。
- **issuer-dn** - 指定匹配项为X509签发者。
- **issuer-dn-commonName** - 指定匹配项为X509证书的签发者名称。
- **issuer-dn-countryName** - 指定匹配项为X509证书签发者的国家。
- **issuer-dn-emailAddress** - 指定匹配项为X509证书签发者的电子邮件。
- **issuer-dn-localityName** - 指定匹配项为X509证书签发者的城市。

- **issuer-dn-organizationalUnit** - 指定匹配项为X509证书签发者的部门。
- **issuer-dn-organizationName** - 指定匹配项为X509证书签发者的公司或机构。
- **issuer-dn-stateOrProvince** - 指定匹配项为X509证书签发者的州或省份。
- **subject-dn** - 指定匹配项为X509证书的主题。
- **subject-dn-commonName** - 指定匹配项为X509证书的主题名称。
- **subject-dn-countryName** - 指定匹配项为X509证书主题的国家。
- **subject-dn-emailAddress** - 指定匹配项为X509证书主题的电子邮件。
- **subject-dn-localityName** - 指定匹配项为X509证书主题的城市。
- **subject-dn-organizationName** - 指定匹配项为X509证书主题的公司或机构。
- **subject-dn-organizationalUnit** - 指定匹配项为X509证书主题的主题。
- **subject-dn-stateOrProvince** - 指定匹配项为X509证书主题的州或省份。
- **version** - 指定匹配项为X509证书版本。
- **contain *string*** - 当客户端请求包含指定字符时，满足匹配条件。
- **not-contain *string*** - 当客户端请求中不包含指定字符时，满足匹配条件。
- **equal *string*** - 当客户端请求等于指定字符时，满足匹配条件。
- **end-with** - 当客户端请求以指定字符结尾时，满足匹配条件。
- **not-end-with** - 当客户端请求不以指定字符结尾时，满足匹配条件。
- **start-with** - 当客户端请求以指定字符开始时，满足匹配条件。
- **not-start-with** - 当客户端请求不以指定字符开始时，满足匹配条件。
- **not-equal *string*** - 当客户端请求不等于指定字符时，满足匹配条件。
- **regex-match *string*** - 当客户端请求符合正则表达式，满足匹配条件。

- **not-regex-match** *string* - 当客户端请求不符合正则表达式，满足匹配条件。
- **exist** *string* - 当客户端请求存在指定字符时，满足匹配条件。
- **not-exist** *string* - 当客户端请求不存在指定字符时，满足匹配条件。
- **in-range** - 当客户端请求的IP地址在指定区间时，满足匹配条件。
- **not-in-range** - 当客户端请求的IP地址不在指定区间时，满足匹配条件。

配置匹配条件区分大小写

用户可根据需要，配置匹配条件区分大小写。在访问控制配置模式下，使用以下命令配置匹配条件是否区分大小写：

- 配置匹配条件区分大小写：**match case-sensitive**
- 配置匹配条件不区分大小写：**match case-insensitive**

配置访问控制动作

系统将对满足匹配条件的请求执行指定的动作。在访问控制配置模式下，使用以下命令配置动作：

action {deny | permit}

action redirect *url-address* [status-code {301 | 302 | 303 | 307 | 308}]

action response {message *string* [status-code *code-num*] | page {200-en.html | 200-zn.html | 301-en.html | 301-zn.html | 302-en.html | 302-zn.html | 403-en.html | 403-zn.html | 404-en.html | 404-zn.html | 50x-en.html | 50x-zn.html | maintain-en.html | maintain-zn.html | ssl-901-en.html | ssl-901-zn.html | ssl-902-en.html | ssl-902-zn.html | ssl-903-en.html | ssl-903-zn.html | ssl-904-en.html | ssl-904-zn.html | ssl-905-en.html | ssl-905-zn.html | ssl-906-en.html | ssl-906-zn.html} }

- **deny** - 对满足匹配条件的流量进行拒绝操作。
- **permit** - 对满足匹配条件的流量进行允许操作。
- **redirect** *url-address* - 对满足匹配条件的流量进行重定向操作，并指定指向的URL地址。

- **response** - 对满足匹配条件的流量返回指定的页面或消息。
 - **message string** - 指定响应类型为“消息”，并指定返回的消息内容。
 - **page** - 指定响应类型为“页面”，并选择返回的页面内容。
- **status-code** - 指定状态码，需在已有状态码中选择。

配置时间表

在访问控制配置模式下，使用以下命令指定时间表：

schedule name

- **name** - 指定时间表的名字

在访问控制配置模式下，使用**no schedule**命令删除绑定的时间表。

查看访问控制规则

查看访问控制规则的配置信息，在任何模式下，使用以下命令：

show slb acl name

- **name** - 指定访问控制规则的名称。

查看SLB规则状态

配置四层或HTTP内容交换规则后，可在任何模式下，使用**show slb l7-content-switch name**或**show slb l4-content-switch name**命令，查看规则的运行状态。包含以下四种：

- **up**：表示规则状态为“正常”。
- **off-line**：表示规则状态为“离线”。
- **unknown**：表示规则状态为“未知”。
- **manual-resume**：表示规则状态为“手动恢复”。

如果四层或HTTP内容交换规则指定到服务池均衡时，其运行状态与服务池保持一致。如果同时配置了服务池和真实服务，四层或HTTP内容交换规则的状态与真实服务保持一致，即：

- 若所指定的真实服务的运行状态为“正常”，该SLB规则的状态为“正常”。
- 若所指定的真实服务的运行状态为“未知”或“禁用中”，该SLB规则的状态为“未知”。
- 若所指定的真实服务的运行状态为“离线”或“禁用”，该SLB规则的状态为“离线”。

配置客户端SSL模板

设备接收到客户端发送来的HTTPS流量后，将数据进行解密，然后将解密后的数据以明文的方式发送给真实的服务器；同时，设备会将真实服务器发送给客户端的数据进行加密，然后发送给客户端。通过设备对HTTPS流量的加解密，减轻了真实服务器的负担，同时也在一定程度上提高了用户访问服务器的速度。

配置客户端SSL模板后，当用户创建HTTPS类型的虚拟服务器时，可以直接引用该模板，从而实现SSL卸载功能。若ADC设备到真实服务器的数据需要加密时，可以通过[服务端SSL模板页面](#)配置服务端SSL模板，实现ADC设备到真实服务间的数据加密。

创建SSL模板

创建SSL模板，在全局配置模式下，使用以下命令：

slb ssl-profile *name*

- *name* - 指定想要创建的SSL模板的名称，并进入客户端SSL模板配置模式。如果指定的名称已存在，则直接进入SSL模板配置模式。

在全局配置模式下，使用**no slb ssl-profile** *name*命令删除SSL模板。

配置握手超时时间

指定客户端与设备之间SSL握手的超时时间。如果在超时时间内，设备与客户端未完成握手，则断开连接。在客户端SSL模板配置模式下，使用以下命令配置握手超时时间：

handshake-timeout *time*

- *time* - 指定客户端与设备之间SSL握手的超时时间。取值范围是1到3600秒，默认值是60秒。

在客户端SSL模板配置模式下，使用**no handshake-timeout**命令恢复握手超时时间的默认值。

配置加密套件

指定客户端与设备之间数据传输的加密套件。可以选择预定义套件，也可以选择自定义。在客户端SSL模板配置模式下，使用以下命令配置加密套件：

预定义：用户可根据需要选择启用系统预定义的加密套件，支持多选。默认使用预定义加密套件。

cipher cipher {top | before cipher1 | after cipher1} - 启用需要的系统预定义的加密套件。

- **top | before cipher1 | after cipher1** - 启用预定义加密套件并指定位置。**before cipher1**指移动到已启用的预定义加密套件的上方；**after cipher1**指移动到已启用的预定义加密套件的下方；**top**指移动到列表顶端。

使用**no cipher cipher**命令禁用不需要的系统预定义的加密套件。

自定义：用户可启用自定义加密套件功能，启用后可以按照OpenSSL语法自定义加密套件。

cipher-customized {enable | cipher-suite value}

- **enable** - 开启自定义加密套件功能，默认关闭。
- **cipher-suite value** - 指定自定义加密套件的内容，需按照OpenSSL语法进行配置。

使用**no cipher-customized enable**命令禁用自定义加密套件功能，同时启用预定义加密套件功能。

启用服务器加密套件优先

开启服务器加密套件优先功能。若不启用该功能，客户端与设备协商加密套件时，筛出双方共有的加密套件，并从中选择在客户端加密套件列表排序靠前的加密套件；启用该功能后，将改为选择设备加密套件列表排序靠前的加密套件。该功能默认为关闭状态。

cipher-server-prefer enable

调整加密套件顺序

系统支持调整SSL模板中加密套件顺序。开启[服务器加密套件优先](#)功能后，设备与客户端协商加密套件时，优先级由设备的加密套件列表决定，加密套件位置越靠前优先级越高。用户通过调整SSL模板中加密套件的顺序，可以改变加密套件优先级。

在客户端SSL模板配置模式下，使用以下命令配置加密套件顺序：

move cipher cipher1 {top | bottom | before cipher2 | after cipher2}

- **cipher1 top** - 将指定加密套件移至列表顶端。
- **cipher1 bottom** - 将指定加密套件移至列表底部。
- **cipher1 before cipher2** - 将加密套件1移至加密套件2的上方。
- **cipher1 after cipher2** - 将加密套件1移至加密套件2的下方。

配置SSL版本

指定客户端与设备之间数据传输的SSL/TLS协议的版本。用户可根据需要选择一个或多个协议版本。默认支持 TLSv1.0, TLSv1.1, TLSv1.2。

在客户端SSL模板配置模式下，使用以下命令配置SSL版本：

```
ssl-version {SSLv3 | TLSv1 | TLSv1.1 | TLSv1.2 | TLSv1.3}
```

- **SSLv3 | TLSv1 | TLSv1.1 | TLSv1.2 | TLSv1.3** - 指定客户端与设备之间数据传输的SSL/TLS协议的版本。

在客户端SSL模板配置模式下，使用 **no ssl-version {SSLv3 | TLSv1 | TLSv1.1 | TLSv1.2 | TLSv1.3}** 命令删除配置的SSL协议版本。

配置证书链

指定客户端与设备建立SSL连接时所需要的证书链。证书链需提前创建完成，可指定为RSA算法证书链或ECC算法证书链。SSL证书链需包含Web服务器证书和密钥对。证书链的创建方法请参考[证书链](#)章节。

在客户端SSL模板配置模式下，使用以下命令配置证书链：

```
cert-chain value
```

- **value** - 指定客户端与设备建立SSL连接时所需要的证书链。

在客户端SSL模板配置模式下，使用 **no cert-chain value** 命令删除指定的证书链。



注意: 用户可以重复配置上述命令，同时指定RSA算法证书链和ECC算法证书链。

配置基于SSL会话ID的会话复用功能

开启基于SSL会话ID的会话复用功能。开启后，当客户端与服务器第一次建立SSL连接时，通过TLS握手计算出的对称密钥及其他状态信息，将存储在ADC设备的缓存中。当客户端再次发起SSL连接请求（或者断开连接

后再次发起连接请求) 时, ADC设备可继续使用缓存中的密钥及状态信息, 进行数据加解密, 无需重新计算, 从而减少了TLS握手以及证书传输过程中的时间耗费。

在客户端SSL模板配置模式下, 使用以下命令配置基于SSL会话ID的会话复用功能:

```
session-reuse {enable | timeout value}
```

- **enable** - 开启该功能。
- **timeout value** - 指定超时时间。取值范围为300至86400。

在客户端SSL模板配置模式下, 使用**no session-reuse {enable | timeout value}**命令取消配置。

配置基于SSL会话票据的会话复用功能

开启基于SSL会话票据的会话复用功能。开启后, 当客户端与服务器第一次建立SSL连接时, 对称密钥及其他状态信息将不再存储在ADC设备的缓存中, 而是被加密后发送给对应的客户端。当客户端再次发起SSL连接时, 会首先将该加密的密钥等信息传输给ADC设备进行解密。然后, ADC设备将使用该解密后的密钥及其他状态信息与客户端进行SSL连接。

在客户端SSL模板配置模式下, 使用以下命令配置基于SSL会话票据的会话复用功能:

```
session-ticket enable
```

- **enable** - 开启该功能。

在客户端SSL模板配置模式下, 使用**no session-ticket enable**命令取消配置。

配置0RTT功能

使用TLSv1.3协议时, 可以开启0RTT功能。在进行PSK会话恢复时, 允许使用0RTT模式, 减少TLSv1.3握手延迟。

在客户端SSL模板配置模式下, 使用以下命令启用/禁用0RTT功能:

- **ssl-early-data enable** - 启用该功能。
- **no ssl-early-data enable** - 禁用该功能。默认情况下, 系统禁用该功能。

配置国密加密套件

指定国密SSL的加密套件。国密SSL当前支持ECDHE-SM1-SM3、ECC-SM1-SM3、ECDHE-SM4-SM3以及ECC-SM4-SM3加密套件。

在客户端SSL模板配置模式下，使用以下命令添加国密加密套件：

```
gm-cipher {ECDHE-SM1-SM3 | ECC-SM1-SM3 | ECDHE-SM4-SM3 | ECC-SM4-SM3} [before cipher | after cipher | top]
```

- **ECDHE-SM1-SM3 | ECC-SM1-SM3 | ECDHE-SM4-SM3 | ECC-SM4-SM3** - 添加使用的国密SSL加密套件。默认使用ECC-SM4-SM3。
- **before cipher | after cipher | top** - 指定添加的国密SSL加密套件的位置，默认添加到列表底部。**before cipher**指添加到已有的国密SSL加密套件的上方；**after cipher**指添加到已有的国密SSL加密套件的下方；**top**指添加到列表顶端。

重复使用上述命令添加多个国密SSL加密套件。

在客户端SSL模板配置模式下，使用**no gm-cipher { ECDHE-SM1-SM3 | ECC-SM1-SM3 | ECDHE-SM4-SM3 | ECC-SM4-SM3}**删除已添加的国密加密套件。



注意：

- 若配置SM1类型的套件，设备需要有国密加密卡。目前，仅SG-6000-AX120S-GM和SG-6000-AX320S-GM设备支持国密加密卡。
- 若配置ECDHE类型的套件，设备需配置国密证书链，客户端需配置加密SM2证书以及签名SM2证书。

调整国密加密套件顺序

系统支持调整SSL模板中国密加密套件顺序。开启[服务器加密套件优先](#)功能后，设备与客户端协商国密加密套件时，优先级由设备的国密加密套件列表决定，国密加密套件位置越靠前优先级越高。用户通过调整SSL模板中国密加密套件的顺序，可以改变国密加密套件优先级。

在客户端SSL模板配置模式下，使用以下命令配置国密加密套件顺序：

```
move gm-cipher cipher1 {top | bottom | before cipher2 | after cipher2}
```

- **cipher1 top** - 将指定国密加密套件移至列表顶端。
- **cipher1 bottom** - 将指定国密加密套件移至列表底部。
- **cipher1 before cipher2** - 将国密加密套件1移至国密加密套件2的上方。
- **cipher1 after cipher2** - 将国密加密套件1移至国密加密套件2的下方。

配置国密签名证书链

指定国密签名证书链。国密签名证书链需提前创建完成。证书链的创建方法请参考[证书链](#)章节。

在客户端SSL模板配置模式下，使用以下命令配置国密签名证书链：

```
gm-cert-chain value
```

- *value* - 指定国密签名证书链的名称。

在客户端SSL模板配置模式下，使用`no gm-cert-chain` 命令删除指定的证书链。

配置国密加密证书链

指定国密SSL的加密证书链。国密加密证书链需提前创建完成。证书链的创建方法请参考[证书链](#)章节。

在客户端SSL模板配置模式下，使用以下命令配置国密加密证书链：

```
gm-enc-cert-chain value
```

- *value* - 指定国密加密证书链。

在客户端SSL模板配置模式下，使用`no gm-enc-cert-chain` 命令删除指定的证书链。

SSL客户端验证

当客户端建立SSL连接访问服务器时，系统支持对客户端的SSL证书进行验证，用户可按需设置验证的方式、需验证的证书内容以及验证后的处理动作等。验证完成后，系统再将连接请求转发给真实的服务器。

指定对客户端验证的方式

指定对客户端验证的方式，在客户端SSL模板配置模式下，使用以下命令配置：

```
verify { disable | optional | required }
```

- **disable** - 指定对客户端验证的方式为禁用，表示当SSL连接建立时，客户端不需提供SSL证书进行验证。
- **optional** - 指定对客户端验证的方式为可选，表示当SSL连接建立时，客户端可以不提供SSL证书，若客户端提供，系统就进行验证。
- **required** - 指定对客户端验证的方式为强制，表示当SSL连接建立时，系统将对所有的客户端进行SSL证书验证。

指定需验证的CA证书

指定需验证的客户端CA证书或证书链，可以指定一个或多个，在客户端SSL模板配置模式下，使用以下命令配置：

```
verify-ca cert-name
```

在客户端SSL模板配置模式下，使用**no verify-ca** *cert-name*命令删除CA证书，系统将不再对客户端进行该证书或证书链的验证。

自动CA证书通告

用户可开启自动CA证书通告功能。开启后，系统将把所有要验证的CA证书的相关信息发给客户端进行通告。若不开启自动CA证书通告，可指定“CA证书通告”进行通告。开启自动CA证书通告，在客户端SSL模板配置模式下，使用以下命令配置：

```
verify-advertised-auto
```

在客户端SSL模板配置模式下，使用**no verify-advertised-auto** 命令关闭自动CA证书通告功能。

指定需通告的CA证书

用户可指定需进行通告的CA证书或证书链，可以指定一个或多个。指定后，系统会将指定CA证书通告给客户端，在客户端SSL模板配置模式下，使用以下命令配置：

```
verify-advertised cert-name
```

在客户端SSL模板配置模式下，使用**no verify-advertised** *cert-name*命令删除指定CA证书或证书链通告。

配置验证证书最小密钥长度

指定客户端证书的RSA和ECC最小密钥长度的限制，默认不限制。当客户端密钥长度小于指定长度时，将验证失败，然后系统将按照证书失败的规则进行处理。配置验证证书最小密钥长度，在客户端SSL模板配置模式下，使用以下命令配置：

```
verify-safe-key { rsa { 512 | 1024 | 2048 | 3072 | 4096 | 7680 } | ecc { 256 | 384 | 521 } }
```

在客户端SSL模板配置模式下，使用**no verify-safe-key** {*rsa* | *ecc*} 命令删除客户端验证证书的最小密钥长度限制。

配置客户端验证的证书最大深度

配置客户端验证的CA证书最大深度，在客户端SSL模板配置模式下，使用以下命令配置：

verify-depth *value*

- *value* - 指定允许的客户端证书的最终根CA的最大深度。取值范围为1-32，默认为9级。当客户端证书的证书深度超过配置的深度时，验证客户端证书会失败。

在客户端SSL模板配置模式下，使用**no verify-depth** 命令取消CA证书最大深度的设置，恢复默认值。

配置客户端验证规则

用户可针对客户端证书的验证结果配置对应的系统处理动作。系统预置了10种不同的客户端验证结果且每种结果都设置了默认处理动作。若不另行配置，系统将按照默认动作进行处理。用户也可按需更改某验证结果的处理动作，生成新的规则。系统将按照新设置的规则，处理该验证结果。

在客户端SSL模板配置模式下，使用以下命令配置匹配条件：

verify-rule { **default** | **cert-chain-too-long** | **cert-has-expired** | **cert-key-unsafe** | **cert-not-yet-valid** | **cert-revoked** | **no-cert** | **ocsp-cert-good** | **ocsp-cert-unknown** | **ocsp-verify-failed** | **result-code** *value* } **action** { **deny** | **permit** | **redirect** *URL* | **response** { **message** *string* | **page** *page-name* } [**status-code** *value*] }

- **default** | **cert-chain-too-long** | **cert-has-expired** | **cert-key-unsafe** | **cert-not-yet-valid** | **cert-revoked** | **no-cert** | **result-code** - 指定需修改的客户端验证结果。**default** 为所有验证结果的默认处理方式，默认为拒绝请求，用户可按需修改为其他处理动作。验证结果共分为以下十种：**cert-chain-too-long** 表示证书链过长；**cert-has-expired** 表示证书链过期；**cert-key-unsafe** 表示证书链密钥不安全；**cert-not-yet-valid** 表示证书链无效；**cert-revoked** 表示证书链已被吊销；**no-cert** 表示无客户端证书；**ocsp-cert-good** 表示OCSP证书状态正常；**ocsp-cert-unknown** 表示OCSP证书状态未知；**ocsp-verify-failed** 表示OCSP验证响应签名失败；**result-code** 表示其他用户自定义的返回码。
- **deny** - 指定客户端验证规则的处理动作为拒绝。系统将拒绝客户端的SSL连接请求。
- **permit** - 指定客户端验证规则的处理动作为允许。系统将允许客户端的SSL连接请求。
- **redirect** *URL* - 指定客户端验证规则的处理动作为重定向，并指定重定向的URL地址。系统会将客户端的SSL连接请求重新定向到指定的URL。

- **response** { **message** *string* | **page** *page-name* } - 指定客户端验证规则的处理动作为响应，并设置响应的信息（**message**）或网页（**page**）。系统会将客户端的SSL连接请求进行特定信息或特定页面的响应。
- **status-code** *value* - 指定重定向或响应的状态码。

在客户端SSL模板配置模式下，使用 **no verify-rule** { **cert-chain-too-long** | **cert-has-expired** | **cert-key-unsafe** | **cert-not-yet-valid** | **cert-revoked** | **no-cert** | **ocsp-cert-good** | **ocsp-cert-unknown** | **ocsp-verify-failed** | *result-code* } 命令删除指定的客户端验证匹配规则。

配置URL验证匹配规则

系统支持对特定的URL进行客户端验证，当客户端访问指定URL时，系统将按照该URL验证匹配规则对客户端进行可选或强制验证处理；而对于未指定的URL，被访问时将继续按照客户端验证设置的“验证方式”进行处理。

在客户端SSL模板配置模式下，使用以下命令配置匹配条件：

verify-url { **contain** *value* | **not-contain** *value* | **equal** *value* | **not-equal** *value* | **regex-match** *value* | **not-regex-match** *value* | **end-with** *value* | **not-end-with** *value* | **start-with** *value* | **not-start-with** *value* } [*id*] [**case-sensitive** | **case-insensitive**] [**before** *id* | **after** *id* | **top** | **bottom**]

- **contain** *value* - 当客户端请求包含指定字符时，满足匹配条件。
- **not-contain** *value* - 当客户端请求中不包含指定字符时，满足匹配条件。
- **equal** *value* - 当客户端请求的URL等于指定URL时，满足匹配条件。
- **not-equal** *value* - 当客户端请求的URL不等于指定URL时，满足匹配条件。
- **regex-match** *value* - 当客户端请求的URL符合正则表达式，满足匹配条件。
- **not-regex-match** *value* - 当客户端请求的URL不符合正则表达式，满足匹配条件。
- **end-with** - 当客户端请求的URL以指定字符结尾时，满足匹配条件。
- **not-end-with** - 当客户端请求的URL不以指定字符结尾时，满足匹配条件。
- **start-with** *value* - 当客户端请求的URL以指定字符开头时，满足匹配条件。
- **not-start-with** *value* - 当客户端请求的URL不以指定字符开头时，满足匹配条件。

- **case-sensitive** - 系统将对客户端请求的URL进行区分大小写验证。
- **case-insensitive** - 系统将对客户端请求的URL进行不区分大小写验证。
- **before id | after id | top | bottom** - 指定URL验证匹配规则的位置。默认情况下，系统会将新创建的规则放到所有规则的末尾。
 - **before id** - 指定规则的位置为某个规则ID或者名称之前。
 - **after id** - 指定URL验证规则的位置为某个规则ID或者名称之后。
 - **top** - 指定URL验证规则的位置为所有规则的首位。
 - **bottom** - 指定URL验证规则的位置为所有规则的末位。

在客户端SSL模板配置模式下，使用 **no verify-url id** 命令删除指定的URL验证匹配规则。

配置客户端证书的OCSP验证

为了验证客户端证书的有效性，设备支持配置OCSP（Online Certificate Status Protocol）功能，即在线证书状态协议。OCSP和CRL都是用来查询CA证书状态的主要方式。与下载CRL文件相比，OCSP功能是由ADC设备向OCSP服务器发送OCSP请求，实时查询某个或某些客户端证书的吊销状态。设备收到OCSP响应后，从中获取客户端证书状态，进而处理客户端的访问请求。通过OCSP的方式验证客户端证书的吊销状态，可以减少网络负担、节约网络资源。

在客户端SSL模板配置模式下，使用以下命令配置OCSP功能：

```
ocsp {enable | verify enable | request-method {GET | POST} | responder-url url | request-timeout value | cache enable | cache-timeout value}
```

- **enable** - 开启OCSP功能。
使用 **no ocsp enable** 命令关闭OCSP功能。
- **verify enable** - 开启验证OCSP响应功能。开启该功能后，系统将验证OCSP响应的签名。若验证成功，系统获取OCSP响应中客户端证书的验证结果，并执行对应的处理动作；若验证失败，且配置了客户端证书验证结果为“OCSP验证响应签名失败”时的处理动作，系统就按照该动作进行处理，否则按照默认动作进行处理。

说明：若不开启该功能，系统直接获取OCSP响应中客户端证书的验证结果，并执行对应的处理动作。

使用 **no ocsp verify enable** 命令关闭验证OCSP响应。

- **request-method {GET | POST}** - 指定设备发送OCSP请求的请求方法，默认使用GET方法。
使用**no obsp request-method**命令恢复默认值。
- **responder-url url** - 指定OCSP服务器的URL地址，以“http://”开头。当发生以下情况时，系统将判定客户端证书验证结果为“OCSP证书状态未知”，然后按照“客户端验证规则”的配置，进行处理：
 - 设备连接OCSP服务器超时。
 - 设备解析OCSP服务器URL失败。
 - 未配置OCSP服务器地址，且系统无法从客户端证书中获取OCSP服务器地址。

使用 **no obsp responder-url**命令删除指定的OCSP服务器地址。

- **request-timeout value** - 指定设备与OCSP服务器建立连接的超时时间。超过该时间，设备将断开与OCSP服务器的连接。取值范围是3到10秒，默认值是5秒。

使用**no obsp request-timeout**命令恢复默认值。

- **cache enable** - 开启OCSP缓存功能。开启该功能后，系统根据获取到的OCSP响应，将客户端证书状态存储在ADC设备缓存中。当新的客户端请求到达时，系统可直接在缓存中查询客户端证书的吊销状态。若查询不到该客户端证书的状态，系统向OCSP服务器发送OCSP请求进行查询，并将查询结果存储在ADC设备缓存中。用户可以手动清除设备缓存中的OCSP缓存，具体方法参照[清除OCSP缓存](#)。

使用**no obsp cache enable**命令关闭OCSP缓存功能。

- **cache-timeout value** - 指定设备保留OCSP缓存的超时时间。超过该时间，系统将清除缓存中相应的客户端证书状态。取值范围是300到604800秒，默认值是86400秒。

使用**no obsp cache-timeout**命令恢复默认值。

清除OCSP缓存

开启OCSP功能后，对于存储在设备中的客户端证书状态信息，用户可以根据需要进行清除。清除设备的OCSP缓存，在任何模式下，使用以下命令：

- **clear slb obsp cache** - 清除所有的客户端证书状态信息。
- **clear slb obsp cache ssl-profile-name name** - 清除指定客户端SSL模板对应的客户端证书状态。

配置OCSP Stapling

设备支持配置OCSP Stapling功能，以满足客户端浏览器开启OCSP Stapling的需求。当客户端与虚拟服务器第一次TLS握手时，设备会发送OCSP请求，查询虚拟服务器证书的状态；设备将从OCSP响应中获取虚拟服务器证书的状态信息，与虚拟服务器证书一起返回给客户端。根据虚拟服务器的证书状态信息，客户端浏览器结合自身策略，选择是否继续访问。

在客户端SSL模板配置模式下，使用以下命令配置OCSP Stapling功能：

```
ocsp-stapling {enable | cert-issuer cert-name | verify {enable | cert cert-name} | request-method {GET | POST} | responder-url url | request-timeout value | cache-timeout {good | others} value | response-all-status enable}
```

- **enable** - 开启OCSP Stapling功能。

使用**no ocsp-stapling enable**命令关闭OCSP Stapling功能。

- **cert-issuer cert-name** - 指定虚拟服务器证书的颁发者证书。若客户端与设备建立SSL连接时指定的RSA/ECC证书链，包含颁发者证书信息，可以不配置该项；若客户端与设备建立SSL连接时指定的RSA/ECC证书链，不包含颁发者证书信息，用户需要配置相应的颁发者证书。系统最多支持配置2个颁发者证书。证书链需提前在“PKI >证书链”创建完成。证书链的创建方法请参考[证书链](#)章节。

使用**no ocsp-stapling cert-issuer**命令删除指定的颁发者证书。

- **verify {enable | cert cert-name}** - 配置验证OCSP响应功能。

- **enable** - 开启验证OCSP响应。开启该功能后，系统将验证OCSP响应的签名。若响应验证失败，客户端浏览器将收不到虚拟服务器的证书状态验证结果；若不开启该功能，系统将直接获取OCSP响应中虚拟服务器证书的状态，返回给客户端。

使用**no ocsp-stapling verify enable**命令关闭验证OCSP响应。

- **cert cert-name** - 指定验证OCSP响应的CA证书。系统最多支持配置2个CA证书。证书链需提前在“PKI >证书链”创建完成。证书链的创建方法请参考[证书链](#)章节。

使用**no ocsp-stapling verify cert**命令删除指定的CA证书。

- **request-method {GET | POST}** - 指定设备发送OCSP请求的请求方法，默认使用GET方法。

使用**no ocsp-stapling request-method**命令恢复默认值。

- **responder-url url** - 指定OCSP服务器的URL地址，以“http://”开头。当发生以下情况时，客户端浏览器将收不到虚拟服务器的证书状态验证结果：

- 设备连接OCSP服务器超时。
- 设备解析OCSP服务器URL失败。
- 未配置OCSP服务器地址，且系统无法从客户端证书中获取OCSP服务器地址。

使用`no ocsdp-stapling responder-url`命令删除指定的OCSP服务器地址。

- **request-timeout value** - 指定设备与OCSP服务器建立连接的超时时间。超过该时间，设备将断开与OCSP服务器的连接。取值范围是3到10秒，默认值是5秒。

使用`no ocsdp-stapling request-timeout`命令恢复默认值。

- **cache-timeout {good | others} value** - 指定设备保留虚拟服务器证书状态的超时时间。超过该时间，系统将清除缓存中相应虚拟服务器的证书状态。

- **good value** - 当设备从OCSP响应中获取到虚拟服务器证书状态正常时，指定保留该状态的超时时间。取值范围是300到604800秒，默认值是86400秒。

- **others value** - 当设备从OCSP响应中获取到虚拟服务器证书状态不为“good”时，指定保留该状态的超时时间。取值范围是300到604800秒，默认值是86400秒。

使用`no ocsdp-stapling cache-timeout {good | others}`命令恢复默认值。

- **response-all-status enable** - 开启响应所有状态。开启后，无论验证的虚拟服务器证书是什么状态，系统都将验证结果返回给客户端；若不开启，系统只将虚拟服务器证书状态为“good”的结果，返回给客户端。

使用`no ocsdp-stapling response-all-status enable`命令关闭响应所有状态。

查看SSL模板配置

在任何模式下，使用以下命令查看SSL模板的配置信息：

```
show slb ssl-profile [name]
```

- *name* - 查看指定模板的具体配置信息。

配置服务端SSL模板

配置服务端SSL模板，ADC设备可对来自客户端的数据进行加密，并将加密后的数据分配到具有SSL功能的真实服务上。配置服务端SSL模板后，当用户创建HTTP或HTTPS类型的虚拟服务器时，可以直接引用该模板，

实现设备与真实服务的HTTPS连接。

创建服务端SSL模板

系统提供一个预定义的服务端SSL模板“default-server-ssl-profile”。该预定义的服务端SSL模板不允许被编辑或删除。

创建服务端SSL模板，在全局配置模式下，使用以下命令：

```
slb server-ssl-profile name type {ssl-tls | gmssl | ssl-tls-gmssl}
```

- *name* - 指定想要创建的服务端SSL模板的名称，并进入SSL模板配置模式。如果指定的名称已存在，则直接进入SSL模板配置模式。
- type {ssl-tls | gmssl | ssl-tls-gmssl} - 指定服务端SSL模板的类型，SSL/TLS类型、国密SSL类型、SSL/TLS/国密类型。若不指定，则为默认的SSL/TLS类型。

在全局配置模式下，使用`no slb server-ssl-profile name`命令删除服务端SSL模板。

配置握手超时时间

指定设备与真实服务之间SSL握手的超时时间。如果在超时时间内，设备与真实服务未完成握手，则断开连接。在服务端SSL模板配置模式下，使用以下命令配置握手超时时间：

```
handshake-timeout time
```

- *time* - 指定设备与真实服务之间SSL握手的超时时间。取值范围是1到3600秒，默认值是60秒。

在服务端SSL模板配置模式下，使用`no handshake-timeout`命令恢复握手超时时间的默认值。

启用SNI功能

启用SNI功能后，当设备转发客户端请求至真实服务时，若真实服务的IP/端口相同、域名不同，通过域名访问时，客户端请求将携带SNI字段，服务器根据SNI字段去响应对应的服务证书。在服务端SSL模板配置模式下，使用以下命令启用/禁用SNI功能：

- **sni enable** - 启用该功能。默认情况下，系统启用该功能。
- **no sni enable** - 禁用该功能。

配置加密套件

指定服务端与设备之间数据传输的加密套件。可以选择预定义套件，也可以选择自定义。在服务端SSL模板配置模式下，使用以下命令配置加密套件：

预定义：用户可根据需要选择启用系统预定义的加密套件，支持多选。默认使用预定义加密套件。

cipher cipher {top | before cipher1 | after cipher1} - 启用需要的系统预定义的加密套件。

- **top | before cipher1 | after cipher1** - 启用预定义加密套件并指定位置。**before cipher1**指移动到已启用的预定义加密套件的上方；**after cipher1**指移动到已启用的预定义加密套件的下方；**top**指移动到列表顶端。

使用**no cipher cipher**命令禁用不需要的系统预定义的加密套件。

自定义：用户可按照OpenSSL语法自定义加密套件。

cipher-customized {enable | cipher-suite value}

- **enable** - 开启自定义加密套件功能，默认关闭。
- **cipher-suite value** - 指定自定义加密套件的内容，需按照OpenSSL语法进行配置。

使用**no cipher-customized enable**命令禁用自定义加密套件功能并启用预定义加密套件功能。

调整加密套件顺序

在服务端与设备协商加密套件时，选择服务端和设备共有加密套件中，在服务端加密套件列表排序靠前的加密套件。用户可调整SSL模板中加密套件顺序。

在SSL模板配置模式下，使用以下命令配置加密套件顺序：

move cipher cipher1 {top | bottom | before cipher2 | after cipher2}

- **cipher1 top** - 将指定加密套件移至列表顶端。
- **cipher1 bottom** - 将指定加密套件移至列表底部。
- **cipher1 before cipher2** - 将加密套件1移至加密套件2的上方。
- **cipher1 after cipher2** - 将加密套件1移至加密套件2的下方。

配置SSL版本

指定服务端与设备之间数据传输的SSL/TLS协议的版本。用户可根据需要选择一个或多个协议版本。默认支持TLSv1.0, TLSv1.1, TLSv1.2。在服务端SSL模板配置模式下, 使用以下命令配置SSL版本:

```
ssl-version {SSLv3 | TLSv1 | TLSv1.1 | TLSv1.2 | TLSv1.3}
```

- **SSLv3 | TLSv1 | TLSv1.1 | TLSv1.2 | TLSv1.3** - 指定服务端与设备之间数据传输的SSL/TLS协议的版本。

在服务端SSL模板配置模式下, 使用**no ssl-version {SSLv3 | TLSv1 | TLSv1.1 | TLSv1.2 | TLSv1.3}**命令删除配置的SSL版本。

配置证书链

指定服务端与设备建立SSL连接时所需要的证书链。证书链需提前创建完成, 可指定为RSA算法证书链或ECC算法证书链。SSL证书链需包含Web服务器证书和密钥对。证书链的创建方法请参考[证书链](#)章节。

在服务端SSL模板配置模式下, 使用以下命令配置证书链:

```
cert-chain value
```

- **value** - 指定服务端与设备建立SSL连接时所需要的证书链。

在服务端SSL模板配置模式下, 使用**no cert-chain value**命令删除指定的证书链。



注意: 用户可以重复配置上述命令, 同时指定RSA算法证书链和ECC算法证书链。

配置国密加密套件

指定国密SSL的加密套件。国密SSL当前支持ECDHE-SM1-SM3、ECC-SM1-SM3、ECDHE-SM4-SM3以及ECC-SM4-SM3加密套件。

在服务端SSL模板配置模式下, 使用以下命令添加国密加密套件:

```
gm-cipher {ECDHE-SM1-SM3 | ECC-SM1-SM3 | ECDHE-SM4-SM3 | ECC-SM4-SM3} [before cipher | after cipher | top]
```

- **ECDHE-SM1-SM3 | ECC-SM1-SM3 | ECDHE-SM4-SM3 | ECC-SM4-SM3** - 添加使用的国密SSL加密套件。默认使用ECC-SM4-SM3。

- **before cipher** | **after cipher** | **top** - 指定添加的加密套件的位置，默认添加到列表底部。**before cipher**指添加到已有的加密套件的上方；**after cipher**指添加到已有的加密套件的下方；**top**指添加到列表顶端。

重复使用上述命令添加多个国密SSL加密套件。

在服务端SSL模板配置模式下，使用**no gm-cipher { ECDHE-SM1-SM3 | ECC-SM1-SM3 | ECDHE-SM4-SM3 | ECC-SM4-SM3 }**删除已添加的加密套件。



注意:

- 若配置SM1类型的套件，设备需要有国密加密卡。目前，仅SG-6000-AX120S-GM和SG-6000-AX320S-GM设备支持国密加密卡。
- 若配置ECDHE类型的套件，设备需配置国密证书链，服务器端需配置加密SM2证书以及签名SM2证书。

调整国密加密套件顺序

在服务端与设备协商国密加密套件时，选择服务端和设备共有国密加密套件中，在服务端国密加密套件列表排序靠前的加密套件。用户可调整SSL模板中国密加密套件顺序。

在服务端SSL模板配置模式下，使用以下命令配置国密加密套件顺序：

move gm-cipher cipher1 {top | bottom | before cipher2 | after cipher2}

- **cipher1 top** - 将指定国密加密套件移至列表顶端。
- **cipher1 bottom** - 将指定国密加密套件移至列表底部。
- **cipher1 before cipher2** - 将国密加密套件1移至国密加密套件2的上方。
- **cipher1 after cipher2** - 将国密加密套件1移至国密加密套件2的下方。

配置国密签名证书链

当SSL模板为国密SSL类型或SSL/TLS/国密类型时，需指定国密签名证书链。国密签名证书链需提前创建完成。证书链的创建方法请参考[证书链](#)章节。

在服务端SSL模板配置模式下，使用以下命令配置国密签名证书链：

gm-cert-chain value

- *value* - 指定国密签名证书链的名称。

在服务端SSL模板配置模式下，使用`no gm-cert-chain` 命令删除指定的证书链。

配置国密加密证书链

当SSL模板为国密SSL类型或SSL/TLS/国密类型时，需指定国密SSL的加密证书链。国密加密证书链需提前创建完成。证书链的创建方法请参考[证书链](#)章节。

在SSL模板配置模式下，使用以下命令配置国密加密证书链：

```
gm-enc-cert-chain value
```

- *value* - 指定国密加密证书链。

在SSL模板配置模式下，使用`no gm-enc-cert-chain`命令删除指定的证书链。

查看SSL模板配置

在任何模式下，使用以下命令查看服务端SSL模板的配置信息：

```
show slb server-ssl-profile [name]
```

- *name* - 查看指定模板的具体配置信息。

SSL加速卡

SSL加速卡利用专门的硬件加速卡，进行SSL通讯过程中需要的加解密操作，从而减轻CPU的负担，提高系统整体的SSL处理能力。目前，SG-6000-AX1000S/SG-6000-AX2000S/SG-6000-AX4060S/SG-6000-AX6060S支持nitrox加速卡，nitrox加速卡支持SSLv3，TLSv1.0，TLSv1.1，TLSv1.2，TLSv1.3协议；SG-6000-AX120S/SG-6000-AX120S-GM/SG-6000-AX220S/SG-6000-AX320S/SG-6000-AX320S-GM/SG-6000-AX520S/SG-6000-AX1200S/AX-6000-AX3200S支持QAT加速，QAT加速卡支持SSLv3，TLSv1.0，TLSv1.1，TLSv1.2，TLSv1.3协议。

SSL加速卡相关命令

查看加速卡统计数据

在任何模式下,使用以下命令查看加速卡的统计数据。（目前仅支持查看SSL中Record协议相关的统计数据。）

show ssl-hardware statistics

SG-6000-AX1000S/SG-6000-AX2000S/SG-6000-AX4060S/SG-6000-AX6060S设备的SSL加速卡统计数据示例:

```
hostname# show ssl-hardware statistics

Encrypt : 180765

Decrypt : 76518

Encrypt IN Bytes : 2178310307

Encrypt OUT Bytes : 2174050298

Decrypt IN Bytes : 70211572

Decrypt OUT Bytes : 67150740
```

SG-6000-AX120S/SG-6000-AX120S-GM/SG-6000-AX220S/SG-6000-AX320S/SG-6000-AX320S-GM/SG-6000-AX520S/SG-6000-AX1200S/AX-6000-AX3200S设备的SSL加速卡统计数据示例:

```
hostname# show ssl-hardware statistics

+-----+
| FW Statistics for Qat Device                               |
+-----+
| Firmware Requests [AE 0]:                                1 |
| Firmware Responses[AE 0]:                                1 |
+-----+
| Firmware Requests [AE 1]:                                0 |
| Firmware Responses[AE 1]:                                0 |
+-----+
| Firmware Requests [AE 2]:                                0 |
| Firmware Responses[AE 2]:                                0 |
+-----+
| Firmware Requests [AE 3]:                                1 |
| Firmware Responses[AE 3]:                                1 |
```

```

+-----+
| Firmware Requests [AE 4]:                                0 |
| Firmware Responses[AE 4]:                                0 |
+-----+
| Firmware Requests [AE 5]:                                0 |
| Firmware Responses[AE 5]:                                0 |
+-----+

SM1 encrypt counter : 3
SM1 encrypt bytes : 544
SM1 decrypt counter : 5
SM1 decrypt bytes : 176

```

清除加速卡统计数据

在任何模式下,使用以下命令清除加速卡的统计数据。

```
clear ssl-hardware statistics
```

测试加速卡功能

SG-6000-AX1000S/SG-6000-AX2000S/SG-6000-AX4060S/SG-6000-AX6060S设备支持测试SSL硬件加速卡的功能。在执行模式下,使用以下命令测试加速卡的功能,如测试加解密功能。

```
exec ssl-hardware check { 3des | aes | hash }
```

- **3des** - 测试加速卡的3DES加密功能是否正常。
- **aes** - 测试加速卡的AES加密功能是否正常。
- **hash** - 测试加速卡的哈希功能是否正常。

示例:

```
hostname# exec ssl-hardware check 3des:
```

```
3DES: Devices detected: 1

dma mode: DIRECT Mode

Starting on device: 0

Encrypting data

Decrypting data

Comparing decrypted data with original

Device id: 0 - SUCCESS
```

说明:

如上, 返回SUCCESS即表明测试成功。对于不支持SSL加速卡的平台, 将返回“NO SUPPORT SSL ACCELERATE DEVICE”。如果返回“3DES_TEST: Failed to open device file”表明设备初始化错误。请重新执行 `show ssl-hardware version` 命令, 获取运行状态。

查看加速卡的驱动版本号

在任何模式下, 使用以下命令查看加速卡的驱动版本号。

show ssl-hardware version

示例:

```
hostname# show ssl-hardware version

Version : 1.1-04
```

说明:

如上, 返回SSL加速卡的驱动版本号。

查看加速卡以及国密卡状态

查看SSL加速卡、国密卡的状态, 在任何模式下, 使用以下命令:

show ssl-hardware status

示例:

```
hostname# show ssl-hardware status
```

SSL hardware device : exist

(“exist”表明设备安装了硬件加速卡。如果返回“no exist”表明设备未安装硬件加速卡。)

SSL hardware driver : load

(“load”表明SSL硬件加速卡已加载成功。如果返回“no load”表明SSL硬件加速卡加载失败。)

SSL hardware running mode : hardware

(“hardware”表明设备当前使用SSL硬件加速卡进行加速。如果返回“software”表明设备当前为SSL软件加速模式。)

Next SSL mode : hardware

(“hardware”表明配置SSL加速模式为硬件加速模式，即设备重启后将使用SSL硬件加速卡进行SSL加速。如果返回“software”表明配置SSL加速模式为软件加速模式。)

Gm card device : exit

(“exist”表明设备安装了国密卡。如果返回“no exist”表明设备未安装国密卡。)

Gm card driver : no load

(“no load”表明国密卡加载失败。如果返回“load”表明设备的国密卡已加载。)

Gm card running mode : offline

(“offline”表明国密卡状态为“离线”。如果返回“online”表明国密卡状态为“在线”。)

Next Gm card mode : online

(“online”表明设备重启后，国密卡状态为“在线”。如果返回“offline”表明设备重启后，国密卡状态为“离线”。)

切换SSL加速模式

用户可以根据需要，选择不使用SSL硬件加速卡进行SSL加速。在执行模式下，使用以下命令切换SSL加速模式：

exec ssl-hardware mode {software | hardware}

- **software** - 指定SSL加速模式为软件加速模式，即不使用硬件加速卡进行SSL加速。
- **hardware** - 指定SSL加速模式为硬件加速模式，即使用硬件加速卡进行SSL加速。该模式为默认模式。



注意: 切换SSL加速模式，重启后配置才能生效。

配置应用模板

应用模板包含HTTP模板、快速HTTP模板、HTTP代理模板、SSL流代理模板、IMAP模板、POP3模板、SMTP模板和MYSQL模板。

HTTP模板可供用户配置HTTP协议层面的参数。AX支持HTTP 1.0、1.1、2.0协议和WebSocket 协议。配置HTTP协议参数后，由于AX设备部署在HTTP客户端和HTTP服务器之间，即AX设备在数据转发过程中既充当HTTP客户端又充当HTTP服务器端，所以这些参数将影响AX设备在此过程中对HTTP的处理行为。

HTTP模板支持HTTP和HTTPS两种协议类型，HTTP类型的模板只能配置在HTTP类型的虚拟服务器上；HTTPS类型的模板只能配置在HTTPS类型的虚拟服务器上。

快速HTTP模板只能被类型是“快速HTTP”的虚拟服务器引用。HTTP代理模板只能被类型是“HTTP代理”的虚拟服务器引用。流模板只能被类型是“SSL流代理”或“SSL-OVER-TCP”的虚拟服务器引用。IMAP模板只能被类型是“IMAP”的虚拟服务器引用。POP3模板只能被类型是“POP3”的虚拟服务器引用。SMTP模板只能被类型是“SMTP”的虚拟服务器引用。MYSQL模板只能被类型是“MYSQL”的虚拟服务器引用。

创建应用模板

创建应用模板，在全局配置模式下，使用以下命令：

```
slb app-profile profile-name [type {any | http | https | http-proxy | ssl-stream-proxy | fast-http | imap | pop3 | smtp | mysql}]
```

- *profile-name* - 创建应用模板的名称并进入应用模板配置模式。如果指定的名称已存在，则直接进入应用模板配置模式。
- **type {any | http | https | http-proxy | ssl-stream-proxy | fast-http | imap | pop3 | smtp | mysql}** - 指定应用模板的类型。

系统支持将某一应用模板快速克隆，用户只要将克隆的应用模板的部分参数进行修改，即可生成一个新的应用模板。克隆已有的应用模板，在全局配置模式下，使用以下命令：

```
slb app-profile profile-name1 clone-from profile-name2
```

- *profile-name1* - 指定新应用模板的名称。
- *profile-name2* - 指定将被克隆的应用模板的名称。

在全局配置模式下，使用**no slb app-profile *profile-name***命令删除指定的应用模板。

HTTP 2.0协议

当应用模板的协议类型为“HTTPS”时，设备支持HTTP 2.0服务。此时，ADC可以作为HTTP 2.0网关，用于在客户端和服务端之间的HTTP 1.0/1.1和HTTP 2.0协议转换。目前，系统支持HTTP 2.0客户端和HTTP 1.0/1.1服务器的协议转换。

开启HTTP 2.0

开启或禁用HTTP 2.0，在应用模板配置模式，使用以下命令：

- 启用：**http2 enable**
- 禁用：**no http2 enable**

配置空闲连接超时时间

指定空闲连接关闭的超时时间，在应用模板配置模式，使用以下命令：

http2 idle-timeout *value*

- *value* - 指定空闲连接关闭的超时时间。取值范围为1至3600秒，默认值为180秒。

使用该命令**no**的形式恢复默认值。

配置最大并发流

指定每个连接中最大并发流的数量，在应用模板配置模式，使用以下命令：

http2 max concurrent-streams *value*

- *value* - 指定每个连接中最大并发流的数量。取值范围为1至256，默认值为128。

使用该命令**no**的形式恢复默认值。

配置接收窗口大小

指定接收窗口的大小，在应用模板配置模式，使用以下命令：

http2 receive-window-size *value*

- *value*-指定接收窗口的大小。取值范围为1至4096K，默认值为64K。

使用该命令no的形式恢复默认值。

配置数据帧大小

指定发送到客户端的数据帧大小，在应用模板配置模式，使用以下命令：

http2 frame-size *value*

- *value*-指定发送到客户端的数据帧大小。取值范围为1至16384，默认值为8192。

使用该命令no的形式恢复默认值。

配置标题表大小

指定请求标头字段的大小，在应用模板配置模式，使用以下命令：

http2 max-table-size *value*

- *value*-指定请求标头字段的大小。取值范围为1至16384，默认值为4096。

使用该命令no的形式恢复默认值。

插入标题X-HTTP2

插入标题X-HTTP2，在应用模板配置模式，使用以下命令：

http2 x-http2 {on | off}

- on - 开启该功能。系统将Header信息发送到源Web服务。
- off - 关闭该功能。

配置网页优化

当应用模板的协议类型为“HTTP”或“HTTPS”时，设备支持网页优化功能。当客户端访问的服务器资源路径没有匹配上用户指定的资源路径时，真实服务返回给客户端的响应页面到达设备后，ADC设备可以对网页进行HTML优化或对网页中的图片进行优化，从而减少网页资源大小、提升页面访问速度。

配置网页的HTML优化

真实服务返回给客户端的响应页面到达设备后，对于符合条件的响应页面，设备将对HTML网页的HTML、JS以及CSS代码进行优化。

配置网页的HTML优化，在HTTP/HTTPS模板配置模式下，使用以下命令：

```
pagespeed html {enable | trim {css | js} | case-insensitive | case-sensitive | exclude-url {contain string | end-with string | equal string | not-contain string | not-end-with string | not-equal string | not-regex-match string | not-start-with string | regex-match string | start-with string} [case-insensitive | case-sensitive]}
```

- **enable** - 开启网页的HTML优化功能。启用后，当客户端访问未指定的URL时，系统将对响应页面的进行HTML优化。
- **trim css** - 指定对HTML网页的CSS代码进行优化。
- **trim js** - 指定对HTML网页的JS代码进行优化。
- **case-insensitive** - 指定后，系统将对客户端请求的URL不进行字母大小写区分。
- **case-sensitive** - 指定后，系统将对客户端请求的URL进行字母大小写区分。
- **exclude-url {contain string | end-with string | equal string | not-contain string | not-end-with string | not-equal string | not-regex-match string | not-start-with string | regex-match string | start-with string} [case-insensitive | case-sensitive]** - 配置排除URL的匹配规则，即当客户端访问排除规则之外的URL时，系统将按照配置对真实服务返回的响应页面进行HTML优化。
 - **contain string** - 当客户端请求的URL包含指定字符时，满足匹配条件。
 - **not-contain string** - 当客户端请求的URL不包含指定字符时，满足匹配条件。
 - **end-with string** - 当客户端请求的URL以指定字符结尾时，满足匹配条件。
 - **not-end-with string** - 当客户端请求的URL不以指定字符结尾时，满足匹配条件。
 - **start-with string** - 当客户端请求的URL以指定字符开始时，满足匹配条件。
 - **not-start-with string** - 当客户端请求的URL不以指定字符开始时，满足匹配条件。
 - **equal string** - 当客户端请求的URL等于指定字符时，满足匹配条件。
 - **not-equal string** - 当客户端请求的URL不等于指定字符时，满足匹配条件。

- **regex-match** *string* - 当客户端请求的URL符合正则表达式时，满足匹配条件。
- **not-regex-match** *string* - 当客户端请求的URL不符合正则表达式时，满足匹配条件。
- **case-insensitive** - 指定该条URL排除规则不区分大小写。
- **case-sensitive** - 指定该条URL排除规则区分大小写。

说明：若没有指定大小写匹配模式，该条URL排除规则的大小写匹配模式将继承**pagespeed html {case-insensitive | case-sensitive}**命令配置的大小写匹配模式。

在HTTP/HTTPS模板配置模式下，使用**no pagespeed html {enable | trim {css | js} | exclude-url *id*}**命令取消配置。

配置网页的图片优化

启用后，当客户端访问的服务器资源路径没有匹配上用户指定的资源路径时，真实服务返回给客户端的响应页面到达设备后，设备可以对网页中包含的图片进行格式转换，压缩图片大小，从而减小流量，提升页面访问速度。

配置网页的图片优化，在HTTP/HTTPS模板配置模式下，使用以下命令：

```
pagespeed image {enable | min-size value | max-size value | convert-format {jpeg | webp} | case-insensitive | case-sensitive | exclude-url {contain string | end-with string | equal string | not-contain string | not-end-with string | not-equal string | not-regex-match string | not-start-with string | regex-match string | start-with string} [case-insensitive | case-sensitive]}
```

- **enable** - 开启网页的图片优化功能。启用后，当客户端访问未指定的URL时，系统将对响应页面中的图片进行优化。
- **min-size** *value* - 指定待优化图片尺寸的最小值，取值范围是0到8192KB，默认值为32KB。当单一图片的尺寸小于该值时，系统不对其进行格式转换。
- **max-size** *value* - 指定待优化图片尺寸的最大值，取值范围是1到8192KB，默认值为2048KB。当单一图片的尺寸大于该值时，系统不对其进行格式转换。
- **convert-format** {**jpeg** | **webp**}
 - **jpeg** - 指定后，系统将PNG、GIF和WEBP格式的图片均转换为JPEG格式。
 - **webp** - 指定后，系统将PNG和JPEG格式的图片均转换为WEBP格式。

- **case-insensitive** - 指定后，系统将对客户端请求的URL不进行字母大小写区分。
- **case-sensitive** - 指定后，系统将对客户端请求的URL进行字母大小写区分。
- **exclude-url** {**contain** *string* | **end-with** *string* | **equal** *string* | **not-contain** *string* | **not-end-with** *string* | **not-equal** *string* | **not-regex-match** *string* | **not-start-with** *string* | **regex-match** *string* | **start-with** *string* } [**case-insensitive** | **case-sensitive**] - 配置排除URL的匹配规则，即当客户端访问排除规则之外的URL时，系统将按照配置对真实服务返回的响应页面进行图片优化。
 - **contain** *string* - 当客户端请求的URL包含指定字符时，满足匹配条件。
 - **not-contain** *string* - 当客户端请求的URL不包含指定字符时，满足匹配条件。
 - **end-with** *string* - 当客户端请求的URL以指定字符结尾时，满足匹配条件。
 - **not-end-with** *string* - 当客户端请求的URL不以指定字符结尾时，满足匹配条件。
 - **start-with** *string* - 当客户端请求的URL以指定字符开始时，满足匹配条件。
 - **not-start-with** *string* - 当客户端请求的URL不以指定字符开始时，满足匹配条件。
 - **equal** *string* - 当客户端请求的URL等于指定字符时，满足匹配条件。
 - **not-equal** *string* - 当客户端请求的URL不等于指定字符时，满足匹配条件。
 - **regex-match** *string* - 当客户端请求的URL符合正则表达式时，满足匹配条件。
 - **not-regex-match** *string* - 当客户端请求的URL不符合正则表达式时，满足匹配条件。
 - **case-insensitive** - 指定该条URL匹配规则不区分大小写。
 - **case-sensitive** - 指定该条URL匹配规则区分大小写。

说明：若没有指定大小写匹配模式，该条URL排除规则的大小写匹配模式将继承**pagespeed image {case-insensitive | case-sensitive}**命令配置的大小写匹配模式。

在HTTP/HTTPS模板配置模式下，使用**no pagespeed image {enable | min-size | max-size | exclude-url id id}**命令取消配置。

开启WebSocket

启用WebSocket后，服务器与客户端将建立一个基于TCP双向数据传输的长连接。在应用模板配置模式下，使用以下命令启用或禁用WebSocket：

- 启用：**websocket enable**
- 禁用：**no websocket enable**（默认配置）

配置保活超时时间

“保活超时”常与“最大保活请求数”同时配置使用。HTTP 1.1协议引入了长连接机制，该“保活超时”时间即HTTP 1.1的长连接机制的超时时间。当客户端使用HTTP 1.1，与ADC设备建立一个TCP连接后，如果在“保活超时”时间内没有收到该客户端在TCP连接上的HTTP请求，即关闭该TCP连接；反之，如果在“保活超时”时间内，该TCP连接上再次收到HTTP请求，那么设备处理完请求后将重新开启“保活时间”计时。当“保活超时”被配置为0时，表示禁用长连接机制。（具体机制参见RFC2068）

配置保活超时时间，在HTTP模板配置模式下，使用以下命令：

keepalive-timeout *value*

- *value* - 指定设备与客户端之间的保活/TCP长连接超时时间。取值范围为0至3600秒，默认值为75秒。

在HTTP模板配置模式下，使用**no keepalive-timeout**命令恢复默认值。

配置连接超时时间

指定设备到真实服务的TCP连接超时的时间。超时后，则表示此次TCP连接失败。在HTTP模板或MYSQL模板配置模式下，使用以下命令：

connect-timeout *value*

- *value* - 指定设备到真实服务的TCP连接超时的时间。HTTP模板的取值范围为0至120秒，默认值为60秒。
MYSQL模板的取值范围为1到3600秒，默认值为10秒。

在HTTP模板或MYSQL模板配置模式下，使用**no connect-timeout**命令恢复默认值。

配置查询时间

指定发往真实服务的单个MySQL请求的超时时间。超时后，则该请求会失效。在MySQL模板配置模式下，使用以下命令：

query-timeout *value*

- *value* - 指定发往真实服务的单个MySQL请求的超时时间。取值范围为1至1728000秒，默认值为86400秒。

在MySQL模板配置模式下，使用**no query-timeout**命令恢复默认值。

配置MySQL保活超时时间

指定ADC设备与真实服务连接的保活超时时间。当ADC设备使用MySQL协议与真实服务建立一个连接后，如果真实服务在“保活超时”时间内没有再收到设备的MySQL请求，即关闭该连接；反之，如果在“保活超时”时间内，该连接上再次收到MySQL请求，那么真实服务处理完请求后将重新开启“保活时间”计时。

配置保活超时时间，在MySQL模板配置模式下，使用以下命令：

keepalive-timeout *value*

- *value* - 指定设备与真实服务之间的保活超时时间。取值范围为0至3600秒，默认值为75秒。当“保活超时”被配置为0时，表示禁止长连接。

在MySQL模板配置模式下，使用**no keepalive-timeout**命令恢复默认值。

配置读写超时时间

当应用模板的类型为“流模板”时，此配置生效。“读写超时时间”包括设备发送请求至目标服务器的超时时间，以及设备读取到目标服务器返回的响应的超时时间，两段超时时间一致。当设备转发HTTPS请求至目标服务器的时间超过该时间时，设备将断开和目标服务器的连接；当设备向目标服务器成功发送请求后，在指定的超时时间内，没有收到到目标服务器的响应时，设备将断开和目标服务器的连接。配置读写超时时间，在流模板配置模式下，使用以下命令：

read-write-timeout *value*

- *value* - 指定读写超时时间，取值范围为1至3600秒，默认值为600秒。

在应用模板配置模式下，使用**no read-write-timeout**命令恢复默认的读取超时时间。

配置连接复用

默认情况下，连接复用功能关闭，此时ADC设备使用HTTP 1.0协议连接到真实服务，即每次请求/应答后该TCP连接将关闭。启用连接复用后，ADC设备使用HTTP 1.1协议连接到真实服务器，将采用长连接机制。对于相同数量的客户端请求，ADC设备与真实服务之间的连接数会因为连接复用而减少，从而减轻了真实服务的压力。

在HTTP/HTTPS模板配置模式下，使用以下命令启用连接复用：

connection-reuse {**enable** | **connection-pool** *number* | **timeout** *time* | **requests** *value*}

- **enable** - 启用连接复用。默认情况下，该功能为关闭状态。
- **connection-pool** *number* - 指定ADC设备与所有真实服务之间的最大空闲TCP连接数量。当设备与真实服务间的TCP长连接个数达到该指定值时，对于新产生的客户端连接，设备将采用TCP短连接机制与真实服务建立连接。取值范围为1至10240，默认值为1024。
- **timeout** *time* - 指定ADC设备与真实服务之间某个TCP长连接上允许建立的最大请求数量。同一TCP长连接上的请求个数达到该指定值时，此TCP连接将断开。取值范围为1至10240，默认值为1000。
- **requests** *value* - 指定ADC设备与真实服务间TCP长连接的超时时间。取值范围为1至86400秒，默认值为300秒。

在HTTP模板配置模式下，使用**no connection-reuse** {**enable** | **connection-pool** | **timeout** | **requests**}命令恢复默认值。

配置读取超时时间

指定设备读取到真实服务返回的HTTP/HTTPS响应的超时时间，即设备发出HTTP/HTTPS请求后，在“读取超时”时间内没收到任何真实服务的数据，则认为超时。指定后，当HTTP/HTTPS请求超过“读取时间”，设备将显示“504网关超时”错误，这样可以保证每个请求等待的最长时间固定，不会过长。

在HTTP模板配置模式下，使用以下命令配置读取超时时间：

read-timeout *value*

- *value* - 配置读取超时时间，取值范围为1至3600秒，默认值为300秒。

在HTTP模板配置模式下，使用**no read-timeout**命令恢复默认的读取超时时间。

配置发送超时时间

指定设备与真实服务之间的发送超时时间。当ADC设备发送一段数据到真实服务的时间超过该时间时，设备将断开该TCP连接。在HTTP模板配置模式下，使用以下命令配置发送超时时间：

send-timeout *value*

- *value* - 配置发送超时时间，取值范围为1至3600秒，默认值为300秒。

在HTTP模板配置模式下，使用**no send-timeout**命令恢复默认的发送超时时间。

开启X-Forward-For

启用X-Forward-For功能后，设备在转发报文时，会在HTTP/HTTPS报文中添加X-Forwarded-For字段，包含客户端的真实IP，使其对真实服务可见。在HTTP模板配置模式下，使用以下命令启用X-Forward-For功能：

x-forward-for {**on** | **off**}

- **on** - 启用X-Forward-For功能。
- **off** - 禁用X-Forward-For功能。

开启X-Real-IP

启用X-Real-IP功能后，设备在转发报文时，会在HTTP/HTTPS报文中添加X-Real-IP字段以及根据X-Real-IP解析出来的源IP地址，使其对真实服务可见。在HTTP模板配置模式下，使用以下命令启用X-Real-IP功能：

x-real-ip {**on** | **off**}

- **on** - 启用X-Real-IP功能。
- **off** - 禁用X-Real-IP功能。

配置缓冲区大小

指定真实服务需返回的HTTP/HTTPS响应报文的缓冲区的大小，在HTTP模板配置模式下，使用以下命令：

buffer-size *value*

- *value* - 指定缓冲区的大小，取值范围为128至4096KB，默认值为128KB。

在HTTP模板配置模式下，使用**no buffer-size** 命令恢复默认值。

配置首片缓冲区大小

指定真实服务需返回的HTTP/HTTPS响应报文的首片缓冲区的大小，在HTTP模板配置模式下，使用以下命令：

first-part-buffer-size *value*

- *value* - 指定首片缓冲区的大小，取值范围为4至2048KB，默认值为16KB。

在HTTP模板配置模式下，使用**no first-part-buffer-size** 命令恢复默认值。

配置最大请求体大小

指定HTTP/HTTPS请求中的上传文件的最大值，在HTTP模板配置模式下，使用以下命令：

client-max-body-size *value*

- *value* - 指定HTTP/HTTPS请求中的上传文件的最大值，取值范围为128至1024000KB，默认值为8192KB。

在HTTP模板配置模式下，使用**no client-max-body-size** 命令恢复默认值。

配置最大请求头大小

指定设备用于读取客户端HTTP/HTTPS请求头的缓冲区大小。在HTTP模板配置模式下，使用以下命令：

client-max-header-size *value*

- *value* - 指定设备用于读取客户端HTTP/HTTPS请求头的缓冲区大小，取值范围是4至128KB，默认值为32KB。

在HTTP模板配置模式下，使用**no client-max-header-size** 命令恢复默认值。

启用/禁用代理缓冲功能

启用代理缓冲功能后，设备将来自真实服务的响应保存到[缓冲大小](#)设置的缓冲区中。在HTTP模板配置模式下，使用以下命令：

- **proxy-buffering enable** - 启用该功能。系统默认启用该功能。
- **proxy-buffering disable** - 禁用该功能。

HTTP缓存

开启HTTP静态资源缓存功能后，系统将把真实服务器返回给客户端的静态资源（如CSS文件，图片等访问量较大但变化较少的资源）缓存至自身内存或磁盘。这样后续客户端再次访问相同的静态资源时，设备可以直接将缓存的内容返回给客户端，从而节省了继续与真实服务器通信的时间，同时也减轻了真实服务器的负载压力。

系统支持内存缓存与磁盘缓存两种HTTP静态资源缓存方式。系统从内存中读取数据的速度大于从磁盘中读取数据的速度。因此，若客户端请求同时符合两种缓存方式的条件，设备会将响应中的资源缓存至内存。

配置HTTP静态资源的内存缓存

配置HTTP静态资源的内存缓存相关信息，在HTTP/HTTPS模板配置模式下，使用以下命令：

```
ramcache { enable | uri uri-path | enforce ignore-header { x-accel-expires | expires | cache-control | set-cookie } | size value | time-out value | min-file-size value | max-file-size value | range-request | convert-head-to-get }
```

- **enable** - 启用将HTTP静态资源缓存至设备内存的功能。启用后，当客户端申请访问的服务器资源路径匹配内存缓存的匹配规则时，系统将把真实服务返回给客户端的静态资源缓存至ADC设备的内存。
- **uri uri-path** - 指定需匹配的URI路径信息，系统支持正则表达式的URI匹配。重复该命令，添加多条URI匹配条目。系统最多支持添加8条URI匹配条目。

说明：若没有配置URI匹配条目，系统对所有响应的静态资源都不进行内存缓存。

- **enforce ignore-header { x-accel-expires | expires | cache-control | set-cookie }** - 指定响应报文中可能携带的首部字段。指定后，系统将忽略其对缓存的影响，并对响应中的静态资源进行强制缓存。重复该命令，指定多个需忽略的首部字段。
- **size value** - 指定引用HTTP/HTTPS模板的虚拟服务器可以提供给Web缓存的最大内存大小。超过最大内存后，系统将会清除部分原先的缓存，用来缓存新的HTTP静态资源。取值范围为1至64MB，默认值为64MB。
- **time-out value** - 指定HTTP静态资源在设备上缓存的时间，取值范围为1至1440分钟，默认值为60分钟。指定后，当客户端第一次访问真实服务器上的某静态资源时，系统会将真实服务器返回给客户端的该资源进行

缓存：

- 若在缓存时间内，客户端再次访问了该静态资源，系统会直接将缓存的资源发送给客户端，从而节省了通信时间。超过缓存时间后，系统会向真实服务器重新请求该资源来刷新缓存。

- 若在缓存时间内，客户端没有访问该静态资源，则超过缓存时间后，系统将清除该静态资源。

例如：设置缓存时间为10分钟，系统缓存了静态资源A。若在第5分钟时，客户端再次访问了资源A，系统直接将自身缓存中的资源返回给客户端，不需要再次向真实服务器发起访问申请。在10分钟后，系统将清除该缓存。若10分钟后，客户端再次发起请求，系统将重新向真实服务器发起访问申请，刷新缓存内容，并返回给客户端。以此类推。

- **min-file-size value** - 指定系统可缓存的文件的最小长度，取值范围为0至512KB，默认值为1KB。只有文件的长度在最小长度和最大长度之间，系统才进行缓存。
- **max-file-size value** - 指定系统可缓存的文件的最大长度，取值范围为1至8192KB，默认值为2048KB。只有文件的长度在最小长度和最大长度之间，系统才进行缓存。
- **range-request** - 启用缓存断点续传请求功能。启用后，当客户端发起HTTP范围请求（Range Request）时，设备向真实服务发起完整请求，并将响应缓存至设备内存。这样后续客户端再次向同一URL发起范围请求时，设备可以直接将对应范围的缓存内容返回给客户端。
- **convert-head-to-get** - 启用HEAD请求转换为GET请求的功能。启用后，当客户端发起HEAD请求时，系统自动将其转换为GET请求。系统向真实服务器发起GET请求，并将响应缓存至设备内存。后续无论客户端是通过HEAD请求还是GET请求访问相同的静态资源时，系统都可以直接将缓存内容返回。系统默认启用该功能。

若不启用该功能，系统直接将客户端发起的HEAD请求或GET请求转发至真实服务器，然后将响应缓存。后续客户端使用与第一次相同的请求方法发起访问时，系统可以将缓存内容返回。

在HTTP/HTTPS模板配置模式下，使用**no ramcache { enable | uri uri-path | enforce ignore-header header-name | size | time-out | min-file-size | max-file-size | range-request | convert-head-to-get }** 命令取消配置。

配置HTTP静态资源的磁盘缓存

配置HTTP静态资源的磁盘缓存相关信息，在HTTP/HTTPS模板配置模式下，使用以下命令：

```
cache { enable | resource-type { jpeg | gif | png | doc | ppt | xls | pdf | html | css | js | swf | mp3 | avi | flv | mp4 } |  
resource-type-customized list | disk-size value | time-out value | min-file-size value | max-file-size value | default-page  
| enforce ignore-header { x-accel-expire | expires | cache-control | set-cookie } | range-request | convert-head-to-  
get }
```

- **enable** - 启用将HTTP静态资源缓存至设备磁盘的功能。启用后，系统将把真实服务返回给客户端的静态资源缓存至ADC设备的磁盘。
- **resource-type** - 指定预定义的HTTP缓存的静态资源类型。系统将对指定类型的静态资源进行缓存，非指定类型将不进行缓存。重复该命令，添加多个预定义的静态资源类型。
- **resource-type-customized list** - 指定自定义的HTTP缓存的静态资源类型，不同类型需用英文分号“；”隔开。系统将对指定类型的静态资源进行缓存，非指定类型将不进行缓存。
- **disk-size value** - 指定引用HTTP/HTTPS模板的虚拟服务器可以提供给Web缓存的最大磁盘空间大小。超过磁盘空间后，系统将会清除部分原先的缓存，用来缓存新的HTTP静态资源。取值范围为1至1024MB，默认值为64MB。
- **time-out value** - 指定HTTP静态资源在设备上缓存的时间，取值范围为5至1440分钟，默认值为60分钟。指定后，当客户端第一次访问真实服务器上的某静态资源时，系统会将真实服务器返回给客户端的该资源进行缓存：
 - 若在缓存时间内，客户端再次访问了该静态资源，系统会直接将缓存的资源发送给客户端，从而节省了通信时间。超过缓存时间后，系统会向真实服务器重新请求该资源来刷新缓存。
 - 若在缓存时间内，客户端没有访问该静态资源，则超过缓存时间后，系统将清除该静态资源。
 例如：设置缓存时间为10分钟，系统缓存了静态资源A。若在第5分钟时，客户端再次访问了资源A，系统直接将自身缓存中的资源返回给客户端，不需要再次向真实服务器发起访问申请。在10分钟后，系统将清除该缓存。若10分钟后，客户端再次发起请求，系统将重新向真实服务器发起访问申请，刷新缓存内容，并返回给客户端。以此类推。
- **min-file-size value** - 指定系统可缓存的文件的最小长度，取值范围为1至8192KB，默认值为1KB。只有文件的长度在最小长度和最大长度之间，系统才进行缓存。
- **max-file-size value** - 指定系统可缓存的文件的最大长度，取值范围为1至8192KB，默认值为2048KB。只有文件的长度在最小长度和最大长度之间，系统才进行缓存。
- **default-page** - 启用缓存默认页面功能。启用后，对于不包含URI信息的客户端请求，系统仍然会将响应中的静态资源信息缓存至磁盘。
- **enforce ignore-header {x-accel-expire | expires | cache-control | set-cookie}**

- **range-request** - 启用缓存断点续传请求功能。启用后，当客户端发起HTTP范围请求（Range Request）时，设备向真实服务发起完整请求，并将响应缓存至设备磁盘。这样后续客户端再次向同一URL发起范围请求时，设备可以直接将对应范围的缓存内容返回给客户端。
- **convert-head-to-get** - 启用HEAD请求转换为GET请求的功能。启用后，当客户端发起HEAD请求时，系统自动将其转换为GET请求。系统向真实服务器发起GET请求，并将响应缓存至设备磁盘。后续无论客户端是通过HEAD请求还是GET请求访问相同的静态资源时，系统都可以直接将缓存内容返回。系统默认启用该功能。
若不启用该功能，系统直接将客户端发起的HEAD请求或GET请求转发至真实服务器，然后将响应缓存。后续客户端使用与第一次相同的请求方法发起访问时，系统可以将缓存内容返回。

在HTTP/HTTPS模板配置模式下，使用**no cache { enable | enforce ignore-header header-name | resource-type type-name | resource-type-customized | disk-size | time-out | min-file-size | max-file-size | default-page | range-request | convert-head-to-get }** 命令取消配置。

清除HTTP缓存

清除设备磁盘和内存的缓存统计信息，在任何配置模式下，使用以下命令：

clear statistics slb cache [vs-name] - 清除指定的虚拟服务器上的磁盘和内存缓存统计数量。*vs-name* 为指定的虚拟服务器的名称。不指定虚拟服务器名称，即清除所有虚拟服务器上的内存缓存统计数量。

清除指定虚拟服务器上的磁盘和内存的缓存内容，在任何配置模式下，使用以下命令：

clear slb cache virtual-server vs-name - 清除指定的虚拟服务器上的磁盘和内存缓存内容。*vs-name* 为指定的虚拟服务器的名称。

查看HTTP缓存统计信息

查看指定虚拟服务器上的磁盘和内存统计信息，在任何配置模式下，使用以下命令：

show statistics slb cache [vs-name] - 显示指定的虚拟服务器上的磁盘和内存缓存统计数量。*vs-name* 为指定的虚拟服务器的名称。不指定虚拟服务器名称，即显示所有虚拟服务器上的内存缓存统计数量。

HTTP压缩

开启HTTP静态资源压缩功能后，若客户端可以接收并能解压压缩包时，设备将会对服务器返回的非压缩文件进行压缩，然后再发送给客户端，从而减轻发送的负载，缩短发送的时间，达到加速的效果。

配置HTTP压缩

compression { **enable** | **content-type** *list* | **buffer-size** *value* | | **min-size** *value* | **max-size** *value* }

- **enable** - 开启HTTP静态资源压缩功能。
- **content-type** *list* - 指定系统压缩的静态资源类型，用户可按需可选择系统预定义的资源类型。系统将对指定类型的静态资源进行压缩，非指定类型将不进行压缩。
- **buffer-size** *value* - 指定引用HTTP模板的虚拟服务器可以提供的压缩缓冲区的大小，超过缓冲区大小后，系统将会清除部分原先的缓存，用来缓存新的HTTP静态资源。取值范围为4至1024KB，默认值为32KB。
- **min-size** *value* - 指定系统可压缩的文件的最小长度。取值范围为1至8192KB，默认值为1KB。只有文件的长度在最小长度和最大长度之间，系统才进行压缩。
- **max-size** *value* - 指定系统可压缩的文件的最大长度。取值范围为1至8192KB，默认值为2048KB。只有文件的长度在最小长度和最大长度之间，系统才进行压缩。

在HTTP模板配置模式下，使用**no compression** { **enable** | **content-type** *list* | **buffer-size** *value*命令取消配置。

清除HTTP压缩

clear slb-statistics compression [*vs-name*]- 清空指定的虚拟服务器上的压缩统计数量。不指定虚拟服务器名称，即清空所有虚拟服务器上的统计数量。

clear slb compression virtual-server [*vs-name*]- 清除指定的虚拟服务器的缓存内容。不指定虚拟服务器名称，即清除所有虚拟服务器上的缓存内容。

查看HTTP缓存信息

show statistics slb compression [*vs-name*]- 显示指定的虚拟服务器上的缓存统计数量。不指定虚拟服务器名称，即显示所有虚拟服务器上的统计数量。

配置Cookie加密

开启Cookie加密并配置加密密码。系统将服务器响应中Set-Cookie里指定的Cookie值进行加密，加密后返回给客户端。当客户端再次发起请求携带指定的Cookie时，系统对该指定的Cookie值解密，若解密成功，则使用解密后的Cookie请求服务器；若解密失败，则使用解密前的Cookie请求服务器。在HTTP/HTTPS模板配置模式下，使用以下命令：

encrypt-cookie { **enable** | **name** *cookie-name* | **password** *password* }

- **enable** - 开启加密Cookie功能。
- **name** *cookie-name* - 指定HTTP Cookie的名称。配置后，系统将对服务器响应中包含该名称的Cookie值进行加密。
- **password** *password* - 指定Cookie加密密码。

在HTTP/HTTPS模板配置模式下，使用**no encrypt-cookie { enable | name *cookie-name* | password *password* }**命令取消配置。

配置客户端缓存大小

指定设备接收客户端的IMAP/SMTP请求报文的缓冲区大小。

在IMAP/SMTP模板配置模式下，使用以下命令配置客户端缓存大小：

client-buffer-size *value*

- *value* - 指定客户端缓冲区大小。取值范围是128到8192字节，默认值为4096字节。

在IMAP/SMTP模板配置模式下，使用**no client-buffer-size**命令恢复客户端缓存的默认值。

配置代理缓存大小

指定真实服务返回的IMAP/POP3/SMTP响应报文的缓冲区大小。在IMAP/POP3/SMTP模板配置模式下，使用以下命令配置代理缓存大小：

proxy-buffer-size *value*

- *value* - 指定代理缓存大小。取值范围是128到8192字节，默认值为4096字节。

在IMAP/POP3/SMTP模板配置模式下，使用**no proxy-buffer-size**命令恢复代理缓存的默认值。

配置读写超时时间

当应用模板的类型为“IMAP”、“POP3”或“SMTP”时，此配置生效。指定客户端与设备间建立连接的超时时间，设备发送请求至目标服务器的超时时间，以及设备读取到目标服务器返回的响应的超时时间，三段超时时间一致。即当设备与客户端没有在超时时间内建立连接时，该连接将断开；当设备转发IMAP/POP3/SMTP请求至目标服务器的时间超过该时间时，设备将断开和目标服务器的连接；当设备向目标

服务器成功发送请求后，在指定的超时时间内，没有收到到目标服务器的响应，设备将断开和目标服务器的连接。

在IMAP/POP3/SMTP模板配置模式下，使用以下命令配置读写超时时间：

```
read-write-timeout value
```

- *value* - 指定读写超时时间。取值范围是60到172800秒，默认值为86400秒。

在IMAP/POP3/SMTP模板配置模式下，使用**no read-write-timeout** 命令恢复读写超时时间的默认值。

查看应用模板信息

在任何模式下，查看应用模板的信息，使用以下命令：

```
show slb app-profile name
```

配置Web防护模板

系统提供Web防护模板来抵御HTTP泛洪攻击，如攻击者发起大量的HTTP报文，消耗服务器资源，使得服务器无法响应正常客户端请求的行为。

配置Web防护模板后，当用户创建HTTP或HTTPS类型的虚拟服务器时，可以直接引用该模板，从而保护内部网络免受恶意攻击，保证内部网络及系统正常运行。

设备对第一次接收到的客户端请求的Web防护流程如下：

1. 客户端发起一个请求，该请求到达设备后，根据设备上应用的配置，匹配到引用了Web防护模板的虚拟服务器；
2. 设备先对请求进行攻击检测，即判断客户端的请求速率是否达到用户设置的阈值，若未超过阈值，系统直接放行该请求，不启用Web防护；若超过阈值，系统认为此网站可能正在经历HTTP泛洪攻击，需要对该请求采取攻击防御手段，执行防护动作；
3. 如防护动作为告警，系统将客户端请求放行，并记录日志；
4. 如防护动作为缓解，需进一步选择缓解的具体方式，包括阻断和重定向。
5. 如选择阻断，系统将请求直接丢弃，并将相应的请求实体加入黑名单；

6. 如选择重定向，系统将返回重定向状态码给客户端，告知客户端需要重定向到新的URL，以验证客户端的真实性。若客户端为攻击客户端，无法识别重定向状态码，即无法完成后续请求。此时，设备认为客户端没有通过攻击防御验证；
7. 若客户端正常，则可以完成重定向过程，再次发送请求至设备。设备认为该客户端通过攻击防御验证，转发其原始请求至服务器后，将响应返回给客户端。同时，系统将通过防御验证的请求实体加入信任名单。



注意:

- 黑名单中记录请求实体包含以下关键词：客户端IP、匹配到的基于URL防护规则ID以及访问的虚拟服务器ID。
- 信任名单中记录请求实体包含以下关键词：客户端IP、访问的虚拟服务器ID以及User-agent字段的MD5摘要。
- 对于直接被系统阻断的客户端请求，系统会将其对应的请求实体加入黑名单。黑名单内的请求实体再次发起访问时，将直接被丢弃，不进入Web防护流程。
- 通过攻击防御验证的请求实体，系统会将其加入信任名单。信任名单内的请求实体再次发起访问时，将直接被放行，不进入Web防护流程。

创建Web防护模板

创建Web防护模板，在全局配置模式下，使用以下命令：

slb web-protect-profile *profile-name* http-flood-defense

- *profile-name* - 创建Web防护模板的名称并进入Web防护模板配置模式。如果指定的名称已存在，则直接进入Web防护模板配置模式。
- **http-flood-defense** - 进入HTTP Flood攻击防护配置模式。

在全局配置模式下，使用**no slb web-protect-profile *profile-name***命令删除指定的Web防护模板。

在全局配置模式下，使用**rename slb web-protect-profile *profile-name* *new-profile-name***命令重新命名已有的Web防护模板。

配置防护动作

当客户端请求速率达到阈值，即未通过攻击检测时，系统将执行指定的攻击防御动作。在HTTP Flood攻击防护配置模式下，使用以下命令配置防护动作：

```
action {alert | mitigation [method {block [duration time]} | redirect]}
```

- **alert** - 指定将请求放行，并生成告警日志。该项为默认配置。
- **mitigation** - 指定对攻击流量采取缓解手段，包括：
 - **method block** - 指定缓解手段为“阻断”，系统将直接丢弃未通过攻击检测的请求。
 - **method block duration time** - 指定请求实体被阻断的持续时间，取值范围是60到86400秒，默认值为600秒。
 - **redirect** - 指定返回重定向状态码给客户端，以验证客户端是否为正常客户端。正常客户端可以完成重定向过程，再次发送请求至设备；攻击客户端无法完成重定向过程，若攻击客户端在请求速率超过阈值的情况下，再次发起访问，系统会为其返回重定向报文，并记录超出阈值的请求日志。该项为缓解手段的默认配置。

在HTTP Flood攻击防护配置模式下，使用**no action**命令恢复防护动作的默认配置。

配置基于虚拟服务器的检测规则

配置基于虚拟服务器的Web防护规则后，当虚拟服务器被访问的速率达到指定阈值时，系统认为此类请求存在攻击行为，将对其执行指定的防护动作。

在HTTP Flood攻击防护配置模式下，使用以下命令配置基于虚拟服务器的检测规则：

```
virtual-server-rule max-rps value
```

- **value** - 指定虚拟服务器被访问的速率的阈值，单位为“个/秒”。取值范围是1到4294967295，默认值为5000000。

在HTTP Flood攻击防护配置模式下，使用**no virtual-server-rule max-rps**命令恢复请求速率阈值的默认值。



注意: Web防护规则生效优先级：基于源IP检测 > 基于URL检测 > 基于虚拟服务器检测。

配置基于源IP的检测规则

配置基于源IP检测的Web防护规则后，当某源IP发起的请求速率达到指定阈值时，系统认为此类请求存在攻击行为，将对其执行指定的防护动作。

在HTTP Flood攻击防护配置模式下，使用以下命令配置基于源IP的检测规则：

src-ip-rule max-rps value

- **value** - 指定源IP发起访问的速率的阈值，单位为“个/秒”。取值范围是1到4294967295，默认值为1500。

在HTTP Flood攻击防护配置模式下，使用**no src-ip-rule max-rps**命令恢复请求速率阈值的默认值。



注意：Web防护规则生效优先级：基于源IP检测 > 基于URL检测 > 基于虚拟服务器检测。

配置客户端IP获取方式

配置基于源IP检测的Web防护规则后，根据需要，配置客户端源IP的获取方式。在HTTP Flood攻击防护配置模式下，使用以下命令配置客户端源IP的获取方式：

client-ip {auto | using-src}

- **auto** - 指定系统从请求报文中获取客户端IP的方式的优先级为：X-Forwarded-For > X-Real-IP > 报文携带的源IP。然后，系统将检测获取到的客户端IP的请求速率是否达到阈值。该项为默认配置。
- **using-src** - 指定从请求中获取源IP，检测该源IP的请求速率是否达到阈值。

在HTTP Flood攻击防护配置模式下，使用**no client-ip**命令恢复客户端IP获取方式的默认配置。

配置基于URL的检测规则

配置基于URL检测的Web防护规则后，当客户端请求的目标URL匹配上指定的资源路径，且请求速率达到指定阈值时，系统认为此类请求存在攻击行为，将对其执行指定的防护动作。系统最多支持配置64条基于URL的检测规则。

在HTTP Flood攻击防护配置模式下，使用以下命令配置基于URL的检测规则：

url-rule [id id] url {contain url-path | equal url-path | start-with url-path} [max-rps value]

- **id id** - 指定该基于URL检测规则的ID。若不配置，系统将自动为其分配ID。取值范围是1到64。
- **contain url-path** - 当客户端请求访问的目标URL包含指定路径时，系统将对请求进行Web防护。
- **equal url-path** - 当客户端请求访问的目标URL等于指定路径时，系统将对请求进行Web防护。
- **start-with url-path** - 当客户端请求访问的目标URL的前缀为指定路径时，系统将对请求进行Web防护。
- **value** - 指定URL被访问的速率的阈值，单位为“个/秒”。取值范围是1到4294967295，默认值为5000。

在HTTP Flood攻击防护配置模式下，使用**no url-rule id id**命令删除指定的基于URL检测规则。

移动基于URL检测规则的位置

流量进入设备后，设备对基于URL的攻击检测规则进行顺序查找，然后按照查找到的相匹配的第一条规则对流量进行检测。但是，基于URL检测规则ID的大小顺序并不是查找时的匹配顺序，规则列表中的显示顺序才是攻击检测查找时的匹配顺序。

此外，若系统对流量执行基于URL的Web防护规则，流量匹配上其中一条规则后，将继续匹配其他规则。如果命中多条规则，那么每条规则的请求计数都增加。

在HTTP Flood攻击防护配置模式下，使用以下命令移动基于URL检测规则的位置：

```
move id id {after id id1 | before id id2 | bottom | top}
```

- **id** - 指定已创建的基于URL检测规则的ID。
- **after id id1** - 指定规则id的位置为规则id1之后。
- **before id id2** - 指定规则id的位置为规则id2之前。
- **bottom** - 指定规则id的位置为所有规则的末尾。
- **top** - 指定规则id的位置为所有规则的首位。



注意：Web防护规则生效优先级：基于源IP检测 > 基于URL检测 > 基于虚拟服务器检测。

查看Web防护模板

在任意配置模式下，使用以下命令查看已创建的Web防护模板：

```
show slb web-protect-profile profile-name
```

- *profile-name* - 指定已创建的Web防护模板的名称。

Web防护黑名单

在设备进行Web防护的攻击检测过程中，若某个请求被初步判定为攻击请求，并且系统对其采取的攻击防御手段为“阻断”，那么系统会将该请求实体加入Web防护黑名单。黑名单内的请求实体再次发起访问时，系统将直接丢弃。请求实体在黑名单内的超时时间，与其配置的阻断时长一致。

在Web防护黑名单存在的情况下：

- 请求实体加入黑名单的时间超过配置的阻断时长时，将被系统从黑名单中移除；
- 修改Web防护模板中除了“防护动作”和“缓解方法”以外的配置，不对Web防护黑名单及其超时时间产生影响；
- 修改Web防护模板的“防护动作”为“告警”或修改“缓解方法”为“重定向”时，该Web防护模板对应的黑名单将被删除；
- HTTP/HTTPS虚拟服务器不再引用Web防护模板时，该Web防护模板对应的黑名单将被删除。

查看或清除Web防护黑名单

查看或清除Web防护黑名单，在任意配置模式下，使用以下命令：

```
show slb http-flood-defense blacklist virtual-server vs-name { src-ip-rule [ src-ip { A.B.C.D | X:X:X:X::X } ] | url-rule [ id id ] | virtual-server-rule }
```

```
clear slb http-flood-defense blacklist virtual-server vs-name [ src-ip-rule [ src-ip { A.B.C.D | X:X:X:X::X } ] | url-rule [ id id ] | virtual-server-rule ]
```

- {**show** | **clear**} **slb http-flood-defense blacklist** - **show**表示系统将显示Web防护黑名单信息；**clear**表示系统将清除Web黑名单信息。
- **virtual-server** *vs-name* - 查看/清除指定虚拟服务器绑定的Web防护模板生成的黑名单。
- **src-ip-rule** - 查看/清除上述虚拟服务器中所有基于源IP检测规则生成的Web防护黑名单。
 - **src-ip** *A.B.C.D* - 查看/清除指定源IPv4地址对应的Web防护黑名单。
 - **src-ip** *X:X:X:X::X* - 查看/清除指定源IPv6地址对应的Web防护黑名单。

- **url-rule** - 查看/清除上述虚拟服务器中所有基于URL检测规则生成的Web防护黑名单。
- **id id** - 指定基于URL检测规则的ID，查看/清除该规则对应的Web防护黑名单。
- **virtual-server-rule** - 查看/清除所有基于虚拟服务器检测规则生成的Web防护黑名单。

Web防护信任名单

在设备进行Web防护的攻击检测过程中，若某个请求被初步判定为攻击请求，并且系统对其采取的攻击防御手段为“重定向”。对于自动完成重定向过程，再次发送请求至设备的请求实体，系统会将其加入Web防护信任名单。信任名单内的请求实体再次发起访问时，系统将直接放行。

目前，系统不支持配置请求实体在信任名单内的超时时间，信任名单的超时时间将由系统随机分配，范围是5到300秒。

在Web防护信任名单存在的情况下：

- 修改Web防护模板中除了“防护动作”和“缓解方法”以外的配置，不对Web防护信任名单及其超时时间产生影响；
- 修改Web防护模板的“防护动作”为“告警”或修改“缓解方法”为“阻断”时，该Web防护模板对应的信任名单将被删除；
- HTTP/HTTPS虚拟服务器不再引用Web防护模板时，该Web防护模板对应的信任名单将被删除。

查看或清除Web防护信任名单

查看或清除Web防护信任名单，在任意配置模式下，使用以下命令：

```
{show | clear} slb http-flood-defense trust-list virtual-server vs-name [src-ip { A.B.C.D | X:X:X:X::X }]
```

- **{show | clear} slb http-flood-defense blacklist - show**表示系统将显示Web防护信任名单信息；**clear**表示系统将清除Web信任名单信息。
- **virtual-server vs-name** - 查看/清除指定虚拟服务器绑定的Web防护模板生成的信任名单。
- **src-ip A.B.C.D** - 查看/清除指定源IPv4地址对应的Web防护信任名单。
- **src-ip X:X:X:X::X** - 查看/清除指定源IPv6地址对应的Web防护信任名单。

配置TCP模板

目前，TCP通信中常用的拥塞控制算法是CUBIC算法和BBR算法。其中，CUBIC算法是基于丢包的拥塞控制算法，BBR算法则是基于链路容量的拥塞控制算法。客户端命中设备上的虚拟服务器，建立起TCP连接后，设备默认采用CUBIC算法进行拥塞控制。但是，当网络丢包率较高时，若继续采用CUBIC算法，对TCP通信的加速效果并不显著。

在上述网络丢包率较高的情况下，用户可以将TCP模板绑定至虚拟服务器。这样，设备就可以采用BBR算法代替CUBIC算法，对TCP通信进行拥塞控制，从而提升通信效率，减少响应时间。

配置TCP模板后，当用户创建HTTP、HTTPS、HTTP代理、TCP、SSL-OVER-TCP、SSL流代理、SMTP、IMAP或POP3类型的虚拟服务器时，可以直接引用该模板。引用该模板后，用户可以根据实际需要，对客户端与ADC设备、ADC设备与真实服务器间的TCP通信进行加速。

创建TCP模板

创建TCP模板，在全局配置模式下，使用以下命令：

```
slb tcp-profile profile-name
```

- *profile-name* - 指定TCP模板的名称并进入该TCP模板配置模式。如果指定的名称已存在，则直接进入TCP模板配置模式。

在全局配置模式下，使用`no slb tcp-profile profile-name`命令删除指定的TCP模板。

在全局配置模式下，使用`rename slb tcp-profile profile-name new-profile-name`命令重新命名已有的TCP模板。

配置TCP单边加速

创建新的TCP模板后，用户可以根据需要，开启TCP单边加速，即只对客户端与ADC设备间的TCP通信进行加速，或只对ADC设备与真实服务器间的TCP通信进行加速；也可以同时开启客户端与ADC设备间、ADC设备与真实服务器间的TCP通信加速功能。

配置客户端侧单边加速

开启/关闭客户端与ADC设备间的TCP通信加速功能。在TCP模板的配置模式下，使用以下命令：

- **client-tcp-acceleration enable** - 开启客户端与ADC设备间的TCP通信加速功能。
- **no client-tcp-acceleration enable** - 关闭客户端与ADC设备间的TCP通信加速功能。默认情况下，该功能关闭。

配置真实服务侧单边加速

开启/关闭ADC设备与真实服务器间的TCP通信加速功能。在TCP模板的配置模式下，使用以下命令：

- **server-tcp-acceleration enable** - 开启ADC设备与真实服务器间的TCP通信加速功能。
- **no server-tcp-acceleration enable** - 关闭ADC设备与真实服务器间的TCP通信加速功能。默认情况下，该功能关闭。

查看TCP模板信息

在任意配置模式下，使用以下命令查看已创建的TCP模板：

```
show slb tcp-profile profile-name
```

- *profile-name* - 指定已创建的TCP模板的名称。

其他命令

显示或清除会话信息

在任何模式下，通过使用以下命令查看或者清除系统中的会话信息：

```
{show | clear} session [virtual-server vs-name] [server-pool pool-name] [real-server rs-name] [id id] [src-ip A.B.C.D
[netmask | wildcard]] [dst-ip A.B.C.D [netmask | wildcard]] [protocol protocol-number] [src-port [port-number]] [dst-
port [port-number]] [application name] [policy policy-id] [vrouter vrouter-name] [src-addr addr-book] [dst-addr addr-
book] [vsys vsys-name] [ipv4 [application app-name | dst-addr addr-book | dst-ip A.B.C.D | dst-port port-number |
policy policy-id | protocol protocol-id | src-addr addr-book | src-ip A.B.C.D | src-port port-number | vrouter vrouter-
name]] [{ flow0-interface | flow1-interface} interface-name] [generic | h323][ipv4 | ipv6] [detail]
```

- **{show | clear} session** - show表示系统将显示会话信息。clear表示系统将清除会话信息。
- **id id** - 显示/清除指定ID的会话信息。
- **virtual-server vs-name** - 显示/清除指定虚拟服务器的会话信息。
- **server-pool pool-name** - 显示/清除指定服务池的会话信息。
- **real-server rs-name** - 显示/清除指定真实服务的会话信息。
- **src-ip A.B.C.D** - 显示/清除指定源IP地址或地址段的会话信息。
- **dst-ip A.B.C.D** - 显示/清除指定目的IP地址或地址段的会话信息。
- **netmask | wildcard** - 指定子网掩码或者通配符掩码。
- **protocol-number** - 显示/清除指定协议号的会话信息。
- **src-port [port-number]** - 显示/清除指定源端口的会话信息。
- **dst-port [port-number]** - 显示/清除指定目的端口的会话信息。
- **application name** - 显示/清除指定应用的会话信息。
- **policy policy-id** - 显示/清除指定策略的会话信息。
- **vrouter vrouter-name** - 显示/清除指定VRouter的会话信息。
- **src-addr addr-book** - 显示/清除指定源地址簿的会话信息。
- **dst-addr addr-book** - 显示/清除指定目的地址簿的会话信息。
- **ipv4 [application app-name | dst-addr addr-book | dst-ip A.B.C.D | dst-port port-number | policy policy-id | protocol protocol-id | src-addr addr-book | src-ip A.B.C.D | src-port port-number | vrouter vrouter-name]** - 显示/清除指定IPv4信息的会话信息。
- **vsys vsys-name** - 显示/清除指定VSYS的会话信息。
- **{ flow0-interface | flow1-interface} interface-name** - 显示指定flow0或者flow1的入接口的会话信息。系统不支持清除该类型的会话信息。

- **generic** - 显示会话概要信息。
- **h323** - 显示H323会话信息。
- **ipv4** | **ipv6** - 显示IPv4类型的会话信息。
- **ipv6** - 显示IPv6类型的会话信息。
- **detail** - 显示会话的详细信息，如该会话中的SNAT和DNAT规则、收发包统计等。

显示或清除会话保持表信息

在任何模式下，通过使用以下命令查看或清除四层和七层的会话保持表信息：

```
{show | clear} slb persistence {14 | 17} [method {src-ip [ip-address | cookie [cookie-content] | header [header-content] | sslid [id] | url [url-value]}] [real-server rs-name] [virtual-server vs-name] [server-pool pool-name]
```

- **14** | **17** - 14表示查看或清除四层会话保持表信息；17表示查看或清除七层会话保持表信息。

延迟删除会话信息

系统提供延迟删除会话信息的功能，即设备在收到FIN/RST报文后不会立即删除会话信息，而是在指定的延迟删除时间结束后删除会话信息。若用户的服务器需要收到第二次RST报文后才能结束会话，延迟删除防火墙设备的会话信息可使第二次RST报文顺利匹配会话信息，成功抵达用户的服务器并使服务器上的会话结束，从而避免用户的服务器出现会话异常增多的情况。

启用/禁用延迟删除会话信息功能

默认情况下，该功能为关闭状态。

在全局配置模式下，使用**flow**命令进入Flow配置模式。启用该功能并配置会话信息的延迟删除时间，在Flow配置模式下，使用以下命令：

```
tcp-session-close-wait timeout-value
```

- *timeout-value* - 指定会话信息的延迟删除时间。取值范围是0到30秒，默认值为0秒，即关闭该功能。

在Flow配置模式下，使用**no tcp-session-close-wait**命令禁用该功能。

查看延迟删除会话信息功能的启用状态

用户可以在任何模式下，通过使用以下命令查看延迟删除会话信息功能的启用状态以及会话信息的延迟删除时间：

```
show flow tcp-session-close-wait
```

SSL透视镜模板

系统支持对SSL加密的HTTP应用流量进行解密，并将解密后的流量发送至其它监听模式下的设备，例如DLP, IDS等设备。配置SSL透视镜模板后，需将该模板绑定到策略或安全域上方可生效。若绑定到安全域上，系统会对该域为源安全域的流量，按照模板配置进行解密和镜像。若绑定到策略上，且该策略规则的源安全域也同时绑定了其他的SSL透视镜模板，策略上的模板将优先生效，而安全域上的模板无效。

配置SSL透视镜模板

在全局配置模式下，使用以下命令新建SSL透视镜模板：

```
ssl-inspection profile profile-name
```

- *profile-name* - 指定SSL透视镜模板的名称。创建好的模板需绑定到策略或安全域上才能生效。执行该命令后，系统将进入SSL透视镜模板配置模式。

使用该命令no的形式删除配置。

指定模式

模式包括透视和不透视。“透视”指客户端连接匹配到域名簿后，系统才对其进行解密；“不透视”指对匹配到域名簿的连接不进行解密。在SSL透视镜模板配置模式下，使用以下命令指定模式：

```
mode {inspect | uninspect}
```

- **inspect** - 指定模式为“透视”。
- **uninspect** - 指定模式为“不透视”。

配置信任域

在SSL透视镜模板配置模式下，使用以下命令选择系统已配置的信任域：

ca-trust-domain *value*

- *value* - 指定系统已配置的信任域。CA证书生成后，需导出并安装至客户端浏览器，用于在ADC与客户端建立SSL连接时验证使用。

配置匹配规则

系统支持对符合条件的客户端流量进行解密，包括SSL加密的HTTP应用流量及邮件协议POP3S、SMTPS和IMAPS报文。

配置解密协议

指定需要解密的协议类型，包括HTTPS、IMAPS、POP3S和SMTPS。系统支持配置多种协议类型，默认选项为HTTPS。在SSL透视镜模板配置模式下，使用以下命令指定需要解密的协议类型：

protocol {**https** | **imaps** | **pop3s** | **smtps**}

- **https** - 指定HTTPS协议类型的流量需要解密。
- **imaps** - 指定IMAPS协议类型的流量需要解密。
- **pop3s** - 指定POP3S协议类型的流量需要解密。
- **smtps** - 指定SMTPS协议类型的流量需要解密。

在SSL透视镜模板配置模式下，使用**no protocol** {**https** | **imaps** | **pop3s** | **smtps**} 命令取消解密协议类型的配置。

配置域名簿

配置域名簿，在SSL透视镜模板配置模式下，使用以下命令：

host-book *host-name*

- *host-name* - 指定解密需要匹配的域名簿。

在SSL透视镜模板配置模式下，使用**no host-book**命令删除配置。

配置解密SNI为空的流量

配置解密协议类型后，系统支持对所选协议类型的SNI为空的流量进行解密。协议选项包括HTTPS、IMAPS、POP3S和SMTPS。默认为不选择。在SSL透视镜模板配置模式下，使用以下命令配置解密SNI为空的流量：

inspect-no-sni-traffic {https | imaps | pop3s | smtps}

- **https** - 指定对HTTPS协议类型的SNI为空的流量进行解密。
- **imaps** - 指定对IMAPS协议类型的SNI为空的流量进行解密。
- **pop3s** - 指定对POP3S协议类型的SNI为空的流量进行解密。
- **smtps** - 指定对SMTPS协议类型的SNI为空的流量进行解密。

在SSL透视镜模板配置模式下，使用**no inspect-no-sni-traffic {https | imaps | pop3s | smtps}**命令删除配置。

启用状态统计

启用状态统计功能。开启后，当客户端访问匹配到域名簿时，系统将根据域名信息，统计客户端对各域名访问成功或失败的次数。状态统计的详细信息，请参阅“[状态统计](#)”部分。在SSL透视镜模板配置模式下，使用以下命令启用/禁用状态统计功能：

- 启用：**access-stats enable**
- 禁用：**access-stats disable**

系统默认禁用状态统计功能。

开启日志开关

开启日志开关，记录SSL透视镜日志信息。默认为关闭状态。在SSL透视镜模板配置模式下，使用以下命令：

- 开启：**log enable**
- 关闭：**log disable**

开启日志开关后，需在全局配置模式下使用**logging traffic ssl-inspection on**启用输出透视镜日志。

启用镜像解密监控

启用镜像解密监控，若客户端请求的目的MAC地址或目的IP不是ADC地址，但流量经过ADC且匹配了域名簿时，设备可对匹配流量进行解密。默认为关闭状态。在SSL透视镜模板配置模式下，使用以下命令启用镜像解密监控：

mirror-decrypted-traffic interface *intef-name* [*dst-mac address*]

mirror-decrypted-traffic {**https** | **imaps** | **pop3s** | **smtps**} **dst-port** *port-number*

- **interface** *intef-name* - 指定镜像流量的出接口。
- **dst-mac** *address* - 输入镜像报文的目的MAC地址。
- **dst-port** *port-number* - 输入客户端请求的目的端口号，输入的目的端口将替换镜像报文的目的端口。

在SSL透视镜模板配置模式下，使用**no mirror-decrypted-traffic**命令关闭镜像解密监控。

验证服务器证书

启用验证服务器证书后，如服务器证书通过验证，ADC与服务器建立SSL连接。默认为关闭状态。在SSL透视镜模板配置模式下，使用以下命令启用/禁用验证服务器证书：

- 启用：**verify-server-certificate enable**
- 禁用：**verify-server-certificate disable**

提醒信任域证书安装

提醒信任域证书安装，即当客户端浏览器发起HTTPS访问时，系统将跳转至安装ADC设备证书的提示页面。在此页面，点击“下载根证书”按钮，页面将自动下载根证书。安装根证书后，系统将不弹出“此站点不安全”或者“您的连接不是私密连接”的提示。在SSL透视镜模板配置模式下，使用以下命令开启提醒信任域证书安装功能：

notify-trust-ca-installation [**mode** {**smart** | **all**} | **host-book** *host-name-entry* | **interval** *value*]

- **mode** {**smart** | **all**} - 指定开启提醒信任域证书安装功能的模式。
 - **smart** - 指定提醒信任域证书安装功能为“智能”模式。开启该模式后，当客户端浏览器发起HTTPS访问时，若浏览器已经安装设备证书，系统将不再为其跳转至安装证书提示页面；若浏览器未安装设备证书，系统将根据“提醒域名簿”和“提醒间隔时间”的配置，为符合条件的HTTPS请求跳转至安装证书提示页面。
 - **all** - 指定提醒信任域证书安装功能为“全部”模式。当客户端浏览器发起HTTPS访问时，无论浏览器是否安装了设备证书，系统都将根据“提醒域名簿”和“提醒间隔时间”的配置，为符合条件的HTTPS请求跳转至安装证书提示页面。

使用`no notify-trust-ca-installation mode`命令关闭提醒信任域证书安装功能。

- **host-book** *host-name-entry* - 开启提醒信任域证书安装功能后，指定信任域证书安装提醒需要匹配的域名簿。使用`no notify-trust-ca-installation host-book`命令删除指定的域名簿。
- **interval** *value* - 开启提醒信任域证书安装功能后，指定信任域证书安装提醒出现的时间间隔。信任域证书安装提醒出现一次后，信任域证书安装提醒会在指定的时间间隔后再次出现。取值范围是60至2592000秒，默认值是86400秒。用`no notify-trust-ca-installation interval`命令删除指定的提醒间隔时间。

使用 `no notify-trust-ca-installation` 命令取消提醒信任域证书安装的配置。



注意: 配置SSL透视镜模板后，需将该模板绑定到策略或安全域上方可生效。在策略配置模式下或域配置模式下，使用`ssl-inspection profile-name`命令绑定SSL透视镜模板。

信任域缓存表

在SSL透视镜模板中开启[提醒信任域证书安装](#)功能后，当客户端浏览器第一次发起HTTPS访问，匹配上模板中的“提醒域名簿”时，系统将为其跳转至安装ADC设备证书的提示页面，并且记录该客户端的源IP地址，存储在信任域缓存表中。当信任域缓存表中的客户端发起HTTPS访问时，系统不会为其跳转至证书安装页面。

查看信任域缓存表

在任何模式下，使用以下命令查看信任域缓存表：

```
show ssl-inspection notify-trust-ca-installation-cache profile profile-name [src-ip ip-address]
```

- *profile-name* - 指定SSL透视镜模板名称，查看命中该模板下所有的信任域缓存表信息。
- **src-ip** *ip-address* - 查看SSL透视镜模板中指定的客户端源IP地址对应的信任域缓存表信息。若不指定，系统将显示指定模板下所有的信任域缓存信息。

清除信任域缓存表

在任何模式下，使用以下命令清除信任域缓存表：

```
clear ssl-inspection notify-trust-ca-installation-cache profile profile-name [src-ip ip-address]
```

- *profile-name* - 指定SSL透视镜模板名称，系统将清除该模板下所有的信任域缓存表信息。
- **src-ip** *ip-address* - 清除指定的客户端源IP地址对应的信任域缓存表信息。若不指定，系统将清除指定模板下所有的信任域缓存信息。

白名单

配置SSL透视镜模板后，用户可以通过配置SSL透视镜模板的白名单域名簿，进一步控制对某些特定网站的访问。在配置SSL透视镜模板的白名单域名簿后，当用户向白名单中的域名发起访问时，系统将只对该访问请求进行转发，即配置的模板对该访问请求不生效。

添加白名单条目

添加SSL透视镜模板的白名单，系统需进入SSL透视镜模板的白名单配置模式。在全局配置模式下，使用以下命令进入SSL透视镜模板的白名单配置模式：

```
ssl-inspection global-white-list
```

在SSL透视镜模板的白名单配置模式下，使用以下命令添加白名单条目：

```
sni string
```

- *string* - 指定需要添加至白名单的域名，取值范围是1至63字符。系统最多支持添加2000条白名单域名条目。

删除白名单条目

在SSL透视镜模板的白名单配置模式下，使用以下命令删除指定的白名单条目：

```
no sni string
```

- *string* - 指定需要删除的白名单条目。

查看白名单

在任何模式下，使用以下命令查看SSL透视镜模板的白名单列表：

```
show ssl-inspection global-white-list
```

状态统计

配置SSL透视镜模板后，当客户端访问匹配到域名簿时，系统将统计各域名被成功或失败访问的次数。用户需提前开启SSL透视镜模板的[状态统计](#)功能。

查看状态统计信息

在任何模式下，使用以下命令查看模板中域名被访问的状态统计信息：

```
show ssl-inspection access-stat [sni string]
```

- **sni string** - 查看指定域名被访问的状态统计信息。若不指定，系统将显示模板中所有域名被访问的状态统计信息。

清除状态统计信息

在任何模式下，使用以下命令清除状态统计信息：

```
clear ssl-inspection access-stat [sni string]
```

- **sni string** - 清除指定的域名被访问的状态统计信息。若不指定，系统将清除模板中所有域名被访问的状态统计信息。

配置状态统计过期时间

系统记录某域名被访问的状态信息后，若在配置的状态过期时间内，客户端没有对该域名发起新的访问，系统将清除该域名的状态信息条目。在全局配置模式下，使用以下命令配置状态统计过期时间：

```
ssl-inspection access-stat expire value
```

- **value** - 指定统计过期时间。取值范围是300至86400秒，默认值是3600秒。

在全局配置模式下，使用**no ssl-inspection access-stat expire**命令恢复状态统计过期时间的默认值。

健康检查

设备可对真实服务的状态进行健康检查。如工作异常，该真实服务将被排除在可用来分配的服务器列表资源之外，以保证客户端请求被分发到可正常工作的真实服务上。

创建健康检查

健康检查用于检查各种服务的可用状态。设备可配置各种检查方法，对协议进行健康检查。系统支持对以下协议进行健康检查：ICMP，TCP，TCP-ECHO，TCP-HALF-OPEN，UDP，HTTP，HTTPS，SMTP，POP3，IMAP，DNS，FTP，SNMP-DCA，SNMP-DCA-BASE，THIRD-PARTY，RADIUS-AUTHENTICATION，RADIUS-ACCOUNTING，WebSocket，WebSocket-SSL，SIP-TCP，SIP-UDP，PASSIVE-HTTP，PASSIVE-TCP，MYSQL。

系统进行健康检查时，若对真实服务器的首次检查结果与其初始状态一致，判定此检查结束，认为真实服务的状态保持不变，此时经过设定的间隔时间，系统会再次对其进行健康检查；若不一致，系统需重新进行检查，以确保健康检查结果可靠。用户可以选择以下两种方式进行重新检查：

- 按次数：
 - 当真实服务的初始运行状态为UP，首次检查结果为DOWN时，系统将重新进行检查，来决定是否将该真实服务的状态置为DOWN。在重新检查的过程中，若连续失败的次数达到失败重试次数设定值，系统判定此检查失败，将真实服务状态置为DOWN；若在连续失败的次数未达到失败重试次数设定值的情况下，某次检查成功，此检查也将结束，系统认为真实服务状态保持不变，为UP。
 - 当真实服务的初始运行状态为DOWN，首次检查结果为UP时，系统将重新进行检查，来决定是否将该真实服务的状态置为UP。在重新检查的过程中，若连续成功的次数达到成功重试次数设定值，系统判定此检查成功，将真实服务状态置为UP；若在连续成功的次数未达到成功重试次数设定值的情况下，某次检查失败，此检查也将结束，系统认为真实服务状态保持不变，为DOWN。
- 按时间：
 - 当真实服务初始运行状态为UP，首次检查结果为DOWN时，系统将重新进行检查，来决定是否将该真实服务的状态置为DOWN。系统将在超时时间内，根据设定的间隔时间，向真实服务发起连续检查，若连续检查均失败，系统判定此检查失败，将真实服务状态置为DOWN；若某次检查成功，此检查也将结束，系统认为真实服务状态保持不变，为UP。
 - 当真实服务初始运行状态为DOWN，首次检查结果为UP时，系统将重新进行检查，来决定是否将该真实服务的状态置为UP。系统将在超时时间内，根据设定的间隔时间，向真实服务发起连续检查，若连续检查均成功，系统判定此检查成功，将真实服务状态置为UP；若某次检查失败，此检查也将结束，系统认为真实服务状态保持不变，为DOWN。

在全局配置模式下，使用以下命令创建健康检查：

`health-check name type {dns | ftp | snmp-dca | snmp-dca-base | http | https | icmp | imap | pop3 | smtp | tcp | tcp-echo | tcp-half-open | udp | third-party | radius-authentication | radius-accounting | websocket | websocket-ssl | sip-tcp | sip-udp | passive-http | passive-tcp | mysql } [mode {by-count | by-time}]`

- `name` - 指定健康检查的名称。
- `dns` - 创建DNS健康检查。
- `ftp` - 创建FTP健康检查。
- `snmp-dca` - 创建SNMP-DCA健康检查。
- `snmp-dca-base` - 创建SNMP-DCA-BASE健康检查。
- `http` - 创建HTTP健康检查。
- `https` - 创建HTTPS健康检查。
- `icmp` - 创建ICMP健康检查。
- `imap` - 创建IMAP健康检查。
- `pop3` - 创建POP3健康检查。
- `smtp` - 创建SMTP健康检查。
- `tcp` - 创建TCP健康检查。
- `tcp-echo` - 创建TCP-ECHO健康检查。
- `tcp-half-open` - 创建TCP-HALF-OPEN健康检查。
- `udp` - 创建UDP健康检查。
- `third-party` - 创建THIRD-PARTY健康检查。
- `radius-authentication` - 创建RADIUS-AUTHENTICATION健康检查。
- `radius-accounting` - 创建RADIUS-ACCOUNTING健康检查。
- `websocket` - 创建WEBSOCKET健康检查。

- **websocket-ssl** - 创建WEBSOCKET-SSL健康检查。
- **sip-tcp** - 创建SIP-TCP健康检查。
- **sip-udp** - 创建SIP-UDP健康检查。
- **passive-http** - 创建PASSIVE-HTTP健康检查。
- **passive-tcp** - 创建PASSIVE-TCP健康检查。
- **mysql** - 创建MYSQL健康检查。
- **mode {by-count | by-time}** - 指定健康检查失败的判定方式。
 - **by-count** - 指定该方式，系统将依据配置的“超时时间”、“重试间隔”和“失败重试次数”判定健康检查是否失败，即是否将真实服务的状态从UP置为DOWN；依据配置的“成功重试次数”和“成功重试间隔”判定健康检查是否成功，即是否将真实服务的状态从DOWN置为UP。该方式为系统默认的判定方式。
 - **by-time** - 指定该方式，系统将依据配置的“间隔时间”和“超时时间”判定检查是否将真实服务的状态从UP置为DOWN。

系统支持将某一健康检查模板快速克隆，用户只要将克隆的健康检查模板的部分参数进行修改，即可生成一个新的健康检查模板。克隆已有的健康检查模板，在全局配置模式下，使用以下命令：

health-check name1 clone-from name2

- *name1* - 指定新健康检查模板的名称。
- *name2* - 指定将被克隆的健康检查模板的名称。

在全局配置模式下，使用**no health-check name**命令删除健康检查。

DNS健康检查

用于对真实服务的DNS（域名解析协议）服务状态进行健康检查。检查时，设备向真实服务发送特定的域名，在超时时间内，若真实服务返回的数据中包含该域名对应的IP地址，则认为DNS健康检查成功，否则将重新进行健康检查；若连续重试的次数超过用户设置的“失败重试次数”，则认为DNS健康检查失败。

在健康检查配置模式下，使用以下命令配置DNS健康检查：

- 指定DNS健康检查的特定的域名。

domain *domain-name*

- 指定DNS健康检查的特定域名对应的IP地址。用于与真实服务实际返回的IP地址进行比较：若匹配，即服务器返回的内容中包含该域名对应的IP地址，即认为此次DNS健康检查成功；若不匹配，即服务器返回的内容中不包含该域名对应的IP地址，即认为此次DNS健康检查失败。当域名IP设置为空时，设备只要接收到真实服务的DNS响应报文即认为此DNS健康检查成功。

domain-ip *ip-address*

- DSR模式：指定设备在DSR模式下开启DNS健康检查。只有开启该项，系统才支持设备在DSR模式下的DNS健康检查功能。DNS健康检查的IP地址需指定为真实服务器的Loopback口地址，且不允许用户配置发送DNS健康检查请求的源接口。

direct-server-return - 开启设备在DSR模式下的DNS健康检查。

使用**no direct-server-return**命令关闭该功能。

- IP地址：指定IP地址。若不指定，系统将直接引用真实服务的IP地址。

ip *ip-address*

- 端口：指定端口。若不指定，系统将直接引用真实服务的端口。

port *port-number*

- 源接口：指定发送DNS健康检查请求的源接口。

source-interface *interface*

- 当该DNS健康检查的失败判定方式为**by-count**时，配置如下参数：

- 间隔时间：指定本次DNS健康检查与下次检查的时间间隔。取值范围是1到900秒，默认值是9秒。

interval *value*

- 超时时间：指定DNS健康检查时，设备收到真实服务的应答报文的超时时间。在超时时间内，若真实服务未返回预期响应，系统将认定此次检查失败。取值范围是1到600秒，默认值是6秒。

timeout *value*

- 失败重试次数：指定DNS健康检查失败，需重新检查时，可重新检查的次数。取值范围是1到10，默认值是3。

retry *value*

- 失败重试间隔：指定DNS健康检查失败，需重新检查时，两次检查的间隔时间。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

retry-interval *value*

- 成功重试次数：指定DNS健康检查成功，需重新检查时，可重新检查的次数。取值范围是1到10，默认值是1。

up-retry *value*

- 成功重试间隔：指定DNS健康检查成功，需重新检查时，两次检查的间隔时间。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

up-retry-interval *value*

详细介绍，请参阅 [“按次数”](#)。

- 当该DNS健康检查的失败判定方式为**by-time**时，配置如下参数：

- 间隔时间：指定本次DNS健康检查与下次检查的时间间隔。取值范围是1到900秒，默认值是5秒。

interval *value*

- 超时时间：指定DNS健康检查因失败进行重新检查时，可重新检查的总时长。取值范围是1到9000秒，默认值是16秒。

timeout *value*

- 成功重试时长：指定DNS健康检查成功，需重新检查时，可重新检查的总时长。取值范围是1到9000秒。

time-util-up *value*

- 成功重试间隔：指定DNS健康检查成功，需重新检查时，两次检查的间隔时间。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

up-interval *value*

详细介绍，请参阅 [“按时间”](#)。

在健康检查配置模式下，使用上述命令 **no** 的形式取消配置。

FTP健康检查

用于对真实服务的FTP服务状态进行健康检查。检查时，若在超时时间内，设备能使用指定的用户名和密码，与真实服务能够连接成功，且下载指定的文件，则认为FTP健康检查成功，否则将重新进行健康检查；若连续重试的次数超过用户设置的“重试次数”，则认为FTP健康检查失败。

在健康检查配置模式下，使用以下命令配置FTP健康检查：

- 名称：指定健康检查的名称。

file-name *file name*

- 模式：指定FTP数据通道模式，系统默认为被动模式。

mode {**pasv** | **port**}

- 用户名：指定FTP健康检查的用户名。

username *value*

- 密码：指定FTP健康检查时用来登录的用户密码。

passwd *value*

- 端口：指定FTP健康检查的端口。默认使用设备真实服务中配置的端口。

port *value*

- DSR模式：指定设备在DSR模式下开启FTP健康检查。只有开启该项，系统才支持设备在DSR模式下的FTP健康检查功能。FTP健康检查的IP地址需指定为真实服务器的Loopback口地址，且不允许用户配置发送FTP健康检查请求的源接口。当FTP健康检查的数据通道配置为主动模式时，无法启用该功能。

direct-server-return - 开启设备在DSR模式下的FTP健康检查。

使用**no direct-server-return**命令关闭该功能。

- IP地址：指定IP地址。若不指定，系统将直接引用真实服务的IP地址。

ip *ip-address*

- 端口：指定端口。若不指定，系统将直接引用真实服务的端口。

port *port-number*

- 源接口：指定发送FTP健康检查请求的源接口。

source-interface *interface*

- 当该FTP健康检查的失败判定方式为**by-count**时，配置如下参数：

- 间隔时间：指定本次FTP健康检查与下次检查的时间间隔。取值范围是1到900秒，默认值是9秒。

interval *value*

- 超时时间：指定FTP健康检查时，设备收到真实服务的应答报文的超时时间。在超时时间内，若真实服务未返回预期响应，系统将认定此次检查失败。取值范围是1到600秒，默认值是6秒。

timeout *value*

- 失败重试次数：指定FTP健康检查失败，需重新检查时，可重新检查的次数。取值范围是1到10，默认值是3。

retry *value*

- 失败重试间隔：指定FTP健康检查失败，需重新检查时，两次检查的间隔时间。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

retry-interval *value*

- 成功重试次数：指定FTP健康检查成功，需重新检查时，可重新检查的次数。取值范围是1到10，默认值是1。

up-retry *value*

- 成功重试间隔：指定FTP健康检查成功，需重新检查时，两次检查的间隔时间。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

up-retry-interval *value*

详细介绍，请参阅“[按次数](#)”。

- 当该FTP健康检查的失败判定方式为**by-time**时，配置如下参数：

- 间隔时间：指定本次FTP健康检查与下次检查的时间间隔。取值范围是1到900秒，默认值是5秒。

interval *value*

- 超时时间：指定FTP健康检查因失败进行重新检查时，可重新检查的总时长。取值范围是1到9000秒，默认值是16秒。

timeout *value*

- 成功重试时长：指定FTP健康检查成功，需重新检查时，可重新检查的总时长。取值范围是1到9000秒。

time-util-up *value*

- 成功重试间隔：指定FTP健康检查成功，需重新检查时，两次检查的间隔时间。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

up-interval *value*

详细介绍，请参阅 [“按时间”](#)。

在健康检查配置模式下，使用上述命令 **no** 的形式取消配置。

SNMP-DCA健康检查

根据系统预定义OID，对真实服务的CPU、内存和磁盘使用情况的负载信息进行检查。

在健康检查配置模式下，使用以下命令配置SNMP-DCA健康检查：

- DSR模式：指定设备在DSR模式下开启SNMP-DCA健康检查。只有开启该项，系统才支持设备在DSR模式下的SNMP-DCA健康检查功能。SNMP-DCA健康检查的IP地址需指定为真实服务器的Loopback口地址，且不允许用户配置发送SNMP-DCA健康检查请求的源接口。

direct-server-return - 开启设备在DSR模式下的SNMP-DCA健康检查。

使用**no direct-server-return**命令关闭该功能。

- IP地址：指定IP地址。若不指定，系统将直接引用真实服务的IP地址。

ip *ip-address*

- 端口：指定端口。若不指定，系统将直接引用真实服务的端口。

port *port-number*

- 源接口：指定发送SNMP-DCA健康检查请求的源接口。

source-interface *interface*

- 代理类型：指定在服务器上运行的代理类型，包括UCD和WIN2000。

agent-type {**ucd** | **win2000**}

- **agent-type ucd** - 当类型为UCD时，系统将使用UCD中CPU、内存、磁盘的OID对真实服务进行负载信息的收集。
- **agent-type win2000** - 当类型为WIN2000时，系统将使用Windows WMI作为SNMP代理，并使用WMI提供的CPU、内存、磁盘的OID对真实服务进行负载信息的收集。

- 团体名：指定服务器的SNMP主机的团体名。团体名是管理进程和代理进程之间的口令，为明文格式。建议此处配置与[系统管理中的SNMP团体字](#)配置一致。

community *community-name*

- CPU：指定CPU相关参数。

cpu {**coefficient** *value* | **threshold** *value*}

- **coefficient** *value* - 指定用于SNMP-DCA健康检查的计算比率权重的CPU系数值，用于反馈真实服务的选择策略，默认值为2000。
- **threshold** *value* - 指定用于SNMP-DCA健康检查的服务器CPU最大可利用率，默认值为80。若超出此值，系统将产生“警报”级别的日志信息。

- 磁盘：指定磁盘相关参数。

disk {**coefficient** *value* | **threshold** *value*}

- **coefficient** *value* - 指定用于SNMP-DCA健康检查的计算比率权重的磁盘系数值，默认值为2000。
- **threshold** *value* - 指定用于SNMP-DCA健康检查的服务器磁盘最大可利用率，默认值为90。若超出此值，系统将产生“警报”级别的日志信息。

- 内存：指定内存相关参数。

mem {**coefficient** *value* | **threshold** *value*}

- **coefficient** *value* - 指定用于SNMP-DCA健康检查的计算比率权重的内存系数值，默认值为1000。
- **threshold** *value* - 指定用于SNMP-DCA健康检查的服务器内存最大可利用率，默认值为70。若超出此值，系统将产生“警报”级别的日志信息。

- 版本：指定用于SNMP-DCA健康检查的版本，包括1和2c。

snmp-version {**1** | **2c**}

- 当该SNMP-DCA健康检查的失败判定方式为**by-count**时，配置如下参数：

- 间隔时间：指定本次SNMP-DCA健康检查与下次检查的时间间隔。取值范围是1到900秒，默认值是9秒。

interval *value*

- 超时时间：指定SNMP-DCA健康检查时，设备收到真实服务的应答报文的超时时间。在超时时间内，若真实服务未返回预期响应，系统将认定此次检查失败。取值范围是1到600秒，默认值是6秒。

timeout *value*

- 失败重试次数：指定SNMP-DCA健康检查失败，需重新检查时，可重新检查的次数。取值范围是1到10，默认值是3。

retry *value*

- 失败重试间隔：指定SNMP-DCA健康检查失败，需重新检查时，两次检查的间隔时间。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

retry-interval *value*

- 成功重试次数：指定SNMP-DCA健康检查成功，需重新检查时，可重新检查的次数。取值范围是1到10，默认值是1。

up-retry *value*

- 成功重试间隔：指定SNMP-DCA健康检查成功，需重新检查时，两次检查的间隔时间。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

up-retry-interval *value*

详细介绍，请参阅 [“按次数”](#)。

- 当该SNMP-DCA健康检查的失败判定方式为**by-time**时，配置如下参数：

- 间隔时间：指定本次SNMP-DCA健康检查与下次检查的时间间隔。取值范围是1到900秒，默认值是5秒。

interval *value*

- 超时时间：指定SNMP-DCA健康检查因失败进行重新检查时，可重新检查的总时长。取值范围是1到9000秒，默认值是16秒。

timeout *value*

- 成功重试时长：指定SNMP-DCA健康检查成功，需重新检查时，可重新检查的总时长。取值范围是1到9000秒。

time-util-up *value*

- 成功重试间隔：指定SNMP-DCA健康检查成功，需重新检查时，两次检查的间隔时间。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

up-interval *value*

详细介绍，请参阅“[按时间](#)”。

在健康检查配置模式下，使用上述命令 `no` 的形式取消配置。

SNMP-DCA-BASE健康检查

根据自定义的OID，对真实服务的当前用户使用情况的负载信息进行检查。

在健康检查配置模式下，使用以下命令配置SNMP-DCA-BASE健康检查：

- DSR模式：指定设备在DSR模式下开启SNMP-DCA-BASE健康检查。只有开启该项，系统才支持设备在DSR模式下的SNMP-DCA-BASE健康检查功能。SNMP-DCA-BASE健康检查的IP地址需指定为真实服务器的Loop-back口地址，且不允许用户配置发送SNMP-DCA-BASE健康检查请求的源接口。

direct-server-return - 开启设备在DSR模式下的SNMP-DCA-BASE健康检查。

使用**no direct-server-return**命令关闭该功能。

- IP地址：指定IP地址。若不指定，系统将直接引用真实服务的IP地址。

ip *ip-address*

- 端口：指定端口。若不指定，系统将直接引用真实服务的端口。

port *port-number*

- 源接口：指定发送SNMP-DCA-BASE健康检查请求的源接口。

source-interface *interface*

- 团体名：指定服务器的SNMP主机的团体名。团体名是管理进程和代理进程之间的口令，为明文格式。建议此处配置与[系统管理中的SNMP团体字](#)配置一致。

community *community-name*

- CPU：指定CPU相关参数。

cpu {**coefficient** *value* | **threshold** *value* | **oid string** **max-value** *value*}

- **coefficient** *value* - 指定用于SNMP-DCA-BASE健康检查的计算比率权重的CPU系数值，用于反馈真实服务的选择策略，默认值为1500。
- **threshold** *value* - 指定用于SNMP-DCA-BASE健康检查的服务器CPU最大可利用率，默认值为80。若超出此值，系统将产生“警报”级别的日志信息。

- **oid string** - 指定CPU的OID值。

- **max-value value** - 指定CPU的最大值，用于计算CPU系数。

- 磁盘：指定磁盘相关参数。

disk {coefficient value | threshold value | oid string max-value value}

- **coefficient value** - 指定用于SNMP-DCA-BASE健康检查的计算比率权重的磁盘系数值，默认值为2000。

- **threshold value** - 指定用于SNMP-DCA-BASE健康检查的服务器磁盘最大可利用率，默认值为90。若超出此值，系统将产生“警报”级别的日志信息。

- **oid string** - 指定磁盘OID值。

- **max-value value** - 指定磁盘的最大值，用于计算磁盘系数。

- 内存：指定内存相关参数。

mem {coefficient value | threshold value | oid string max-value value}

- **coefficient value** - 指定用于SNMP-DCA-BASE健康检查的计算比率权重的内存系数值，默认值为90。

- **threshold value** - 指定用于SNMP-DCA-BASE健康检查的服务器磁盘最大可利用率，默认值为90。若超出此值，系统将产生“警报”级别的日志信息。

- **oid string** - 指定磁盘OID值。

- **max-value value** - 指定磁盘的最大值，用于计算磁盘系数。

- 版本：指定用于SNMP-DCA-BASE健康检查的版本，包括1和2c。

snmp-version {1 | 2c}

- 当该SNMP-DCA-BASE健康检查的失败判定方式为**by-count**时，配置如下参数：

- 间隔时间：指定本次SNMP-DCA-BASE健康检查与下次检查的时间间隔。取值范围是1到900秒，默认值是9秒。

interval value

- 超时时间：指定SNMP-DCA-BASE健康检查时，设备收到真实服务的应答报文的超时时间。在超时时间内，若真实服务未返回预期响应，系统将认定此次检查失败。取值范围是1到600秒，默认值是6

秒。

timeout *value*

- 失败重试次数：指定SNMP-DCA-BASE健康检查失败，需重新检查时，可重新检查的次数。取值范围是1到10，默认值是3。

retry *value*

- 失败重试间隔：指定SNMP-DCA-BASE健康检查失败，需重新检查时，两次检查的间隔时间。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

retry-interval *value*

- 成功重试次数：指定SNMP-DCA-BASE健康检查成功，需重新检查时，可重新检查的次数。取值范围是1到10，默认值是1。

up-retry *value*

- 成功重试间隔：指定SNMP-DCA-BASE健康检查成功，需重新检查时，两次检查的间隔时间。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

up-retry-interval *value*

详细介绍，请参阅 [“按次数”](#)。

- 当该SNMP-DCA-BASE健康检查的失败判定方式为**by-time**时，配置如下参数：

- 间隔时间：指定本次SNMP-DCA-BASE健康检查与下次检查的时间间隔。取值范围是1到900秒，默认值是5秒。

interval *value*

- 超时时间：指定SNMP-DCA-BASE健康检查因失败进行重新检查时，可重新检查的总时长。取值范围是1到9000秒，默认值是16秒。

timeout *value*

- 成功重试时长：指定SNMP-DCA-BASE健康检查成功，需重新检查时，可重新检查的总时长。取值范围是1到9000秒。

time-util-up *value*

- 成功重试间隔：指定SNMP-DCA-BASE健康检查成功，需重新检查时，两次检查的间隔时间。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

up-interval *value*

详细介绍，请参阅[“按时间”](#)。

在健康检查配置模式下，使用上述命令 `no` 的形式取消配置。

HTTP/HTTPS健康检查

用于对真实服务的HTTP/HTTPS服务进行检查。检查时，设备与真实服务通过HTTP/HTTPS发送特定的内容，在超时时间内，若真实服务返回的内容包含配置的预期内容，则认为HTTP/HTTPS健康检查成功，否则将重新进行健康检查；若连续重试的次数超过用户设置的“重试次数”，则认为HTTP/HTTPS健康检查失败。

在健康检查配置模式下，使用以下命令配置HTTP/HTTPS健康检查：

- DSR模式：指定设备在DSR模式下开启HTTP/HTTPS健康检查。只有开启该项，系统才支持设备在DSR模式下的HTTP/HTTPS健康检查功能。HTTP/HTTPS健康检查的IP地址需指定为真实服务器的Loopback口地址，且不允许用户配置发送HTTP/HTTPS健康检查请求的源接口。

direct-server-return - 开启设备在DSR模式下的HTTP/HTTPS健康检查。

使用**no direct-server-return**命令关闭该功能。

- 请求路径：指定HTTP/HTTPS健康检查的URL请求路径。默认为“/”。

path *value*

- 接收内容：指定HTTP/HTTPS健康检查时，用户期望接收到的返回内容，用于与真实服务实际返回的内容进行比较：若匹配，即服务器返回的内容中包含该“接收内容”，即认为此次HTTP/HTTPS健康检查成功。若不匹配，即服务器返回的内容中不包含该“接收内容”，即认为此次HTTP/HTTPS健康检查失败。当接收内容被配置为空时，请求路径为非空时，表示只检查到真实服务的是否连接成功及真实服务是否回应，不检查真实服务返回的内容。

recv-string *value*

- 状态码：指定HTTP/HTTPS健康检查时，用户期望接收到HTTP/HTTPS状态码，若服务器返回的内容中包含该状态码，即认为此次HTTP/HTTPS健康检查成功。若“接收内容”和“状态码”同时配置，服务器返回的内容需同时包含，才能认为此次健康检查成功。状态码可配置多个，需以英文分号“;”间隔，如：200;302;503。状态码支持配置通配符“x”，如：30x; 5xx，不支持将通配符放在2个数字中间，如2x3。

status-code *value*

- SSL类型：当设备向真实服务发起HTTPS健康检查时，若真实服务器要求对设备证书进行验证，根据真实服务的证书链类型，指定设备支持的证书验证方式，可以为SSL/TLS和国密。

ssl {**gmssl** | **ssl-tls**} [**cert-chain** *value*]

- **gmssl** - 指定设备支持SSL/TLS认证。
- **ssl-tls** - 指定设备支持国密认证。
- *value* - 指定系统中已创建好的证书链。

说明：证书链需提前在“PKI > 证书链”创建完成。证书链的创建方法请参考[证书链](#)章节。

- 用户代理：配置HTTP/HTTPS健康检查时，可指定User Agent 字段。配置后，健康检查时发送的Request请求会使用已配置的用户代理。默认字段为“HealthCheckClient”。

user-agent *value*

- 主机名称：配置HTTP/HTTPS健康检查时，可指定Host字段。配置后，健康检查时发送的Request请求会使用已配置的Host字段。默认为引用真实服务的IP地址。

host *value*

- HTTP版本：配置HTTP健康检查时，可指定HTTP版本。配置后，健康检查时发送的Request请求会使用配置的HTTP版本。

http-version {**1.0** | **1.1**}

- 自定义请求：配置HTTP健康检查时，可指定HTTP Request 消息中的全部内容。指定该选项后，HTTP健康检查将**优先**使用自定义请求中的内容发送Request请求。

customized-request *value*

- 启用SNI：配置HTTPS健康检查时，用户可开启SNI。启用后，SNI允许客户端在发起SSL握手请求时，就提交请求的Host信息，使得服务器能够切换到正确的域并返回相应的证书。

enable-SNI

使用**no enable-SNI**命令关闭该功能。

- IP地址：指定IP地址。若不指定，系统将直接引用真实服务的IP地址。

ip *ip-address*

- 端口：指定端口。若不指定，系统将直接引用真实服务的端口。

port *port-number*

- 源接口：指定发送HTTP/HTTPS健康检查请求的源接口。

source-interface *interface*

- 当该HTTP/HTTPS健康检查的失败判定方式为**by-count**时，配置如下参数：

- 间隔时间：指定本次HTTP/HTTPS健康检查与下次检查的时间间隔。取值范围是1到900秒，默认值是9秒。

interval *value*

- 超时时间：指定HTTP/HTTPS健康检查时，设备收到真实服务的应答报文的超时时间。在超时时间内，若真实服务未返回预期响应，系统将认定此次检查失败。取值范围是1到600秒，默认值是6秒。

timeout *value*

- 失败重试次数：指定HTTP/HTTPS健康检查失败，需重新检查时，可重新检查的次数。取值范围是1到10，默认值是3。

retry *value*

- 失败重试间隔：指定HTTP/HTTPS健康检查失败，需重新检查时，两次检查的间隔时间。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

retry-interval *value*

- 成功重试次数：指定HTTP/HTTPS健康检查成功，需重新检查时，可重新检查的次数。取值范围是1到10，默认值是1。

up-retry *value*

- 成功重试间隔：指定HTTP/HTTPS健康检查成功，需重新检查时，两次检查的间隔时间。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

up-retry-interval *value*

详细介绍，请参阅 [“按次数”](#)。

- 当该HTTP/HTTPS健康检查的失败判定方式为**by-time**时，配置如下参数：

- 间隔时间：指定本次HTTP/HTTPS健康检查与下次检查的时间间隔。取值范围是1到900秒，默认值是5秒。

interval *value*

- 超时时间：指定HTTP/HTTPS健康检查因失败进行重新检查时，可重新检查的总时长。取值范围是1到9000秒，默认值是16秒。

timeout *value*

- 成功重试时长：指定HTTP/HTTPS健康检查成功，需重新检查时，可重新检查的总时长。取值范围是1到9000秒。

time-util-up *value*

- 成功重试间隔：指定HTTP/HTTPS健康检查成功，需重新检查时，两次检查的间隔时间。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

up-interval *value*

详细介绍，请参阅 [“按时间”](#)。

在健康检查配置模式下，使用上述命令 **no** 的形式取消配置。

ICMP健康检查

用于对真实服务的UP/DOWN状态进行简单检查。检查时，设备向真实服务发送ICMP ECHO数据包，在超时时间内，收到真实服务的回应报文，则认为ICMP健康检查成功，否则将重新进行健康检查；若连续重试的次数超过用户设置的“重试次数”，则认为ICMP健康检查失败。

在健康检查配置模式下，使用以下命令配置ICMP健康检查：

- DSR模式：指定设备在DSR模式下开启ICMP健康检查。只有开启该项，系统才支持设备在DSR模式下的ICMP健康检查功能。ICMP健康检查的IP地址需指定为真实服务器的Loopback口地址，且不允许用户配置发送ICMP健康检查请求的源接口。

direct-server-return - 开启设备在DSR模式下的ICMP健康检查。

使用**no direct-server-return**命令关闭该功能。

- IP地址：指定IP地址。若不指定，系统将直接引用真实服务的IP地址。

ip *ip-address*

- 源接口：指定发送ICMP健康检查请求的源接口。

source-interface *interface*

- 当该ICMP健康检查的失败判定方式为**by-count**时，配置如下参数：

- 间隔时间：指定本次ICMP健康检查与下次检查的时间间隔。取值范围是1到900秒，默认值是9秒。

interval *value*

- 超时时间：指定ICMP健康检查时，设备收到真实服务的应答报文的超时时间。在超时时间内，若真实服务未返回预期响应，系统将认定此次检查失败。取值范围是1到600秒，默认值是6秒。

timeout *value*

- 失败重试次数：指定ICMP健康检查失败，需重新检查时，可重新检查的次数。取值范围是1到10，默认值是3。

retry *value*

- 失败重试间隔：指定ICMP健康检查失败，需重新检查时，两次检查的时间间隔。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

retry-interval *value*

- 成功重试次数：指定ICMP健康检查成功，需重新检查时，可重新检查的次数。取值范围是1到10，默认值是1。

up-retry *value*

- 成功重试间隔：指定ICMP健康检查成功，需重新检查时，两次检查的时间间隔。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

up-retry-interval *value*

详细介绍，请参阅“[按次数](#)”。

- 当该ICMP健康检查的失败判定方式为**by-time**时，配置如下参数：

- 间隔时间：指定本次ICMP健康检查与下次检查的时间间隔。取值范围是1到900秒，默认值是5秒。

interval *value*

- 超时时间：指定ICMP健康检查因失败进行重新检查时，可重新检查的总时长。取值范围是1到9000秒，默认值是16秒。

timeout *value*

- 成功重试时长：指定ICMP健康检查成功，需重新检查时，可重新检查的总时长。取值范围是1到9000秒。

time-util-up *value*

- 成功重试间隔：指定ICMP健康检查成功，需重新检查时，两次检查的间隔时间。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

up-interval *value*

详细介绍，请参阅 [“按时间”](#)。

在健康检查配置模式下，使用上述命令 **no** 的形式取消配置。

IMAP健康检查

用于对IMAP（互联网邮件访问协议）服务状态进行健康检查。检查时，若在超时时间内，设备与真实服务能够连接成功，且能够使用指定的用户名&密码登录成功并能够打开指定的文件夹，然后退出，则认为IMAP健康检查成功，否则将重新进行健康检查；若连续重试的次数超过用户设置的“重试次数”，则认为IMAP健康检查失败。

在健康检查配置模式下，使用以下命令配置IMAP健康检查：

- DSR模式：指定设备在DSR模式下开启IMAP健康检查。只有开启该项，系统才支持设备在DSR模式下的IMAP健康检查功能。IMAP健康检查的IP地址需指定为真实服务器的Loopback口地址，且不允许用户配置发送IMAP健康检查请求的源接口。

direct-server-return - 开启设备在DSR模式下的IMAP健康检查。

使用**no direct-server-return**命令关闭该功能。

- 指定用来IMAP健康检查的真实服务上的特定文件夹。

folder *value*

- IP地址：指定IP地址。若不指定，系统将直接引用真实服务的IP地址。

ip *ip-address*

- 端口：指定端口。若不指定，系统将直接引用真实服务的端口。

port *port-number*

- 源接口：指定发送IMAP健康检查请求的源接口。

source-interface *interface*

- 指定IMAP健康检查时用来登录的用户名。

username *value*

- 指定IMAP健康检查时用来登录的用户密码。

passwd *value*

- 当该IMAP健康检查的失败判定方式为**by-count**时，配置如下参数：

- 间隔时间：指定本次IMAP健康检查与下次检查的时间间隔。取值范围是1到900秒，默认值是9秒。

interval *value*

- 超时时间：指定IMAP健康检查时，设备收到真实服务的应答报文的超时时间。在超时时间内，若真实服务未返回预期响应，系统将认定此次检查失败。取值范围是1到600秒，默认值是6秒。

timeout *value*

- 失败重试次数：指定IMAP健康检查失败，需重新检查时，可重新检查的次数。取值范围是1到10，默认值是3。

retry *value*

- 失败重试间隔：指定IMAP健康检查失败，需重新检查时，两次检查的时间间隔。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

retry-interval *value*

- 成功重试次数：指定IMAP健康检查成功，需重新检查时，可重新检查的次数。取值范围是1到10，默认值是1。

up-retry *value*

- 成功重试间隔：指定IMAP健康检查成功，需重新检查时，两次检查的时间间隔。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

up-retry-interval *value*

详细介绍，请参阅“[按次数](#)”。

- 当该IMAP健康检查的失败判定方式为**by-time**时，配置如下参数：

- 间隔时间：指定本次IMAP健康检查与下次检查的时间间隔。取值范围是1到900秒，默认值是5秒。

interval *value*

- 超时时间：指定IMAP健康检查因失败进行重新检查时，可重新检查的总时长。取值范围是1到9000秒，默认值是16秒。

timeout *value*

- 成功重试时长：指定IMAP健康检查成功，需重新检查时，可重新检查的总时长。取值范围是1到9000秒。

time-util-up *value*

- 成功重试间隔：指定IMAP健康检查成功，需重新检查时，两次检查的间隔时间。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

up-interval *value*

详细介绍，请参阅 [“按时间”](#)。

在健康检查配置模式下，使用上述命令 **no** 的形式取消配置。

POP3健康检查

用于对POP3（邮局协议版本3）服务状态进行健康检查。检查时，若在超时时间内，设备与真实服务能够连接成功，且能够使用指定的用户名&密码登录成功，然后退出，则认为POP3健康检查成功，否则将重新进行健康检查；若连续重试的次数超过用户设置的“重试次数”，则认为POP3健康检查失败。

在健康检查配置模式下，使用以下命令配置POP3健康检查：

- DSR模式：指定设备在DSR模式下开启POP3健康检查。只有开启该项，系统才支持设备在DSR模式下的POP3健康检查功能。POP3健康检查的IP地址需指定为真实服务器的Loopback口地址，且不允许用户配置发送POP3健康检查请求的源接口。

direct-server-return - 开启设备在DSR模式下的IMAP健康检查。

使用**no direct-server-return**命令关闭该功能。

- IP地址：指定IP地址。若不指定，系统将直接引用真实服务的IP地址。

ip *ip-address*

- 端口：指定端口。若不指定，系统将直接引用真实服务的端口。

port *port-number*

- 源接口：指定发送POP3健康检查请求的源接口。

source-interface *interface*

- 指定POP3健康检查时用来登录的用户名。

username *value*

- 指定POP3健康检查时用来登录的用户密码。

passwd *value*

- 当该POP3健康检查的失败判定方式为**by-count**时，配置如下参数：

- 间隔时间：指定本次POP3健康检查与下次检查的时间间隔。取值范围是1到900秒，默认值是9秒。

interval *value*

- 超时时间：指定POP3健康检查时，设备收到真实服务的应答报文的超时时间。在超时时间内，若真实服务未返回预期响应，系统将认定此次检查失败。取值范围是1到600秒，默认值是6秒。

timeout *value*

- 失败重试次数：指定POP3健康检查失败，需重新检查时，可重新检查的次数。取值范围是1到10，默认值是3。

retry *value*

- 失败重试间隔：指定POP3健康检查失败，需重新检查时，两次检查的时间间隔。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

retry-interval *value*

- 成功重试次数：指定POP3健康检查成功，需重新检查时，可重新检查的次数。取值范围是1到10，默认值是1。

up-retry *value*

- 成功重试间隔：指定POP3健康检查成功，需重新检查时，两次检查的时间间隔。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

up-retry-interval *value*

详细介绍，请参阅“[按次数](#)”。

- 当该POP3健康检查的失败判定方式为**by-time**时，配置如下参数：

- 间隔时间：指定本次POP3健康检查与下次检查的时间间隔。取值范围是1到900秒，默认值是5秒。

interval *value*

- 超时时间：指定POP3健康检查因失败进行重新检查时，可重新检查的总时长。取值范围是1到9000秒，默认值是16秒。

timeout *value*

- 成功重试时长：指定POP3健康检查成功，需重新检查时，可重新检查的总时长。取值范围是1到9000秒。

time-util-up *value*

- 成功重试间隔：指定POP3健康检查成功，需重新检查时，两次检查的间隔时间。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

up-interval *value*

详细介绍，请参阅 [“按时间”](#)。

在健康检查配置模式下，使用上述命令 **no** 的形式取消配置。

SMTP健康检查

用于对真实服务的SMTP（简单邮件传输协议）服务的状态进行健康检查。检查时，设备与真实服务首先建立TCP连接，设备向真实服务发送HELO或QUIT报文，在超时时间内，若真实服务能返回标准的SMTP HELO或QUIT响应报文，则认为SMTP健康检查成功，否则将重新进行健康检查；若连续重试的次数超过用户设置的“重试次数”，则认为SMTP健康检查失败。

在健康检查配置模式下，使用以下命令配置SMTP健康检查：

- DSR模式：指定设备在DSR模式下开启SMTP健康检查。只有开启该项，系统才支持设备在DSR模式下的SMTP健康检查功能。SMTP健康检查的IP地址需指定为真实服务器的Loopback口地址，且不允许用户配置发送SMTP健康检查请求的源接口。

direct-server-return - 开启设备在DSR模式下的SMTP健康检查。

使用**no direct-server-return**命令关闭该功能。

- 指定SMTP健康检查时，SMTP邮件发送者的主机名。

domain *domain-name*

- IP地址：指定IP地址。若不指定，系统将直接引用真实服务的IP地址。

ip *ip-address*

- 端口：指定端口。若不指定，系统将直接引用真实服务的端口。

port *port-number*

- 源接口：指定发送SMTP健康检查请求的源接口。

source-interface *interface*

- 当该SMTP健康检查的失败判定方式为**by-count**时，配置如下参数：

- 间隔时间：指定本次SMTP健康检查与下次检查的时间间隔。取值范围是1到900秒，默认值是9秒。

interval *value*

- 超时时间：指定SMTP健康检查时，设备收到真实服务的应答报文的超时时间。在超时时间内，若真实服务未返回预期响应，系统将认定此次检查失败。取值范围是1到600秒，默认值是6秒。

timeout *value*

- 失败重试次数：指定SMTP健康检查失败，需重新检查时，可重新检查的次数。取值范围是1到10，默认值是3。

retry *value*

- 失败重试间隔：指定SMTP健康检查失败，需重新检查时，两次检查的时间间隔。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

retry-interval *value*

- 成功重试次数：指定SMTP健康检查成功，需重新检查时，可重新检查的次数。取值范围是1到10，默认值是1。

up-retry *value*

- 成功重试间隔：指定SMTP健康检查成功，需重新检查时，两次检查的时间间隔。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

up-retry-interval *value*

详细介绍，请参阅 [“按次数”](#)。

- 当该SMTP健康检查的失败判定方式为**by-time**时，配置如下参数：

- 间隔时间：指定本次SMTP健康检查与下次检查的时间间隔。取值范围是1到900秒，默认值是5秒。

interval *value*

- 超时时间：指定SMTP健康检查因失败进行重新检查时，可重新检查的总时长。取值范围是1到9000秒，默认值是16秒。

timeout *value*

- 成功重试时长：指定SMTP健康检查成功，需重新检查时，可重新检查的总时长。取值范围是1到9000秒。

time-util-up *value*

- 成功重试间隔：指定SMTP健康检查成功，需重新检查时，两次检查的间隔时间。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

up-interval *value*

详细介绍，请参阅 [“按时间”](#)。

在健康检查配置模式下，使用上述命令 **no** 的形式取消配置。

TCP健康检查

用于对设备与真实服务之间的TCP的连接状态进行检查。检查时，设备与真实服务建立TCP连接并发送特定的内容，在超时时间内，若真实服务返回的内容包含配置的预期内容，则认为TCP健康检查成功，否则将重新进行健康检查；若连续重试的次数超过用户设置的“重试次数”，则认为TCP健康检查失败。

在健康检查配置模式下，使用以下命令配置TCP健康检查：

- DSR模式：指定设备在DSR模式下开启TCP健康检查。只有开启该项，系统才支持设备在DSR模式下的TCP健康检查功能。TCP健康检查的IP地址需指定为真实服务器的Loopback口地址，且不允许用户配置发送TCP健康检查请求的源接口。

direct-server-return - 开启设备在DSR模式下的TCP健康检查。

使用**no direct-server-return**命令关闭该功能。

- IP地址：指定IP地址。若不指定，系统将直接引用真实服务的IP地址。

ip *ip-address*

- 端口：指定端口。若不指定，系统将直接引用真实服务的端口。

port *port-number*

- 源接口：指定发送TCP健康检查请求的源接口。

source-interface *interface*

- 指定TCP健康检查时，用户期望接收到的返回内容，用于与真实服务实际返回的内容进行比较：若匹配，即服务器返回的内容中包含该“接收内容”，即认为此次TCP健康检查成功。若不匹配，即服务器返回的内容中不包含该“接收内容”，即认为TCP健康检查失败。当接收内容被配置为空，而发送内容不为空时，则表示只检查真实服务的是否连接成功以及真实服务是否能够响应，不检查真实服务响应的内容。

recv-string *value*

- 指定用于TCP健康检查的特定的发送内容。当发送内容被配置为空时，则表示只检查TCP连接是否成功。

send-string *value*

- 当该TCP健康检查的失败判定方式为**by-count**时，配置如下参数：

- 间隔时间：指定本次TCP健康检查与下次检查的时间间隔。取值范围是1到900秒，默认值是9秒。

interval *value*

- 超时时间：指定TCP健康检查时，设备收到真实服务的应答报文的超时时间。在超时时间内，若真实服务未返回预期响应，系统将认定此次检查失败。取值范围是1到600秒，默认值是6秒。

timeout *value*

- 失败重试次数：指定TCP健康检查失败，需重新检查时，可重新检查的次数。取值范围是1到10，默认值是3。

retry *value*

- 失败重试间隔：指定TCP健康检查失败，需重新检查时，两次检查的间隔时间。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

retry-interval *value*

- 成功重试次数：指定TCP健康检查成功，需重新检查时，可重新检查的次数。取值范围是1到10，默认值是1。

up-retry *value*

- 成功重试间隔：指定TCP健康检查成功，需重新检查时，两次检查的间隔时间。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

up-retry-interval *value*

详细介绍，请参阅“[按次数](#)”。

- 当该TCP健康检查的失败判定方式为**by-time**时，配置如下参数：

- 间隔时间：指定本次TCP健康检查与下次检查的时间间隔。取值范围是1到900秒，默认值是5秒。

interval *value*

- 超时时间：指定TCP健康检查因失败进行重新检查时，可重新检查的总时长。取值范围是1到9000秒，默认值是16秒。

timeout *value*

- 成功重试时长：指定TCP健康检查成功，需重新检查时，可重新检查的总时长。取值范围是1到9000秒。

time-util-up *value*

- 成功重试间隔：指定TCP健康检查成功，需重新检查时，两次检查的间隔时间。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

up-interval *value*

详细介绍，请参阅 [“按时间”](#)。

在健康检查配置模式下，使用上述命令 **no** 的形式取消配置。

TCP-ECHO健康检查

用于对设备与真实服务之间的TCP的连接状态进行检查。检查时，设备通过ECHO端口（默认端口为7）与真实服务建立TCP连接并发送特定的字符串，若真实服务返回的字符串与原先发送的字符串相同，则认为TCP-ECHO健康检查成功，否则将重新进行健康检查；若连续重试的次数超过用户设置的“重试次数”，则认为TCP-ECHO健康检查失败。

在健康检查配置模式下，使用以下命令配置TCP-ECHO健康检查：

- DSR模式：指定设备在DSR模式下开启TCP-ECHO健康检查。只有开启该项，系统才支持设备在DSR模式下的TCP-ECHO健康检查功能。TCP-ECHO健康检查的IP地址需指定为真实服务器的Loopback口地址，且不允许用户配置发送TCP-ECHO健康检查请求的源接口。

direct-server-return - 开启设备在DSR模式下的TCP-ECHO健康检查。

使用**no direct-server-return**命令关闭该功能。

- 超时时间：指定TCP-ECHO健康检查时，设备收到真实服务的应答报文的超时时间。

timeout *value*

- 重试次数：指定TCP-ECHO健康检查失败时，可重新检查的次数。

retry *value*

- 重试间隔：指定TCP-ECHO健康检查重新检查时，两次检查的间隔时间。

retry-interval *value*

- 间隔时间：指定TCP-ECHO健康检查与下次检查的时间间隔。

interval *value*

- IP地址：指定IP地址。若不指定，系统将直接引用真实服务的IP地址。

ip *ip-address*

- 端口：指定端口。若不指定，系统将直接引用真实服务的端口。

port *port-number*

- 源接口：指定发送TCP-ECHO健康检查请求的源接口。

source-interface *interface*

- 当该TCP-ECHO健康检查的失败判定方式为**by-count**时，配置如下参数：

- 间隔时间：指定本次TCP-ECHO健康检查与下次检查的时间间隔。取值范围是1到900秒，默认值是9秒。

interval *value*

- 超时时间：指定TCP-ECHO健康检查时，设备收到真实服务的应答报文的超时时间。在超时时间内，若真实服务未返回预期响应，系统将认定此次检查失败。取值范围是1到600秒，默认值是6秒。

timeout *value*

- 失败重试次数：指定TCP-ECHO健康检查失败，需重新检查时，可重新检查的次数。取值范围是1到10，默认值是3。

retry *value*

- 失败重试间隔：指定TCP-ECHO健康检查失败，需重新检查时，两次检查的时间间隔。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

retry-interval *value*

- 成功重试次数：指定TCP-ECHO健康检查成功，需重新检查时，可重新检查的次数。取值范围是1到10，默认值是1。

up-retry *value*

- 成功重试间隔：指定TCP-ECHO健康检查成功，需重新检查时，两次检查的时间间隔。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

up-retry-interval *value*

详细介绍，请参阅 [“按次数”](#)。

- 当该TCP-ECHO健康检查的失败判定方式为**by-time**时，配置如下参数：

- 间隔时间：指定本次TCP-ECHO健康检查与下次检查的时间间隔。取值范围是1到900秒，默认值是5秒。

interval *value*

- 超时时间：指定TCP-ECHO健康检查因失败进行重新检查时，可重新检查的总时长。取值范围是1到9000秒，默认值是16秒。

timeout *value*

- 成功重试时长：指定TCP-ECHO健康检查成功，需重新检查时，可重新检查的总时长。取值范围是1到9000秒。

time-util-up *value*

- 成功重试间隔：指定TCP-ECHO健康检查成功，需重新检查时，两次检查的间隔时间。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

up-interval *value*

详细介绍，请参阅 [“按时间”](#)。

在健康检查配置模式下，使用上述命令 **no** 的形式取消配置。

TCP-HALF-OPEN健康检查

用于对设备与真实服务之间的TCP连接进行检查。检查时，设备通过与真实服务建立TCP半连接进行检查。设备发送SYN报文给真实服务，若真实服务返回SYN ACK报文，则认为TCP-HALF-OPEN健康检查成功，否则将重新进行健康检查；若连续重试的次数超过用户设置的“重试次数”，则认为TCP-HALF-OPEN健康检查失败。

在健康检查配置模式下，使用以下命令配置TCP-HALF-OPEN健康检查：

- DSR模式：指定设备在DSR模式下开启TCP-HALF-OPEN健康检查。只有开启该项，系统才支持设备在DSR模式下的TCP-HALF-OPEN健康检查功能。TCP-ECHO健康检查的IP地址需指定为真实服务器的Loopback口地址，且不允许用户配置发送TCP-HALF-OPEN健康检查请求的源接口。

direct-server-return - 开启设备在DSR模式下的TCP-HALF-OPEN健康检查。

使用**no direct-server-return**命令关闭该功能。

- IP地址：指定IP地址。若不指定，系统将直接引用真实服务的IP地址。

ip *ip-address*

- 端口：指定端口。若不指定，系统将直接引用真实服务的端口。

port *port-number*

- 源接口：指定发送TCP-HALF-OPEN健康检查请求的源接口。

source-interface *interface*

- 当该TCP-HALF-OPEN健康检查的失败判定方式为**by-count**时，配置如下参数：

- 间隔时间：指定本次TCP-HALF-OPEN健康检查与下次检查的时间间隔。取值范围是1到900秒，默认值是9秒。

interval *value*

- 超时时间：指定TCP-HALF-OPEN健康检查时，设备收到真实服务的应答报文的超时时间。在超时时间内，若真实服务未返回预期响应，系统将认定此次检查失败。取值范围是1到600秒，默认值是6秒。

timeout *value*

- 失败重试次数：指定TCP-HALF-OPEN健康检查失败，需重新检查时，可重新检查的次数。取值范围是1到10，默认值是3。

retry *value*

- 失败重试间隔：指定TCP-HALF-OPEN健康检查失败，需重新检查时，两次检查的间隔时间。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

retry-interval *value*

- 成功重试次数：指定TCP-HALF-OPEN健康检查成功，需重新检查时，可重新检查的次数。取值范围是1到10，默认值是1。

up-retry *value*

- 成功重试间隔：指定TCP-HALF-OPEN健康检查成功，需重新检查时，两次检查的间隔时间。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

up-retry-interval *value*

详细介绍，请参阅 [“按次数”](#)。

- 当该TCP-HALF-OPEN健康检查的失败判定方式为**by-time**时，配置如下参数：
 - 间隔时间：指定本次TCP-HALF-OPEN健康检查与下次检查的时间间隔。取值范围是1到900秒，默认值是5秒。
interval value
 - 超时时间：指定TCP-HALF-OPEN健康检查因失败进行重新检查时，可重新检查的总时长。取值范围是1到9000秒，默认值是16秒。
timeout value
 - 成功重试时长：指定TCP-HALF-OPEN健康检查成功，需重新检查时，可重新检查的总时长。取值范围是1到9000秒。
time-util-up value
 - 成功重试间隔：指定TCP-HALF-OPEN健康检查成功，需重新检查时，两次检查的间隔时间。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。
up-interval value
- 详细介绍，请参阅 [“按时间”](#)。

在健康检查配置模式下，使用上述命令 **no** 的形式取消配置。

UDP健康检查

用于对设备与真实服务之间的UDP服务进行检查。检查时，设备向真实服务通过UDP发送特定的内容，在超时时间内，若真实服务返回的内容包含配置的预期内容，则认为UDP健康检查成功；若连续失败的次数超过重试次数，则认为UDP健康检查失败。

在健康检查配置模式下，使用以下命令配置UDP健康检查：

- DSR模式：指定设备在DSR模式下开启UDP健康检查。只有开启该项，系统才支持设备在DSR模式下的UDP健康检查功能。UDP健康检查的IP地址需指定为真实服务器的Loopback口地址，且不允许用户配置发送UDP健康检查请求的源接口。
direct-server-return - 开启设备在DSR模式下的UDP健康检查。
使用**no direct-server-return**命令关闭该功能。
- IP地址：指定IP地址。若不指定，系统将直接引用真实服务的IP地址。
ip ip-address

- 端口：指定端口。若不指定，系统将直接引用真实服务的端口。

port *port-number*

- 源端口：指定源端口。若不指定，系统将引用当前设备的可用端口。

src-port *port-number*

- 源接口：指定发送UDP健康检查请求的源接口。

source-interface *interface*

- 指定UDP健康检查时，用户期望接收到的返回内容，用于与真实服务实际返回的内容进行比较：若匹配，即服务器返回的内容中包含该“接收内容”，即认为此次UDP健康检查成功。若不匹配，即服务器返回的内容中不包含该“接收内容”，即认为此次UDP健康检查失败。当接收内容被配置为空，而发送内容不为空时，则表示只检查真实服务的是否连接成功以及真实服务是否能够响应，不检查真实服务响应的内容。

recv-string *value*

- 指定用于UDP健康检查的特定的发送内容。当发送内容被配置为空时，则表示只检查UDP连接是否成功。

send-string *value*

- 当该UDP健康检查的失败判定方式为**by-count**时，配置如下参数：

- 间隔时间：指定本次UDP健康检查与下次检查的时间间隔。取值范围是1到900秒，默认值是9秒。

interval *value*

- 超时时间：指定UDP健康检查时，设备收到真实服务的应答报文的超时时间。在超时时间内，若真实服务未返回预期响应，系统将认定此次检查失败。取值范围是1到600秒，默认值是6秒。

timeout *value*

- 失败重试次数：指定UDP健康检查失败，需重新检查时，可重新检查的次数。取值范围是1到10，默认值是3。

retry *value*

- 失败重试间隔：指定UDP健康检查失败，需重新检查时，两次检查的间隔时间。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

retry-interval *value*

- 成功重试次数：指定UDP健康检查成功，需重新检查时，可重新检查的次数。取值范围是1到10，默认值是1。

up-retry *value*

- 成功重试间隔：指定UDP健康检查成功，需重新检查时，两次检查的间隔时间。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

up-retry-interval *value*

详细介绍，请参阅 [“按次数”](#)。

- 当该UDP健康检查的失败判定方式为**by-time**时，配置如下参数：

- 间隔时间：指定本次UDP健康检查与下次检查的时间间隔。取值范围是1到900秒，默认值是5秒。

interval *value*

- 超时时间：指定UDP健康检查因失败进行重新检查时，可重新检查的总时长。取值范围是1到9000秒，默认值是16秒。

timeout *value*

- 成功重试时长：指定UDP健康检查成功，需重新检查时，可重新检查的总时长。取值范围是1到9000秒。

time-util-up *value*

- 成功重试间隔：指定UDP健康检查成功，需重新检查时，两次检查的间隔时间。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

up-interval *value*

详细介绍，请参阅 [“按时间”](#)。

在健康检查配置模式下，使用上述命令 **no** 的形式取消配置。

Third-Party健康检查

系统支持用户上传第三方脚本文件进行健康检查。目前支持上传Python脚本文件（UNIX格式的.py文件）。另外，设备自带基于Exchange的第三方健康检查脚本，用于对Exchange服务器进行健康检查。检查时，设备根据脚本内容来执行相关的健康检查，在超时时间内，脚本执行成功则认为健康检查成功。

在健康检查配置模式下，使用以下命令配置Third-Party健康检查：

- IP地址：指定IP地址。若不指定，系统将直接引用真实服务的IP地址。

ip *ip-address*

- 端口：指定端口。若不指定，系统将直接引用真实服务的端口。

port *port-number*

- 指定Third-Party健康检查中脚本文件中的脚本启动参数。

arguments *value*

- 指定Third-Party健康检查脚本文件，脚本文件需提前上传完成。

file-name *value*

- 当该Third-Party健康检查的失败判定方式为**by-count**时，配置如下参数：

- 间隔时间：指定本次Third-Party健康检查与下次检查的时间间隔。取值范围是1到900秒，默认值是9秒。

interval *value*

- 超时时间：指定Third-Party健康检查时，设备收到真实服务的应答报文的超时时间。在超时时间内，若真实服务未返回预期响应，系统将认定此次检查失败。取值范围是1到600秒，默认值是6秒。

timeout *value*

- 失败重试次数：指定Third-Party健康检查失败，需重新检查时，可重新检查的次数。取值范围是1到10，默认值是3。

retry *value*

- 失败重试间隔：指定Third-Party健康检查失败，需重新检查时，两次检查的间隔时间。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

retry-interval *value*

- 成功重试次数：指定Third-Party健康检查成功，需重新检查时，可重新检查的次数。取值范围是1到10，默认值是1。

up-retry *value*

- 成功重试间隔：指定Third-Party健康检查成功，需重新检查时，两次检查的间隔时间。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

up-retry-interval *value*

详细介绍，请参阅 [“按次数”](#)。

- 当该Third-Party健康检查的失败判定方式为**by-time**时，配置如下参数：

- 间隔时间：指定本次Third-Party健康检查与下次检查的时间间隔。取值范围是1到900秒，默认值是5秒。

interval *value*

- 超时时间：指定Third-Party健康检查因失败进行重新检查时，可重新检查的总时长。取值范围是1到9000秒，默认值是16秒。

timeout *value*

- 成功重试时长：指定Third-Party健康检查成功，需重新检查时，可重新检查的总时长。取值范围是1到9000秒。

time-util-up *value*

- 成功重试间隔：指定Third-Party健康检查成功，需重新检查时，两次检查的间隔时间。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

up-interval *value*

详细介绍，请参阅“[按时间](#)”。

在健康检查配置模式下，使用上述命令 **no** 的形式取消配置。

RADIUS-AUTHENTICATION健康检查

用于对RADIUS-AUTHENTICATION服务进行健康检查。检查时，设备向真实服务发送包含如下配置项的RADIUS数据包，在超时时间内，若真实服务能返回Access-Accept报文，则认为RADIUS-AUTHENTICATION健康检查成功，否则将重新进行健康检查；若连续重试的次数超过用户设置的“重试次数”，则认为RADIUS-AUTHENTICATION健康检查失败。

在健康检查配置模式下，使用以下命令配置RADIUS-AUTHENTICATION健康检查：

- DSR模式：指定设备在DSR模式下开启RADIUS-AUTHENTICATION健康检查。只有开启该项，系统才支持设备在DSR模式下的RADIUS-AUTHENTICATION健康检查功能。RADIUS-AUTHENTICATION健康检查的IP地址需指定为真实服务器的Loopback口地址，且不允许用户配置发送RADIUS-AUTHENTICATION健康检查请求的源接口。

direct-server-return - 开启设备在DSR模式下的RADIUS-AUTHENTICATION健康检查。

使用**no direct-server-return**命令关闭该功能。

- IP地址：指定IP地址。若不指定，系统将直接引用真实服务的IP地址。

ip *ip-address*

- NAS IP地址：指定NAS地址，包括IPv4或IPv6地址。

nap-ip-address {*x.x.x.x* | *X.X.X.X::X*}

- 端口：指定端口。若不指定，系统将直接引用真实服务的端口。

port *port-number*

- 源接口：指定发送RADIUS-AUTHENTICATION健康检查请求的源接口。

source-interface *interface*

- 用户名：指定RADIUS-AUTHENTICATION健康检查的用户名。

username *value*

- 密码：指定用户名对应的密码。

passwd *value*

- 共享密钥：指定设备与真实服务之间的共享密钥。

secret *shared-secret*

- 当该RADIUS-AUTHENTICATION健康检查的失败判定方式为**by-count**时，配置如下参数：

- 间隔时间：指定本次RADIUS-AUTHENTICATION健康检查与下次检查的时间间隔。取值范围是1到900秒，默认值是9秒。

interval *value*

- 超时时间：指定RADIUS-AUTHENTICATION健康检查时，设备收到真实服务的应答报文的超时时间。在超时时间内，若真实服务未返回预期响应，系统将认定此次检查失败。取值范围是1到600秒，默认值是6秒。

timeout *value*

- 失败重试次数：指定RADIUS-AUTHENTICATION健康检查失败，需重新检查时，可重新检查的次数。取值范围是1到10，默认值是3。

retry *value*

- 失败重试间隔：指定RADIUS-AUTHENTICATION健康检查失败，需重新检查时，两次检查的间隔时间。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

retry-interval *value*

- 成功重试次数：指定RADIUS-AUTHENTICATION健康检查成功，需重新检查时，可重新检查的次数。取值范围是1到10，默认值是1。

up-retry *value*

- 成功重试间隔：指定RADIUS-AUTHENTICATION健康检查成功，需重新检查时，两次检查的间隔时间。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

up-retry-interval *value*

详细介绍，请参阅“[按次数](#)”。

- 当该RADIUS-AUTHENTICATION健康检查的失败判定方式为**by-time**时，配置如下参数：

- 间隔时间：指定本次RADIUS-AUTHENTICATION健康检查与下次检查的时间间隔。取值范围是1到900秒，默认值是5秒。

interval *value*

- 超时时间：指定RADIUS-AUTHENTICATION健康检查因失败进行重新检查时，可重新检查的总时长。取值范围是1到9000秒，默认值是16秒。

timeout *value*

- 成功重试时长：指定RADIUS-AUTHENTICATION健康检查成功，需重新检查时，可重新检查的总时长。取值范围是1到9000秒。

time-util-up *value*

- 成功重试间隔：指定RADIUS-AUTHENTICATION健康检查成功，需重新检查时，两次检查的间隔时间。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

up-interval *value*

详细介绍，请参阅“[按时间](#)”。

在健康检查配置模式下，使用上述命令 **no** 的形式取消配置。

RADIUS-ACCOUNTING健康检查

用于对RADIUS-ACCOUNTING服务进行健康检查。检查时，设备向真实服务发送包含如下配置项的RADIUS数据包，在超时时间内，若真实服务能返回Accounting-Response报文，则认为RADIUS-ACCOUNTING健康检查成功，否则将重新进行健康检查；若连续重试的次数超过用户设置的“重试次数”，则认为RADIUS-ACCOUNTING健康检查失败。

在健康检查配置模式下，使用以下命令配置RADIUS-ACCOUNTING健康检查：

- DSR模式：指定设备在DSR模式下开启RADIUS-ACCOUNTING健康检查。只有开启该项，系统才支持设备在DSR模式下的RADIUS-ACCOUNTING健康检查功能。RADIUS-ACCOUNTING健康检查的IP地址需指定

为真实服务器的Loopback口地址，且不允许用户配置发送RADIUS-ACCOUNTING健康检查请求的源接口。

direct-server-return - 开启设备在DSR模式下的RADIUS-ACCOUNTING健康检查。

使用**no direct-server-return**命令关闭该功能。

- IP地址：指定IP地址。若不指定，系统将直接引用真实服务的IP地址。

ip *ip-address*

- NAS IP地址：指定NAS地址，包括IPv4或IPv6地址。

nap-ip-address {*x.x.x.x* | *X.X.X.X::X*}

- 端口：指定端口。若不指定，系统将直接引用真实服务的端口。

port *port-number*

- 源接口：指定发送RADIUS-ACCOUNTING健康检查请求的源接口。

source-interface *interface*

- 用户名：指定RADIUS-ACCOUNTING健康检查的用户名。

username *value*

- 共享密钥：指定设备与真实服务之间的共享密钥。

secret *shared-secret*

- 当该RADIUS-ACCOUNTING健康检查的失败判定方式为**by-count**时，配置如下参数：

- 间隔时间：指定本次RADIUS-ACCOUNTING健康检查与下次检查的时间间隔。取值范围是1到900秒，默认值是9秒。

interval *value*

- 超时时间：指定RADIUS-ACCOUNTING健康检查时，设备收到真实服务的应答报文的超时时间。在超时时间内，若真实服务未返回预期响应，系统将认定此次检查失败。取值范围是1到600秒，默认值是6秒。

timeout *value*

- 失败重试次数：指定RADIUS-ACCOUNTING健康检查失败，需重新检查时，可重新检查的次数。取值范围是1到10，默认值是3。

retry *value*

- 失败重试间隔：指定RADIUS-ACCOUNTING健康检查失败，需重新检查时，两次检查的间隔时间。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

retry-interval *value*

- 成功重试次数：指定RADIUS-ACCOUNTING健康检查成功，需重新检查时，可重新检查的次数。取值范围是1到10，默认值是1。

up-retry *value*

- 成功重试间隔：指定RADIUS-ACCOUNTING健康检查成功，需重新检查时，两次检查的间隔时间。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

up-retry-interval *value*

详细介绍，请参阅 [“按次数”](#)。

- 当该RADIUS-ACCOUNTING健康检查的失败判定方式为**by-time**时，配置如下参数：

- 间隔时间：指定本次RADIUS-ACCOUNTING健康检查与下次检查的时间间隔。取值范围是1到900秒，默认值是5秒。

interval *value*

- 超时时间：指定RADIUS-ACCOUNTING健康检查因失败进行重新检查时，可重新检查的总时长。取值范围是1到9000秒，默认值是16秒。

timeout *value*

- 成功重试时长：指定RADIUS-ACCOUNTING健康检查成功，需重新检查时，可重新检查的总时长。取值范围是1到9000秒。

time-util-up *value*

- 成功重试间隔：指定RADIUS-ACCOUNTING健康检查成功，需重新检查时，两次检查的间隔时间。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

up-interval *value*

详细介绍，请参阅 [“按时间”](#)。

在健康检查配置模式下，使用上述命令 **no** 的形式取消配置。

WebSocket健康检查

用于对WebSocket服务状态进行健康检查。检查时，设备向真实服务发送数据，在超时时间内，收到真实服务的回应报文，则认为WebSocket健康检查成功，否则将重新进行健康检查；若连续重试的次数超过用户设置的“重试次数”，则认为WebSocket健康检查失败。

在健康检查配置模式下，使用以下命令配置WebSocket健康检查：

- DSR模式：指定设备在DSR模式下开启WebSocket健康检查。只有开启该项，系统才支持设备在DSR模式下的WebSocket健康检查功能。WebSocket健康检查的IP地址需指定为真实服务器的Loopback口地址，且不允许用户配置发送WebSocket健康检查请求的源接口。

direct-server-return - 开启设备在DSR模式下的WebSocket健康检查。

使用**no direct-server-return**命令关闭该功能。

- IP地址：指定IP地址。若不指定，系统将直接引用真实服务的IP地址。

ip *ip-address*

- 端口：指定端口。若不指定，系统将直接引用真实服务的端口。

port *port-number*

- 源接口：指定发送WebSocket健康检查请求的源接口。

source-interface *interface*

- Sec-WebSocket-Key键值：用于防止跨协议攻击。

websocket-key *value*

- 主机名称：配置WEBSOCKET健康检查时，可指定Host字段。配置后，健康检查时发送的Request请求会使用已配置的Host字段。默认为引用真实服务的IP地址。

host *value*

- 源域：指定Origin头字段。

origin *value*

- 扩展字段：指定扩展字段的值，服务器会根据客户端支持的扩展字段来判断是否建立连接。

sec-websocket-extensions *value*

- 子协议：客户端可以通过在握手阶段中的Sec-WebSocket-Protocol字段来请求服务端使用指定的子协议。如果指定了这个字段，服务器需要包含相同的字段，并从子协议中选择一个值作为建立连接的响应。

sec-websocket-protocol *value*

- 当该WEBSOCKET健康检查的失败判定方式为**by-count**时，配置如下参数：

- 间隔时间：指定本次WEBSOCKET健康检查与下次检查的时间间隔。取值范围是1到900秒，默认值是9秒。

interval *value*

- 超时时间：指定WEBSOCKET健康检查时，设备收到真实服务的应答报文的超时时间。在超时时间内，若真实服务未返回预期响应，系统将认定此次检查失败。取值范围是1到600秒，默认值是6秒。

timeout *value*

- 失败重试次数：指定WEBSOCKET健康检查失败，需重新检查时，可重新检查的次数。取值范围是1到10，默认值是3。

retry *value*

- 失败重试间隔：指定WEBSOCKET健康检查失败，需重新检查时，两次检查的间隔时间。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

retry-interval *value*

- 成功重试次数：指定WEBSOCKET健康检查成功，需重新检查时，可重新检查的次数。取值范围是1到10，默认值是1。

up-retry *value*

- 成功重试间隔：指定WEBSOCKET健康检查成功，需重新检查时，两次检查的间隔时间。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

up-retry-interval *value*

详细介绍，请参阅 [“按次数”](#)。

- 当该WebSocket健康检查的失败判定方式为**by-time**时，配置如下参数：

- 间隔时间：指定本次WebSocket健康检查与下次检查的时间间隔。取值范围是1到900秒，默认值是5秒。

interval *value*

- 超时时间：指定WebSocket健康检查因失败进行重新检查时，可重新检查的总时长。取值范围是1到9000秒，默认值是16秒。

timeout *value*

- 成功重试时长：指定WebSocket健康检查成功，需重新检查时，可重新检查的总时长。取值范围是1到9000秒。

time-util-up *value*

- 成功重试间隔：指定WebSocket健康检查成功，需重新检查时，两次检查的间隔时间。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

up-interval *value*

详细介绍，请参阅 [“按时间”](#)。

在健康检查配置模式下，使用上述命令 **no** 的形式取消配置。

WebSocket-SSL健康检查

用于对使用SSL证书进行加密的WebSocket服务状态进行健康检查。检查时，设备向真实服务发送数据，在超时间内，收到真实服务的回应报文，则认为WebSocket-SSL健康检查成功，否则将重新进行健康检查；若连续重试的次数超过用户设置的“重试次数”，则认为WebSocket-SSL健康检查失败。

在健康检查配置模式下，使用以下命令配置WebSocket-SSL健康检查：

- DSR模式：指定设备在DSR模式下开启WebSocket-SSL健康检查。只有开启该项，系统才支持设备在DSR模式下的WebSocket-SSL健康检查功能。WebSocket-SSL健康检查的IP地址需指定为真实服务器的Loopback口地址，且不允许用户配置发送WebSocket-SSL健康检查请求的源接口。

direct-server-return - 开启设备在DSR模式下的WebSocket-SSL健康检查。

使用**no direct-server-return**命令关闭该功能。

- IP地址：指定IP地址。若不指定，系统将直接引用真实服务的IP地址。

ip *ip-address*

- 端口：指定端口。若不指定，系统将直接引用真实服务的端口。

port *port-number*

- 源接口：指定发送WebSocket-SSL健康检查请求的源接口。

source-interface *interface*

- Sec-WebSocket-Key键值：用于防止跨协议攻击。

websocket-key *value*

- 主机名称：配置WebSocket-SSL健康检查时，可指定Host字段。配置后，健康检查时发送的Request请求会使用已配置的Host字段。默认为引用真实服务的IP地址。

host *value*

- 源域：指定Origin头字段。

origin *value*

- 扩展字段：指定扩展字段的值，服务器会根据客户端支持的扩展字段来判断是否建立连接。

sec-websocket-extensions *value*

- 子协议：客户端可以通过在握手阶段中的Sec-WebSocket-Protocol字段来请求服务端使用指定的子协议。如果指定了这个字段，服务器需要包含相同的字段，并从子协议中选择一个值作为建立连接的响应。

sec-websocket-protocol *value*

- 当该WebSocket-SSL健康检查的失败判定方式为**by-count**时，配置如下参数：

- 间隔时间：指定本次WebSocket-SSL健康检查与下次检查的时间间隔。取值范围是1到900秒，默认值是9秒。

interval *value*

- 超时时间：指定WebSocket-SSL健康检查时，设备收到真实服务的应答报文的超时时间。在超时时间内，若真实服务未返回预期响应，系统将认定此次检查失败。取值范围是1到600秒，默认值是6秒。

timeout *value*

- 失败重试次数：指定WebSocket-SSL健康检查失败，需重新检查时，可重新检查的次数。取值范围是1到10，默认值是3。

retry *value*

- 失败重试间隔：指定WebSocket-SSL健康检查失败，需重新检查时，两次检查的间隔时间。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

retry-interval *value*

- 成功重试次数：指定WebSocket-SSL健康检查成功，需重新检查时，可重新检查的次数。取值范围是1到10，默认值是1。

up-retry *value*

- 成功重试间隔：指定WebSocket-SSL健康检查成功，需重新检查时，两次检查的间隔时间。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

up-retry-interval *value*

详细介绍，请参阅 [“按次数”](#)。

- 当该WebSocket-SSL健康检查的失败判定方式为**by-time**时，配置如下参数：

- 间隔时间：指定本次WebSocket-SSL健康检查与下次检查的时间间隔。取值范围是1到900秒，默认值是5秒。

interval *value*

- 超时时间：指定WebSocket-SSL健康检查因失败进行重新检查时，可重新检查的总时长。取值范围是1到9000秒，默认值是16秒。

timeout *value*

- 成功重试时长：指定WebSocket-SSL健康检查成功，需重新检查时，可重新检查的总时长。取值范围是1到9000秒。

time-util-up *value*

- 成功重试间隔：指定WebSocket-SSL健康检查成功，需重新检查时，两次检查的间隔时间。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

up-interval *value*

详细介绍，请参阅 [“按时间”](#)。

在健康检查配置模式下，使用上述命令 **no** 的形式取消配置。

SIP-TCP健康检查

用于对真实服务中使用TCP协议的SIP服务进行检查。检查时，设备向真实服务通过TCP发送SIP服务特定的内容，在实际超时时间内，若真实服务返回的内容包含配置的预期内容，则认为SIP-TCP健康检查成功；若连续失败的次数超过重试次数，则认为SIP-TCP健康检查失败。

在健康检查配置模式下，使用以下命令配置SIP-TCP健康检查：

- DSR模式：指定设备在DSR模式下开启SIP-TCP健康检查。只有开启该项，系统才支持设备在DSR模式下的SIP-TCP健康检查功能。SIP-TCP健康检查的IP地址需指定为真实服务器的Loopback口地址，且不允许用户配置发送SIP-TCP健康检查请求的源接口。

direct-server-return - 开启设备在DSR模式下的SIP-TCP健康检查。

使用**no direct-server-return**命令关闭该功能。

- IP地址：指定IP地址。若不指定，系统将直接引用真实服务的IP地址。

ip *ip-address*

- 端口：指定端口。若不指定，系统将直接引用真实服务的端口。

port *port-number*

- 源接口：指定发送SIP-TCP健康检查请求的源接口。

source-interface *interface*

- 状态码：指定SIP-TCP健康检查时，用户期望接收到SIP-TCP状态码。若服务器返回的内容中包含该状态码，即认为SIP-TCP健康检查成功。状态码可配置多个，需以英文分号“;”间隔，如：200;302;503。状态码支持配置通配符“x”，如：30x; 5xx，不支持将通配符放在2个数字中间，如2x3。

status-code *value*

- 当该SIP-TCP健康检查的失败判定方式为**by-count**时，配置如下参数：

- 间隔时间：指定本次SIP-TCP健康检查与下次检查的时间间隔。取值范围是1到900秒，默认值是9秒。

interval *value*

- 超时时间：指定SIP-TCP健康检查时，设备收到真实服务的应答报文的超时时间。在超时时间内，若真实服务未返回预期响应，系统将认定此次检查失败。取值范围是1到600秒，默认值是6秒。

timeout *value*

- 失败重试次数：指定SIP-TCP健康检查失败，需重新检查时，可重新检查的次数。取值范围是1到10，默认值是3。

retry *value*

- 失败重试间隔：指定SIP-TCP健康检查失败，需重新检查时，两次检查的间隔时间。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

retry-interval *value*

- 成功重试次数：指定SIP-TCP健康检查成功，需重新检查时，可重新检查的次数。取值范围是1到10，默认值是1。

up-retry *value*

- 成功重试间隔：指定SIP-TCP健康检查成功，需重新检查时，两次检查的间隔时间。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

up-retry-interval *value*

详细介绍，请参阅 [“按次数”](#)。

- 当该SIP-TCP健康检查的失败判定方式为**by-time**时，配置如下参数：

- 间隔时间：指定本次SIP-TCP健康检查与下次检查的时间间隔。取值范围是1到900秒，默认值是5秒。

interval *value*

- 超时时间：指定SIP-TCP健康检查因失败进行重新检查时，可重新检查的总时长。取值范围是1到9000秒，默认值是16秒。

timeout *value*

- 成功重试时长：指定SIP-TCP健康检查成功，需重新检查时，可重新检查的总时长。取值范围是1到9000秒。

time-util-up *value*

- 成功重试间隔：指定SIP-TCP健康检查成功，需重新检查时，两次检查的间隔时间。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

up-interval *value*

详细介绍，请参阅 [“按时间”](#)。

在健康检查配置模式下，使用上述命令 **no** 的形式取消配置。

SIP-UDP健康检查

用于对真实服务中使用UDP协议的SIP服务进行检查。检查时，设备向真实服务通过UDP发送SIP服务特定的内容，在超时时间内，若真实服务返回的内容包含配置的预期内容，则认为SIP-UDP健康检查成功，否则将重新进行健康检查；若连续失败的次数超过重试次数，则认为SIP-UDP健康检查失败。

在健康检查配置模式下，使用以下命令配置SIP-UDP健康检查：

- DSR模式：指定设备在DSR模式下开启SIP-UDP健康检查。只有开启该项，系统才支持设备在DSR模式下的SIP-UDP健康检查功能。SIP-UDP健康检查的IP地址需指定为真实服务器的Loopback口地址，且不允许用户配置发送SIP-UDP健康检查请求的源接口。

direct-server-return - 开启设备在DSR模式下的SIP-UDP健康检查。

使用**no direct-server-return**命令关闭该功能。

- IP地址：指定IP地址。若不指定，系统将直接引用真实服务的IP地址。

ip *ip-address*

- 端口：指定端口。若不指定，系统将直接引用真实服务的端口。

port *port-number*

- 源端口：指定源端口。若不指定，系统将引用当前设备的可用端口。

src-port *port-number*

- 源接口：指定发送SIP-UDP健康检查请求的源接口。

source-interface *interface*

- 状态码：指定SIP-UDP健康检查时，用户期望接收到SIP-UDP状态码。若服务器返回的内容中包含该状态码，即认为SIP-UDP健康检查成功。状态码可配置多个，需以英文分号“;”间隔，如：200;302;503。状态码支持配置通配符“x”，如：30x; 5xx，不支持将通配符放在2个数字中间，如2x3。

status-code *value*

- 当该SIP-UDP健康检查的失败判定方式为**by-count**时，配置如下参数：

- 间隔时间：指定本次SIP-UDP健康检查与下次检查的时间间隔。取值范围是1到900秒，默认值是9秒。

interval *value*

- 超时时间：指定SIP-UDP健康检查时，设备收到真实服务的应答报文的超时时间。在超时时间内，若真实服务未返回预期响应，系统将认定此次检查失败。取值范围是1到600秒，默认值是6秒。

timeout *value*

- 失败重试次数：指定SIP-UDP健康检查失败，需重新检查时，可重新检查的次数。取值范围是1到10，默认值是3。

retry *value*

- 失败重试间隔：指定SIP-UDP健康检查失败，需重新检查时，两次检查的间隔时间。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

retry-interval *value*

- 成功重试次数：指定SIP-UDP健康检查成功，需重新检查时，可重新检查的次数。取值范围是1到10，默认值是1。

up-retry *value*

- 成功重试间隔：指定SIP-UDP健康检查成功，需重新检查时，两次检查的间隔时间。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

up-retry-interval *value*

详细介绍，请参阅 [“按次数”](#)。

- 当该SIP-UDP健康检查的失败判定方式为**by-time**时，配置如下参数：

- 间隔时间：指定本次SIP-UDP健康检查与下次检查的时间间隔。取值范围是1到900秒，默认值是5秒。

interval *value*

- 超时时间：指定SIP-UDP健康检查因失败进行重新检查时，可重新检查的总时长。取值范围是1到9000秒，默认值是16秒。

timeout *value*

- 成功重试时长：指定SIP-UDP健康检查成功，需重新检查时，可重新检查的总时长。取值范围是1到9000秒。

time-util-up *value*

- 成功重试间隔：指定SIP-UDP健康检查成功，需重新检查时，两次检查的间隔时间。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

up-interval *value*

详细介绍，请参阅 [“按时间”](#)。

在健康检查配置模式下，使用上述命令 **no** 的形式取消配置。

PASSIVE-HTTP健康检查

用于对真实服务的HTTP服务进行检查。检查时，当客户端申请访问设备监测的URL时，在统计时间内，若真实服务返回的内容中包含配置的状态码，或真实服务没有在超时时间内返回响应，则认为该URL失效。若判定被监测的URL失效次数大于用户设置的“异常上限”，则认为此次PASSIVE-HTTP健康检查失败。

在健康检查配置模式下，使用以下命令配置PASSIVE-HTTP健康检查：

- 监测URL：指定设备将监测的URL地址。

check-url *url*

使用**no check-url**命令取消监测URL的配置。

- 状态码：指定判定被监测的URL地址失效的响应状态码。若真实服务返回的内容中包含该状态码，即认为该URL此次的健康检查失败。

状态码可配置多个，需以英文分号“;”间隔，如 200;302;503。状态码支持配置通配符“x”，如：30x;5xx，不支持将通配符放在2个数字中间，如2x3。

status-code *value*

使用**no status-code**命令取消状态码的配置。

- 超时时间：指定设备进行PASSIVE-HTTP健康检查时，收到真实服务响应的超时时间。取值范围为0至3600秒，默认值为5秒。

response-timeout *value*

使用**no response-timeout**命令恢复超时时间的默认值。

- 异常上限：指定在统计时间内，被监测的URL地址失效次数的上限值。在统计时间内，当被监测的URL的失效次数达到指定上限值时，系统判定此次真实服务的PASSIVE-HTTP健康检查失败。取值范围为1至65535，默认值为10000。

failure-limit *value*

使用**no failure-limit**命令恢复异常上限的默认值。

- 统计时间：指定PASSIVE-HTTP健康检查的统计周期。启用PASSIVE-HTTP健康检查后，在每个统计周期内，系统根据被监测的URL失效次数是否达到异常上限值，重新判定真实服务的健康检查状态。取值范围为1至65535秒，默认值为100秒。

failure-interval *value*

使用**no failure-interval**命令恢复异常上限的默认值。

在健康检查配置模式下，使用上述命令 **no** 的形式取消配置。

PASSIVE-TCP健康检查

用于对设备与真实服务之间的TCP的连接状态进行检查。检查时，在统计时间内，若系统监控到真实服务发送了指定类型的TCP报文，且发送指定类型TCP报文的次数大于用户设置的“异常上限”，则认为PASSIVE-TCP健康检查失败。

在健康检查配置模式下，使用以下命令配置PASSIVE-TCP健康检查：

- 监控类型：指定设备将监控的来自真实服务的TCP报文类型。

check-type {**tcp-rst** | **tcp-zero-window**}

tcp-rst - 指定设备将监控真实服务是否发送了TCP-RST报文，当真实服务发送的TCP-RST报文个数达到指定

的异常上限值时，系统判定此次PASSIVE-TCP健康检查失败。

tcp-zero-window - 指定设备将监控真实服务是否发送了TCP零窗口，当真实服务发送的TCP-RST报文个数达到指定的异常上限值时，系统判定此次PASSIVE-TCP健康检查失败。

- 异常上限：指定在统计时间内，判定PASSIVE-TCP健康检查失败的TCP-RST报文/TCP零窗口个数的上限值。当设备监控到的TCP-RST报文或TCP零窗口个数达到该上限值时，判定PASSIVE-TCP健康检查失败。取值范围为1至65535，默认值为10000。

failure-limit *value*

使用**no failure-limit**命令恢复异常上限的默认值。

- 统计时间：指定PASSIVE-TCP健康检查的统计周期。启用PASSIVE-TCP健康检查后，在每个统计周期内，系统根据真实服务发送的TCP-RST报文/TCP零窗口是否达到异常上限值，重新判定真实服务的健康检查状态。取值范围为1至65535秒，默认值为100秒。

failure-interval *value*

使用**no failure-interval**命令恢复异常上限的默认值。

在健康检查配置模式下，使用上述命令 **no** 的形式取消配置。

MYSQL健康检查

用于对设备与真实服务之间的MYSQL服务进行检查。检查时，设备查询指定数据库表中的内容，在超时时间内，若真实服务返回的内容包含配置的预期内容，则认为MYSQL健康检查成功，否则将重新进行健康检查；若连续失败的次数超过重试次数，则认为MYSQL健康检查失败。

在健康检查配置模式下，使用以下命令配置MYSQL健康检查：

- IP地址：指定IP地址。若不指定，系统将直接引用真实服务的IP地址。

ip *ip-address*

- 端口：指定端口。若不指定，系统将直接引用真实服务的端口。

port *port-number*

- 文本编码方式：设备同数据库服务器的交互报文协商的编码格式。用户可以选择系统提供的编码方式，也可输入编码名称来选择其他编码方式。

charset {**gb2313** | **uft8** | **gb18030** | **gbk** | **ascii** | *value*}

- 源接口：指定发送MYSQL健康检查请求的源接口。

source-interface *interface*

- DSR模式：指定设备在DSR模式下开启MYSQL健康检查。只有开启该项，系统才支持设备在DSR模式下的MYSQL健康检查功能。MYSQL健康检查的IP地址需指定为真实服务器的Loopback口地址，且不允许用户配置发送MYSQL健康检查请求的源接口。

direct-server-return - 开启设备在DSR模式下的MYSQL健康检查。

使用**no direct-server-return**命令关闭该功能。

- 用户名：指定虚拟服务器中配置的数据库账号名。 **user-name** *name*

- 密码：输入数据库账号名对应的密码。 **passwd** *password*

- 数据库：指定健康检查的数据库名。 **database-name** *name*

- 发送内容：指定设备向数据库发送的内容。

query-string

- 预期结果：指定健康检查时，用户希望返回的内容以及在表中的位置。若返回结果符合预期，则健康检查成功。 **result** *value* [**row** *position*] [**column** *position*]

- 当该MYSQL健康检查的失败判定方式为**by-count**时，配置如下参数：

- 间隔时间：指定本次MYSQL健康检查与下次检查的时间间隔。取值范围是1到900秒，默认值是9秒。

interval *value*

- 超时时间：指定DNS健康检查时，设备收到真实服务的应答报文的超时时间。在超时时间内，若真实服务未返回预期响应，系统将认定此次检查失败。取值范围是1到600秒，默认值是6秒。

timeout *value*

- 失败重试次数：指定MYSQL健康检查失败，需重新检查时，可重新检查的次数。取值范围是1到10，默认值是3。

retry *value*

- 失败重试间隔：指定MYSQL健康检查失败，需重新检查时，两次检查的时间间隔。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

retry-interval *value*

- 成功重试次数：指定MYSQL健康检查成功，需重新检查时，可重新检查的次数。取值范围是1到10，默认值是1。

up-retry *value*

- 成功重试间隔：指定MySQL健康检查成功，需重新检查时，两次检查的间隔时间。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

up-retry-interval *value*

详细介绍，请参阅“[按次数](#)”。

- 当该MySQL健康检查的失败判定方式为**by-time**时，配置如下参数：

- 间隔时间：指定本次MySQL健康检查与下次检查的时间间隔。取值范围是1到900秒，默认值是5秒。

interval *value*

- 超时时间：指定MySQL健康检查因失败进行重新检查时，可重新检查的总时长。取值范围是1到9000秒，默认值是16秒。

timeout *value*

- 成功重试时长：指定MySQL健康检查成功，需重新检查时，可重新检查的总时长。取值范围是1到9000秒。

time-util-up *value*

- 成功重试间隔：指定MySQL健康检查成功，需重新检查时，两次检查的间隔时间。取值范围是1到700秒。默认不配置，此时该值与间隔时间的设定值一致。

up-interval *value*

详细介绍，请参阅“[按时间](#)”。

在健康检查配置模式下，使用上述命令 **no** 的形式取消配置。

健康检查组

系统支持创建健康检查组，可将多项健康检查组合在一起，对真实服务一次进行多项健康检查。进行某健康检查组检查时，需组内各项健康检查都成功，才表示检查成功。一个健康检查组最多支持添加16个健康检查。

在全局配置模式下，使用以下命令配置健康检查组：

health-check-group *name*

- *name* - 指定要创建的健康检查组的名称。如果名称已存在，则直接进入该健康检查组配置模式。

在全局配置模式下，使用以下命令删除健康检查组：

no health-check-group *name*

配置健康检查组操作符

配置健康检查组的操作符，即健康检查组结果集合的操作方法，包括“与”、“或”、“阈值”。

在全局配置模式下，使用以下命令配置健康检查组操作符：

health-check-group operation {and | or | threshold}

- **and** - 指定健康检查组操作符为“与”，表示所有组成员的状态均为“UP”时，该健康检查组状态为“UP”。
- **or** - 指定健康检查组操作符为“或”，表示至少有一个组成员的状态为“UP”时，该健康检查组状态为“UP”。
- **threshold value** - 指定健康检查组操作符为“阈值”，取值范围为1至255，默认值为255。系统将根据健康检查组内成员的状态，计算组成员的权重值之和，大于等于该警戒值时，该健康检查组的状态为“Down”。

配置健康检查组成员

在健康检查组配置模式下，使用以下命令配置健康检查组成员：

health-check *name* [weight | scoring-when-up]

- *name* - 指定想要加入健康检查组的成员名称。
- **weight value** - 配置组成员的权重值。
- **scoring-when-up** - 开启组成员的健康检查Up时计分功能。开启后，当组成员的健康检查状态为Up时，系统将该成员的权重计入组权重之和。系统默认关闭该功能，此时，当组成员的健康检查状态为Down时，系统将该成员的权重计入组权重之和。

例如：健康检查组已有健康检查成员HC1、HC2、HC3和HC4，其配置及健康检查状态如下表。

名称	权重	健康检查Up时计分	健康检查状态	是否计入组权重之和
HC1	10	开启	Up	是
HC2	20	开启	Down	否

名称	权重	健康检查Up时计分	健康检查状态	是否计入组权重之和
HC3	30	关闭	Up	否
HC4	40	关闭	Down	是

如上表所示，健康检查成员HC1和HC4的权重，将计入组权重之和。原因是：HC1的健康检查状态为Up且“健康检查Up时计分”功能开启，需计入组权重之和；HC4的健康检查状态为Down且“健康检查Up时计分”功能关闭，需计入组权重之和。因此，该健康检查组的权重之和为：10+40=50。

使用`no health-check name`删除指定健康检查组成员。

第2章 全局负载均衡

全局负载均衡（GSLB，Global Server Load Balance）基于DNS服务实现。在多数数据中心环境下，当客户端发起DNS查询，GSLB可依据客户端所属的地域和运营商等来源进行解析；通过返回最优的解析记录实现智能引流，使不同地域或运营商的用户可以就近访问服务器，以最优的路径获取服务。

GSLB需安装[GSLB许可证](#)并且在许可证未过期的情况下，授权使用。

本节包含以下内容：

- 实现GSLB，配置智能DNS，参见：[智能DNS](#)。
- 配置DNS服务器，包括配置视图、权威区域、转发区域、递归查询等。参见：[DNS服务器](#)。
- GSLB会持续不断的监控各服务器的健康状况，对其进行健康检查。参见：[健康检查](#)。
- 配置数据中心，实现多地GSLB设备的配置同步，即多数数据中心的全局负载均衡。参见：[负载均衡 > 全局负载均衡 > 数据中心](#)。

DNS服务器

本节包含以下内容：

- [实现流程](#)
- [部署场景](#)
- [配置DNS服务器](#)

实现流程

DNS服务器模块的实现可参考如下流程。本节以视图中启用了全部配置为例，进行阐述。

当客户端请求的域名到达设备，ADC会先根据其源地址、目的地址，找到匹配的“DNS视图”。然后根据视图中的配置，进行DNS解析。

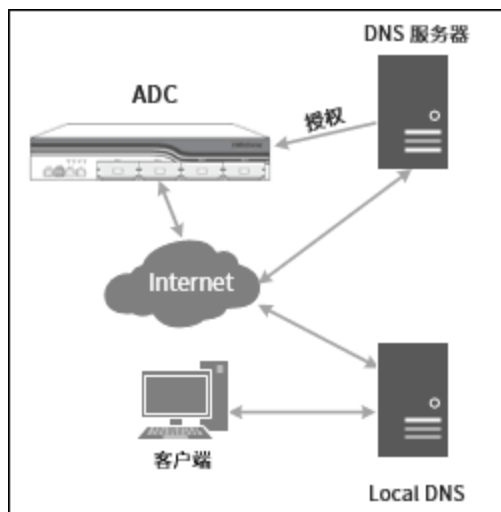
1. 匹配“视图”后，系统将客户端请求的域名，根据域名最长匹配的算法，匹配视图中配置的“权威区域”域名。

2. 若匹配到权威区域，交由权威区域处理，原则为：
 - 2.1) 先由权威区域的SmartDNS处理，若成功，返回结果给客户端。
 - 2.2) 若失败继续交由资源记录进行查询。解析成功则返回结果给客户端。若权威区域的配置均无法解析域名，系统返回给客户端相应的状态码，解析失败。
3. 若没有匹配到权威区域，
 - 3.1) 先由该视图中配置的“智能DNS”进行解析。若成功，返回结果给客户端。
 - 3.2) 若失败，继续交由视图中缓存的资源记录进行查询。解析成功则返回结果给客户端。
 - 3.3) 失败则以域名最长匹配的算法，继续匹配视图中配置的“转发区域”。
 - 3.3.1) 若匹配到转发区域，根据用户配置的转发目的地址进行查询，并将查询到的结果缓存、返回给客户端。如无匹配，返回失败结果给客户端。
 - 3.3.2) 若没有匹配到转发区域，则由视图中的“递归查询”与“转发配置”继续解析。转发配置优先级高于递归查询。

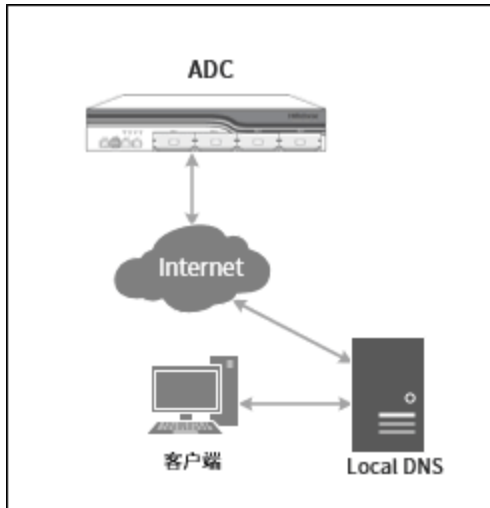
DNS Server的部署场景

ADC的DNS Server部署有以下方式，可满足大部分用户场景：

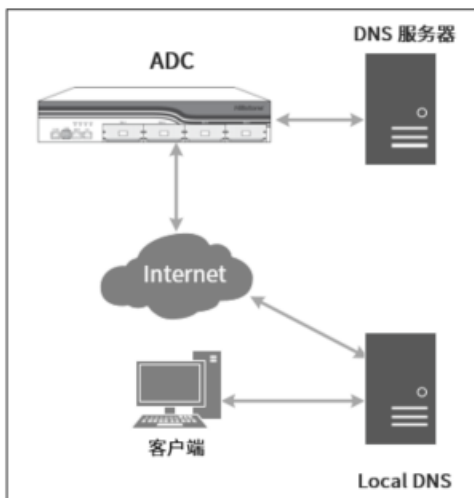
- 授权部署模式：DNS服务器的部署保持不变，通过授权，将ADC作为子域部署。



- 替代DNS服务器部署：将ADC作为DNS服务器部署，接收所有对这个域名的DNS请求。



- 代理部署模式：ADC接替了原有DNS服务器，进行DNS请求的监听。真正的权威DNS服务器部署在ADC后面。所有DNS查询流量均通过ADC转发到DNS服务器。



配置DNS服务器

DNS服务器配置包含：

- [配置DNS视图](#)
- [配置默认DNS视图](#)

- [配置区域](#)
- [全局配置](#)

配置DNS视图

当客户端的源IP、目的IP，分别与DNS视图中配置的源IP、目的IP相匹配时，系统认为客户端的请求与该DNS视图相匹配。只有与视图匹配的客户端才能访问视图中关联的资源，如定义的权威区域、转发区域、SmartDNS、递归转发等。用户可创建多个DNS视图，各个视图中的资源无法共享。

创建DNS视图

创建DNS视图，在全局配置模式下，使用以下命令：

```
gslb dns-server view name name [id id][top | bottom | after {id id | name name} | before {id id | name name}]
```

- **view name name** - 指定DNS视图的名称。
- **id id** - 指定该视图的ID。
- **[top | bottom | after {id id | name name} | before {id id | name name}]** - 指定该规则的位置：top表示DNS视图最上方，bottom表示DNS视图最下方，after表示在指定DNS视图之后，before表示在指定的DNS视图之前。

执行该命令后，系统将进入DNS视图的配置模式。

在全局配置模式下，使用**no gslb dns-server view name name**删除DNS视图。

用户也可以使用**gslb dns-server view move {id id | name name} {top | bottom | after {id id | name name} | before {id id | name name}}**命令移动DNS视图的位置。

启用DNS视图

启用或禁用DNS视图，在相应DNS视图配置模式下，使用以下命令：

- **enable** - 启用该DNS视图。默认情况下，启用该视图。
- **no enable** - 禁用该DNS视图。

配置源IP

只有客户端请求源IP、目的IP均与视图中配置的源IP、目的IP相匹配，才可访问该视图的资源。如视图中未配置源、目的IP，系统将选择默认地址Any，即匹配所有请求的地址。

配置源IP，在DNS视图模式下，使用以下命令：

src-ip {*A.B.C.D/Mask* | *X:X:X:X:XX/Prefix*}

- *A.B.C.D/Mask*- 指定IPv4地址和掩码。
- *X:X:X:X:XX/Prefix*- 指定IPv6地址和前缀。

使用该命令**no**的形式删除配置。

配置源IP地址段，在DNS视图模式下，使用以下命令：

src-range {*ipv4-address1 ipv4-address2* | *ipv6-address1 ipv6-address2*}

- *ipv4-address1 ipv4-address2* - 指定IPv4地址段。
- *ipv6-address1 ipv6-address2* - 指定IPv6地址段。

使用该命令**no**的形式删除配置。

配置目的IP

只有客户端请求源IP、目的IP均与视图中配置的源IP、目的IP相匹配，才可访问该视图的资源。如视图中未配置源、目的IP，系统将选择默认地址Any，即匹配所有请求的地址。

配置目的IP，在DNS视图模式下，使用以下命令：

dst-ip {*A.B.C.D/Mask* | *X:X:X:X:XX/Prefix*}

- *A.B.C.D/Mask*- 指定IPv4地址和掩码。
- *X:X:X:X:XX/Prefix*- 指定IPv6地址和前缀。

使用该命令**no**的形式删除配置。

配置目的IP地址段，在DNS视图模式下，使用以下命令：

dst-range {*ipv4-address1 ipv4-address2* | *ipv6-address1 ipv6-address2*}

- *ipv4-address1 ipv4-address2* - 指定IPv4地址段。
- *ipv6-address1 ipv6-address2* - 指定IPv6地址段。

使用该命令**no**的形式删除配置。

关联区域

为DNS视图关联区域对象，在DNS视图模式下，使用以下命令：

zone *zone-name*

- *zone-name* - 指定区域名称。匹配了视图的请求，将根据域名最大长度的方式进行权威区域匹配的选择。成功匹配后，可访问区域中的资源。也可以不配置该项。

使用该命令**no**的形式，删除配置。

关联智能DNS

为DNS视图关联智能DNS对象，在DNS视图模式下，使用以下命令：

smart-dns *host-name*

- *host-name* - 指定智能DNS的主机名称。

使用该命令**no**的形式，删除配置。

递归查询

开启递归查询，使用系统内置的DNS根服务器地址去完成DNS查询。缓存记录只属于该DNS视图，不会与其他视图共享。在DNS视图模式下，使用以下命令：

recursion enable：只查询IPv4的根服务器。

recursion ipv6 enable：允许使用IPv6的根服务器。

使用以上命令**no**的形式，关闭递归查询功能。

转发配置

开启转发配置，若DNS服务器本身无法解析，则系统向其他的DNS服务器发出查询请求，得到结果后返回给客户端。在DNS视图配置模式下，使用以下命令开启转发配置：

forward enable

使用**no forward enable**禁用转发配置。

配置转发目的地址

开启转发配置后，用户可指定DNS服务器的IP，支持IPv4或IPv6。当系统无法解析DNS时，由该地址完成DNS的查询。在DNS视图下，使用以下命令配置转发地址：

forward {**ip** *ip-address* | **ipv6** *ipv6-address*} [**port** *port-number*]

- **ip** *ip-address* - 指定转发的IPv4地址。
- **ipv6** *ipv6-address* - 指定转发的IPv6地址。
- **port** *port-number* - 指定端口号。

使用该命令**no**的形式，删除配置。

当配置多个转发地址后，系统查询时与配置顺序无关，如没有查到结果就通过下一个地址进行查询。

强制RD标志

启用强制RD标志的功能后，在开启[递归查询](#)或[转发配置](#)的情况下，无论客户端DNS请求报文中的RD标志是什么，系统都会对该DNS请求进行递归转发。开启/关闭强制RD标志，在DNS视图的配置模式下，使用以下命令：

- **force-query-flag-rd enable** - 启用该功能。
- **no force-query-flag-rd enable** - 关闭该功能。

配置默认DNS视图

系统提供一个默认的DNS视图，即客户端请求的源地址和目的地址均为Any的视图。默认DNS视图与其他自定义的DNS视图相互独立。当客户端请求到达设备时，默认DNS视图匹配顺序处于视图列表的最后一个。并且，不可以禁用或删除默认的DNS视图。



注意: 根VSYS和每一个非根VSYS创建后，均有其各自的默认DNS视图。

在全局配置模式下，使用以下命令进入默认DNS视图的配置模式：

```
gslb dns-server view name default_view
```

关联智能DNS

在默认DNS视图中引入智能DNS对象，在默认DNS视图的配置模式下，使用以下命令：

```
smart-dns host-name
```

- *host-name* - 指定智能DNS的主机名称。

使用该命令**no**的形式，删除配置。

关联区域

为默认的DNS视图关联区域对象，在默认DNS视图模式下，使用以下命令：

zone zone-name

- **zone-name** - 指定区域名称。匹配了视图的请求，将根据域名最大长度的方式进行权威区域匹配的选择。成功匹配后，可访问区域中的资源。也可以不配置该项。

使用该命令**no**的形式，删除配置。

递归查询

开启递归查询，使用系统内置的DNS根服务器地址去完成DNS查询。在默认DNS视图的配置模式下，使用以下命令开启递归查询：

- **recursion enable** - 只查询IPv4的根服务器。
- **recursion ipv6 enable** - 允许使用IPv6的根服务器。

使用以上命令**no**的形式，关闭递归查询功能。

转发配置

开启转发配置，若DNS服务器本身无法解析，则系统向其他的DNS服务器发出查询请求，得到结果后返回给客户端。在默认DNS视图的配置模式下，使用以下命令开启转发配置：

forward enable

开启转发配置后，用户可指定DNS服务器的IP，支持IPv4或IPv6。当系统无法解析DNS时，由该地址完成DNS的查询。在默认DNS视图的配置模式下，使用以下命令：

forward {ip ip-address | ipv6 ipv6-address} [port port-number]

- **ip ip-address** - 指定转发的IPv4地址。
- **ipv6 ipv6-address** - 指定转发的IPv6地址。
- **port port-number** - 指定端口号。

使用该命令**no**的形式，删除配置。

当配置多个转发地址后，系统查询时与配置顺序无关，如没有查到结果就通过下一个地址进行查询。



注意: 如配置“转发区域”，系统在转发前，会优先在转发区域中进行匹配。匹配成功则会使用“转发区域”中的配置进行DNS查询，否则将使用DNS视图中配置的转发目的地址。

启用强制RD标志

启用强制RD标志的功能后，在开启[递归查询](#)或[转发配置](#)的情况下，无论客户端DNS请求报文中的RD标志是什么，系统都会对该DNS请求进行递归转发。开启/关闭强制RD标志，在默认DNS视图的配置模式下，使用以下命令：

- `force-query-flag-rd enable` - 启用该功能。
- `no force-query-flag-rd enable` - 关闭该功能。

清除DNS缓存

清除由递归查询或转发存储的DNS缓存，在任意配置模式下，使用以下命令：

```
clear gslb dns-server cache [view-name]
```

- `view-name` - 指定DNS视图的名称，可以为自定义的DNS视图，也可以为默认DNS视图。

配置区域

用户可通过配置区域及其域名信息，来管理该区域的资源记录。DNS区域包括权威区域（Master zone）和转发区域（Forward zone）：

- 权威区域：处理客户端请求的权威DNS服务器。
- 转发区域：转发指定域名的客户端请求。根据用户配置的转发目的地址进行查询，并将查询到的结果缓存、返回给客户端。



注意: 区域中域名的配置，需符合主机域名规范，由大小写字母、数字、“-”组成。主机名每一个label（即两个“.”之间）不能空白，且长度不能超过63字节。域名总长度不能超过254字节。

创建区域

在全局配置模式下，使用以下命令创建区域：

```
gslb dns-server zone zone-name domain-name [type {master | forward}][id id]
```

- *zone-name* - 指定需创建的区域名称。
- *domain-name* - 指定该区域的域名。配置后，域名与其名称均不可更改。通过在不同区域里配置相同域名，即可在不同视图下，得到解析同一资源记录的不同结果。
- **type {master | forward}** - 指定区域的类型，包括权威区域（master）和转发区域（forward）。
- **id id** - 指定该区域的ID。

执行该命令后，系统将进入区域配置模式，并可进行其他参数的配置。

在全局模式下，使用 **no gslb dns-server zone zone-name** 删除配置的区域。

配置SOA资源

在区域配置模式下，使用以下命令配置SOA资源：

```
soa name-server mail [ip ip-address][ipv6 ipv6-address]
```

- *name-server* - 管理该权威区域的服务器的名称，支持配置主机名或者完全限定域名（FQDN）且总长度不能超过254字节。配置后，域名由该权威DNS服务器来进行解析。
- *mail* - 指定负责管理该区域的人员的邮箱，总长度不能超过254字节。
注意：管理员邮箱的格式为“username.domain.com”。此处以“.”进行分割，而不是“@”。
- **ip ip-address** - 指定名称服务器的IPv4地址。
- **ipv6 ipv6-address** - 指定名称服务器的IPv6地址。



注意：1) 该名称不能与CNAME的主机名相同。2) 如果配置的是主机名，字符长度与“区域”中域名长度相加后，总长度不能超过254字节。（需使用“.”进行分割，如果域名不是以“.”结尾，系统自动补充。）

在DNS区域配置模式下，使用以下命令删除配置：

```
no soa ip ip-address
```


`no soa ipv6 ipv6-address`

配置资源记录

配置权威区域的资源记录时，系统将自动生成一个ID。权威区域的资源记录类型如下：

- A记录 - 用于指定域名对应的IP记录。
- AAAA - 用于指定域名对应的IPv6地址记录。
- CNAME - 用于指定域名的别名，可将多个域名映射到同一个主机。
- NS - 域名服务器信息的记录，用于指定该域名由哪个DNS服务器来进行解析。
- MX - 邮件交换记录，用于将某个域名的邮件映射到对应的邮件服务器进行处理。
- PTR - IP地址反向解析记录，用于电子邮件发送过程中的反向地址查询。
- TXT - 文本信息记录，用于保存与域名相关的信息。
- SRV - 服务器资源记录，记录服务器提供的服务。



注意:

- 区域里资源记录的个数有限，不同平台支持的资源记录个数不同。
- 资源记录的名称只允许配置主机名，不能以“.”结尾。与“区域”中配置的域名长度相加后，总长度不能超过254字节。域名的长度以“.”结尾，如没有“.”,系统自动补充。
- 主机名需符合主机域名规范，由大小写字母、数字、“-”组成。主机名每一个label（即两个“.”之间）不能空白，且长度不能超过63字节。

配置A记录

创建A记录，用户需在所创建的权威区域的配置模式下，使用以下命令：

```
resource-record type A owner name [id id | status {enable | disable}] | TTL ttl-value | ipv4 ip-address
```

- **owner name** - 指定DNS记录的域名所对应的主机名称。
- **id id** - 指定该资源记录的ID号。

- **status** {**enable** | **disable**} - 指定该资源记录的状态，enable为启用，disable为禁用。
- **TTL** *ttl-value* - 指定该记录在DNS服务器上的缓存时间。当缓存时间耗尽后，DNS服务器将对它所包含的信息进行更新。
- **ipv4** *ip-address* - 指定该域名对应的IPv4地址。

配置AAAA记录

AAAA记录用于指定域名对应的IPv6地址记录。创建AAAA记录，用户需在所创建的权威区域的配置模式下，使用以下命令：

```
resource-record type AAAA owner name [id id | status {enable | disable} | TTL ttl-value | ipv6 ipv6-address]
```

- **owner name** - 指定DNS记录的域名所对应的主机名称。
- **id** *id* - 指定该资源记录的ID号。
- **status** {**enable** | **disable**} - 指定该资源记录的状态，enable为启用，disable为禁用。
- **TTL** *ttl-value* - 指定该记录在DNS服务器上的缓存时间。当缓存时间耗尽后，DNS服务器将对它所包含的信息进行更新。
- **ipv6** *ipv6-address* - 指定该域名对应的IPv6地址。

配置NS记录

NS记录即域名服务器信息的记录，用于指定该域名由哪个DNS服务器来进行解析。创建NS记录，用户需在所创建的权威区域的配置模式下，使用以下命令：

```
resource-record type NS owner name [id id | status {enable | disable} | TTL ttl-value | name-server value [ip ip-address][ipv6 ipv6-address]]
```

- **owner name** - 指定DNS记录的域名所对应的主机名称。
- **id** *id* - 指定该资源记录的ID号。
- **status** {**enable** | **disable**} - 指定该资源记录的状态，enable为启用，disable为禁用。
- **TTL** *ttl-value* - 指定该记录在DNS服务器上的缓存时间。当缓存时间耗尽后，DNS服务器将对它所包含的信息进行更新。

- **name-server** *value* - 指定权威的DNS服务器的名称。
- **ip** *ip-address* - 指定名称服务器的IPv4地址。
- **ipv6** *ipv6-address* - 指定名称服务器的IPv6地址。

配置CNAME记录

CNAME记录即别名记录，用于将多个域名映射到同一个主机的情况。创建CNAME记录，用户需在所创建的权威区域的配置模式下，使用以下命令：

```
resource-record type CNAME owner name [id id | status {enable | disable} | TTL ttl-value | alias value]
```

- **owner** *name* - 指定DNS记录的域名所对应的主机名称。
- **id** *id* - 指定该资源记录的ID号。
- **status** {**enable** | **disable**} - 指定该资源记录的状态，enable为启用，disable为禁用。
- **TTL** *ttl-value* - 指定该记录在DNS服务器上的缓存时间。当缓存时间耗尽后，DNS服务器将对它所包含的信息进行更新。
- **alias** *value* - 指定DNS记录的域名的别名。

配置PTR记录

PTR记录即指针记录，用于电子邮件发送过程中的反向地址查询。创建PTR记录，用户需在所创建的权威区域的配置模式下，使用以下命令：

```
resource-record type PTR owner ptr-info [id id | status {enable | disable} | TTL ttl-value | host host-name]
```

- **owner** *ptr-info* - 指定DNS记录的域名所对应的主机名称。
- **id** *id* - 指定该资源记录的ID号。
- **status** {**enable** | **disable**} - 指定该资源记录的状态，enable为启用，disable为禁用。
- **TTL** *ttl-value* - 指定该记录在DNS服务器上的缓存时间。当缓存时间耗尽后，DNS服务器将对它所包含的信息进行更新。
- **host** *host-name* - 指定PTR记录信息，通常是MX记录对应的域名。

配置MX记录

MX记录即邮件交换记录，用于将某个域名的邮件映射到对应的邮件服务器进行处理。创建MX记录，用户需在所创建的权威区域的配置模式下，使用以下命令：

```
resource-record type MX owner name [id id | status {enable | disable} | TTL ttl-value | preference value exchange host]
```

- **MX owner name** - 指定DNS记录的域名所对应的主机名称。
- **id id** - 指定该资源记录的ID号。
- **status {enable | disable}** - 指定该资源记录的状态，enable为启用，disable为禁用。
- **TTL ttl-value** - 指定该记录在DNS服务器上的缓存时间。当缓存时间耗尽后，DNS服务器将对它所包含的信息进行更新。
- **preference value** - 指定MX记录的优先级。该值越小，代表优先级越高，系统将选择优先级高的服务器发送邮件。
- **exchange host**指定收件人的电子邮件的域名。

配置TXT记录

TXT记录即文本信息记录。创建TXT记录，用户需在所创建的权威区域的配置模式下，使用以下命令：

```
resource-record type TXT owner name [id id | status {enable | disable} | TTL ttl-value | string value]
```

- **owner name** - 指定DNS记录的域名所对应的主机名称。
- **id id** - 指定该资源记录的ID号。
- **status {enable | disable}** - 指定该资源记录的状态，enable为启用，disable为禁用。
- **TTL ttl-value** - 指定该记录在DNS服务器上的缓存时间。当缓存时间耗尽后，DNS服务器将对它所包含的信息进行更新。
- **string value** - 指定域名的文本信息。

配置SRV记录

SRV记录即服务器资源记录，记录服务器提供的服务。创建SRV记录，用户需在所创建的权威区域的配置模式下，使用以下命令：

```
resource-record type SRV owner name [id id | status {enable | disable}] | TTL ttl-value | priority value weight value  
port number target name]
```

- **owner name** - 指定DNS记录的域名所对应的主机名称。
- **id id** - 指定该资源记录的ID号。
- **status {enable | disable}** - 指定该资源记录的状态，enable为启用，disable为禁用。
- **TTL ttl-value** - 指定该记录在DNS服务器上的缓存时间。当缓存时间耗尽后，DNS服务器将对它所包含的信息进行更新。
- **priority value** - 当多台服务器均可提供相同的服务时，指定服务器的优先级。该值越小，代表优先级越高。
- **weight value** - 指定SRV记录的优先级。该值越小，代表优先级越高。
- **port number** - 指定提供服务的端口。
- **target name** - 指定SRV记录值。

启用资源记录

资源记录被创建后，在区域配置模式下，使用以下命令对指定ID的资源记录进行启用或禁用：

- 启用：**resource-record id id enable**
- 禁用：**no resource-record id id enable**

关联智能DNS

为权威区域引入智能DNS对象，在区域配置模式下，使用以下命令：

```
smart-dns host-name
```

- **host-name** - 指定智能DNS的主机名称。

使用该命令**no**的形式，删除配置。

转发配置

开启转发配置，若DNS服务器本身无法解析，则系统向其他的DNS服务器发出查询请求，得到结果后返回给客户端。在DNS视图配置模式下，使用以下命令开启转发配置：

```
forward enable
```

使用`no forward enable`禁用转发配置。

转发目的地址

开启转发配置后，用户可指定DNS服务器的IP，支持IPv4或IPv6。当系统无法解析DNS时，由该地址完成DNS的查询。在DNS视图下配置转发地址：

```
forward {ip ip-address | ipv6 ipv6-address} [port port-number]
```

- `ip ip-address` - 指定转发的IPv4地址。
- `ipv6 ipv6-address` - 指定转发的IPv6地址。
- `port port-number` - 指定端口号。

使用该命令`no`的形式，删除配置。

当配置多个转发地址后，系统查询时与配置顺序无关，如没有查到结果就通过下一个地址进行查询。



注意：如配置“转发区域”，系统在转发前，会优先在转发区域中进行匹配。匹配成功则会使用“转发区域”中的配置进行DNS查询，否则将使用DNS视图中配置的转发目的地址。

配置全局配置

DNS服务器的全局配置，即配置ADC设备对外提供DNS解析服务的IP地址、端口号以及DNS缓存等相关信息。

在全局配置模式下，使用以下命令进入DNS服务器的全局配置模式：

```
gslb global-config
```

配置DNS服务器监听地址

配置DNS服务器提供服务的IP地址。用户可以将IP地址对应的DNS服务器绑定至指定的流量组。当客户端访问该DNS服务器时，流量组的生效设备将发送ARP报文或NA（邻居通告）报文，将此次访问请求引流至自

身，并对其进行处理。若不指定，默认加入系统预定义的default流量组。配置DNS服务器提供服务的IP地址，并将其绑定至集群流量组，在DNS服务器的全局配置模式下，使用以下命令：

```
ip ip-address[traffic-group traffic-group-name]
```

- *ip-address* - 指定DNS服务器提供服务的IPv4地址。
- **traffic-group** *traffic-group-name* - 指定集群流量组，与配置的IPv4地址进行绑定。

```
ipv6 ipv6-address [traffic-group traffic-group-name]
```

- *ipv6-address* - 指定DNS服务器提供服务的IPv6地址。
- **traffic-group** *traffic-group-name* - 指定集群流量组，与配置的IPv6地址进行绑定。

使用以上命令**no**的形式，删除配置。

配置监听端口

配置DNS服务器提供服务的TCP和UDP端口，在DNS服务器的全局配置模式下，使用以下命令：

```
port port-number
```

- *port-number* - 指定端口号，默认53。该端口对TCP和UDP同时生效。

使用该命令**no**的形式，删除配置。

发布监听地址路由

DNS服务器监听地址的路由发布，即将[监听地址](#)发布给ADC设备所在网络中的动态路由，供网络中的动态路由协议进行路由计算。然后，根据计算结果，选择最优的路由路径将客户端DNS请求转发至正常运行的ADC设备。

该功能需和动态路由的“引入路由”功能一起使用才可以生效，例如OSPF的[引入路由](#)。

发布监听地址路由，在DNS服务器的全局配置模式下，使用以下命令：

```
route-advertisement {enable | disable}
```

- **enable** - 启用该功能。
- **disable** - 关闭该功能。系统默认关闭该功能。

配置UDP会话超时

配置UDP超时设置，在DNS服务器的全局配置模式下，使用以下命令：

```
udp-session-timeout {invalidate-after-answer | value}
```

- **invalidate-after-answer** - 指定后，系统在服务器应答后，删除UDP报文请求
- **value** - 指定UDP的超时时间。在超时时间内未收到服务器响应，系统将删除UDP报文的请求。取值范围是1到65535秒，默认值是5秒。

配置缓存

指定每个DNS视图的缓存大小。通过递归查询获取的DNS解析结果将存储在视图的缓存中，每个视图相互独立。在DNS服务器的全局配置模式下，使用以下命令配置缓存：

```
cache value
```

- **value** - 指定每个视图缓存的大小，取值范围2至20M，默认值2M。

在DNS服务器的全局配置模式下，使用 **no cache** 命令恢复默认值。

开启GSLB统计

在GSLB全局模式中，开启统计GSLB信息，在DNS服务器的全局配置模式下，使用以下命令：

```
statistics enable
```

在DNS服务器的全局配置模式下，使用 **no statistics enable** 命令禁用GSLB统计。

开启GSLB日志

开启GSLB日志，在DNS服务器的全局配置模式下，使用以下命令：

```
log enable
```

使用该命令开启后，用户需在全局配置模式下输入 **logging traffic gslb on** 启用日志功能，才可输出GSLB日志。

在DNS服务器的全局配置模式下，使用 **no log enable** 命令禁用GSLB日志。

智能DNS

系统可以根据DNS请求的源地理位置将域名解析成最靠近该位置的IP地址，并将不同ISP用户的请求解析成对应ISP的IP地址，从而达到减少跨区域跨ISP访问的目的。这种解析方式被称为智能域名解析（SmartDNS）。

智能DNS，可被DNS全局配置、视图、权威区域引用，且查找的优先级最高。智能DNS仅解析A或AAAA DNS 查询记录。

负载均衡算法

系统支持多种负载均衡算法，包括：

算法	描述
轮询（Round Robin）	将客户端的请求轮流分配给每个真实服务。
加权轮询（Weighted Round Robin）	根据真实服务的不同处理能力，分配不同的权重。设备根据真实服务的权重，按比例分发请求。权重大的真实服务，接收的请求多。
IP哈希（Hash IP）	对客户端的源地址进行哈希运算，根据运算的结果转发给服务器进行处理。若服务列表不变，同一IP地址的客户端，每次都会分配到同一个服务器。
静态就近性（Topology）	根据客户端源地址的地区分配服务器。当有多个服务器配置了同一地区时，返回权重较大的服务器IP。并且，选择此算法时，可以配置返回服务器IP的个数，最多返回16个IP。
所有（All）	选择此算法时，可以配置返回服务器IP的个数，最多返回16个IP。
优先权（Priority）	根据优先权值分配服务器。获得高优先权的将优先分配资源。优先级的数值越小，表示优先权越高。
动态比率（Dynamic-ratio）	根据服务器的不同处理能力，设备计算不同的动态权重。设备根据服务器的动态权重，按比例分发请求。动态权重大的服务器，接收的请求多。动态权重为0时，服务器不参与分发请求。一般情况下，动态权重值是由SNMP类型的健康检查计算得出的结果；对于其他情况，如果服务器可以提供服务时，动态权重值为1，否则为0。
动态就近性（Dynamic-proximity）	根据服务器绑定接口的上行与下行带宽利用率之和，分配服务器。在绑定了接口的服务器中，设备将接口带宽利用率之和较小的服务器地址返回给客户端。

配置智能DNS

智能DNS配置包含：

1. [配置ISP](#)
2. [配置地区](#)

3. [配置服务器和服务池](#)
4. [配置DNS主机](#)

配置ISP

系统预定义电信、联通、移动、教育四个ISP对象，预定义对象不可删除、重命名。系统支持创建自定义ISP对象。预定义与自定义的ISP，均可在地区中引用。

在全局配置模式下，使用以下命令创建ISP：

```
gslb isp isp-name
```

- *isp-name* - 指定想要创建的ISP的名称。

使用**no gslb isp** *isp-name*删除ISP。

在全局配置模式下，使用**rename gslb isp** *old-name new-name*命令重命名ISP。

添加IP网段

为ISP添加IP网段，在ISP配置模式下，使用以下命令：

- **ip range** *min-value max-value* - 指定IPv4地址网段的起始地址。
- **ip subnet** *IPv4-address/Mask* - 指定IPv4地址及其子网掩码。
- **ipv6 range** *min-value max-value* - 指定IPv6地址网段的起始地址。
- **ipv6 subnet** *IPv6-address/Prefix* - 指定IPv6地址及其前缀长度。

在ISP配置模式下，使用**no**的形式删除配置。

配置地区

配置地区，在全局配置模式下，使用以下命令：

```
gslb region name
```

- *name* - 指定想要创建的地区的名称。

执行该命令后，系统将进入地区配置模式。可在该模式下，指定国家、省份等详细信息。

使用**no gslb region** *name* 删除所配置的地区。

在全局配置模式下，使用`rename gslb region old-name new-name`命令重命名所创建的地区。

配置国家信息

为地区配置具体的国家信息，在地区配置模式下，使用以下命令指定所属国家：

```
country {CN | US | AU.....}
```

- CN | US | AU..... - 指定所属国家。

使用该命令`no`的形式删除配置。

配置省份信息

为地区配置具体的省份信息，在地区配置模式下，使用以下命令指定所属省：

```
province {CN} {BJ | JS | SH.....}
```

- CN - 指定的省份为中国省份。
- BJ | JS | SH..... - 指定省份名称。

使用该命令`no`的形式删除配置。

配置IP网段

为地区配置具体的IP网段信息，在地区配置模式下，使用以下命令：

```
ip ip-address - 指定IPv4地址网段。
```

```
ipv6 ipv6-address - 指定IPv6地址网段。
```

配置ISP

为地区配置具体的ISP，在地区配置模式下，使用以下命令：

```
isp isp-name - 指定创建好的ISP对象。
```

使用命令 `no isp isp-name` 删除配置。



注意: 当用户同时配置省份、国家、ISP与自定义IP网段多种类型时，客户端源地址的匹配顺序为自定义IP网段>自定义ISP>预定义ISP>省份>国家。当同一类型配置多项时，客户端源地址匹配上任一项，即匹配上该地区。

配置服务器和服务池

服务器即为DNS主机提供服务的服务器；服务器池即服务器的集合。

创建服务器

在全局配置模式下，使用以下命令创建服务器：

```
gslb smart-dns server name
```

- *name* - 指定提供服务的服务器的名称。执行该命令后，系统将进入服务器配置模式。

使用该命令no的形式删除配置。

服务器状态

在服务器配置模式下，使用以下命令启用或禁用服务器。禁用的服务器不可用。

- 启用： **status enable**
- 禁用： **status disable**

服务器IP

在服务器配置模式下，使用以下命令指定该服务器的IP地址类型，包含IPv4或IPv6。

ip *ipv4-address* - 指定IPv4地址。

ip *ipv6-address* - 指定IPv6地址。



注意: 当设备的系统固件为IPv4单栈版本时，若服务器成员配置IPv6类型的地址，则无法通过健康检查判定该成员是否可用。

服务器权重

指定该服务器的权重，系统会按权值的比例来分配流量。在服务器配置模式下，使用以下命令：

```
weight value
```

- *value* - 指定该服务器的权重值。取值范围为1至255，默认值50。

使用该命令no的形式恢复默认值。

指定健康检查

指定健康检查或健康检查组，用于检查各种服务的可用状态。在服务器配置模式下，使用以下命令：

health-check *value*

- *value* - 指定健康检查或健康检查组对象。

使用该命令no的形式删除配置。



注意：当服务器成员或该成员所属服务器池未配置健康检查时，该服务器成员是否可用，将由其所在本地数据中心对应设备配置的健康检查结果决定。数据中心的详细信息，请参阅[“数据中心”](#) 章节。

指定健康检查端口

指定健康检查端口，在服务器配置模式下，使用以下命令：

health-check-port *value*

- *value* - 指定健康检查端口。该端口一般为服务器的监听端口。

使用该命令no的形式删除配置。

引用地区

指定服务器所属的地区。在服务器池配置静态就近性算法的情况下，根据地区划分服务器，当客户端源地址匹配到某地区时，才能访问该地区的服务器。

在服务器配置模式下，使用以下命令为服务器引用地区：

region *region-name*

- *region-name* - 指定服务器的所属地区。

在服务器配置模式下，使用**no region**命令取消地区的配置。

绑定接口

为服务器绑定接口。服务器池[启用链路繁忙保护](#)功能后，服务器的繁忙状态由其绑定接口的带宽利用率是否达到阈值决定，若接口的带宽利用率达到阈值，系统认为该服务器处于繁忙状态，不为其分配客户端请求。并且，服务器池配置动态就近性算法时，系统将按照各服务器绑定接口的上行与下行带宽利用率之和，为客户端返回该值较小的服务器IP。

在服务器配置模式下，使用以下命令为服务器绑定接口：

interface *interface-name*

- *interface-name* - 指定接口，与该服务器绑定。

在服务器配置模式下，使用**no interface**命令删除服务器绑定的接口。

服务器优先级

在服务器配置模式下，使用以下命令指定该服务器的优先级：

priority *value*

- *value* - 指定该服务器的优先级。取值为1至100，默认值50。数值越小，该服务器的优先级越高。

使用该命令**no**的形式删除配置。

启用服务器可用性验证

系统支持开启验证服务器可用性功能。若开启该功能，当该服务器健康检查结果为Up时，系统将其列入可分配的服务器资源列表；当该服务器健康检查结果为Down时，系统将其从可分配的服务器资源列表中排除。若关闭该功能，无论该服务器的健康检查结果是什么，系统都将其列入可用的服务器资源列表。在服务器配置模式下，使用以下命令开启服务器可用性的验证功能：

verify-server-availability **enable**

- **enable** - 开启服务器可用性的验证。

使用该命令**no**的形式删除配置。

绑定数据中心

用户可以将服务器绑定至某一数据中心，系统根据数据中心的地理位置，标识该服务器。在服务器配置模式下，使用以下命令绑定服务器所属数据中心：

data-center *data-center-name*

- *data-center-name* - 指定数据中心的名称，将该服务器绑定至指定的数据中心。

使用该命令no的形式删除配置。

创建服务器池

在全局配置模式下，使用以下命令创建服务器池：

gslb smart-dns pool *name*

- *name* - 指定提供服务的服务器池的名称。执行该命令后，系统将进入服务器池配置模式。

使用该命令no的形式删除配置。

服务器池状态

在服务器池配置模式下，使用以下命令启用或禁用服务器池。禁用的服务器池不可用。

- 启用：**status enable**
- 禁用：**status disable**

指定首选算法

为服务器池指定首选负载均衡算法，在服务器池配置模式下，使用以下命令：

preferred {**dynamic-proximity** | **dynamic-ratio** | **round-robin** | **weighted-round-robin** | **hash-ip** [*value*] | **topology** | **priority** | **all** [*number*]}

- **dynamic-proximity** - 指定算法为动态就近性算法。
- **dynamic-ratio** - 指定算法为动态比率算法。
- **round-robin** - 指定算法为轮询。
- **weighted-round-robin** - 指定算法为加权轮询。此选项为默认配置。

- **hash-ip** [*value*] - 指定算法为IP哈希。
 - *value* - 指定IP地址的前多少位用于哈希计算，取值范围是1至128。
- **topology** - 根据客户端源地址的地区就近选择服务器。当有多个服务器配置了同一地区时，返回权重较大的服务器IP。
- **priority** - 指定优先权算法。
- **all** [*number*] - 返回所有的服务器地址。若指定*number*数值，则返回指定数量的服务器个数。取值1至16，默认值为3。

使用**no preferred**恢复默认配置。

指定备选算法

为服务器池指定备选负载均衡算法，在服务器池配置模式下，使用以下命令：

```
alternative {dynamic-proximity| dynamic-ratio | round-robin | weighted-round-robin | hash-ip [ value ] | topology |
priority | all [ number ] | drop}
```

- **dynamic-proximity** - 指定算法为动态就近性算法。
- **dynamic-ratio** - 指定算法为动态比率算法。
- **round-robin** - 指定算法为轮询。
- **weighted-round-robin** - 指定算法为加权轮询。此选项为默认配置。
- **hash-ip** [*value*] - 指定算法为IP哈希。
 - *value* - 指定IP地址的前多少位用于哈希计算，取值范围是1至128。
- **topology** - 根据客户端源地址的地区就近选择服务器。当有多个服务器配置了同一地区时，返回权重较大的服务器IP。
- **priority** - 指定优先权算法。
- **all** [*number*] - 返回所有的服务器地址。若指定*number*数值，则返回指定数量的服务器个数。取值1至16，默认值为3。
- **drop** - 指定为该选项，系统将直接丢弃客户端请求。

使用**no alternative**恢复默认配置。

服务器池所属地区

指定该服务器池所属地区。在DNS主机配置静态就近性算法的情况下，根据地区划分服务器池，当客户端源地址匹配到某地区时，才能访问该地区服务器池中的服务器。在服务器池配置模式下，使用以下命令：

region *value*

- *value* - 指定该服务器池所属地区。

使用该命令**no**的形式删除配置。

服务器池权重

指定该服务器池的权重，系统会按权值的比例来分配流量。在服务器池配置模式下，使用以下命令：

weight *value*

- *value* - 指定该服务器池的权重值。取值范围为1至255，默认值50。

使用该命令**no**的形式恢复默认值。

指定健康检查

指定健康检查或健康检查组，用于检查服务池的可用状态。在服务器池配置模式下，使用以下命令：

health-check *value*

- *value* - 指定健康检查或健康检查组对象。

使用该命令**no**的形式删除配置。

指定健康检查端口

指定健康检查端口，在服务器池配置模式下，使用以下命令：

health-check-port *value*

- *value* - 指定健康检查端口。

使用该命令**no**的形式删除配置。

启用链路繁忙保护

启用链路繁忙保护功能后，若服务器成员绑定的接口的带宽利用率达到阈值，系统判定该链路处于繁忙状态，该链路对应的服务器也将不参与负载均衡调度。在参与调度的服务器成员中，若系统根据首选算法和备选算法，均无法选出可用的服务器成员，系统将忽略该链路繁忙保护功能，重新根据均衡算法选择服务器。

在服务器池配置模式下，使用以下命令启用/禁用链路繁忙保护：

```
busy-protect {enable | disable}
```

- **enable** - 开启服务器池的链路繁忙保护功能。默认情况下，开启该功能。
- **disable** - 关闭服务器池的链路繁忙保护功能。

配置服务器池成员

添加服务器成员，在服务器池配置模式下，使用以下命令：

```
server server-name
```

- *server-name* - 指定服务器成员的名称。多次执行该命令，可向服务器池中添加多个服务器。

使用该命令no的形式删除配置。

服务器成员运行状态

当设备没有加入GSLB同步组时，服务器成员的运行状态由其自身或其所属服务器池配置的健康检查结果决定。

当设备加入GSLB同步组时，该GSLB设备上的智能DNS服务器成员可以分为两类，一类是设备自身添加的服务器成员；另一类是非设备自身添加的服务器成员，包括GSLB设备发现自身及其本地设备的虚拟服务器作为服务器成员、GSLB同步组内其他GSLB设备同步过来的服务器成员。

GSLB同步组建立后，各SLB设备向对应的本地数据中心同步自身的虚拟服务器信息（包括虚拟服务器的配置及其运行状态），然后该本地数据中心会将此虚拟服务器信息同步至GSLB同步组内其他GSLB设备。

因此，GSLB设备上服务器成员的运行状态有以下两种获取方式：1) 在该GSLB设备上，为服务器成员或其所属服务器池配置了健康检查，检查得到的服务器成员运行状态。2) GSLB设备发现的虚拟服务器信息中包含的运行状态、GSLB同步组内其他GSLB设备同步过来的服务器成员运行状态。

在GSLB设备上，决定服务器成员的运行状态的优先级为：方式1) > 方式2)。

配置Smart DNS主机

创建Smart DNS主机，在全局配置模式下，使用以下命令：

gslb smart-dns host *name*

- *name* - 指定DNS主机的名称。指定该命令后，系统将进入DNS主机配置模式。

使用该命令**no**的形式删除配置。

DNS主机状态

在DNS主机配置模式下，使用以下命令启用或禁用DNS主机。禁用的DNS主机不可用。

- 启用：**status enable**
- 禁用：**status disable**

配置域名

指定需要被智能解析的域名，在DNS主机配置模式下，使用以下命令：

domain *domain-name*

- *domain-name* - 指定需要被智能解析的域名，DNS主机支持添加1-128个域名以及主机段含有通配符*的域名。不同的DNS主机可配置相同的域名。当DNS主机配置的所有域名均属于某区域的域时，DNS主机才能与该区域绑定。

配置TTL

指定智能DNS返回给客户端的A或AAAA记录的缓存时间。在缓存时间内，若客户端再次请求该域名，可使用缓存中的记录。若超过缓存时间，缓存记录将被删除，系统需重新解析。

在DNS主机配置模式下，使用以下命令配置TTL：

ttd *value*

- *value* - 指定缓存时间。取值范围为1至65535，默认值为60秒。

在DNS主机配置模式下，使用该命令**no**的形式删除配置。

配置算法

对于命中DNS主机的客户端请求，系统将按照指定的算法为其选出服务器池。指定负载均衡算法，在DNS主机配置模式下，使用以下命令：

```
selection {round-robin | weighted-round-robin | topology}
```

- **round-robin** - 指定算法为轮询。指定后，设备将客户端的请求轮流分配给服务器池。
- **weighted-round-robin** - 指定算法为加权轮询。指定后，设备根据为服务器池分配的不同权重，按比例分发请求。权重大的服务器池，接收的请求多。此选项为默认配置。
- **topology** - 指定算法为静态就近性。指定后，设备根据客户端源地址的地区分配服务器池。当有多个服务器池配置了同一地区时，选择权重较大的服务器池。

在DNS主机配置模式下，使用**no selection**命令恢复默认配置。

配置保持算法

指定保持算法后，设备可以将携带保持算法特征的客户端请求，保持到同一个服务器池进行处理。指定保持算法，在DNS主机配置模式下，使用以下命令：

```
persistence src-ip [granularity-ipv4 value | granularity-ipv6 value | timeout time]
```

- **src-ip** - 将来自同一个源IP地址的客户端请求（包含后续的所有连接请求）都发送至同一个服务器池。支持IPv4和IPv6地址。
- **granularity-ipv4 value** - 指定IPv4地址的粒度，即该IPv4地址的子网掩码，取值范围为1至32，默认值为32。使用 **no granularity-ipv4**命令恢复IPv4地址子网掩码的默认值。
- **granularity-ipv6 value** - 指定IPv6地址的粒度，即该IPv6地址的前缀长度，取值范围为1至128，默认值为128。使用 **no granularity-ipv6**命令恢复IPv6地址前缀长度的默认值。
- **timeout time** - 指定保持表的超时时间。超过指定的时间值，设备将清除相应客户端的保持表信息。取值范围是60到65535秒，默认值是300秒。使用**no timeout**命令恢复保持表超时时间的默认值。

在DNS主机配置模式下，使用**no persistence**命令取消保持算法的配置。

配置服务器池成员

指定为所创建的DNS主机提供服务的服务器池，在DNS主机配置模式下，使用以下命令：

```
pool name
```

- *name* - 指定服务器池的名称。

在DNS主机配置模式下，使用该命令**no**的形式删除配置。

配置默认服务器池

在DNS主机配置模式下，使用以下命令，添加默认服务器池：

default-pool *name*

- *name* - 指定服务器池的名称。在设备按照静态就近性算法没有为客户端请求选出服务器池的情况下，将请求分配给该默认服务器池。如不配置缺省服务池，系统将按照加权轮询算法从可用的服务器池成员中，为客户端请求进行选择。

在DNS主机配置模式下，使用该命令**no**的形式删除配置。

数据中心

系统支持通过组建数据中心，将属于不同数据中心的多个GSLB设备建立同步组，同步其配置和状态，以实现多个GSLB设备场景下的负载均衡。通常，该功能与设备集群功能不可同时开启。

组建数据中心同步组后，当客户端发起DNS查询时，系统将根据客户端所属地域为其解析出距离最近的服务器地址；若距离客户端最近的数据中心无法提供服务，系统将返回其他数据中心的服务器地址给客户端，保证客户端访问不中断。同时，数据中心还可以自发现本地SLB中的虚拟服务器配置，并将其作为智能DNS服务器成员，为客户端提供服务。

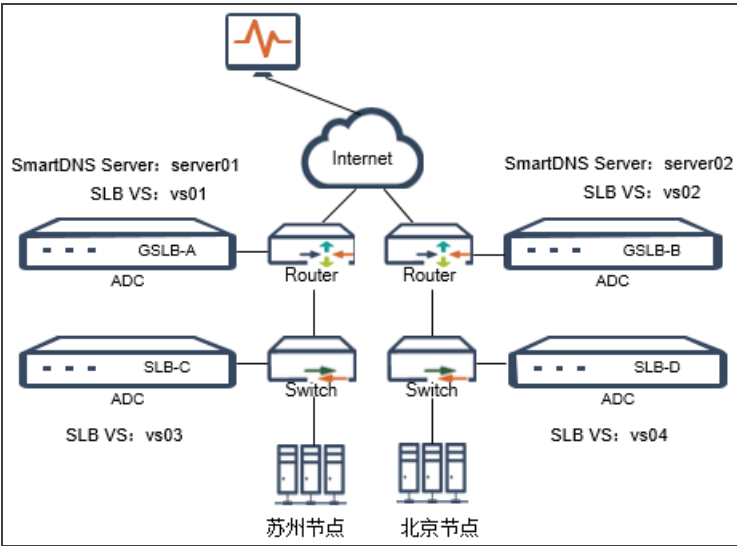
数据中心分为本地数据中心和远端数据中心，在一台GSLB设备上创建的本地数据中心，将作为另一台设备上的远端数据中心。在各台ADC设备完成本地数据中心的配置并添加远端数据中心后，可以将这些设备加入GSLB同步组。GSLB同步组建立后，用户可以将本台设备的GSLB配置信息和同步组信息同步到组内的其他设备，但不包括健康检查的配置和DNS服务器的监听地址。

同时，对于未配置数据中心的SLB设备（即开启服务器负载均衡功能的ADC设备），可以根据其地理位置，将SLB设备注册到相应的数据中心。数据中心对应的GSLB设备就可以自发现或手动发现本地SLB设备的虚拟服务器配置，然后将其作为智能DNS服务器成员，并在GSLB同步组内进行同步，为客户端提供服务。

在SLB设备属于HA组的情况下，因为HA组内成员间可以同步虚拟服务器配置，所以该SLB设备注册到本地数据中心、相应GSLB同步组建立后，HA组内的虚拟服务器配置，都可以作为GSLB设备的智能DNS服务器成员，对外提供服务。

应用场景举例

建立GSLB同步组的典型应用场景如下：



如上图所示，现有苏州和北京两个数据中心节点，苏州节点部署GSLB设备GSLB-A和SLB设备SLB-C，北京节点部署GSLB设备GSLB-B和SLB设备SLB-D。组建设备GSLB-A和设备GSLB-B的GSLB同步组，并将设备SLB-C注册到设备GSLB-A的苏州数据中心，将设备SLB-D注册到设备GSLB-B的北京数据中心。然后在设备GSLB-A上配置智能DNS服务器成员server01、SLB虚拟服务器vs01；在设备SLB-C上配置SLB虚拟服务器vs03；在设备GSLB-B上配置智能DNS服务器成员server02、SLB虚拟服务器vs02；在设备SLB-D上配置SLB虚拟服务器vs04。

完成以上配置后，设备GSLB-A和GSLB-B的智能DNS服务器成员列表将显示以下所有服务器信息：server01、server02、vs01、vs02、vs03和vs04。因此，当客户端发起DNS查询时，系统可以根据其地理位置以及各服务器成员的实际状态，返回最优服务器的IP地址给客户端，实现多数据中心的全局负载均衡。

配置数据中心

配置数据中心，实现GSLB同步组的建立，包含以下配置步骤：

1. 创建本地数据中心，即各GSLB设备根据自身的地理位置，完成相应数据中心的配置。具体操作，请参考[创建本地数据中心](#)部分。
2. 添加远端数据中心，即发现、认证并添加其他数据中心至本台设备，使得相关设备的列表中均包含所有数据中心。具体操作，请参考[发现数据中心](#)部分。

3. 创建GSLB同步组，即将数据中心列表中的设备添加至GSLB同步组，并向组内成员同步GSLB配置信息和同步组信息。具体操作，请参考[配置GSLB同步组](#)部分。
4. 配置本地SLB设备的地址信息，即在开启了服务器负载均衡功能的ADC设备上，配置用来注册到数据中心的IP地址和端口号。具体操作，请参考[注册SLB设备到数据中心](#)部分。
5. 注册本地设备至数据中心。

创建本地数据中心

若要组建GSLB同步组，首先应在每台设备上创建本地数据中心。

创建本地数据中心，在全局配置模式下，使用以下命令：

```
gslb data-center name node value
```

- *name* - 指定本地数据中心的名称，取值范围是1到95个字符。GSLB同步组内不允许存在相同名称的数据中心。
- *value* - 指定本地数据中心的节点ID。GSLB同步组内不允许存在相同节点ID的数据中心。

指定IP地址

指定本地数据中心的IP地址。用户配置的IP地址需能够与远端数据中心的IP地址通信。在本地数据中心配置模式下，使用以下命令配置IP地址：

```
ip interface-address
```

- *interface-address* - 指定接口的IP地址作为本地数据中心的IP地址。

在本地数据中心配置模式下，使用**no ip** 命令删除本地数据中心IP地址的配置。

指定联系人

指定本地数据中心的联系人信息，在本地数据中心配置模式下，使用以下命令：

```
contact value
```

- *value* - 指定本地数据中心的联系人信息，取值范围是1到128个字符。

在本地数据中心配置模式下，使用**no contact** 命令删除本地数据中心联系人的配置。

指定地理位置

指定本地数据中心的地理位置，在本地数据中心配置模式下，使用以下命令：

location *value*

- *value* - 指定本地数据中心的地理位置，取值范围是1到128个字符。

在本地数据中心配置模式下，使用**no location** 命令删除本地数据中心地理位置的配置。

启用虚拟服务器发现

开启本地数据中心的虚拟服务器发现功能。该功能开启后，当GSLB同步组建立好时，系统将自动发现自身和本地设备的SLB虚拟服务器相关配置信息，并且在组内所有设备的“智能DNS > 服务器成员”列表显示。

启用本地数据中心的虚拟服务器发现功能，在本地数据中心配置模式下，使用以下命令：

virtual-server discovery *enable*

- *enable* - 开启本地数据中心的虚拟服务器发现功能。

在本地数据中心配置模式下，使用**no virtual-server discovery**命令关闭本地数据中心的虚拟服务器发现功能。

指定本地IP地址

指定设备上配置好的接口地址作为本地IP地址，设备将使用该地址与其本地设备进行通信。若不指定，系统将使用对应路由条目的出接口，与本地设备进行通信。在本地数据中心配置模式下，使用以下命令指定本地IP地址：

local-ip *interface-address*

- *interface-address* - 指定设备接口的IP地址作为本地IP地址。

在本地数据中心配置模式下，使用**no local-ip**命令删除本地IP地址的配置。

指定本地设备

本地设备表示注册到该本地数据中心的ADC设备。用户需提前在本地设备上完成注册的相应配置，具体信息请参阅[配置本地设备](#)部分。指定本地数据中心的本地设备信息，将其注册到本地数据中心。在本地数据中心配置模式下，使用以下命令指定本地设备：

local-device *address* [*port-number*]

- *address* - 指定本地设备的IP地址，可以为IPv4地址或IPv6地址。
- *port-number* - 指定本地设备的端口号，取值范围是1到65535。

在本地数据中心配置模式下，使用**no local-device** 命令删除本地数据中心的本地设备配置。

发现数据中心

完成本地数据中心的配置后，系统需要发现、认证及添加其他数据中心。当待发现数据中心认证通过时，系统将其添加到数据中心列表。

发现数据中心，并将其添加至数据中心列表，在任何模式下，使用以下命令：

exec gslb data-center add address

- *address* - 指定待发现数据中心的IP地址。

在本台设备上将指定设备移出后，该设备会同时将本台设备移出。若指定为远端数据中心，系统将该远端数据中心移出列表；若指定为本地数据中心，系统将所有远端数据中心移出列表。移出设备，在任何模式下，使用以下命令：

exec gslb data-center delete name - 将在线设备移出数据中心列表。

exec gslb data-center delete name force - 将离线的设备移出数据中心列表。



注意: 被添加到GSLB同步组的设备不能被移除，若用户需要移除该设备，应先将该设备从同步组中删除。将设备从同步组中删除，请参阅[配置GSLB同步组](#)部分。

查看数据中心

在任何模式下，使用以下命令查看数据中心信息，包含数据中心类型、节点ID、IP地址和在数据中心列表中的状态等：

show gslb data-center name

- *name* - 指定数据中心的名称。

配置GSLB同步组

用户可以根据需要，将数据中心列表中的设备加入到GSLB同步组中，组内设备间应同步配置信息和GSLB同步组信息。同步组信息仅支持手动同步；GSLB配置信息支持手动同步或系统自动同步，但不包括健康检查和DNS服务器的监听地址。

添加GSLB同步组成员

添加GSLB同步组成员，在全局配置模式下，使用以下命令：

```
gslb sync-group name
```

- *name* - 指定数据中心的名称。

在全局配置模式下，使用`no gslb sync-group name`命令将数据中心从GSLB同步组中删除。



注意：系统仅支持删除本地数据中心或同步组列表中离线的远端数据中心。

配置同步

配置同步，在全局配置模式下，使用以下命令：

```
exec gslb sync {configuration [data-center name] | sync-group [data-center name]}
```

- **configuration** - 指定同步配置信息。
- **sync-group** - 指定同步GSLB同步组信息。
- *name* - 指定将信息同步到指定设备。若不指定，系统将信息同步到同步组内的所有设备。

查看GSLB同步组

在任何模式下，使用以下命令查看GSLB同步组信息，包含数据中心类型、节点ID、和IP地址和在同步组中的状态等：

```
show gslb sync-group
```

注册SLB设备到数据中心

在未加入GSLB同步组时，设备可以作为本地设备注册到数据中心。本地设备注册到相应数据中心后，本地设备的虚拟服务器信息可以同步至对应GSLB同步组内的所有设备，即GSLB同步组内所有设备将在“智能DNS

> 服务器成员”列表显示本地设备的虚拟服务器。

配置本地设备

配置本地设备，在全局配置模式下，使用以下命令：

```
slb device address [port-number]
```

- *address* - 指定本地设备的IP地址，用来注册到数据中心。
- *port-number* - 指定本地设备注册到数据中心的端口号，默认值是1616。

在全局配置模式下，使用**no slb device**命令删除本地设备的配置。

手动发现虚拟服务器

系统支持用户手动发现本地数据中心或其本地设备上配置的虚拟服务器。手动发现虚拟服务器，在全局配置模式下，使用以下命令：

```
exec gslb virtual-server discovery
```

在本地数据中心设备上执行该命令，GSLB设备向GSLB同步组内每台SLB设备发送虚拟服务器发现请求，然后SLB设备向其同步自己的虚拟服务器信息（包括虚拟服务器的配置及其运行状态），该GSLB设备再将收到的虚拟服务器信息同步至组内其他GSLB设备。

查看本地设备

在任何模式下，使用以下命令查看本地设备的配置信息：

```
show slb device
```

第3章 链路负载均衡

用户可以在出站方向启用链路负载均衡功能。系统可以根据流量目的地址所属的ISP，将其合理地分配到相应的ISP链路进行转发；也可以利用实时链路监控技术、动态链路探测技术将流量分发到不同链路，缩小各链路上的网络时延、抖动、丢包率，从而获得较为平衡的带宽利用率；还可以根据流量的源/目的地址信息将其合理地分配到不同链路等。

目前，系统支持以下15种流量负载均衡算法，包括任意域名就近算法、动态就近算法、目的IP哈希、加权目的IP哈希、源IP哈希、加权源IP哈希、源IP端口哈希、加权源IP端口哈希、ISP、最小带宽、最小连接数算法、加权最小连接、轮询、加权源IP哈希、加权最小带宽和加权轮询，实现出站流量的自动负载均衡。



注意: 升级到AX 2.8及其以后版本后，原AX 2.7及其以前版本的LLB Profile 配置可能丢失，需重新配置。

链路负载均衡配置包含：

- "出站负载均衡" 在第260页
- "查看链路负载均衡信息" 在第273页

出站负载均衡

系统提供流量的出站负载均衡功能。对于出站链路流量，系统按照特定的流量负载均衡算法，将到达设备的流量均匀地调度到各条链路进行转发。用户通过配置灵活的LLB 模板，并配置LLB规则将LLB模板绑定到路由上（目前系统仅支持目的路由和策略路由），以实现对外站链路流量的控制及负载均衡。

创建LLB Profile

用户新建或配置LLB Profile，在全局配置模式下，使用以下命令：

```
llb profile llb-profile-name [ipv6]
```

- *llb-profile-name* - 指定LLB Profile的名称。执行该命令后，系统创建指定名称的LLB Profile，并且进入该LLB Profile配置模式；如果指定的名称已存在，则直接进入LLB Profile配置模式。
- *ipv6* - 指定该LLB Profile处理IPv6类型的流量。

在全局配置模式下，使用**no llb profile llb-profile-name**命令删除指定的LLB Profile。

配置负载均衡算法

配置负载均衡算法后，当新的出站流量到达时，系统将按照指定的算法为其选择出口链路。

系统支持多种流量出站的负载均衡算法，包括：

算法	描述
任意域名就近 (Host Any Dynamic Prox- imity)	对于客户端发起的域名形式的访问请求，由设备的DNS代理转发给DNS服务器解析后，对于客户端后续的业务访问请求，设备可以对相应出口链路质量进行主动探测，然后根据探测结果，选择质量最优的链路对业务流量进行转发。 对于业务发起的IP地址形式的访问请求，也将触发设备对访问地址相应出口链路的主动探测，后续客户端请求达到时，设备将根据探测结果，选择质量最优的链路对业务流量进行转发。 • 主动探测功能开启：设备按照上述流程为客户端访问请求选择合适的链路。 • 主动探测功能关闭：对于域名形式的访问请求，设备为业务流量选择DNS响应报文的入接口进行转发；对于IP地址形式的访问请求，该算法不生效，设备将根据备选调度算法进行选路。
动态就近算法 (Dynamic Proximity)	设备将主动探测或实时监控各链路的时延、抖动、丢包率和带宽利用率。 • 链路动态探测功能开启：当链路带宽利用率低于用户设定的接口带宽阈值时，系统将只根据延时、丢包、抖动计算链路质量，优先选择质量高的链路；当链路带宽利用率高于用户设定的接口带宽阈值时，系统将综合延时、丢包、抖动和带宽利用率来计算链路质量，优先选择质量高的链路。 • 链路动态探测功能关闭：系统仅根据各出口链路的带宽利用率来选路，优先选用带宽利用率低的链路。
目的IP哈希 (Hash Dst IP)	对流量的目的地址进行哈希运算，根据运算的结果进行选路。

加权目的IP哈希 (Weighted Hash Dst IP)	在目的IP哈希的基础上，设备根据接口的权值，按比例进行选路。当新的出站流量到达时，接口权值越大对应的出口链路转发的流量越多。
源IP哈希 (Hash Src IP)	对流量的源地址进行哈希运算，根据运算的结果进行选路。
加权源IP哈希 (Weighted Hash Src IP)	在源IP哈希的基础上，设备根据接口的权值，按比例进行选路。当新的出站流量到达时，接口权值越大，对应的出口链路转发的流量越多。
源IP端口哈希 (Hash Src IP Port)	对流量的源地址和端口进行哈希运算，根据运算的结果进行选路。
加权源IP端口哈希 (Weighted Hash Src IP Port)	在源IP端口哈希的基础上，设备根据接口的权值，按比例进行选路。当新的出站流量到达时，接口权值越大，对应的出口链路转发的流量越多。
ISP	将流量的目的地址与系统ISP信息进行匹配，根据匹配的结果进行选路。
最小带宽 (Least Bandwidth)	设备会记录每个接口上的上行带宽、下行带宽或上行与下行带宽总和。当新的出站流量到达时，设备将选择带宽或带宽总和最小的接口进行转发。
最小连接数算法 (Least Connection)	设备会记录每个接口上的连接数。当新的出站流量到达时，设备将选择连接数最少的接口进行转发。
加权最小连接 (Weighted Least Connection)	在最少连接数分发的基础上，设备根据接口的权值，按比例进行选路。当新的出站流量到达时，将为其选择当前连接数与接口权值的比值最小的链路。（计算方法：接口上的连接数除以接口权值）。
轮询 (Round Robin)	设备将流量轮流分配给每条出口链路。
加权最小带宽 (Weighted Least Bandwidth)	在最小带宽的基础上，设备根据接口的权值，按比例进行选路。当新的出站流量到达时，将为其选择当前带宽（总和）与接口权值的比值最小的链路。（计算方法：上行带宽、下行带宽或上行与下行带宽总和除以接口权值）。
加权轮询 (Weighted Round Robin)	在轮询的基础上，设备根据接口的权值，按比例进行选路。接口权值越大，对应的出口链路流量越多。



提示: 接口权值的具体配置信息, 请参阅接口配置的“[链路负载均衡权值](#)”部分。

在LLB Profile配置模式下, 使用以下命令配置负载均衡算法:

```
balance {prefer {host-any-dynamic-proximity | dynamic-proximity | hash-dst-ip | weighted-hash-dst-ip | hash-src-ip | weighted-hash-src-ip | hash-src-ip-port | weighted-hash-src-ip-port | least-bandwidth | least-connection | weighted-least-connection | round-robin | weighted-least-bandwidth | weighted-round-robin | isp [dynamic-proximity | hash-dst-ip | weighted-hash-dst-ip | hash-src-ip | weighted-hash-src-ip | hash-src-ip-port | weighted-hash-src-ip-port | least-bandwidth | least-connection | weighted-least-connection | round-robin | weighted-least-bandwidth | weighted-round-robin] } | alternative {dynamic-proximity | hash-dst-ip | weighted-hash-dst-ip | hash-src-ip | weighted-hash-src-ip | hash-src-ip-port | weighted-hash-src-ip-port | least-bandwidth | least-connection | weighted-least-connection | round-robin | weighted-least-bandwidth | weighted-round-robin}} [bandwidth-direction {bidirection | downstream | upstream}]
```

- **prefer** - 指定负载均衡的首选算法。
 - **host-any-dynamic-proximity** - 指定首选均衡算法为任意域名就近算法。指定该算法后, 系统将根据主动探测的相关配置, 为出站流量智能选路。主动探测的详细信息, 请参阅“[配置主动探测](#)”。
 - **dynamic-proximity** - 指定首选均衡算法为动态就近算法。指定该算法后, 根据链路探测相关参数的配置, 系统为出站流量智能选路。链路探测配置的详细信息, 请参阅“[配置链路探测](#)”。
 - **hash-dst-ip** - 指定首选均衡算法为目的IP哈希算法。
 - **weighted-hash-dst-ip** - 指定首选均衡算法为加权目的IP哈希算法。
 - **hash-src-ip** - 指定首选均衡算法为源IP哈希算法。
 - **weighted-hash-src-ip** - 指定首选均衡算法为加权源IP哈希算法。
 - **hash-src-ip-port** - 指定首选均衡算法为源IP端口哈希算法。
 - **weighted-hash-src-ip-port** - 指定首选均衡算法为加权源IP端口哈希算法。
 - **least-bandwidth** - 指定首选均衡算法为最小带宽算法。

- **least-connection** - 指定首选均衡算法为最小连接数算法。
- **weighted-least-connection** - 指定首选均衡算法为加权最小连接数算法。
- **round-robin** - 指定首选均衡算法为轮询算法。该参数为默认算法。
- **weighted-least-bandwidth** - 指定首选均衡算法为加权最小带宽算法。
- **weighted-round-robin** - 指定首选均衡算法为加权轮询算法。

说明：当指定负载均衡算法为**weighted-hash-src-ip**、**weighted-hash-dst-ip**、**weighted-hash-src-ip-port**、**weighted-least-connection**、**weighted-least-bandwidth**或者**weighted-round-robin**时，系统将根据接口的权值，按比例进行选路。接口权值的具体配置信息，请参阅“[配置接口的链路负载均衡权值](#)”部分。

- **isp** [**dynamic-proximity** | **hash-dst-ip** | **weighted-hash-dst-ip** | **hash-src-ip** | **weighted-hash-src-ip** | **hash-src-ip-port** | **weighted-hash-src-ip-port** | **least-bandwidth** | **least-connection** | **weighted-least-connection** | **round-robin** | **weighted-least-bandwidth** | **weighted-round-robin**] - 指定首选均衡算法为ISP算法，并且同时需指定二级均衡算法。若存在多条链路与流量目的IP的ISP相匹配，需要根据二级算法，在多条链路中再次进行选路。系统默认的二级均衡算法为 **round-robin**。

说明：当指定负载均衡算法为**isp**时，系统将接口配置的ISP信息，作为链路对应的ISP信息，从而进行选路。配置接口ISP的具体信息，请参阅“[配置接口所属ISP](#)”部分。

- **alternative** {**dynamic-proximity** | **hash-dst-ip** | **weighted-hash-dst-ip** | **hash-src-ip** | **weighted-hash-src-ip** | **hash-src-ip-port** | **weighted-hash-src-ip-port** | **least-bandwidth** | **least-connection** | **weighted-least-connection** | **round-robin** | **weighted-least-bandwidth** | **weighted-round-robin**} - 当首选均衡算法为 **isp** 或 **host-any-dynamic-proximity** 时，指定备选均衡算法。指定备选调度算法。系统通过首选调度算法没有为流量匹配到合适的链路，需要根据备选调度算法，为流量重新进行选路。
- **bandwidth-direction** {**bidirection** | **downstream** | **upstream**} - 指定均衡算法为 **least-bandwidth**、**weighted-least-bandwidth** 时，计算链路的实际带宽，需指定数据流量的方向。并且，仅当均衡算法为 **least-bandwidth**、**weighted-least-bandwidth** 时，该配置生效。
 - **bidirection** - 系统将计算数据流的入和出两个方向上带宽之和，进而调整选路方法。该参数为默认方向。

- **downstream** - 系统将计算数据流的入方向上的带宽，进而调整选路方法。
- **upstream** - 系统将计算数据流的出方向上的带宽，进而调整选路方法。

在LLB Profile配置模式下，使用 **no balance {prefer | alternative}** 命令恢复默认负载均衡算法。



注意:

- 当均衡算法配置为“任意域名就近”时，绑定该调度策略的LLB规则需绑定域名簿“any”。绑定域名的详细信息，请参阅“[绑定域名簿](#)”。
- 当均衡算法配置为“动态就近”，并且绑定该调度策略的LLB规则绑定了域名簿时，若客户端的访问请求匹配上了绑定的域名簿，系统将对相应出口链路的质量发起主动探测，然后将主动探测的结果作为选路的依据；否则，系统将通过监控各出口链路上的流量统计信息，判断链路质量，从而进行选路。
- 若根据负载均衡算法选出的链路均处于繁忙状态，系统将使用默认路由对流量进行转发。

配置带宽统计周期

当流量出站的负载均衡算法配置为“最小带宽”或“加权最小带宽”时，用户可以根据需要，指定流量带宽的统计周期。为出站流量的负载均衡配置带宽统计周期，在全局配置模式下，使用以下命令：

llb bandwidth-statistics-period value

- **value** - 指定带宽统计周期。取值范围是1到300秒，默认值为120秒。

在全局配置模式下，使用**no llb bandwidth-statistics-period**命令恢复默认值。

查看系统当前的带宽统计周期，在任意配置模式下，使用以下命令：

show llb bandwidth-statistics-period

开启综合考虑其它调度结果功能

当均衡算法指定为“轮询”或“加权轮询”时，系统支持开启链路负载均衡的综合调度功能。开启该功能后，系统将综合会话保持算法对链路的调度结果，进行智能选路。当新的出站流量到达时，系统会根据当前各链路承载流量的情况，优先选择承载流量较少的链路对其进行转发。

在LLB Profile配置模式下，使用以下命令开启综合调度功能：

balance comprehensive

- **comprehensive** - 开启链路负载均衡的综合调度功能，系统默认关闭该功能。

在LLB Profile配置模式下，使用 **no balance comprehensive** 命令关闭综合调度功能。

配置链路负载均衡的优先级调度策略

启用链路的优先级调度策略，需指定最小活跃链路数，即参与链路负载均衡调度的链路的最少个数，取值范围是1到32。

在LLB Profile配置模式下，使用以下命令开启链路负载均衡的优先级调度策略：

min-active-link value

- **value** - 指定最小活跃链路数。取值范围是0到32，默认值是0，表示关闭链路负载均衡的优先级调度功能。

在LLB Profile配置模式下，使**no min-active-link**命令恢复最小活跃链路数的默认值。

设备出口链路的优先级由其对应接口的[链路负载均衡优先级](#)决定。如设备上存在10条出口链路，最小活跃链路数为6，那么根据出口链路对应接口的优先级排序，最高优先级的所有可用链路优先加入调度；如果最高优先级的链路小于6条，次优先级的所有可用链路将加入调度。以此类推，直到参与调度的可用链路数大于等于6或者所有的可用链路均参与调度为止。当某条参与调度的链路不可用，导致实际参与调度的链路条数小于6时，设备会继续从未参与调度的链路中，选择最高优先级的所有可用链路加入调度，直到满足条件；当高优先级的链路从不可用变为可用时，将重新加入调度。

举例说明，接口eth0/1、eth0/2、eth0/3和eth0/4的链路负载均衡优先级分别为10、20、30和20；接口eth0/1、eth0/2、eth0/3和eth0/4的ISP分别为China-telecom、China-telecom、China-telecom和China-mobile。LLB模板的首选均衡算法为“ISP”，备选均衡算法为“轮询”，开启优先级调度策略，最小活跃链路数为2。其他选项保持默认配置，并为LLB模板关联LLB规则。使用电信运营商的客户发送请求达到设备后，因为LLB均衡算法为ISP，所以接口eth0/1、eth0/2和eth0/3对应的出口链路将参与调度；因为接口eth0/1和eth0/2优先级较高，所以设备最终将该电信客户端请求轮流分配给接口eth0/1、eth0/2。

配置主动探测

当指定流量的首选均衡算法为“任意域名就近”时，系统会自动启用主动探测功能。客户端的DNS请求经设备转发给DNS服务器解析，返回的DNS响应到达设备时，设备会在探测表中记录解析得到的IP

地址，及IP地址对应的设备出接口。当客户端收到DNS响应，首次发起的业务访问流量到达设备时，设备将选择之前DNS响应到达设备的入接口作为业务访问流量的出接口；同时，对于客户端访问的记录在探测表中的IP地址，系统将主动从该IP地址对应的各出接口发送探测报文，用来探测各出接口对应链路的质量。当客户端再次发起业务访问时，系统将根据探测结果，选择质量最优的链路进行转发。

在LLB Profile配置模式下，使用以下命令配置主动探测功能的相关参数：

host-detect {**interval** *interval* | **max-table-size** *value* | **timeout** *time*}

- *interval* - 指定系统主动发送探测报文的时间间隔。取值范围是60到86400秒，默认值是600秒。
- *value* - 指定探测表可以记录的表项的最大个数。不同平台支持配置的表项大小不同，请以实际页面为准。
- *time* - 指定探测表项的超时时间。如果超过该时间，系统将清除相应的探测表项。取值范围是300到86400秒，默认值是3600秒。

在LLB Profile配置模式下，使用**no host-detect** {**interval** | **timeout**} 命令恢复默认值。

配置链路探测

当指定流量的负载均衡算法为“动态就近性”时，需配置链路状态探测的各项参数。系统将根据链路探测的配置，为出站流量智能选路。

开启链路探测

在LLB Profile配置模式下，使用以下命令关闭或开启链路探测功能：

dynamic-extra-conf detect {**disable** | **enable**}

- **disable** - 禁用探测功能。禁用探测功能后，系统仅根据各出口链路的带宽占用率来选路，优先选用带宽占用率低的链路。
- **enable** - 启用探测功能。开启探测功能后，系统会根据用户配置的参数对网络链路状态进行探测，然后选出最优路由。对于用户需配置的参数，详细信息请参阅“[配置计算链路状态时各项权值](#)”部分。

配置链路探测掩码/前缀

在LLB Profile配置模式下，使用以下命令配置链路探测时的掩码：

dynamic-extra-conf detect {**netmask** {*A.B.C.D* | *num*} | **prefix** *prefix-len*}

- **netmask** {*A.B.C.D* | *num*} - 指定需要探测的IPv4类型目的IP网段。系统将对该IPv4网段的流量进行实时监控，并根据监控统计结果进行流量负载均衡调整。系统支持两种格式，*A.B.C.D*和*num*。*A.B.C.D*的取值范围255.255.240.0到255.255.255.255，默认值为255.255.255.240；*num*的取值范围是20到32，默认值为28。
- **prefix** *prefix-len* - 指定需要探测的IPv6类型目的IP网段。系统将对该IPv6网段的流量进行实时监控，并根据监控统计结果进行流量负载均衡调整。*prefix-len*的取值范围是64到96，默认值为64。

配置带宽利用率阈值

指定接口带宽利用率阈值，在LLB Profile配置模式下，使用以下命令：

dynamic-extra-conf detect threshold *value*

- *value* - 指定接口带宽利用率阈值。当接口的带宽利用率没有超过阈值时,系统将只分析链路的时延、抖动、丢包状况来动态调整选路的方法；当接口的带宽利用率超过阈值时，系统将同时分析各链路上“带宽利用率”这一参数来调整选路方法。*value*的取值范围为1至100（1%-100%），默认为60%。

配置计算链路状态时各项权值

指定计算各链路状态权重时，链路的时延、抖动、丢包率和带宽利用率的占比。在LLB Profile配置模式下，使用以下命令：

dynamic-extra-conf detect weight-factors *delay-factor jitter-factor loss-rate-factor BW-rate-threshold-factor* [*BW-rate-factor*]

- *delay-factor* - 指定链路时延的占比。取值范围是0到15，默认值是1。
- *jitter-factor* - 指定链路抖动的占比。取值范围是0到15，默认值是2。
- *loss-rate-factor* - 指定链路丢包率的占比。取值范围是0到15，默认值是4。
- *BW-rate-threshold-factor* - 指定链路带宽利用率超过阈值时，带宽利用率的占比。取值范围是0到15，默认值是1。
- *BW-rate-factor* - 指定链路当前带宽利用率的占比。取值范围是0到15，默认值是1。

配置链路权重刷新时间

指定更新链路各项权重的间隔时间，在LLB Profile配置模式下，使用以下命令：

dynamic-extra-conf detect weight-update-interval *value*

- *value* - 指定更新系统链路状态权重的间隔时间。取值范围是1到300秒，默认值是1秒。

配置子网条目最大值

配置LLB Profile子网条目的最大数目，在LLB Profile配置模式下，使用以下命令：

```
dynamic-extra-conf detect max-entry-number value
```

- *value* - 指定系统可配置LLB profile子网条目的最大数值。默认值依据平台不同而不同，请以实际为准。

配置带宽探测方向

系统计算负载均衡的带宽利用率时，需配置数据流量的方向。在LLB Profile配置模式下，使用以下命令：

```
dynamic-extra-conf bandwidth-balance-direction {bidirection | downstream | upstream}
```

- **bidirection** - 系统将取数据流的入和出两个方向上带宽利用率较大的值与带宽利用率阈值进行比较，进而调整选路方法。
- **downstream** - 系统将取数据流的入方向上的带宽利用率的值与带宽利用率阈值进行比较，进而调整选路方法。该参数为默认方向。
- **upstream** - 系统将取数据流出方向上带宽利用率的值与带宽利用率阈值进行比较，进而调整选路方法。

配置负载均衡的模式

配置流量负载均衡的模式，在LLB Profile配置模式下，使用以下命令：

```
dynamic-extra-conf mode {compatibility [upper-limit value lower-limit value] | performance}
```

- **compatibility** - 配置负载均衡模式为高兼容模式。当链路负载变动时，系统不会频繁地切换链路，而是优先保证业务尽量在先前链路上。此模式多适用于对链路切换比较敏感的业务，如银行业务。
upper-limit *value*表示上行流量带宽利用率阈值，**lower-limit** *value*表示下行流量带宽利用率阈值。
upper-limit和**lower-limit**的取值范围是1到100（1%到100%）。
- **performance** - 配置负载均衡为高性能模式，此模式下系统会跟据链路实时的时延、抖动、丢包情况，迅速调整以最大限度的保持链路负载均衡。该模式为流量负载均衡的默认模式。

配置会话保持方法

指定负载均衡的会话保持方法。通过配置会话保持方法，系统将符合会话保持条件的流量，都保持到同一条链路进行转发。在LLB Profile配置模式下，使用以下命令配置会话保持方法：

```
persistence method {dst-ip | src-dst-ip | src-ip}
```

- **src-ip** - 对于来自同一客户端的流量，选择同一条链路进行转发。
- **src-dst-ip** - 对于来自同一客户端且目的地址相同的流量，选择同一条链路进行转发。
- **dst-ip** - 对于目的地址相同的流量，选择同一条链路进行转发。

在LLB Profile配置模式下，使用 **no persistence method** 命令删除会话保持方法。



注意: 为出站流量选择出口链路时，先匹配会话保持。若匹配到了会话保持表中的链路，即使该链路处于繁忙状态，设备仍然使用该链路转发流量。

配置会话保持超时时间

指定会话保持的超时时间。超过指定的时间值，设备将清除相应的会话保持表信息。在LLB Profile配置模式下，使用以下命令配置会话保持超时时间：

```
persistence timeout value
```

- **value** - 指定会话保持的超时时间。取值范围是60到65535秒，默认值是300秒。

在LLB Profile配置模式下，使用 **no persistence timeout** 命令恢复会话超时时间的默认值。

配置链路繁忙保护

用户可以为出口链路配置繁忙保护。当某条链路的出口流量达到接口指定的带宽阈值时，若系统通过负载均衡算法为流量选择出口链路时，将优先选择其他不繁忙的链路；当系统通过会话保持算法为流量选择出口链路时，若匹配到了相应的会话保持表项，则忽略链路繁忙保护功能，选择匹配到的链路转发流量。

配置链路的繁忙保护功能，在接口配置模式下，使用以下命令：

```
bandwidth {downstream | upstream} threshold value
```

- **downstream** - 配置接口下行方向上的带宽阈值。
- **upstream** - 配置接口上行方向上的带宽阈值。
- **threshold value** - 指定接口的带宽阈值。取值范围是0到100（0%到100%），默认值是0。

在接口配置模式下，使用 **no bandwidth {downstream | upstream} threshold** 命令恢复接口带宽阈值的默认值。

说明：接口带宽配置的具体信息，请参阅“[配置接口带宽](#)”部分。

配置日志记录

当链路的带宽利用率超过指定阈值时，系统将会记录日志信息。在LLB Profile配置模式下，使用以下命令配置记录日志信息：

log enable [utilization-limit value]

- **utilization-limit value** - 指定链路带宽利用率的阈值。取值范围是1到100，默认值是90。

用户取消记录日志信息，在LLB Profile配置模式下，使用命令 **no log enable**。

添加描述信息

在LLB Profile配置模式下，使用以下命令为LLB Profile添加描述信息：

description value

- **value** - 指定描述信息的内容。取值为1至256字符。

用户删除描述信息，在LLB Profile配置模式下，使用命令 **no description**。

绑定LLB Profile

LLB Profile配置完毕后，需与路由绑定，形成LLB规则才能生效。目前支持绑定到目的路由（DBR）和策略路由（PBR）。绑定LLB规则，在全局模式下，使用以下命令：

llb rule rule-name [ipv6] [id llb-id] {pbr pbr-name id match-id | dbr [vrouter vr-name] {A.B.C.D/M | A.B.C.D A.B.C.D | X:X:X:X::X/prefix-len} } profile profile-name [host host-book-name]

- *rule-name* – 指定LLB规则名称。
- **ipv6** - 指定LLB规则处理的是IPv6流量。
- **id llb-id** - 指定LLB规则的ID。
- **pbr pbr-name** – 指定策略路由名称。
- **id match-id** – 配置策略路由ID。
- **dbf vrouter vr-name** – 指定目的路由的VRouter。
- *A.B.C.D/M | A.B.C.D A.B.C.D | X:X:X:X::X/prefix-len* - 指定VRouter目的地址。当该条LLB规则处理的是IPv4流量时，设备支持两种方式指定IPv4类型的VRouter目的地址：A.B.C.D/M或者A.B.C.D A.B.C.D，例如1.1.1.0/24或者1.1.1.0 255.255.255.0；当该条LLB规则处理的是IPv6流量时，指定IPv6类型的VRouter目的地址：X:X:X:X::X/prefix-len。
- **profile profile-name** – 绑定指定的LLB Profile。
- **host hosk-book-name** - 绑定指定的域名簿，仅当该LLB规则绑定目的路由时，系统支持配置该项。
 - 当绑定的调度策略的首选调度算法为“任意域名就近”时，需绑定预定义域名簿“any”，“任意域名就近”算法才能生效。
 - 当绑定的调度策略的首选调度算法为“动态就近”时，用户需选择配置了精确域名的域名簿，实现对各链路质量的主动探测。详细信息，请参阅“[首选调度算法](#)”。

在全局配置模式下，使用**no llb rule llb-rule-name**命令删除指定的LLB规则。

查看会话保持表

查看会话保持表，在任意模式下，使用以下命令：

show llb persistence rule rule-name [detail | dst-ip address [detail] | scr-ip address [detail]]

- **rule rule-name** – 查看指定LLB规则的会话保持表。
- **detail** – 指定查看会话保持表的详细信息，若不配置则展示简约的信息。
- **dst-ip address** – 查看指定目的地址的会话保持表信息。
- **scr-ip address** – 查看指定源地址的会话保持表信息。

查看链路负载均衡信息

查看出站方向链路负载均衡的配置信息，在任意模式下，使用以下命令：

```
show llb {profile [profile-name] | rule [rule-name] }
```

- **profile** [profile-name] - 查看出站方向链路负载均衡模板。*profile-name*为模板名称。
- **rule** [rule-name] - 查看出站方向链路负载均衡的规则。*rule-name*为规则名称。

第4章 设备集群

在通信线路或设备产生故障时，为了满足用户对通信畅通性、网络可靠性的高要求，系统提供具备更高冗余能力的设备集群功能。实现设备集群功能，用户需要配置两台及以上采用完全相同的硬件平台、固件版本、软件版本和许可证信息的AX设备。当集群内某台AX设备发生故障或者无法处理来自客户端的请求时，该请求会及时转移到集群内另外的可用设备处理。通常，设备集群功能与高可靠性功能不可同时开启；若同时开启，高可靠性功能生效。

集群基础概念

设备发现与认证

设备发现与认证，是系统对其他AX设备与本地设备的证书链进行匹配的过程。只有通过认证的设备，才可以与本地设备组成设备集群，实现集群功能。设备通过认证后，系统将其添加至集群设备列表，表示其与本地设备形成相互信任的关系。

设备组

设备组是能够支撑某个或某些服务（比如服务器负载均衡）、且相互信任的设备组成的群组。设备组内设备通过ID进行标识。创建好设备组，组内设备均上线后，设备进入集群运行状态，准备执行集群功能。设备间的集群关系一旦建立，就会进行相关配置信息的同步。然后，当设备组内某台AX设备发生故障，无法继续处理客户端请求时，系统便可以选择组内另一台设备接替故障设备的工作。因此，对外部网络而言，设备组相当于一个设备。

流量组

流量组是集群内相关服务的集合，是设备进行高可用切换的基本单位。AX设备通过将不同的服务与流量组进行绑定，当流量组的生效设备无法处理请求或发生故障时，另一台设备将接替其继续处理客户端流量。比如，在指定虚拟服务器的IP地址时，将其绑定到已有流量组；当客户端访问该虚拟服务器时，系统根据用户配置的设备切换顺序或特定算法，将该客户端请求分配给集群内的一台可用设备，即流量组创建后选出的生效设备。

作为设备集群功能的生效单位，每个接口IP都可以关联特定的流量组，流量通过接口进行传输。流量组生效设备的切换可能引起报文丢失，为了降低报文丢失对业务的影响，用户需为流量组配置虚拟MAC地址。流量

通过具有虚拟MAC地址的接口进行转发。当流量组的生效设备发生变化时，虚拟MAC地址随之切换到下一台设备的接口。

同一个流量组可以绑定多种服务类型的多个IP地址，例如可以将多个虚拟服务器IP地址和多个全局负载均衡中对外提供的DNS服务器地址绑定到同一个流量组。但是，同一个IP地址代表的服务，只可以绑定到一个流量组。

集群同步

当集群内某台设备发生故障无法继续处理客户端请求时，为保证其他设备能够代替其工作，故障设备需要与接替其工作的设备完成信息同步。集群设备间进行同步的信息包括：配置信息和部分RDO（Runtime Dynamic Object）。集群设备间进行同步的RDO信息主要包括：会话信息和四层会话保持表（支持同步IPv6会话保持表）。

用户可以通过以下两种方法进行集群内设备间的信息同步：批量同步和实时同步。当设备组建立后，系统会选出其中一台设备作为数据中心，由数据中心将配置信息批量同步至其他设备或者新加入设备组的设备；当配置发生变化时，系统会将变化的信息实时同步至其他设备。除设备集群相关配置、需要导入本地文件的相关配置和本地配置（例如，主机名称配置），其它的配置都会被同步。

配置集群

使用设备集群功能，用户需要按照以下步骤进行配置：

1. 配置本地设备的管理地址。
2. 配置本地设备信息。
3. 发现需要加入集群的ADC设备，并对其进行认证。
4. 创建设备组，即为本地设备与认证通过的设备建立设备组。
5. 创建流量组。
6. 配置相关服务时，选择已有流量组进行绑定。



注意：配置集群功能时：设备IP不能与SLB虚拟服务器IP相同。设备主镜像IP、主故障转移IP、次故障转移IP均不能与SLB虚拟服务器IP相同。

配置本地管理地址

当本地设备进入集群运行状态时，自身的管理地址将加入默认的default流量组，导致用户无法继续通过该地址对设备进行管理、设备无法正常处理集群外的其他业务。为了避免这种情况，用户在配置集群功能之前，需先将本地设备的管理地址配置为Local IP，即关闭设备管理地址对应的“配置同步”功能，或者开启设备管理地址的“配置为Local IP”功能。

设备发现与认证

在设备集群中，用户当前登录的设备称为本地设备。使用设备集群功能时，需先完成本地设备的配置，再进行其他设备的发现与认证。

配置本地设备

本地设备的配置需要在本地设备配置模式下进行。进入本地设备配置模式，在全局配置模式下，使用以下命令：

cluster device *name* node *num*

- *name* - 指定设备的名称，取值范围是1到95个字符。名称相同的设备不可以加入同一集群设备列表。
- *num* - 指定设备加入集群的节点ID，不同设备需指定不同的节点ID。

在全局配置模式下，使用**no cluster device *name***命令删除本地设备的配置。

配置证书链

为本地设备指定证书链，用于集群内设备的认证。在本地设备配置模式下，使用以下命令配置证书链：

cert-chain *value*

- *value* - 指定创建好的证书链，用于设备认证。

配置设备IP

配置本地设备的IP地址，在本地设备配置模式下，使用以下命令：

device-ip *address*

- *address* - 指定设备接口的Local IP地址作为设备的IP地址。

在本地设备配置模式下，使用**no device-ip**命令取消本地设备IP的配置。

配置主故障转移IP

通过主故障转移IP地址，设备向设备组内其他设备发送心跳报文，检测设备的工作状态。当通过主故障转移IP地址检测到某台设备故障时，下一台设备将接替其继续工作。在本地设备配置模式下，使用以下命令配置设备的主故障转移IP地址：

```
primary-failover-ip interface-address interface-name
```

- *interface-address* - 指定设备接口的Local IP地址作为设备的主故障转移IP地址。
- *interface-name* - 输入设备接口名称。

在本地设备配置模式下，使用**no primary-failover-ip** 命令取消本地设备主故障转移IP的配置。

配置次故障转移IP

当主故障转移IP地址不可用时，使用该IP地址。在本地设备配置模式下，使用以下命令配置设备的次故障转移IP地址：

```
secondary-failover-ip interface-address interface-name
```

- *interface-address* - 指定设备接口的Local IP地址作为设备的次故障转移IP地址。
- *interface-name* - 输入设备接口名称。

在本地设备配置模式下，使用**no secondary-failover-ip** 命令取消本地设备次故障转移IP的配置。

配置主镜像IP

流量组开启“[同步数据对象](#)”功能后，若流量组生效设备处理客户端流量产生了数据信息，系统通过该IP地址将数据信息镜像给集群内下一台接替其工作的设备，包括会话信息和四层会话保持表信息。在本地设备配置模式下，使用以下命令配置设备的主镜像IP地址：

```
primary-mirror-ip address
```

- *address* - 指定设备接口的Local IP地址作为设备的主镜像IP地址。当设备发生故障时，通过该IP将自身的数据信息镜像给下一台接替其工作的设备。

在本地设备配置模式下，使用**no primary-mirror-ip** 命令取消本地设备主镜像IP的配置。

配置设备联系方式

在本地设备配置模式下，使用以下命令添加设备的联系方式：

contact *contact*

- *contact* - 添加设备的联系方式，可输入1-127字符。通常为设备管理员的联系方式。

在本地设备配置模式下，使用**no contact**命令删除设备的联系方式。

配置设备地理位置

在本地设备配置模式下，使用以下命令添加设备的地理位置：

location *location*

- *location* - 添加设备的地理位置，可输入1-127字符。

在本地设备配置模式下，使用**no contact**命令取消设备地理位置的配置。

配置设备发现超时时间

指定发现设备的超时时间。用户执行**exec cluster device add address**命令后，若超过指定的时间值，未收到对端设备的回应，则认为发现该设备失败。

add-device-timeout *time*

- *time* - 指定设备发现的超时时间。取值范围是5到30秒，默认值是5秒。

在本地设备配置模式下，使用**no add-device-timeout**命令恢复默认值。

配置设备在线超时时间

指定设备的在线超时时间。用户执行**exec cluster device add address**命令成功后，系统将周期性发送探测报文，确认对端设备是否在线；若超过指定的时间值，未收到对端设备的回应，则认为对端设备离线。在本地设备配置模式下，使用以下命令：

peer-device-response-timeout *time*

- *time* - 指定设备的在线超时时间。当设备状态由在线变为离线时，经过该时间，系统将在设备列表更新设备的状态。取值范围是5到30秒，默认值是5秒。

在本地设备配置模式下，使用**no peer-device-response-timeout**命令恢复默认值。

添加设备描述信息

在本地设备配置模式下，使用以下命令添加设备的描述信息：

description *description*

- *description* - 添加设备的描述信息，可输入1-255字符。

在本地设备配置模式下，使用**no description**命令删除设备的描述信息。

发现设备

完成本地设备的配置后，系统需要发现、认证及添加其他设备。当待发现设备关联的证书链与本地设备一致时，系统认为该设备通过认证，并将其添加至集群设备列表。发现设备，并将其添加至集群设备列表，在全局配置模式下，使用以下命令：

```
exec cluster device add address
```

- *address* - 指定待发现设备的IP地址。

将设备从集群设备列表移出，在全局配置模式下，使用以下命令：

- **exec cluster device delete name** - 将在线的设备移出设备列表。
- **exec cluster device delete name force** - 将在离线的设备移出设备列表。

集群同步

集群设备在进行高可用切换时，为了保证下一台设备可以正常工作，集群内设备间需同步数据信息，包括配置数据和RDO数据。用户可以登录设备组内其他设备，重复第一台设备上的设备组配置步骤，完成集群内设备间信息同步；或者在一台设备上，配置集群设备的信息同步，在全局配置模式下，使用以下命令：

```
exec cluster sync {configuration [device device-name] | device-group [device device-name] | rdo [traffic-group traffic-group-name] }
```

- **configuration** - 指定同步本地设备的配置信息。
- **device-group** - 指定同步设备组信息。
- *device-name* - 指定将信息同步到指定设备。若不指定，系统将信息同步至集群内所有设备。
- **rdo** - 指定同步RDO信息，包括：会话信息和四层会话保持表信息（支持同步IPv6会话保持表）。
- *traffic-group-name* - 指定流量组，系统将RDO信息同步至该流量组的下一台生效设备。若不指定，系统将同步RDO信息至运行在当前设备上，所有流量组的下一台生效设备。



注意: 只能将信息同步至于本地设备所在设备组的其他设备。

配置设备组

集群设备组的配置需要在设备组配置模式下进行。进入设备组配置模式，在全局配置模式下，使用以下命令：

```
cluster device-group name type {failover | sync-only}
```

- *name* - 指定设备组的名称，取值范围是1到95个字符。
- type {failover | sync-only}
 - **failover** - 指定设备组类型为“Failover”，该类型设备组内的设备可以高可用切换，即设备组内某台AX设备发生故障，无法继续工作时，组内另一台设备将接替其继续处理客户端流量。
 - **sync-only** - 指定设备组类型为“仅同步”，该类型设备组内的设备只可以进行相关数据信息的同步，且系统支持配置同步的数据信息类型。

在全局配置模式下，使用**no cluster device-group *name***命令删除指定的设备组。

说明：

- 若设备组为“Failover”类型，在全局配置模式下，使用**cluster device-group *name***命令即可进入Failover类型设备组的配置模式；
- 若设备组为“仅同步”类型，在全局配置模式下，使用**cluster device-group *name***命令即可进入仅同步类型设备组的配置模式。

配置同步范围

当设备组类型为“仅同步”时，需配置组内设备间同步的信息类型。在仅同步类型设备组的配置模式下，使用以下命令配置同步范围：

```
sync-scope {system | slb | gslb}
```


- **system** - 指定将设备的系统配置信息同步至与组内其他设备。
- **slb** - 指定将设备的服务器负载均衡配置信息同步至组内其他设备。
- **gslb** - 指定将设备的全局负载均衡配置信息同步至组内其他设备。

在仅同步类型设备组配置模式下，使用**no sync-scope**命令取消同步范围的配置。

添加设备

用户可将集群设备列表中的设备添加至设备组。一个设备组最多允许添加32台设备，且每台设备只能添加到一个组里。在设备组配置模式下，使用以下命令添加设备至设备组：

device *name*

- *name* - 指定需要加入设备组的设备名称。系统最多支持32台AX设备加入同一设备组。

在设备组配置模式下，使用**no device** *name*命令将指定设备移出设备组。

配置心跳时间间隔

心跳时间间隔是指设备发送心跳报文给设备组内其他设备的时间间隔。在设备组配置模式下，使用以下命令指定心跳时间间隔：

heartbeat-interval *time*

- *time* - 指定发送心跳的时间间隔。取值范围是55到10000毫秒，默认值是200毫秒。

在设备组配置模式下，使用**no heartbeat-interval**命令恢复默认值。

配置心跳阈值

心跳阈值是指设备发送心跳报文个数给设备组内其他设备的阈值。若设备向组内其他设备发送的心跳报文个数达到设定值，仍未收到对端设备的响应，则认为对端设备离线。在设备组配置模式下，使用以下命令指定心跳阈值：

heartbeat-threshold *value*

- *value* - 指定发送心跳报文的阈值。取值范围是3到255，默认值是15。

在设备组配置模式下，使用**no heartbeat-threshold**命令恢复默认值。

配置流量组

流量组创建完成后，本地设备所在设备组内的所有设备，都可能成为流量组的生效设备。当符合流量组条件的客户端请求到达时，生效设备发出ARP报文或NA（邻居通告）报文，将该请求引流至自身系统，并对其进行处理。不同型号的AX设备支持的流量组个数不同。

集群流量组的配置需要在流量组配置模式下进行。进入流量组配置模式，在全局配置模式下，使用以下命令：

```
cluster traffic-group name
```

- *name* - 指定流量组的名称，取值范围是1到95个字符。

在全局配置模式下，使用**no cluster device-group** *name*命令删除指定的流量组。

配置故障转移顺序

指定Failover类型设备组内设备进行高可用切换时，设备切换的顺序。当符合流量组条件的客户端请求到达时，根据指定的故障转移顺序，系统将该请求分配给相应设备。添加Failover类型设备组内设备至流量组的故障转移顺序列表，同时配置故障转移顺序，在流量组配置模式下，使用以下命令：

```
failover-order device-name {before device-name | after device-name | top}
```

- *device-name* - 指定加入流量组故障转移顺序列表的设备。
- **before** *device-name* - 指定设备的位置为某个设备之前。
- **after** *device-name* - 指定设备的位置为某个设备之后。
- **top** - 指定设备的位置为所有设备之前。

用户可以修改流量组故障转移顺序列表中设备的切换顺序。在流量组配置模式下，使用以下命令修改故障转移顺序：

```
move device-name {before device-name | after device-name | top | bottom}
```

- *device-name* - 指定需调整顺序的设备名称。
- **before** *device-name* - 指定设备的位置为某个设备之前。
- **after** *device-name* - 指定设备的位置为某个设备之后。

- **top** - 指定设备的位置为所有设备的首位。
- **bottom** - 指定设备的位置为所有设备的末尾。



注意: 若流量组未指定设备的故障转移顺序, 当流量组内的客户端请求到达时, 系统根据本地设备所在设备组内各设备当前的处理能力, 将请求分配给处理能力最大的设备。

配置负载系数

指定流量组的负载系数。当符合流量组条件的客户端请求被分配给设备组内某台设备时, 该设备的负载权重将根据此设定值相应增加, 系统将会根据设备的负载情况分配新的客户端请求。在流量组配置模式下, 使用以下命令指定流量组的负载系数:

load-factor *value*

- *value* - 指定流量组的负载系数。取值范围是1到100, 默认值是1。
例如: Failover类型的设备组DG中包含以下设备: 设备AX1、AX2和AX3。配置流量组TG1: 故障转移顺序为AX1>AX3, 负载系数为10; 配置流量组TG2: 故障转移顺序为AX2>AX3, 负载系数为20。当前, 流量组TG1在设备AX1上生效, 流量组TG2在设备AX2上生效。此时, 创建流量组TG3, 且不指定故障转移顺序, 当符合流量组TG3条件的客户端请求到达时, 系统根据负载系数计算当前设备组DG内各设备的负载权重: AX1为10, AX2为20, AX3为0。因此, 系统会将客户端请求分配给设备AX3。

在流量组配置模式下, 使用**no load-factor**命令恢复流量组负载系数的默认值。

指定监测对象

利用监测对象判定流量组的状态, 当监测对象失效时, 系统判定该流量组失效。在流量组配置模式下, 使用以下命令指定流量组的监测对象:

monitor *track-object-name*

- *track-object-name* - 指定监测对象的名称。

在流量组配置模式下, 使用**no monitor**命令取消监测对象的配置。

启用抢占功能

启用流量组的抢占功能后，当流量组故障转移顺序中的第一台设备恢复正常工作时，将从其他设备接回原来的工作。在流量组配置模式下，使用以下命令开启流量组的抢占功能：

auto-failback-to-first-device enable

在流量组配置模式下，使用**no auto-failback-to-first-device enable**命令关闭流量组的抢占功能。

配置抢占时间

指定设备进行抢占的时间，即流量组故障转移顺序中的第一台设备恢复正常工作后，经过设定值，从其他设备接回原来的工作。在流量组配置模式下，使用以下命令指定抢占时间：

auto-failback-time *value*

- *value* - 指定流量组的抢占时间。取值范围是30到300秒，默认值是60秒。

在流量组配置模式下，使用**no auto-failback-time**命令恢复流量组抢占时间的默认值。

启用数据对象同步

开启后，当流量组生效设备处理客户端流量产生了数据信息，系统通过主镜像IP将数据信息镜像给集群内下一台接替其工作的设备，包括会话信息和四层会话保持表信息。在流量组配置模式下，使用以下命令启用数据对象同步功能：

mirror rdo

在流量组配置模式下，使用**no mirror rdo**命令关闭数据对象同步功能。

配置虚拟MAC

指定流量组对应接口的虚拟MAC地址，在流量组配置模式下，使用以下命令：

virtual-mac interface *interface* {**auto** | *H.H.H*}

- **interface interface** - 指定接口，并配置虚拟MAC地址，供流量组生效时使用。
- **auto** - 指定流量组接口的虚拟MAC地址类型为“自动”，系统将自动为相应接口生成虚拟MAC地址。
- **HH.HH** - 指定流量组接口的虚拟MAC地址。

在流量组配置模式下，使用**no virtual-mac interface interface**命令取消流量组接口的虚拟MAC配置。

配置虚拟MAC前缀

当指定流量组对应接口的虚拟MAC地址类型为“自动”时，系统支持为该类型地址指定虚拟MAC前缀。指定虚拟MAC前缀，在全局配置模式下，使用以下命令：

cluster virtual-mac-prefix prefix

- **prefix** - 指定集群流量组接口的虚拟MAC前缀，格式为十六进制，且只能输入六位。

在全局配置模式下，使用**no cluster virtual-mac-prefix**命令取消虚拟MAC前缀的配置。

配置非对称流量转发

在由两台集群设备组成的非对称路由环境（即进出流量可能经过不同路径）中，客户端的请求报文经过生效设备到达服务器后，响应报文可能会被发送到备设备。用户可以在流量组上启用非对称流量转发功能。生效设备处理请求报文时会将与该报文相关的信息同步到备设备，备设备接收到响应报文后，会将响应报文重新封装后转发给生效设备，从而确保业务流量的请求和响应报文在同一设备上处理。

启用非对称流量转发功能

默认情况下，非对称流量转发功能为禁用状态。启用或禁用该功能，在流量组配置模式下，使用以下命令：

asymmetric-traffic-forward {enable | disable}

- **enable** - 启用非对称流量转发功能。
- **disable** - 禁用非对称流量转发功能。



注意：由于启用非对称流量转发功能后设备间的流量会增大，需要保证设备[镜像接口](#)的带宽足够。

查看集群配置

在全局配置模式下，使用以下命令查看设备集群的配置信息：

- **show cluster device** - 查看集群设备列表。
- **show cluster device *device-name*** - 查看集群设备列表中指定的设备信息。
- **show cluster device-group** - 查看集群设备组列表。
- **show cluster device-group *device-group-name*** - 查看集群设备组列表中指定的设备组信息。
- **show cluster traffic-group** - 查看集群流量组列表。
- **show cluster traffic-group *traffic-group-name*** - 查看集群流量组列表中指定的流量组信息。
- **show cluster virtual-mac-prefix** - 查看集群流量组接口的虚拟MAC前缀。

第5章 网络连接

网络相关功能配置包括如下：

- [安全域](#)
- [接口](#)
- [LLDP](#)
- [DNS](#)
- [DHCP](#)
- [DDNS](#)
- [PPPoE](#)
- [虚拟交换机](#)
- [NAT](#)
- [IP包数据处理选项](#)
- [应用层网关（ALG）](#)

安全域

在系统中，域是一个逻辑的实体，一个或多个接口可以绑定到域。被应用了策略规则的域即为安全域，为实现某个特定功能而存在的域即为功能域。域具有以下特点：

- 接口绑定到域，二层域绑定到VSwitch，三层域绑定到VRouter。因此，二层域所在的VSwitch决定了该域中接口的VSwitch，三层域所在的VRouter决定了该域中接口的VRouter。
- 二层和三层域决定其接口工作在二层模式或是三层模式。

系统中为用户预定义了7个安全域，分别是：trust、untrust、L2-trust、L2-untrust、mgt、ha（HA功能域）以及proxy（七层SLB功能域）。用户也可以自定义域。Proxy安全域主要应用于七层场景下。当ADC设备启动后，系统将默认创建proxy安全域，并绑定到trust-vr。Proxy安全域仅可以配置为策略的目的安全域，且无法编辑或删除。

配置安全域

用户可以对域进行以下操作：

- 显示域信息
- 创建安全域
- 指定描述信息
- 绑定二层域到VSwitch
- 绑定三层域到VRouter
- 配置安全域WAN属性

显示域信息

用户可以在任何模式下通过使用show命令随时查看系统中的域信息。具体命令如下：

```
show zone [ zone-name ]
```

- *zone-name* - 指定域的名称显示指定域的信息。

创建安全域

用户创建安全域时,如果不指定二层域参数,则默认为三层域。创建的域如果不用参数指明为二层域,则默认为三层域。

创建一个域并且进入域配置模式,在全局配置模式下,使用以下命令：

```
zone zone-name [l2]
```

- *zone-name*- 创建域的名称。
- **l2**- 指定所创建域为二层域。

如果所指定的域的名称存在,则直接进入域配置模式。

在全局配置模式下,使用**no zone *zone-name* [**L2**]**命令删除指定域。



注意: 预定义域不可以被删除。

指定描述信息

为所配置的域指定描述信息，请在域配置模式下，使用以下命令：

description *description*

- *description* – 安全域的描述信息。

使用**no description**命令删除安全域的描述信息。

绑定二层域到VSwitch

用户通过把二层域绑定到VSwitch来实现接口与VSwitch的绑定。默认情况下，每一个二层域都被绑定到VSwitch1中。改变二层域的VSwitch，在域配置模式下，使用以下命令：

bind *vswitch-name*

- *vswitch-name* - 指定将二层域绑定到的VSwitch的名称。

恢复域到VSwitch1的绑定，在域配置模式下，使用**no bind**命令。



注意: 改变域所属的VSwitch时，必须保证域中没有绑定的接口。

绑定三层域到VRouter

用户通过把三层域绑定到VRouter来实现接口与VRouter的绑定。默认情况下，所有的三层域都绑定到trust-vr中。改变三层域的VRouter，在域配置模式下，使用以下命令：

vrouter *vrouter-name*

- *vrouter-name* – 指定将三层域绑定到的VRouter的名称。

恢复域到trust-vr的绑定，在域配置模式下，使用**no vrouter**命令。



注意: 改变域所属的VRouter时，必须保证域中没有绑定的接口。

配置安全域WAN属性

为了统计设备的上下行WAN流量，系统支持为安全域配置WAN属性，将所选安全域指定为WAN安全域，那么绑定在该安全域的接口即为WAN接口。在域配置模式下，使用以下命令：

```
type wan
```

在域配置模式下，使用`no type`删除WAN属性。

接口

接口允许流量进出安全域。因此，为使流量能够流入和流出某个安全域，必须将接口绑定到该安全域，并且，如果是三层安全域，还需要为接口配置IP地址。然后，必须配置相应的策略规则，允许流量在不同安全域中的接口之间传输。多个接口可以被绑定到一个安全域，但是一个接口不能被绑定到多个安全域。

设备具有多种类型接口，根据性质的不同，分为物理接口和逻辑接口。

- 物理接口：设备上的每一个以太网接口都表示一个物理接口。物理接口的名称是预先定义的，由媒体类型、插槽号和位置参数组成，例如ethernet2/1或ethernet0/2。
- 逻辑接口：系统中的逻辑接口包括子接口、回环接口、集聚接口、冗余接口、PPPoE接口。

根据接口所处安全域的不同，接口还可以分为二层接口和三层接口。

- 二层接口：属于二层域的接口均为二层接口。
- 三层接口：属于三层域的接口为三层接口。只有三层接口可以在NAT/路由模式下工作。

不同类型的接口在设备中具有不同的功能。下表列出各种逻辑接口的描述：

逻辑接口类型	说明
子接口	子接口的名称是它来源的接口名字的扩展，例如ethernet0/2.1。系统支持以下类型子接口：以太网子接口、集聚子接口和冗余子接口。接口和它的子接口可以被绑定到同一个安全域中，也可以被绑定到不同的安全域中。
回环接口	回环接口是逻辑接口，并且只要回环接口所在的设备处于工作状态，回环接口就一直处于工作状态。因此，回环接口具有稳定的特性。
隧道接口	隧道接口充当VPN通道的入口。流量通过隧道接口进出VPN通道。隧

逻辑接口类型	说明
	道接口只能是三层接口。
集聚接口	集聚接口是物理接口的集合，一个集聚可以包含1到16个物理接口。这些物理接口平均分担流到该集聚接口IP地址的流量负载。因此集聚接口可以提高单个IP地址的可用带宽。如果集聚接口中的一个物理接口出现故障，不能工作，其它接口可以继续处理流量，只是可使用的带宽变小了。
冗余接口	冗余接口能够实现两个物理接口的备份。一个物理接口为主接口处理流向该冗余接口的流量。另外一个接口作为备用接口在主接口发生故障时继续处理流量。
PPPoE接口	使用PPPoE协议连接PPPoE服务器的逻辑接口，基于以太网口创建。

查看接口信息

通过CLI查看所有接口信息，请使用**show interface**命令。接口表中显示每个接口的下列信息：

项目	描述
Interface name	显示接口的名称。
IP address/mask	显示接口的IP地址。
Zone name	显示接口的绑定域的名称。
H (Physical state)	显示接口的物理状态是否为可用（UP/DOWN）。
A (Admin state)	显示接口的管理状态是否为可用（UP/DOWN）。
L (Link state)	显示接口的链路状态是否为可用（UP/DOWN）。
P (Protocol state)	显示接口的协议状态是否为可用（UP/DOWN）。
MAC address	显示接口的MAC地址。
Description	显示接口的描述信息。

H、A、L和P是接口的四种状态。状态的值为可用（UP）或不可用（DOWN）。

- H (Physical state)：接口的物理状态。如果接口的物理连接是完好的，该接口PHY值就是UP，反之则为DOWN。
- A (Admin state)：接口的管理状态。用户可以通过no shutdown和shutdown命令来打开和关闭接口。如果接口被打开，该接口的A值就是UP，反之则为DOWN。
- L (Link state)：接口的链路状态。链路状态的值由H和A的值来决定。只有H和A均为UP时，L的值才为UP。
- P (Protocol state)：接口的协议状态。只有当接口的链路状态为UP并且IP地址已经被分配到该接口，P的值才会为UP。

查看某个指定接口的信息，请在**show interface**命令后添加要查看接口名称，即**show interface interface-name**。

配置接口

对接口的配置与操作，必须在接口模式下输入相应的命令来完成。接口模式有以下4种：

- 路由模式：该模式的接口是三层接口，绑定到三层域。
- VSwitch模式：该模式的接口是二层接口，绑定到二层域。
- 集聚模式：该模式的接口是集聚接口的成员，不能绑定到任何域。
- 冗余模式：该模式的接口是冗余接口的成员，不能绑定到任何域。
- 隧道模式：该模式的接口是三层接口，绑定到三层域。

接口的基本配置操作，具体内容有：

- 绑定接口到域
- 配置接口描述信息
- 配置接口IP地址
- 配置接口所属ISP
- 配置接口的链路负载均衡优先级
- 配置接口的链路负载均衡权值
- 配置接口带宽

- 配置接口最大传输单元（MTU）
- 强制关闭接口
- 设置接口ARP超时时间
- 配置接口功能管理
- 关闭记录接口IP地址冲突日志功能（DAD模式ARP报文触发）
- 配置接口代理ARP功能
- 配置基于策略的接口镜像过滤功能
- 配置接口逆向路由功能
- 配置接口备份功能
- 配置接口保持时间
- 配置接口保活功能
- 配置接口联动功能
- 配置接口Local属性
- 配置接口WAN属性
- 回环接口
- 以太网接口
- VSwitch接口
- 集聚接口
- 冗余接口
- PPPoE子接口
- 链路聚合

绑定接口到域

用户可以将任何物理接口绑定到已定义的二层或三层域。将接口绑定到域，在接口配置模式下输入以下命令：

```
zone zone-name
```

在接口配置模式下使用**no zone**命令取消接口与域的绑定。在取消三层接口与域的绑定前，必须将三层接口配置的IP地址取消。



注意：将接口绑定到域时，

- 如果想让接口在二层工作，就必须把该接口绑定到二层域。
- 把接口从三层接口转换成二层接口前，必须将三层接口配置的IP地址取消。

配置接口描述信息

用户可以为所配置的接口指定描述信息，请在接口配置模式下，使用以下命令：

```
description description
```

- *description* – 指定的描述信息。

使用**no description**命令删除指定接口的描述信息。

配置接口IP地址

设备上所有接口配置的IP地址都必须在不同网段。用户可以为接口配置静态IP地址，也可以让接口通过DHCP或者PPPoE协议动态获得IP地址。配置接口的IP地址，在接口配置模式下，输入以下命令：

```
ip address {ip-address/mask | dhcp [setroute] | pppoe [setroute]}
```

- *ip-address/mask* – 为接口指定静态IP地址。
- **dhcp** [**setroute**] – 指定接口通过DHCP协议获得IP地址。如果配置**setroute**参数，系统会将DHCP服务器提供的网关信息设置为默认网关路由。

- **pppoe [setroute]** - 指定接口通过PPPoE协议获得IP地址。如果配置setroute参数，系统会将PPPoE服务器提供的网关信息设置为默认网关路由。

例如把IP地址1.1.1.1分配给以太网接口ethernet1/0，请输入以下命令：

```
进入接口ethernet1/0配置模式：

hostname(config)# interface ethernet1/0

配置接口ethernet1/0的主IP地址：

hostname (config-if-eth1/0)# ip address 1.1.1.1/24

退出接口配置模式：

hostname(config-if)# exit
```

在为接口指定IP地址时，请注意以下两点：

- 系统支持两种子网掩码书写方法，所以1.1.1.1/24也可写成1.1.1.1 255.255.255.0。
- 只有已经绑定到域的接口才可以配置IP地址。

在接口配置模式下，使用**no ip address [ip-address/mask | dhcp | pppoe]**命令取消接口的IP地址配置。

配置接口IP地址的Local属性

用户可以开启接口IP地址的Local属性。开启后，当设备加入HA组网或者集群时，该接口的IP配置不会同步到HA对端或者集群内其他设备。开启接口IP地址的Local属性，在接口配置模式下使用以下命令：

```
ip address ip-address/mask local
```

- **local** - 指定接口IP地址为Local IP。

在接口配置模式下，使用**no ip address ip-address/mask local**命令取消接口IP地址的Local属性。

配置接口IP地址所属流量组

用户可以将接口的静态IP地址或二级IP地址与集群流量组进行绑定。当符合流量组条件的流量到达接口时，相应的接口IP在流量组当前生效设备上工作。为接口IP地址绑定集群流量组，在接口配置模式下使用以下命令：

```
ip address ip-address/mask [secondary] [traffic-group traffic-group-name]
```

- **secondary** - 为接口二级IP地址指定集群流量组。
- **traffic-group** *traffic-group-name* - 为接口IP地址/二级IP地址指定集群流量组。

在接口配置模式下，使用**no ip address** *ip-address/mask* [**secondary**] 命令取消接口IP地址及其绑定的流量组配置。取消接口的主IP地址之前，必须先取消接口的二级IP地址。

配置接口浮动IP

为接口指定浮动IP，并指定集群流量组。接口的浮动IP用于响应ARP报文，并对指定流量组的流量进行引流。为接口指定浮动IP地址，请在接口配置模式下输入以下命令：

floating-ip *ipv4-address* [**traffic-group** *traffic-group-name*]

- *ipv4-address* - 指定接口的浮动IPv4地址。
- *traffic-group-name* - 指定该浮动IP所属流量组。

floating-ipv6 *ipv6-address* [**traffic-group** *traffic-group-name*]

- *ipv6-address* - 指定接口的浮动IPv6地址。
- *traffic-group-name* - 指定该浮动IP所属流量组。

在接口配置模式下，使用**no {floating-ip | floating-ipv6}** *ip-address* 命令取消接口浮动IP地址的配置。

配置接口二级IP地址

用户可以为已经配置了静态IP地址的接口配置最多十个二级IP地址。为接口指定二级IP地址，请在接口配置模式下输入以下命令：

ip address *ip-address/mask* **secondary**

- *ip-address/mask* - 指定接口的二级IP地址。

在接口配置模式下，使用**no ip address** *ip-address/mask* **secondary**命令取消接口的二级IP地址配置。取消接口的主IP地址之前，必须先取消接口的二级IP地址。

配置接口二级管理IP地址

接口的二级IP与集群流量组绑定后，需配置与该二级IP同网段的二级管理IP，即不会同步至设备组内其它设备的接口IP。当系统处理上述流量组的业务时，可以通过该二级管理IP进行健康检查；或者，通过该二级管理IP发送探测报文，判断监测对象是否可达。为接口指定二级管理IP地址，请在接口配置模式下输入以下命令：

manage ip ip-address secondary

- *ip-address* - 指定接口的二级管理IP地址。

在接口配置模式下，使用**no manage ip ip-address secondary**命令取消接口二级管理IP地址的配置。

配置接口所属ISP

配置接口所属的IPv4 ISP或IPv6 ISP，接口对应的链路也将与指定的ISP绑定。在接口配置模式下，使用以下命令配置接口所属ISP：

{isp | isp-v6} isp-name

- **isp isp-name**- 指定创建好的IPv4 ISP信息，与接口进行绑定。
- **isp-v6 isp-name**- 指定创建好的IPv6 ISP信息，与接口进行绑定。

在接口配置模式下，使用**no {isp | isp-v6}**命令取消接口与ISP的绑定。

配置接口的链路负载均衡优先级

指定接口的链路负载均衡优先级。当系统对流量进行出站负载均衡，并且采用优先级调度策略时，该值决定了接口对应链路的优先级。配置接口的链路负载均衡优先级，在接口配置模式下，使用以下命令：

llb priority value

- *value* - 指定接口的链路负载均衡优先级。取值范围是1到100，默认值是50。数值越小，表示该出口链路的优先级越高。

在接口配置模式下，使用**no llb priority**命令恢复接口链路负载均衡优先级的默认值。

配置接口的链路负载均衡权值

指定接口的链路负载均衡权值。当系统对流量进行出站负载均衡，不同的负载均衡算法根据该权值采用不同的方式进行计算和选路。配置接口的链路负载均衡权值，在接口配置模式下，使用以下命令：

llb weight value

- *value* - 指定接口的链路负载均衡权值。取值范围是1到255，默认值是50。

在接口配置模式下，使用**no llb weight**命令恢复接口链路负载均衡权值的默认值。

配置接口带宽

根据需要配置接口的实际带宽值和带宽阈值。当配置链路负载均衡功能时，将根据接口配置的带宽阈值进行智能选路。在接口配置模式下，使用以下命令：

```
bandwidth {downstream | upstream} {threshold value| bandwidth}
```

- **downstream** - 配置接口下行方向上的最大带宽值与带宽阈值。
- **upstream** - 配置接口上行方向上的最大带宽值与带宽阈值。
- **threshold** *value* - 指定接口的带宽阈值。取值范围是0到100（0%到100%），默认值是0，表示不限制。
- *bandwidth* - 指定接口的最大带宽值。范围是512,000 到1000,000,000,000bps。默认值是1000,000,000bps。

在接口配置模式下，使用**no bandwidth {downstream | upstream} [threshold]**命令恢复接口的最大带宽和带宽阈值的默认值。

配置接口最大传输单元（MTU）

默认情况下，接口的最大传输单元值为1500字节。用户可以根据自己的需要改变最大传输单元的值。配置接口的最大传输单元，请在接口配置模式下输入以下命令：

```
ip mtu value
```

在接口配置模式下，使用**no ip mtu**命令恢复接口的默认MTU值。

强制关闭接口

设备支持接口的强制关闭功能。用户不仅可以根据需要用命令强制关闭特定接口，还可以通过时间表控制接口的关闭时间，或者根据监测接口的链路状态控制接口的关闭。在CLI中强制关闭接口，请在接口配置模式下输入以下命令：

```
shutdown [track track-object] [schedule schedule-name]
```

- **shutdown** - 立即关闭接口。
- **track** *track-object* - 指定监测对象名称。如果指定该参数，接口会在监测对象失败时处于关闭状态。关于如何配置监测对象，请参阅“[配置监测对象](#)”部分。

- **schedule** *schedule-name* – 指定时间表名称。如果指定该参数，接口会在时间表指定的时间范围内处于关闭状态。关于如何配置时间表，请参阅“[配置时间表](#)”部分。

在接口配置模式下，使用**no shutdown**命令，取消强制关闭接口功能并清除此功能的所有相关配置。

设置接口ARP超时时间

默认情况下，接口的ARP超时时间是1200秒（s）。用户可以根据需要改变该值。该值的范围在5到65535秒之间。

改变ARP超时时间，请在接口配置模式下使用以下命令：

arp timeout *value*

在接口配置模式下，使用**no arp timeout**命令恢复接口的默认ARP超时时间。

配置接口管理功能

接口的以下功能需要通过命令开启后才可以使用，包括SSH、Telnet、Ping、SNMP、HTTP、HTTPS和FTP。开启这些功能后，用户可以使用接口上的IP地址通过相应的功能管理和配置设备。开启以上所述功能，在接口配置模式下，使用以下命令：

manage {**ssh** | **telnet** | **ping** | **snmp** | **http** | **https** | **ftp**}

- **ssh** - 开启接口的SSH功能。
- **telnet** - 开启接口的Telnet功能。
- **ping** - 开启接口的Ping功能。
- **snmp** - 开启接口的SNMP功能。
- **http** - 开启接口的HTTP功能。
- **https** - 开启接口的HTTPS功能。
- **ftp** - 开启接口的FTP服务功能。

使用**manage** {**ssh** | **telnet** | **ping** | **snmp** | **http** | **https** | **ftp**}命令关闭相应的功能。

配置FTP服务功能

用户可以通过接口的FTP服务功能获取设备的日志和配置等信息。开启接口的FTP服务功能后，用户可以创建FTP用户和修改FTP端口号。

创建FTP用户，在全局配置模式下，使用以下命令：

```
ftp user user-name password password
```

- **user** *user-name* – 指定FTP用户名。
- **password** *password* – 指定FTP用户密码。

系统允许最多配置3个FTP用户。在全局配置模式下，使用**no ftp user** *user-name*命令取消FTP用户配置。

修改FTP端口号，在全局配置模式下，使用以下命令：

```
ftp port number
```

- **number** – 指定FTP端口号，取值范围为1-65535，缺省值21。

在全局配置模式下，使用**no ftp port**命令恢复缺省配置。

用户可以在任何模式下通过使用show命令查看系统中的FTP服务配置信息。具体命令如下：

```
show ftp {port | user}
```

- **port** – 查看FTP端口号。
- **user** – 查看FTP用户名、密码和在线状态。

关闭记录接口IP地址冲突日志功能（DAD模式ARP报文触发）

DAD模式ARP报文，即地址重复检测（Duplicate Address Detection）模式ARP报文，该报文是一种特殊类型的免费ARP报文，其源IP为0.0.0.0、目的IP为具体的报文检测IP地址，主要用于检测地址冲突。

默认情况下，当设备接口收到ARP报文时，系统将会判断该ARP报文是否为DAD模式ARP报文，如果该ARP报文是DAD模式ARP报文，且ARP报文目的IP地址与接口IP地址或NAT地址池中地址冲突，那么系统将记录接口IP地址冲突日志。用户如果希望提高设备性能，减少设备内存占用率及误报，可以关闭记录DAD模式ARP报文触发的接口IP地址冲突日志功能。

关闭记录接口地址冲突日志功能，在接口配置模式下，使用以下命令：

```
no dad-alarm
```

重新开启记录接口地址冲突日志功能，在接口配置模式下，使用以下命令：

```
dad-alarm
```

配置接口代理ARP功能

代理ARP功能是指设备接口在收到以不同网段IP地址为目的IP的ARP请求报文时，以自己的MAC地址作为源地地址回应ARP请求。

代理ARP功能仅适用于三层接口。在接口配置模式下，使用以下命令配置接口的代理ARP功能：

```
proxy-arp [dns]
```

- **proxy-arp** - 开启接口的代理ARP功能。
- **dns** - 当需要实现IP即插即用功能时，使用该参数。

在接口配置模式下，使用**no proxy-arp**命令取消接口的代理ARP配置。

配置了代理ARP功能（使用DNS参数）和DNS代理的接口可以实现IP即插即用，即配有任意IP地址和DNS地址的内网PC客户端都可以通过接口访问外网。使用IP即插即用功能需要注意以下两点：

- 配置了接口的IP即插即用功能后，如果PC的IP地址和接口的IP地址在同一网段，为保证PC能够正常访问Internet，请保证PC的网关必须为接口的IP地址。例如，接口IP地址为192.168.1.1/24，PC的IP地址为192.168.1.55/24，这时为了使PC能够通过接口正常访问Internet，PC的网关地址必须为192.168.1.1。
- 当设备的接口为即插即用专用接口时，建议配置接口IP地址为32位掩码长度的罕见IP地址，例如10.199.199.199/32。这样能保证不会有与接口相同网段IP地址的存在，可以实现真正意义上的即插即用。

配置基于策略的接口镜像过滤功能

通过在设备上配置mirror Profile，然后指定策略规则引用配置好的mirror Profile。从而实现基于策略的流量镜像过滤功能，将匹配策略条件的流量镜像到用户指定的目的接口或者目的IP地址。通常情况下，配置基于策略的流量镜像过滤功能，需要以下两个步骤：

1. 配置mirror Profile。

mirror Profile定义了流量镜像目的接口或者目的IP地址。

2. 指定策略规则引用mirror Profile。

配置mirror Profile

mirror Profile定义了流量镜像目的接口或者目的IP地址。

mirror Profile的配置需要在mirror Profile配置模式下进行。进入mirror Profile配置模式，在全局配置模式下，输入以下命令：

mirror-profile *mirror-profile-name*

- *mirror-profile-name* - 指定所创建的mirror Profile的名称。执行该命令后，系统将创建指定名称的mirror Profile，并进入mirror Profile配置模式；如果指定的名称已存在，则直接进入mirror Profile配置模式。一个mirror Profile允许最多4条同类型的规则。

在全局配置模式下使用该命令的no形式删除指定的mirror Profile：

no mirror-profile *mirror-profile-name*

在mirror Profile配置模式下，用户可以为匹配策略的流量指定镜像操作，当匹配流量到接口时，需要指定镜像流量的目的接口及镜像流量的方向，当匹配流量到目的IP地址时，需要指定镜像流量的目的IP地址、出接口、下一条地址以及镜像流量的方向。

指定流量镜像目的接口

系统可以将匹配策略的流量镜像到指定的目的接口进行分析。用户可以根据匹配策略的流量方向指定镜像流量的方向（上行、下行、双向），系统将根据镜像流量方向实现基于策略的镜像过滤功能。默认情况下，镜像流量方向为双向。指定流量镜像的目的接口及镜像流量的方向，在mirror Profile配置模式下，使用以下命令：

destination interface *interface-name* [**direction** {**forward** | **backward** | **bidirection**}]

- *interface-name* - 指定镜像流量的目的接口名称。
- **direction** {**forward** | **backward** | **bidirection**} - 使用**forward**参数指定镜像流量的方向为上行，即与匹配策略规则的流量方向相同。使用**backward**参数指定镜像流量的方向为下行，即与匹配策略规则的流量方向相反。使用**bidirection**参数指定镜像流量的方向为双向，即将匹配策略规则的流量双向进行镜像。

在mirror Profile配置模式下使用该命令的no形式删除指定的镜像目的接口：

no destination interface *interface-name*

指定流量镜像目的地址

系统可以将匹配策略的流量镜像到指定的目的IP地址进行分析。用户可以根据匹配策略的流量方向指定镜像流量的方向（上行、下行），系统将根据镜像流量方向实现基于策略的镜像过滤功能。默认情况下，镜像流量方向为双向。指定流量镜像的目的IP 地址及镜像流量的方向，在mirror Profile配置模式下，使用以下命令：

```
destination ip ip-address-1 interface-name [ip-address-2] [direction {forward | backward}]
```

- *ip-address-1* - 指定镜像流量的目的IP地址。设备将对数据包的目的地址进行替换。
- *interface-name* - 指定镜像流量的出接口。
- *ip-address-2* - 指定镜像流量的下一跳地址。
- **direction** {**forward** | **backward**} - 使用**forward**参数指定镜像流量的方向为上行，即与匹配策略规则的流量方向相同。使用**backward**参数指定镜像流量的方向为下行，即与匹配策略规则的流量方向相反。

在mirror Profile配置模式下使用该命令的no形式删除指定的镜像目的地址：

```
no destination ip ip-address
```

指定策略规则引用mirror Profile

接口镜像过滤mirror Profile配置完成后，只有把它引用到策略规则中，流量镜像过滤功能才能生效。指定策略规则引用mirror Profile，在策略配置模式下，使用以下命令：

```
mirror profile-name
```

- *profile-name* - 指定被策略规则引用的mirror Profile名称。

在策略配置模式下使用该命令的no形式取消mirror Profile被策略规则的引用：

```
no mirror profile-name
```

显示mirror Profile信息

用户可以在任何模式下随时使用show命令查看mirror Profile的配置信息。

```
show mirror-profile [mirror-profile-name]
```

- *mirror-profile-name* - 显示指定名称的mirror Profile的信息。如果不指定该参数，则显示系统中所有mirror Profile的信息。

配置接口逆向路由功能

逆向路由功能是指用于转发反向数据的路由。反向是相对于初始化数据流方向。逆向路由功能仅适用于三层接口。默认情况下，三层接口关闭逆向路由。

在接口配置模式下，使用以下命令完成逆向路由功能的配置：

reverse-route [**force** | **prefer** | **direct-forward** [**per-packet**]]

- **force** – 强制逆向路由。如果能找到逆向路由则使用逆向路由转发反向数据；如果找不到逆向路由则丢弃数据包。
- **prefer** – 优先逆向路由。如果能找到逆向路由则使用逆向路由转发反向数据；如果找不到逆向路由则按原路径返回（即从当前接口转发出去）。
- **direct-forward** - 禁用逆向路由功能。所有反向数据原路返回，不进行逆向路由检查。默认情况下，该功能为关闭状态。
 - **per-packet** - 逐包检查功能。在禁用逆向路由功能且指定该参数时，即开启逐包检查功能，系统逐包检查会话的MAC信息。若会话的MAC信息与正向数据的源MAC信息不一致，系统将按照正向数据的源MAC信息更新会话的MAC信息。

在接口配置模式下，使用**no reverse-route**命令取消逆向路由的使用。不使用逆向路由时，所有反向数据原路返回，不进行逆向路由检查。

显示逆向路由功能的配置状态，在接口配置模式下，使用以下命令：

show reverse-route



注意: 如果找到的逆向路由出接口和原入接口不在同一个安全域，设备仍会丢弃数据包。

配置接口备份功能

设备支持接口备份功能。结合设备的时间表和监测对象功能，当为接口指定备份接口后，设备将在时间表指定时间内或者监测对象失败时将主接口的流量转移到备份接口，当时间表指定时间段结束或者监测对象恢复正常时，流量又会从备份接口转移回到主接口。

配置接口备份功能，在接口配置模式下，使用以下命令：

backup-interface *interface-name* {**schedule** *schedule-name* [**overlap-time** *time*] | **track** *track-object-name* [**schedule** *schedule-name* [**overlap-time** *time*]]}

- *interface-name* - 指定备份接口的名称。
- *schedule-name* - 指定时间表的名称。接口将在时间表指定时间内将流量转移到备份接口。
- *time* - 指定主接口切换到备份接口之前将流量转移到备份接口的过渡时间，单位为分钟。取值范围为1到60。主接口会在切换到备份接口前的一段时间，即此处指定的过渡时间，将流量从主接口平滑转移到备份接口。默认情况下无平滑过渡时间，所有的流量会立刻从主接口转移到备份接口。
- *track-object-name* - 指定监测对象的名称。当监测对象失败时，流量将从主接口转移到备份接口；当监测对象恢复正常后，流量将从备份接口转移回主接口。

在接口配置模式下使用该命令**no**的形式取消备份接口的配置：

no backup-interface

配置接口保持时间

物理接口有两种物理层连接状态：**up** 和 **down**。在保持时间内，接口物理层状态之间的切换，不会被系统感知；而是等待保持时间后，如果物理层状态仍然没有恢复，再向系统报告物理连接状态的变化。该功能能够避免因接口物理状态在短时间内频繁改变，从而导致网络不稳定的问题。

配置接口保持时间，在接口配置模式下（仅适用于物理接口），使用下列命令：

- **holddown time** - 指定接口保持down状态的时间。配置该命令后，如果处于down状态的接口突然up，X秒（X通过time参数指定）后，如果接口仍为up状态，系统才认为接口已经up。取值范围为1到3600，单位为500毫秒。比如，若配置**holddown 10**，则相应接口的保持down时间为5秒。
- **holdup time** - 指定接口保持up状态的时间。配置该命令后，如果处于up状态的接口突然down，X秒（X通过time参数指定）后，如果接口仍为down状态，系统才认为接口已经down。取值范围为1到3600，单位为500毫秒。比如，若配置**holdup 10**，则相应接口的保持up时间为5秒。

在接口配置模式下使用**no holddown**或者**no holdup**命令取消接口保持时间的配置。

配置接口保活功能

接口通过PPPoE协议获得IP地址后，如果长时间不使用PPPoE功能，一段时间以后会自行老化进而被删除。接口的保活功能即防止PPPoE接口老化，保持激活的状态。

配置接口保活功能，在接口配置模式下，使用以下命令：

keepalive *IP-address*

- *IP-address* – 指定PPPoE服务器的IP地址。

在接口配置模式下使用该命令no的形式取消接口保活的配置：

no keepalive

配置接口联动功能

接口联动功能指将多个物理接口的状态相互绑定，组成一个接口组。如果接口组内任何一个接口发生故障，组内其他接口状态会被设置为Down；只有当接口组内所有接口恢复正常后，接口组内接口状态才被设置为Up。系统支持跨模块卡进行接口联动。

新建接口组并进入指定接口组视图，在全局配置模式下，使用以下命令：

interface-group *group-name* **type linkage**

- *group-name* – 指定接口组的名称。长度范围是1至31个字符。

添加接口至接口组中，在接口组配置模式下，使用以下命令：

interface *interface-name*

- *interface-name* – 指定添加至接口组的接口名称。可添加最多8个接口至指定接口组中。

例如将接口ethernet1/0和ethernet1/1联动到接口组test中实现接口联动，在全局配置模式下输入以下命令：

```
hostname(config)# interface-group test type linkage  
hostname(config-if-group)# interface ethernet1/0  
hostname(config-if-group)# interface ethernet1/1
```

在全局配置模式下，使用该命令no的形式取消指定接口组的联动配置：

no interface-group *group-name*

显示指定接口组的联动信息，在任意模式下，使用以下命令：

```
show interface-group group-name
```

配置接口Local属性

为了解决在同一个二层网络管理大量HA设备时MAC地址冲突的问题，系统支持为所有接口（除VSwitch口）配置一个可编辑的HA Local属性。子接口和虚拟转发接口不需要配置，可直接继承主接口的HA Local属性。在接口配置模式下，使用以下命令：

```
local
```

在接口配置模式下，使用**no local**删除HA Local属性。

配置接口WAN属性

为了统计设备的上下行WAN流量，系统支持为所有接口（除回环接口）配置WAN属性，将所选接口指定为WAN接口。在接口配置模式下，使用以下命令：

```
type wan
```

在接口配置模式下，使用**no type**删除WAN属性。

回环接口

回环接口为逻辑接口，其特征为：回环接口一直处于工作状态，只有当回环接口所在安全设备关闭，回环接口才会关闭。回环接口的命名规则为loopback*Number*，其中*Number*为1到256的整数，用来作为回环接口的唯一标识。

创建回环接口

在CLI全局配置模式下，使用以下命令创建回环接口并且进入回环接口配置模式；如果指定的接口名称已存在，则直接进入该接口的配置模式：

```
interface loopbackNumber
```

- *Number* – 用来标识所创建的回环接口的整数。

例如创建名为loopback1的回环接口，在全局配置模式下输入以下命令：

```
hostname(config)# interface loopback1
```

```
hostname(config-if-loo1)#
```

在全局配置模式下，使用**no interface loopback***Number*删除指定的回环接口。

以太网接口

设备全部使用千兆以太网接口。千兆以太网接口符合1000Base-T物理层规范，可以在10Mbit/s、100Mbit/s 和1000Mbit/s三种速率下工作，有全双工和半双工两种工作方式。但是，设备不支持千兆半双工工作方式。

创建以太网子接口

用户可以为以太网口创建子接口。在CLI全局配置模式下使用以下命令，可以创建一个以太网子接口并且进入子接口配置模式；如果指定的子名称已存在，则直接进入该接口的配置模式：

```
interface ethernetm/n.tag
```

- *.tag* – 用来标识子接口的数字。范围是从1到4094的整数。例如，命令**interface ethernet0/0.1**为以太网接口ethernet0/0.创建了名为“ethernet0/0.1”的子接口。

在全局配置模式下使用**no interface ethernet***m/n.tag*命令删除指定的子接口。

以太网子接口支持PPPoE拨号功能。一个以太网子接口仅支持绑定一个PPPoE实例。

进入以太网接口配置模式

对以太网口的配置，例如接口速率、接口工作方式以及Combo口的光口电口切换等，都需要在以太网接口的配置模式下进行。进入以太网接口的配置模式，在全局配置模式下，使用以下命令：

```
interface ethernetm/n
```

- *ethernetm/n* – 指定以太网接口的名称进入相应接口的配置模式。

配置以太网接口的速率

千兆以太网电接口支持10Mbit/s、100Mbit/s、1000Mbit/s三种速率，而千兆以太网光接口只支持1000Mbit/s速率。因此，请不要对光接口的速率进行配置。在CLI中配置以太网电接口速率，在接口配置模式下，输入以下命令：

```
speed value
```

- *value*- 值为auto、10、100或者1000。默认值为auto，即系统自动测定并使用接口的最佳工作速率。指定的速率应与实际所连接网络和对端设备接口的速率相同。

在接口配置模式下，使用**no speed**命令恢复接口的默认速率。



注意: 当接口的速率值为“auto”时，接口的工作方式也必须是“auto”。

配置以太网接口的工作方式

千兆以太网电接口可以工作在全双工和半双工两种方式下，而千兆以太网光接口只能工作在全双工方式下。因此，请不要对千兆以太网光接口的工作方式进行配置。在CLI中配置以千兆以太网电接口的工作方式，请在接口配置模式下输入以下命令：

duplex method

- *method*- 值为auto（自动）、full（全双工）或者half（半双工）。默认值为auto，即系统自动选择最佳的双工模式。

例如，将以太网口ethernet1/2的速率设置成1000Mbit/s，工作方式设置为全双工，请参考以下命令：

```
hostname(config)# interface ethernet1/2
hostname(config-if-eth1/2)# speed 1000
hostname(config-if-eth1/2)# duplex full
hostname(config-if-eth1/2)# exit
hostname(config)#
```

在接口配置模式下，使用**no duplex**命令恢复接口的默认工作方式。



注意: 当接口的工作方式为“auto”时，接口的速率值也必须是“auto”。

克隆MAC地址

将指定的MAC地址克隆到以太网子接口，在以太网子接口配置模式下，输入以下命令：

mac-clone H.H.H

- *H.H.H* - 指定MAC地址。

在以太网子接口配置模式下，使用**no mac-clone**命令删除MAC地址的指定。



注意: 若在PPPoE拨号成功后修改MAC地址，用户需要重新连接PPPoE客户端以使修改后的MAC地址生效。

配置Combo口

设备配有光口+电口的Combo口。默认情况下，如果光口与电口均有线缆连接，设备会优先使用光口；如果设备最初使用的是电口，连接好光口电缆，重启设备后，设备会使用光口进行数据传输。用户可以通过命令控制光口与电口的使用。配置Combo口，请在接口配置模式下，使用以下命令：

```
combo {copper-forced | copper-preferred | fiber-forced | fiber-preferred}
```

- **copper-forced** – 强制使用电口。
- **copper-preferred** – 优先使用电口。
- **fiber-forced** – 强制使用光口。
- **fiber-preferred** – 优先使用光口。配置了该选项后，设备会将电口的流量自动切换到光口，无需重启设备。

使用**no combo**命令恢复Combo口的默认工作状态。

VSwitch接口

VSwitch接口是三层接口。它代表了VSwitch上所有端口的集合。用户在创建VSwitch的同时，也创建了该VSwitch的VSwitch接口。

创建VSwitch接口

在CLI的全局配置模式下，输入以下命令，用户可以创建一个VSwitch，同时创建该VSwitch的VSwitch接口：

```
vswitch vswitch Number
```

- *Number* - 用来标识所创建的VSwitch和VSwitch接口，其范围是根据设备平台的不同而不同。
- 执行该命令后，系统创建相应的VSwitch和VSwitch接口，并且进入VSwitch配置模式；如果指定的VSwitch名称已存在，则直接进入VSwitch配置模式。

在全局配置模式下使用**no vswitch vswitch Number**命令删除指定的VSwitch，同时删除相应的VSwitch接口。

集聚接口

一个集聚接口是两个或者多个物理接口的集合。这些物理接口平均分担通过该集聚接口的流量。集聚接口能够提高接口的可用带宽。如果集聚接口中的一个物理接口出现故障，不能工作，其它接口可以继续处理流量，只是可使用的带宽变小了。以下介绍集聚接口的基本配置操作。

创建集聚接口以及集聚子接口

在全局配置模式下，输入以下命令可创建一个集聚接口并且进入集聚接口配置模式；如果指定的接口名称已存在，则直接进入该接口的配置模式：

interface aggregate*Number*

- *Number* - 用来标识所创建的集聚接口。例如，命令“**interface aggregate2**”创建名为“aggregate2”的集聚接口。

在全局配置模式下使用**no interface aggregate***Number*命令删除指定的集聚接口。删除接口之前，必须取消其它接口与集聚接口的绑定、集聚子接口的配置、接口的IP地址配置以及接口与安全域的绑定。

用户可以为已存在的集聚接口创建子接口。创建集聚子接口，在全局配置模式下使用以下命令：

interface aggregate*Number.tag*

- *.tag* - 用来标识子接口的数字。范围是从1到4094的整数。例如，命令**interface aggregate2.1**为集聚接口aggregate2创建了名为“aggregate2.1”的子接口。

在全局配置模式下使用**no interface aggregate***Number.tag*命令删除指定的集聚子接口。

添加接口到集聚接口

一个集聚接口是两个或多个物理接口的集合，因此用户可以根据需要给集聚接口添加或者删除物理接口。添加物理接口到集聚接口，在被添加的物理接口的接口配置模式下请输入以下命令：

aggregate *aggregatenum*

- *aggregatenum* - 把物理接口添加到的集聚接口的名称。添加物理接口时，必须保证被添加的物理接口不属于任何其它接口也不属于任何安全域。

从集聚接口中取消某物理接口，在要取消的物理接口的接口配置模式下，使用**no aggregate**命令。

指定报文发送均衡方式

用户可以指定聚合组发送报文的均衡方式。系统支持按照报文的源IP、源MAC、源端口、目的IP、目的MAC、目的端口或者协议类型进行均衡转发的方式，也支持将以上方式进行组合的均衡转发方式。在聚合组成员为二层端口时，系统只支持按照源MAC或目的MAC进行均衡转发。例如，配置使用按照报文的源IP进行均衡转发的方式后，所有源IP相同的报文都会从聚合组中的同一接口转发。当集聚接口内的物理接口属于不同模块时，系统支持指定优先从报文入接口所在模块的接口进行转发。

指定报文发送均衡方式，在集聚接口配置模式下，使用以下命令：

```
load-balance mode {flow | tuple [src-ip | src-mac | src-port | dest-ip | dest-mac | dest-port | protocol]}
```

- **flow** - 指定从数据流中自动获取均衡方式。该方式为系统默认方式。
- **tuple [src-ip | src-mac | src-port | dest-ip | dest-mac | dest-port | protocol]** - 指定报文发送均衡方式为源IP（**src-ip**）、源MAC（**src-mac**）、源端口（**src-port**）、目的IP（**dest-ip**）、目的MAC（**dest-mac**）、目的端口（**dest-port**）或者协议类型（**protocol**）方式，也可以将以上方式进行组合。

在集聚接口配置模式下，使用**no load-balance** 命令恢复默认均衡方式。

冗余接口

一个冗余接口绑定到两个物理接口。一个物理接口为主接口处理流向该冗余接口的流量。另外一个接口作为备用接口在主接口发生故障时升级为主接口继续处理流量。

创建冗余接口以及冗余子接口

在全局配置模式下，输入以下命令可创建一个冗余接口并且进入冗余接口配置模式；如果指定的接口名称已存在，则直接进入该接口的配置模式：

```
interface redundant Number
```

- *Number* - 用来标识所创建的冗余接口。例如，命令“**interface redundant2**”创建名为“redundant 2”的冗余接口。

在全局配置模式下使用**no interface redundant *Number***命令删除指定的冗余接口。删除接口之前，必须取消其它接口与冗余接口的绑定、冗余子接口的配置、接口的IP地址配置以及接口与安全域的绑定。

用户可以为已存在的冗余接口创建子接口。创建冗余子接口，在全局配置模式下使用以下命令：

```
interface redundantnNumber.tag
```


- *.tag* – 用来标识子接口的数字。范围是从1到4094的整数。例如，命令**interface redundant2.1**为集聚接口redundant2创建了名为“redundant2.1”的子接口。

在全局配置模式下使用**no interface redundantNumber.tag**命令删除指定的冗余子接口。

添加接口到冗余接口

添加一个物理接口到冗余接口，在要添加的接口的接口配置模式下，输入以下命令：

redundant *interface-name*

- *interface-name* – 将物理接口添加到的冗余接口的名称。添加物理接口时，必须保证被添加的物理接口不属于任何其它接口也不属于任何安全域。

从冗余接口中取消某物理接口，在要取消的物理接口的接口配置模式下，使用**no redundant**命令。如果被取消的接口是冗余接口的主接口，要先取消主接口的配置再将其从冗余接口中取消。

指定主接口

用户需要在两个物理接口中为冗余接口指定一个主接口。在冗余接口配置模式下，输入以下命令：

primary *interface-name*

- *interface-name* - 指定为主接口的接口名称。

取消接口的主接口设置，在冗余接口配置模式下使用**no primary**命令。

开启或关闭ARP回环告警日志

某接口收到ARP报文后，判断报文源MAC地址与该接口MAC地址是否一致，如果一致，则系统会形成环路。

如果此时ARP回环告警日志功能是开启的，系统会频繁产生ARP回环告警日志。用户可以通过如下命令来控制是否开启该告警日志。

默认情况下，接口的ARP回环告警日志功能是开启的。关闭冗余接口的ARP回环告警日志功能，在冗余接口配置模式下，使用以下命令：

arp-loop-alarm-disable

在接口配置模式下，使用以下命令恢复默认值：

no arp-loop-alarm-disable

隧道接口

设备支持VPN功能。隧道接口充当VPN通道的入口。流量通过隧道接口进出VPN通道。隧道接口只能是三层接口。

创建隧道接口

在全局配置模式下，输入以下命令可创建一个隧道接口并且进入隧道接口配置模式；如果指定的接口名称已存在，则直接进入该接口的配置模式：

```
interface tunnel Number
```

- *Number* - 用来标识所创建的隧道接口。例如，命令“**interface tunnel2**”创建名为“**tunnel 2**”的隧道接口。

在全局配置模式下使用**no interface tunnel** *Number*命令删除指定的隧道接口。

绑定隧道

隧道接口可以绑定IPSec VPN隧道、GRE隧道、SCVPN隧道或者L2TP隧道。一个隧道接口可以绑定多个IPSec VPN隧道或多个GRE隧道，但仅可以绑定一个SCVPN隧道或者一个L2TP隧道。

绑定隧道，在隧道接口配置模式下，使用以下命令：

```
tunnel { {ipsec | gre} tunnel-name [gw ip-address] | scvpn vpn-name | l2tp tunnel-name | ikev2 ikev2-name | ip4in6 ipv4-tunnel-name | ip6in4 ipv6-tunnel-name}
```

- {**ipsec** | **gre**} *tunnel-name* - 指定绑定到隧道接口的IPSec VPN隧道的名称或者GRE隧道的名称。
- **gw** *ip-address* - 指定隧道的下一跳IP地址，可以为对端隧道接口的IP地址或者对端出接口的IP地址。当需要为隧道接口绑定多个IPSec VPN或GRE隧道时，此配置参数有效。系统默认值为0.0.0.0。
- **scvpn** *vpn-name* - 指定绑定到隧道接口的SCVPN隧道的名称。一个隧道接口最多只能绑定一个SCVPN隧道。
- **l2tp** *tunnel-name* - 指定绑定到隧道接口的L2TP隧道的名称。一个隧道接口最多只能绑定一个L2TP隧道。
- **ip4in6** *ipv4-tunnel-name* - 指定绑定到隧道接口的IPv6 4to6隧道的名称。一个隧道接口最多只能绑定一个IPv6 4to6隧道。
- **ip6in4** *ipv6-tunnel-name* - 指定指定绑定到隧道接口的IPv6 6to4隧道的名称。一个隧道接口最多只能绑定一个IPv6 6to4隧道。

多次配置该命令为隧道接口绑定多个IPSec VPN隧道或者多个GRE隧道。在隧道接口配置模式下使用**no tunnel** {**ipsec** *vpn-name* | **gre** *tunnel-name* | **scvpn** *vpn-name* | **l2tp** *tunnel-name* | **ikev2** *ikev2-name* | **ip4in6** *ipv4-tunnel-name* | **ip6in4** *ipv6-tunnel-name*} 命令取消接口与隧道的绑定。

多隧道OSPF支持

当一个隧道接口绑定到多个VPN隧道实现多站点VPN互联时，如果使用OSPF动态路由方式进行站点间数据交换管理，该隧道接口需要支持点到多点（Point-to-multipoint）网络类型（隧道接口默认支持点到点，即Point-to-point，网络类型）。配置点到多点支持功能，在隧道接口配置模式下，使用以下命令：

```
ip ospf network point-to-multipoint
```

在隧道接口配置模式下，使用该命令**no**的形式恢复点到点的支持：

```
no ip ospf network point-to-multipoint
```

配置借用IP地址功能（IP Unnumbered）

有些情况下，使用隧道接口转发数据包时，并不需要为隧道接口配置IP地址，例如使用隧道接口转发通过设备的数据包。为节省有限的IP地址资源，设备的隧道接口支持IP地址借用功能（IP Unnumbered），即隧道接口本身不配置IP地址，而是借用其它接口的IP地址。

为隧道接口配置借用IP地址功能，在隧道接口配置模式下，使用以下命令：

```
ip address unnumber interface-name
```

- *interface-name* – 指定被借用IP地址的接口的名称。

在隧道接口配置模式下，使用该命令**no**的形式取消借用IP地址功能的配置：

```
no ip address unnumber
```



注意：IPSec VPN隧道两端的隧道接口不可以同时配置借用IP地址功能。

查看隧道接口信息

用户可以在任何模式下，通过show命令查看特定隧道接口的配置信息。具体命令以下：

```
show interface bind-tunnels tunnel-name
```

- *tunnel-name* – 指定需要查看的隧道接口的名称。

PPPoE子接口

设备支持多个PPPoE接口功能。多个PPPoE接口功能指基于以太网口创建多个PPPoE子接口后，一个物理以太网口便可以通过多个PPPoE子接口连接多个ISP。创建PPPoE子接口，在全局配置模式下，使用以下命令：

```
interface ethernetX/Y-pppoeZ
```

- **ethernetX/Y** – 指定以太网口的名称，例如ethernet0/5。
- **pppoeZ** – 指定PPPoE子接口的名称，“Z”为PPPoE子接口的标识，取值范围因不同平台而异。

在全局配置模式下使用该命令no的形式删除指定的PPPoE子接口：

```
no interface ethernetX/Y-pppoeZ
```

链路聚合

链路聚合将多条物理链路捆绑在一起，成为一条逻辑链路，从而实现增加链路带宽的目的。同时，这些捆绑在一起的链路通过相互间的动态备份，能够有效地提高链路的可靠性。

设备支持强制聚合和LACP动态协商聚合。强制聚合即系统中已有的集聚接口（Aggregate IF），详细信息请参阅“[集聚接口](#)”一节。本节将主要介绍LACP动态协商聚合。

LACP动态协商聚合

LACP（Link Aggregation Control Protocol，链路聚合控制协议）是一种实现链路动态聚合与解聚合的协议，该协议通过LACPDU（Link Aggregation Control Protocol Data Unit，链路聚合控制协议数据单元）与对端交互链路聚合的相关信息。LACP动态协商聚合通过在链路两端均开启LACP协议来动态协商聚合链路。设备通过在集聚接口上启用LACP协议实现LACP链路聚合功能。开启LACP协议的集聚接口称为聚合组，加入聚合组的物理接口称为聚合组成员接口。在某集聚接口启用LACP协议后，该聚合组的成员接口将通过发送LACPDU向对端通告自己的系统优先级、系统MAC、端口优先级、端口号和操作Key，对端接收到这些信息后，将与其他接口所保存的信息比较，以选择能够聚合的接口，从而双方可以对使用哪部分链路传输用户数据达成一致。

聚合组成员接口状态

聚合组中的成员接口有以下四种状态：

- **Unselected**: 表示接口没能被聚合组选中, 不可参与流量转发。处于此状态一般是由于物理原因, 比如, 接口工作模式非双工、速率不匹配、物理连接断开等;
- **Selected**: 表示接口被聚合组选中, 但是相连的对端没有准备好, 不可参与流量转发。一旦收到对端的LACPDU报文, 并解析出对端状态也为Selected, 接口将切换为Active状态, 参与流量转发;
- **Standby**: 表示接口目前处于备份状态, 不可参与流量转发。提升本接口LACP优先级, 接口将自动替换较低优先级的已选接口, 变为Selected状态, 而被替换接口则变成Standby状态。当其他已选接口出现故障变成Unselected状态时, 接口将自动切换为Selected状态;
- **Active**: 表示接口聚合成功, 处于活跃状态, 可参与流量转发。连续三个LACPDU超时周期没有收到对端的LACPDU报文, 协议认为链路已断开, 接口状态将切换为Selected, 停止流量转发。

配置LACP动态协商聚合

LACP动态协商聚合的配置包括以下各项:

- 启用/禁用LACP协议
- 指定LACP系统优先级
- 指定接口LACP优先级
- 指定LACP超时时间
- 指定最大活动链路数
- 指定最小活动链路数
- 指定报文发送均衡方式

启用/禁用LACP协议

在集聚接口上启用LACP协议后, 该集聚接口即切换为聚合组。目前只支持在集聚接口上启用LACP, 不支持在集聚子接口及集聚前向转发接口上启用LACP协议。启用/禁用接口的LACP协议, 在集聚接口配置模式下, 使用以下命令:

- 启用: **lacp enable**
- 禁用: **no lacp enable**

指定LACP系统优先级

LACP系统优先级用于区分两端设备优先级的高低，以确保两端设备选中的接口一致。协议会以LACP系统优先级高的一端为标准选择接口。数值越小，优先级越高。当两端的LACP系统优先级一致时，比较两端设备的MAC地址，MAC地址小的一端优先级高。配置LACP系统的优先级，在集聚接口配置模式下，使用以下命令：

```
lacp system-priority value
```

- *value* – 指定LACP系统的优先级。取值范围为1到32768，默认值为32768。

使用该命令no的形式恢复LACP系统的默认优先级：

```
no lacp system-priority
```

指定接口LACP优先级

接口LACP优先级用于区分聚合组各成员接口变成Selected状态的优先程度，优先级高的成员接口将被优先选作Selected接口。数值越小，优先级越高。成员接口LACP优先级和LACP系统优先级通常配合使用，决定聚合组内的哪些链路将被成功聚合。

指定成员接口LACP优先级，在被添加到集聚接口的物理接口的接口配置模式下，使用以下命令：

```
lacp port-priority value
```

- *value* – 指定接口的LACP优先级。取值范围为1到32768，默认值为32768。

使用该命令no的形式恢复成员接口的默认LACP优先级：

```
no lacp port-priority
```

指定LACP超时时间

LACP超时时间是指成员接口等待接收LACPDU的超时时间。在三倍LACP超时时间之后，如果本端成员接口仍未收到来自对端的LACPDU，则认为对端成员接口已失效，接口会从Active状态切换到Selected状态，停止流量转发。LACP超时时间有短超时（1秒）和长超时（30秒）两种取值。

成员接口的LACP超时时间默认为长超时。为成员接口指定短超时模式，在被添加到集聚接口的物理接口的接口配置模式下，使用以下命令：

```
lacp period-short
```

使用该命令no的形式恢复接口为长超时模式：

```
no lacp period-short
```

指定最大活动链路数

用户可以指定聚合组中的最大活动链路数，即最大Active接口数。当Active接口数达到最大值时，其它合法接口将变为Standby状态。例如，聚合组中有4个Active接口，若设置最大活动链路数为2，系统将自动选择优先级最高的两个接口为Active状态，另外两个低优先级的接口则设置为Standby状态。当Active接口出现故障导致链路断开时，系统会自动将Standby接口切换为Active状态，从而实现链路备份。

指定最大活动链路数，在集聚接口配置模式下，使用以下命令：

```
lacp max-bundle number
```

- *number* – 指定最大活动链路数。取值范围为1到16，默认值为16。

使用该命令no的形式恢复最大活动链路数的默认值：

```
no lacp max-bundle
```

指定最小活动链路数

用户可以指定聚合组中的最小活动链路数，即最小Active接口数量。当聚合组中的Active接口数量小于该最小值时，系统会自动将聚合组中的所有合法接口都设置为Standby状态，不可参与流量转发。最小活动链路数不能大于最大活动链路数。

指定最小活动链路数，在集聚接口配置模式下，使用以下命令：

```
lacp min-bundle number
```

- *number* – 指定最小活动链路数。取值范围为1到8，默认值为1。

使用该命令no的形式恢复最小活动链路数的默认值：

```
no lacp min-bundle
```

指定报文发送均衡方式

用户可以指定聚合组发送报文的均衡方式。系统支持按照报文的源IP、源MAC、源端口、目的IP、目的MAC、目的端口或者协议类型进行均衡转发的方式，也支持将以上方式进行组合的均衡转发方式。在聚合组成员为二层端口时，系统只支持按照源MAC或目的MAC进行均衡转发。例如，配置使用按照报文的源IP进行均衡转发的方式后，所有源IP相同的报文都会从聚合组中的同一接口转发。指定报文发送均衡方式，在集聚接口配置模式下，使用以下命令：

```
load-balance mode {flow | tuple {dest-ip dest-mac dest-port protocol src-ip src-mac src-port}}
```

- **flow** – 指定从数据流中自动获取均衡方式。该方式为系统默认方式。
- **tuple [dest-ip dest-mac dest-port protocol src-ip src-mac src-port]** – 指定报文发送均衡方式为源IP (**src-ip**)、源MAC (**src-mac**)、源端口 (**src-port**)、目的IP (**dest-ip**)、目的MAC (**dest-mac**)、目的端口 (**dest-port**) 或者协议类型 (**protocol**) 方式，也可以将以上方式进行组合。

使用该命令**no**的形式恢复聚合组发送报文的默认均衡方式：

```
no load-balance
```

查看聚合组信息

用户可以在任何模式下，通过**show**命令查看特定LACP聚合组的配置信息。具体命令如下：

```
show lacp aggregate-name
```

- *aggregate-name* – 指定需要查看的聚合组名称。

LLDP

网络设备的种类日益繁多且各自的配置错综复杂，为了方便管理，需要使不同厂商的设备能够在网络中相互发现并交互各自的系统及配置信息。LLDP (Link Layer Discovery Protocol) 协议是IEEE 802.1ab中定义的邻居发现协议，提供了一种链路层网络的发现方式。通过LLDP技术，在网络规模迅速扩大时，系统可以快速掌握二层网络的拓扑信息和拓扑变化信息。

通过LLDP标准协议，可以将本端设备的LLDP信息（包括设备信息、系统名称、系统描述、接口描述、网络管理地址等）通过标准的TLV (Type Length Value, 类型长度值) 由物理接口定期向直连的邻居发送组播报文，如果邻居也开启了LLDP功能，那么双方将建立邻居关系；邻居收到这些信息后以标准的MIB形式存储在SNMP MIB库中，以供网络管理系统查询、分析当前网络的二层拓扑结构以及拓扑结构中存在的问题。

LLDP工作模式

LLDP的工作模式包括有以下四种：

- **txrx**：既发送也接收LLDP报文。
- **tx**：只发送不接收LLDP报文。
- **rx**：只接收不发送LLDP报文。
- **disable**：既不发送也不接收LLDP报文。

配置LLDP功能

通过配置LLDP功能，可以实现邻居设备对网络拓扑变化信息的收集。

- 开启/关闭全局LLDP功能
- 开启/关闭接口的LLDP功能
- 配置接口的LLDP工作模式
- 配置接口初始化延迟时间
- 配置LLDP报文发送间隔
- 配置LLDP报文发送延迟时间
- 配置TTL乘数
- 显示LLDP本地信息
- 显示接口的LLDP邻居信息
- 显示LLDP统计信息
- 显示LLDP状态信息

开启/关闭全局LLDP功能

LLDP功能必须在设备的“全局LLDP功能”和“接口的LLDP功能”同时启用后才能生效，相应的接口才能够发送和接收LLDP报文。

- 默认情况下，全局LLDP功能、接口的LLDP功能均处于关闭状态。
- 当开启全局LLDP功能后，设备上所有接口的LLDP功能都将会自动开启。
- 当关闭全局LLDP功能后，设备上所有接口的LLDP也将会同时被关闭。
- 开启全局LLDP功能后，用户可以无需修改LLDP配置信息，使用默认配置即可实现LLDP功能。

开启/关闭全局LLDP功能，在全局配置模式下，使用以下命令：

- 开启：**lldp global enable**
- 关闭：**lldp global disable**

开启/关闭接口的LLDP功能

开启接口的LLDP功能前，在全局配置模式下，使用`interface ethernetm/n`命令，进入需要开启LLDP功能的接口配置模式。

开启/关闭接口的LLDP功能，在接口配置模式下，使用以下命令：

- 开启：`lldp enable`
- 关闭：`lldp disable`



注意: 仅设备中的物理接口支持开启LLDP功能，逻辑接口不支持该功能。

配置接口的LLDP工作模式

用户可以配置LLDP的工作模式，指定接口是否发送或接收LLDP报文。默认情况下，接口的LLDP工作模式为txrx（既发送也接收LLDP报文）。

配置接口的LLDP工作模式，在接口配置模式下，使用以下命令：

```
lldp admin-status {disable | rx | tx | txrx}
```

- disable- 指定接口既不发送也不接收LLDP报文。
- txrx- 指定接口既发送也接收LLDP报文。
- tx- 指定接口只发送不接收LLDP报文。
- rx- 指定接口只接收不发送LLDP报文。

使用`no lldp admin-status`命令恢复默认LLDP工作模式。

配置接口初始化延迟时间

当接口的LLDP工作模式发生变化时，系统将会对接口状态进行初始化操作。通过配置接口初始化的延迟时间，可以避免由于工作模式的频繁改变而造成接口不断的进行初始化。

配置接口的初始化延迟时间，在全局配置模式下，使用以下命令：

```
lldp reinit-delay delay-value
```

- *delay-value*- 指定接口初始化延迟时间，单位是秒，范围是1到10秒，默认值是2秒。

使用**no lldp reinit-delay**命令恢复接口初始化延迟时间默认值。

配置LLDP报文发送间隔

发送间隔是指在设备状态一直没有发生变化的情况下，向邻居设备发送LLDP报文的时间周期。

配置LLDP报文发送间隔，在全局配置模式下，使用以下命令：

lldp message-transmission interval *interval*

- *interval*- 指定LLDP报文的发送周期。单位是秒，范围是1到3600秒，默认值是30秒。

使用**no lldp message-transmission interval**命令恢复LLDP报文发送间隔默认值。

配置LLDP报文发送延迟时间

发送延时是指设备状态频繁发生变化的时候，向邻居设备发送LLDP报文的最小延迟时间。

配置LLDP报文发送延迟时间，在全局配置模式下，使用以下命令：

lldp message-transmission delay *delay-value*

- *delay-value* - 指定发送LLDP报文的最小延迟时间。单位是秒，范围是1到900秒，默认值是1秒。

使用**no lldp message-transmission delay**命令恢复发送LLDP报文的最小延迟时间默认值。

配置TTL乘数

TTL是指设备信息在邻居设备中保持的时间。TTL乘数用于调整设备信息在邻居设备中保持的有效时间（TTL），计算公式是： $TTL = \text{发送间隔} (interval) \times \text{TTL乘数} (hold-multiplier)$ 。

配置TTL乘数，在全局配置模式下，使用以下命令：

lldp message-transmission hold-multiplier *hold-multiplier*

- *hold-multiplier*- 指定TTL乘数数值，范围是1到100，默认值是4。

使用**no lldp message-transmission hold-multiplier**命令恢复TTL乘数默认值。

显示LLDP本地信息

在任意模式下，使用以下命令查看LLDP本地信息：

```
show lldp local-information [global | interface-name]
```

- **global**- 显示待发送给邻居设备的全局LLDP本地信息。
- *interface-name* - 显示指定接口上待发送给邻居设备的LLDP信息。

显示接口的LLDP邻居信息

在任意模式下，使用以下命令查看接口的LLDP邻居信息，即显示由邻居设备发送到本端设备的LLDP 信息：

```
show lldp neighbor-information [ interface-name]
```

- *interface-name*- 显示指定接口收到的由邻居设备发送到本端设备的LLDP信息。如果未指定该参数，将会显示所有接口的LLDP邻居信息。

显示LLDP统计信息

在任意模式下，使用以下命令查看LLDP统计信息：

```
show lldp statistics [global | interface-name]
```

- **global**- 显示全局LLDP统计信息。
- *interface-name* - 显示指定接口的LLDP统计信息。

显示LLDP报文收发信息

在任意模式下，使用以下命令查看LLDP报文收发信息：

```
show dp-info lldp
```

显示LLDP状态信息

在任意模式下，使用以下命令查看LLDP状态信息：

```
show lldp status [ interface-name]
```

- *interface-name*- 显示指定接口的LLDP状态信息。

DNS

DNS为域名系统（Domain Name System）的缩写。DNS是一种组织成域层次结构的计算机和网络服务命名系统，用于TCP/IP网络，主要用来寻找Internet域名（如www.xxxx.com）并转化为IP地址（如“10.1.1.1”）以定位相应的计算机和相应服务。

系统的DNS功能如下：

- 名字服务：为设备配置DNS服务器和默认域名。
- 代理：设备作为DNS代理服务器，为与其连接的PC等（客户端）提供DNS代理功能。同时，山石网科设备可以根据域名选择不同的域名服务器。
- 解析：为设备的DNS功能设置重试次数和响应超时时间。
- 缓存：将DNS映射项储存在缓存中，用以提高查找速度。

配置DNS名字服务

DNS名字服务的配置包含：

- 为设备配置域名
- 为设备设置DNS服务器

设置域名

用户可以为设备指定一个域名。设备会将域名作为后缀添加到用户输入的不完全的名称后。例如，如果设置域名为“sina.com”，在设备上Ping“www”，系统会把域名加上去查找“www.sina.com”。并且，把域名设置为“sina.com”和“com”后的解析顺序不同：设置为“sina.com”后，Ping“www”，系统会先查找www.sina.com；而设置为“com”后，Ping“www.sina”，系统会先查找www.sina然后再查找www.sina.com。

设置系统域名，在全局配置模式下使用以下命令：

ip domain name *domain-name*

- *domain-name* – 指定域名。名称长度可以是1到255个字符，但是在两个句点（.）之间，最多可以有63个字符。

使用**no ip domain name**命令恢复默认域名。

以下是设置默认域名名称为hillstonenet.com的命令配置示例：

```
hostname(config)# ip domain name hillstonenet.com
```

设置DNS域名服务器

该命令指定的DNS域名服务器为设备进行DNS解析时使用的服务器。设置DNS域名服务器，在全局配置模式下使用以下命令：

```
ip name-server server-address1 [server-address2] ... [server-address6] [vrouter vrouter-name]
```

- *server-address1* – 指定域名服务器的IP地址。用户最多可配置6个域名服务器。用户可以使用一条命令配置6个域名服务器，也可分多条命令配置，即运行命令ip name-server 1.1.1.1 2.2.2.2与运行命令ip name-server 1.1.1.1和ip name-server 2.2.2.2等效，最多可以配置64个域名服务器。
- *vrouter-name* – 为指定的VRouter指定DNS代理服务器。

使用**no ip name-server** *server-address1* [*server-address2*] ... [*server-address6*]取消对DNS域名服务器的配置。

配置DNS代理功能

DNS代理功能通过DNS代理规则来实现。DNS代理规则分为过滤条件和动作两部分。入接口、源地址、目的地址及DNS域名，构成DNS代理规则的过滤条件。DNS代理规则的动作包括代理、转发、放行及阻断共四种。当代理规则的动作被指定为“代理”时，用户需同时配置DNS代理服务器，这样满足条件的DNS请求将通过指定的DNS代理服务器进行地址解析；当代理规则的动作被指定为“转发”时，用户也需同时配置DNS服务器，满足条件的DNS请求将通过指定的DNS服务器进行地址解析。

每条DNS代理规则都有其独有的ID号。规则ID会在定义规则时自动生成，同时用户也可以按自己的需求为规则指定ID号。整个系统的所有策略规则有特定的排列顺序。在流量进入系统时，系统会对流量按照找到的第一条与过滤条件相匹配的规则进行处理。

系统支持IPv4和IPv6两种类型的DNS代理。IPv4类型的DNS代理实现域名与IPv4地址的转换，IPv6类型的DNS代理实现域名与IPv6地址的转换。

DNS代理功能的配置包括：

- 配置DNS代理规则
- 修改DNS代理规则的排列顺序
- 配置DNS代理服务器探测功能

- 开启/关闭DNS代理的UDP报文校验和功能
- 指定DNS代理响应报文的TTL

配置DNS代理规则

用户可以通过配置DNS代理规则，对进入设备的DNS流量进行控制。DNS代理规则配置包括：

- 创建DNS代理规则
- 配置DNS代理匹配条件
- 指定DNS代理规则动作
- 配置DNS服务器调度算法
- 配置DNS服务器
- 配置描述信息
- 启用/禁用DNS代理规则

创建DNS代理规则

创建DNS代理规则或进入DNS代理规则配置模式，在全局配置模式下，使用以下命令：

dns-proxy rule [*id id*]

- **id id** – 指定DNS代理规则的ID，并进入DNS代理规则配置模式。如果不指定，系统将会为DNS代理规则自动分配一个ID。规则ID在整个系统中必须是唯一的。

在全局配置模式下，使用命令**no dns-proxy rule id id**删除DNS代理规则。

配置DNS代理过滤条件

DNS代理过滤条件包括DNS请求的入接口、源地址、目的地址及DNS域名共四种。用户需同时配置四种过滤条件，配置完成后，系统将对DNS请求进行过滤。只有DNS请求同时满足以上四种条件时，系统才认为匹配成功。

指定DNS入接口

用户可指定DNS请求的入接口，对DNS请求报文进行过滤，可指定多个入接口。指定后，系统将按照规则设定的动作，对该入接口流量进行处理。在DNS代理规则配置模式下，使用以下命令：

- **ingress-interface** *interface-name* - 添加DNS流量的入接口。

使用**no ingress-interface** *interface-name*命令删除DNS流量的入接口。

指定DNS源地址

用户可指定DNS请求的源地址，对DNS请求报文进行过滤。用户可指定多条源地址类目。指定后，系统将按照规则设定的动作，对匹配成功的流量进行处理。在DNS代理规则配置模式下，使用以下命令：

- **src-addr** { *addr-name* | **any** | **ipv6-any** } - 添加地址簿条目类型源地址。
- **no src-addr** { *addr-name* | **any** | **ipv6-any** } - 删除地址簿条目类型源地址。
- **src-ip** { *ipv4/netmask* | *ipv4-address netmask* | *ipv6-address/prefix* } - 添加IP成员类型源地址。
- **no src-ip** { *ipv4/netmask* | *ipv4-address netmask* | *ipv6-address/prefix* } - 删除IP成员类型源地址。
- **src-range** *min-ip max-ip* - 添加IPv4或IPv6地址范围类型源地址。
- **no src-range** *min-ip max-ip* - 删除IPv4或IPv6地址范围类型源地址。

指定DNS目的地址

用户可指定DNS请求的目的地址，对DNS请求报文进行过滤。用户可指定多条目的地址类目。指定后，系统将按照规则设定的动作，对匹配成功的流量进行处理。在DNS代理规则配置模式下，使用以下命令：

- **dst-addr** { *addr-name* | **any** | **ipv6-any** } - 添加地址簿条目类型目的地址。
- **no dst-addr** { *addr-name* | **any** | **ipv6-any** } - 删除地址簿条目类型目的地址。
- **dst-ip** { *ipv4/netmask* | *ipv4-address netmask* | *ipv6-address/prefix* } - 添加IP成员类型目的地址。
- **no dst-ip** { *ipv4/netmask* | *ipv4-address netmask* | *ipv6-address/prefix* } - 删除IP成员类型目的地址。
- **dst-range** *min-ip max-ip* - 添加IPv4或IPv6地址范围类型目的地址。
- **no dst-range** *min-ip max-ip* - 删除IPv4或IPv6地址范围类型目的地址。

指定DNS 域名

用户可指定DNS域名，用来匹配DNS请求中的域名，对DNS请求报文进行过滤。用户可指定多条域名过滤条件。指定后，系统将按照规则设定的动作，对相应的DNS请求流量进行处理。在DNS代理规则配置模式下，使用以下命令：

```
domain { any | domain-name | host-book host-book-entry }
```

- *domain-name* - 指定需匹配的具体域名。
- **any** - 指定为可匹配任意域名。
- **host-book** *host-book-entry* - 指定需匹配的域名条目的名称。

使用**no domain** { **any** | *domain-name* | **host-book** *host-book-entry* } 删除DNS域名。

配置DNS代理规则动作

对符合过滤条件的DNS请求，系统可对其进行代理、转发、放行和阻断流量共4种处理动作，用户可按需进行设定，在DNS代理规则配置模式下，使用以下命令：

```
action { proxy | forward | bypass | block }
```

- **proxy** - 将DNS代理规则的动作指定为代理，即DNS请求将通过代理服务器进行DNS解析。
- **forward** - 将DNS代理规则的动作指定为转发，即DNS请求将通过DNS服务器进行DNS解析。
- **bypass** - 将DNS代理规则的动作指定为放行，即DNS请求将被转发给原始报文的DNS服务器。
- **block** - 将DNS代理规则的动作指定为阻断，即DNS请求将被丢弃。

配置DNS服务器调度算法

当指定DNS代理规则的动作作为“代理”或“转发”后，选择调度算法，系统将按照指定的调度算法，合理地将客户端的DNS请求调度至相应的DNS服务器进行解析。调度算法的详细介绍，请参阅“[调度算法](#)”。

配置DNS服务器的调度算法，在DNS代理规则配置模式下，使用以下命令：

```
balance method { least-bandwidth | least-connection | round-robin | weighted-least-bandwidth | weighted-least-connection | weighted-round-robin }
```

- **least-bandwidth** - 指定调度算法为最小带宽算法。
- **least-connection** - 指定调度算法为最小连接数算法。
- **weighted-least-connection** - 指定调度算法为加权最小连接数算法。
- **round-robin** - 指定调度算法为轮询算法。该参数为默认算法。
- **weighted-least-bandwidth** - 指定调度算法为加权最小带宽算法。
- **weighted-round-robin** - 指定调度算法为加权轮询算法。

在DNS代理规则配置模式下，使用**no balance method**命令恢复默认算法。

DNS服务器调度算法

DNS代理支持多种调度算法，包括：

算法	描述
轮询（Round Robin）	设备将客户端的DNS请求轮流分配给每个DNS服务器。
加权轮询（Weighted Round Robin）	在轮询的基础上，设备根据DNS服务器的权值，按比例进行选路。DNS服务器权值越大，接收的DNS请求越多。
最小带宽（Least Bandwidth）	设备会记录DNS服务器绑定接口的上行与下行带宽总和。当新的DNS请求到达时，设备将选择带宽总和最小接口对应的DNS服务器进行处理。
最小连接数（Least Connection）	设备会记录DNS服务器绑定接口上的连接数。当新的DNS请求到达时，设备将选择连接数最少接口对应的DNS服务器进行处理。
加权最小连接（Weighted Least Connection）	在最少连接数分发的基础上，设备根据DNS服务器的权值，按比例进行选路。当新的DNS请求到达时，将为其选择当前DNS服务器绑定的接口上的连接数与其权值的比值最小的DNS服务器。（计算方法：接口上的连接数除以权值）。
加权最小带宽（Weighted Least Bandwidth）	在最小带宽的基础上，设备根据DNS服务器的权值，按比例进行选路。当新的DNS请求到达时，将为其选择当前DNS服务器绑定接口的带宽总和与其权值的比值最小的DNS服务器。（计算方法：上行与下行带宽总和除以权值）。

配置DNS服务器

当用户将DNS代理规则的动作指定为“代理”或“转发”时，需继续指定DNS服务器。每条DNS规则最多可指定6个DNS服务器。用户可按需为DNS服务器指定出接口和首选属性，作为选择DNS服务器的依据。当用户配置多个DNS服务器时，将按照如下顺序选择DNS服务器：

- 首先选择首选DNS服务器进行域名解析。
- 若没有指定首选服务器，系统将查询是否有指定出接口的DNS服务器；若有，则按照指定的调度算法选择出接口DNS服务器。
- 若没有指定首选DNS服务器，也没有绑定出接口的DNS服务器，即只有普通的DNS服务器，则按照指定的调度算法（此时只有轮询或加权轮询算法生效）选择此类普通的DNS服务器。

在DNS代理规则配置模式下，使用以下命令添加DNS服务器：

```
name-server server-ip [vrouter vrouter-name] egress-interface interface-name weight value [preferred]
```

- *server-ip* - 指定DNS服务器的IP地址。
- **vrouter** *vrouter-name* - 指定虚拟路由器。
- **egress-interface** *interface-name* - 为该DNS服务器指定出接口。
- **weight** *value* - 指定DNS服务器的权值。取值范围是0到255，默认值是50。
- **preferred** - 指定DNS服务器为首选服务器，一条DNS代理规则仅可指定一台服务器为首选服务器。

在DNS代理规则配置模式下，使用**no name-server** *server-ip* 命令删除DNS服务器。



注意:

- 当选择调度算法为最小带宽、最小连接数、加权最小带宽或加权最小连接时，需为DNS服务器绑定出接口，并根据实际情况，为DNS服务器指定相应的权重。
- 当DNS代理规则的动作指定为代理时，DNS代理服务器的实际转发出口将由配置的虚拟路由器以及出接口决定。



- 当DNS代理规则的动作指定为转发时，为DNS服务器配置的虚拟路由器、绑定出接口和首选服务器属性，仅作为DNS服务器顺序选择依据。选定DNS服务器后，实际转发出口由相关路由配置决定。

开启/关闭DNS64功能

DNS64功能用于当IPv6客户端主机收到DNS查询时，先解析DNS查询信息中的AAAA记录（IPv6地址），如果解析成功，则直接将IPv6地址返回给客户端；如果解析失败，那么DNS64将会解析DNS查询信息中的A记录（IPv4地址），并将A记录（IPv4地址）合成AAAA记录（IPv6地址）返回给客户端。

用户可以指定开启或关闭DNS64功能。默认情况下DNS64功能是关闭的，在DNS代理规则配置模式下，使用以下命令：

- 开启：**dns64 enable**（执行该命令后，系统进入DNS64配置模式）
- 关闭：**no dns64 enable**



注意：仅支持在IPv6 DNS代理规则中开启DNS64功能，IPv4 DNS代理规则中不支持。

配置DNS64服务器

DNS64服务器用于解析DNS查询信息中的A记录（IPv4地址），每条IPv6 DNS代理规则最多可以指定6个DNS64服务器。配置DNS64服务器，在DNS64配置模式下，使用以下命令：

server server-ip [vrouter vrouter-name]

- **server-ip** – 指定DNS64服务器的IP地址，该IP地址只能为IPv4地址。
- **vrouter-name** – 指定DNS64服务器所属的虚拟路由器。

使用**no server server-ip [vrouter vrouter-name]** 删除DNS64服务器。

配置DNS64前缀

用户需要指定DNS64前缀来用于将A记录（IPv4地址）合成AAAA记录（IPv6地址），合成的IPv6地址为“DNS64前缀+IPv4地址”形式。默认情况下，DNS64前缀为“64:ff9b::/96”。指定DNS64前缀以及前缀长

度，在DNS64配置模式下，使用以下命令：

prefix *ipv6-address/prefix*

- *ipv6-address* – 指定DNS64前缀地址。
- *prefix* – 指定前缀长度。取值范围为1到96。

使用**no prefix** *ipv6-address/prefix*取消DNS64前缀的配置。

配置描述信息

对DNS代理规则添加描述信息，在DNS代理规则配置模式下，使用以下命令：

description *description*

- *description* – 指定描述信息，如规则的作用。取值范围是0到127个字符。

使用**no description**删除描述信息。

启用/禁用DNS代理规则

默认情况下，配置完成的DNS代理规则会在系统中立即生效。用户可以通过命令禁用某条规则，使其不对流量进行控制。禁用或者启用某条规则，在DNS代理规则配置模式下，使用以下命令：

- **disable** - 禁用DNS代理规则。
- **enable** - 启用DNS代理规则。

修改DNS代理规则的排列顺序

DNS代理规则通过ID进行唯一标识。DNS请求到达设备后，设备对DNS代理规则进行顺序查找，然后按照查找到的相匹配的第一条规则对DNS请求进行处理。但是，DNS代理规则ID的大小顺序并不是规则查找时的匹配顺序。使用**show dns-proxy**命令列出的规则顺序才是规则匹配顺序（系统将由上到下进行查找匹配）。默认情况下，系统会将新创建的DNS代理规则放到所有规则的末尾，用户可以修改DNS代理规则的排列位置。DNS代理规则的排列位置可以是绝对位置，即处在首位（Top）或者处在末位（Bottom），也可以是相对位置，即位于某个ID之前或之后。修改规则排列顺序，在全局配置模式下，使用以下命令：

dns-proxy move *rule-id* {**top** | **bottom** | **before** *rule-id* | **after** *rule-id*}

- **move** *rule-id* – 指定需排列顺序的DNS代理规则的ID。

- **top** | **bottom** | **before rule-id** | **after rule-id** – 指定DNS代理规则的位置。默认情况下，系统会将新创建的DNS代理规则放到所有规则的末尾。
- **top** – 指定DNS代理规则的位置为所有规则的首位。
- **bottom** – 指定DNS代理规则的位置为所有规则的末尾。
- **before rule-id** – 指定DNS代理规则的位置为某个规则ID之前。
- **after rule-id** – 指定DNS代理规则的位置为某个规则ID之后。

配置DNS代理服务器探测功能

DNS代理服务器探测功能即对DNS代理服务器的可达性进行检测。配置该功能后，系统将按照指定的探测间隔周期性地对DNS代理服务器进行探测，并且及时将不可达的服务器IP地址从DNS解析列表中删除，待链路恢复后再重新加入到轮询解析列表。默认情况下，DNS解析探测功能是开启的。配置DNS代理服务器探测的探测间隔，在全局配置模式下使用以下命令：

dns-proxy server-track [*interval interval-time*]

- *interval-time* – 指定DNS代理解析探测的探测间隔。取值范围为3至60s，默认值为10s。

在全局配置模式下，使用**no dns-proxy server-track**关闭DNS代理解析探测功能。

开启/关闭DNS代理的UDP报文校验和功能

ADC设备开启DNS代理功能后，DNS代理的UDP报文校验和功能默认情况下是开启的，即UDP报文头部经过更改后设备会重新计算UDP校验和。用户如果希望提高设备的性能，可以关闭DNS代理UDP报文校验和功能，设备将不再进行UDP校验和的计算。开启/关闭DNS代理的UDP报文校验和功能，在全局配置模式下使用以下命令：

- 开启DNS代理的UDP报文校验和功能：**dns-proxy udp-checksum enable**
- 关闭DNS代理的UDP报文校验和功能：**dns-proxy udp-checksum disable**

指定DNS代理响应报文的TTL

DNS代理响应报文的TTL(Time-to-Live)是指域名解析记录在DNS客户端上的保存时间。设置DNS代理响应报文的TTL，在全局配置模式下使用以下命令：

dns-proxy ttl *ttl-time*

- *ttl-time* – 指定DNS代理响应报文的TTL。如果超过设定的TTL值，DNS客户端上缓存的域名解析记录将被清除。取值范围是30到600秒，默认值是60。

使用**dns-proxy ttl disable**关闭修改报文TTL值的功能。

查看DNS代理规则信息

用户可以在任何模式下，通过show命令查看DNS代理规则的具体信息。具体命令以下：

```
show dns-proxy [rule id rule-id]
```

- *rule-id* – 显示指定DNS代理规则的详细信息。如果不指定名称则显示所有DNS代理规则。

解析

用户可以为设备的DNS功能设置DNS请求重试次数、DNS请求响应超时时间、DNS响应报文的TTL和负载均衡分发DNS请求。

设置DNS请求的响应超时时间

设备向DNS服务器发送DNS请求后，会等待DNS服务器的DNS响应，如果一定时间内，仍没有响应，设备会再次发送请求。该命令指定设备再次发送请求前，等待响应的的时间。设置DNS请求的响应超时时间，在全局配置模式下，使用以下命令：

```
ip domain timeout timeout-value
```

- *timeout-value* – 指定超时时间。取值范围为1到3秒。默认超时时间为2秒。

使用no ip domain timeout恢复默认超时时间。

设置DNS请求重试次数

当设备发送DNS请求时，如果在超时时间内得不到对方的DNS响应，设备会再次发出DNS请求。该命令设置的是发送DNS请求的重试次数。如果在指定的重试次数内仍得不到响应，设备会向下一个DNS服务器发送DNS请求。设置重试次数，在全局配置模式下，使用以下命令：

```
ip domain retry times
```

- *times* – 指定重试次数。取值范围为1到3次。默认重试次数为2次。

使用no ip domain retry恢复默认重试次数。

指定链路权值

用户可以设置出接口通过ISP链路流量的权值大小，设备根据已设定的权值按比例发送DNS请求到ISP链路上的DNS服务器。

设备有以下三种获取设备DNS域名地址的方法：

- 静态设置DNS域名地址
- 通过DHCP方式获取DNS域名地址
- 通过PPPoE方式获取DNS域名地址

静态设置DNS域名地址时，用户可以在全局配置模式下使用以下命令设置链路权值：

```
ip name-server server-ip1 [server-ip2] ... [server-ip6] [vrouter vrouter-name] [egress-interface interface-name [weight weight-value]]
```

- *server-ip1* [*server-ip2*] ... [*server-ip6*] – 指定DNS域名服务器的IP地址。用户最多可配置6个域名服务器。用户可以使用一条命令配置6个域名服务器，也可分多条命令配置。
- *vrouter-name* – 为VRouter指定DNS域名服务器。
- *interface-name* – 指定出接口的名称。
- *weight-value* – 指定出接口通过ISP链路流量的权值大小，权值决定负载均衡中流量转发的比例。取值范围为0到255。默认值为0，表示不参与负载均衡。

通过DHCP方式获取DNS域名地址时，用户可以在接口配置模式下，使用以下命令设置链路权值：

```
dhcp-client dns weight weight-value
```

- *weight-value* – 指定出接口通过ISP链路流量的权值大小，权值决定负载均衡中流量转发的比例，取值范围为0到255分钟。默认值为0，表示不参与负载均衡分发。

通过PPPoE方式获取DNS域名地址（请参考“[PPPoE配置](#)”）时，用户可以进入PPPoE实例配置模式，使用以下命令设置链路权值：

```
dns weight weight-value
```

- *weight-value* – 指定出接口通过ISP链路流量的权值大小，权值决定负载均衡中流量转发的比例，取值范围为0到255分钟，默认值为0，表示不参与负载均衡分发。

指定DNS解析动态缓存的TTL

TTL(Time-to-Live)是域名解析动态缓存在设备上的保存时间。设置DNS解析动态缓存的TTL，在全局配置模式下使用以下命令：

```
ip domain ttl ttl-time
```

- *ttl-time* – 指定DNS解析动态缓存的TTL。如果超过设定的TTL值，系统将清除设备上缓存的域名解析记录。取值范围是60到600秒。默认值是60。

开启DNS解析日志功能

用户可以通过开启记录DNS解析日志功能，将DNS解析结果进行记录，并且生成日志信息，日志内容包括域名、解析后的IP地址以及生成时间。默认情况下，该功能是关闭的。开启记录DNS解析日志功能，在全局配置模式下，使用以下命令：

```
ip domain response-log
```

使用`no ip domain response-log`关闭记录DNS解析日志功能。

缓存

在使用DNS功能过程中，系统可以将DNS映射条目储存到缓存中以提高查找速度。系统有以下三种获得DNS映射条目的方法：

- 动态获得：来自DNS响应。
- 静态获得：手动添加DNS映射条目到缓存。
- 注册获得：设备的一些功能模块，例如NTP、AAA和地址簿等，定义的DNS主机。

用户可以通过命令添加静态DNS映射条目到缓存、查看系统的DNS映射条目以及清除DNS动态映射条目。

添加静态DNS映射条目

手动添加DNS映射条目到缓存，在全局配置模式使用以下命令：

```
ip host host-name { address1 [address2] ... [address8] } [vrouter vrouter-name]
```

- *host-name* – 指定主机名称。名称范围是1到255个字符。
- {*address1* [*address2*] ... [*address8*]} – 指定主机的IP地址。最多可设置8个IP地址。
- *vrouter-name* – 添加指定VRouter下的DNS映射条目。

使用**no ip host** *host-name*删除指定的静态DNS映射条目。

查看DNS映射条目

使用show命令可以查看系统中所有的DNS映射条目。查看DNS映射条目，在任何模式下使用以下命令：

show ip hosts [*host-name*] [**vrouter** *vrouter-name*]

- *host-name* – 显示指定主机的DNS映射条目。
- *vrouter-name* - 显示指定VRouter下的DNS映射条目。

清除动态DNS映射条目

手动清除动态DNS映射条目，在执行模式下使用以下命令。

clear host [*host-name* [**vrouter** *vrouter-name*]]

- *host-name* – 清除指定主机的DNS映射条目。
- *vrouter-name* – 清除指定VRouter下主机的DNS映射条目。

该命令用来清除指定的或者所有动态DNS映射条目。手工配置的静态DNS映射项使用**no ip host**命令清除。

DNS Snooping

开启DNS Snooping功能后，当DNS流量经过设备时，系统可对DNS响应报文中的域名进行探测。若探测到的域名与地址簿中已配置的域名相匹配，系统将自动建立监测列表，同时将监测列表中的IP地址下发到地址簿。下发成功后，用户可以通过策略路由引用地址簿的信息，使流量按指定链路转发。



注意: 使用DNS Snooping功能前，请先在地址簿中配置精确域名或通配符域名。关于如何配置，请参考[配置地址簿](#)。

DNS Snooping支持通过以下两种域名解析方式获取域名和IP地址映射关系：

- 主动模式（Active mode）：设备向配置的域名服务器（Name server）定期发送DNS查询报文，获取域名和IP地址映射关系信息。
- 被动模式（Passive mode）：系统监测经过设备的DNS响应报文，获取域名和IP地址映射关系信息。

DNS Snooping的配置包括：

- 指定域名解析方式
- 指定精确域名最大映射IP数
- 指定转发响应报文延时时间
- 指定最大通配符域名数
- 指定DNS Snooping映射缓存TTL
- 查看DNS Snooping配置信息
- 查看DNS Snooping域名及IP映射信息

指定域名解析方式

指定DNS Snooping的域名解析方式，在全局配置模式下使用以下命令：

dns snooping mode {active | passive | all}

- **active** – 指定DNS Snooping的域名解析方式为主动模式（Active mode）。该方式下，设备向配置的域名服务器（Name server）定期发送DNS查询报文，获取域名和IP地址映射关系信息，并将IP地址返回到引用该域名的功能模块。
- **passive** – 指定DNS Snooping的域名解析方式为被动模式（Passive mode）。该方式下，系统监测经过设备的DNS响应报文，获取域名和IP地址映射关系信息，并将IP地址返回到引用该域名的功能模块。
- **all** – 指定DNS Snooping的域名解析方式为主动模式（Active mode）和被动模式（Passive mode），IP地址为两种方式解析出的IP地址的并集。该值为默认值。

使用**no dns snooping mode**命令恢复默认值。

指定精确域名最大映射IP数

当域名解析方式为被动模式时，用户可以指定每个精确域名可以映射的最大IP数量。指定每个精确域名可以映射的最大IP数量，在全局配置模式下使用以下命令：

dns snooping host-ip-num *number*

- *number* – 指定每个精确域名可以映射的最大IP数量。取值范围为32到256，默认值为64。

使用**no dns snooping host-ip-num**命令恢复默认值。

指定转发响应报文延时时间

当DNS Snooping接收到DNS响应报文，并且需要更新域名和IP地址映射关系时，支持延时转发DNS响应报文给客户端，使客户端延迟一段时间获取IP地址。指定延时转发时间，在全局配置模式下使用以下命令：

dns snooping pak-delay *time*

- *time* – 指定延时转发时间。取值范围为0到2000毫秒，默认值为5毫秒。

使用**no dns snooping pak-delay**命令恢复默认值。

指定最大通配符域名数

系统支持通配符域名（如“*.test.com”）解析，用户可以指定系统支持的最大通配符域名数量。指定系统支持的最大通配符域名数，在全局配置模式下使用以下命令：

dns snooping wildcard-num *number*

- *number* – 指定系统支持的最大通配符域名数量。取值范围为128到512，默认值为128。

使用**no dns snooping wildcard-num**命令恢复默认值。



注意：系统只支持通过被动模式对通配符域名进行解析。

指定DNS Snooping映射缓存TTL

TTL(Time-to-Live)是域名解析映射信息缓存在设备上的保存时间。设置DNS Snooping映射缓存的TTL，在全局配置模式下使用以下命令：

```
dns snooping ttl ttl-value
```

- *ttl-value* - 指定DNS Snooping映射缓存的TTL。取值范围是60到3600秒。默认值是3600秒。

使用`no dns snooping ttl`命令恢复默认值。



注意: 系统将定期清除设备上达到域名IP映射缓存超时时间的缓存信息：

- 被动模式下，域名IP映射缓存超时时间=响应报文TTL+指定的DNS Snooping TTL；
- 主动模式下，域名IP映射缓存超时时间=系统DNS缓存TTL。关于的配置，请参阅[指定DNS解析动态缓存的TTL](#)。

查看DNS Snooping配置信息

用户通过`show`命令查看DNS Snooping的配置信息，包括域名解析方式、TTL、精确域名映射的最大IP数、最大通配符域名数、转发响应报文延时时间以及最大精确域名数。在任何模式下使用以下命令：

```
show dns snooping configuration
```

查看DNS Snooping域名及IP映射信息

用户可以通过`show`命令查看DNS Snooping域名及IP映射关系信息。在任何模式下使用以下命令：

```
show dns snooping domain {active | passive} [domain-name][vrouter vrouter-name]
```

- **active | passive** - 查看通过主动模式（**active**）或者被动模式（**passive**）获取的域名及IP映射关系信息。
- *domain-name* - 查看指定域名的IP映射关系信息。
- *vrouter-name* - 查看指定虚拟路由器下的域名及IP映射信息。

开启/关闭DNS功能

默认情况下，DNS功能是开启的。开启/关闭DNS功能，在全局配置模式下使用以下命令：

- 开启： `ip domain lookup`
- 关闭： `no ip domain lookup`

开启DNS解析日志功能

用户可以通过开启记录DNS解析日志功能，将DNS解析结果进行记录，并且生成日志信息，日志内容包括域名、解析后的IP地址以及生成时间。默认情况下，该功能是关闭的。开启记录DNS解析日志功能，在全局配置模式下，使用以下命令：

`ip domain response-log`

使用`no ip domain response-log`关闭记录DNS解析日志功能。

显示DNS配置信息

用户可以在任何模式下使用以下命令查看系统中DNS的配置信息：

`show dns`

DHCP

DHCP为动态主机配置协议（Dynamic Host Configuration Protocol）的缩写。DHCP能够自动为子网分配适当的IP地址以及相关网络参数，从而减少网络管理需求。同时，DHCP能够保证不会出现地址冲突，能够重新分配闲置资源。

系统支持DHCP客户端功能、DHCP服务器功能和DHCP中继代理功能。

- DHCP客户端：设备的接口可以设置成DHCP客户端，从DHCP服务器动态获得IP地址及网络参数配置。
- DHCP服务器：设备的接口可以设置成DHCP服务器，通过配置的地址池，向与该接口相连的主机分配IP地址及网络参数。
- DHCP中继代理：设备的接口可以设置成DHCP中继代理，中继代理从DHCP服务器获得DHCP信息，然后将获得信息传递到与接口相连的主机。

虽然设备同时具有以上三种DHCP功能，但是在为设备配置DHCP功能时，一个接口只能配置一种功能。

配置DHCP客户端功能

用户可以将设备的接口配置成DHCP客户端，从DHCP服务器获得IP地址。接口的DHCP客户端配置需要在接口配置模式下进行。DHCP客户端配置包括：

- 配置DHCP方式获取IP地址
- 释放和重新获取IP地址
- 配置路由优先级（管理距离）和路由权值

配置DHCP方式获取IP地址

使接口通过DHCP方式获取IP地址，在接口配置模式下使用以下命令：

ip address dhcp [setroute]

- **setroute** – 将DHCP服务器提供的网关信息设置为默认网关路由。

使用**no ip address dhcp**取消接口的DHCP获取IP地址方式。

例如，将ethernet0/1设置为动态DHCP方式获取IP地址，并且设置默认网关路由，请使用以下命令：

```
hostname(config)# interface ethernet0/1

hostname(config-if-eth0/1)# zone untrust

hostname(config-if-eth0/1)# ip address dhcp setroute

hostname(config-if-eth0/1)# exit

hostname(config)#
```

释放和重新获取IP地址

通过DHCP动态获取IP地址的接口可以释放已经获得的IP地址，然后重新获取IP地址。释放和重新获取IP地址，在接口配置模式下使用以下命令：

- 释放：**dhcp-client ip release**
- 重新获取：**dhcp-client ip renew**

设备提供命令查看接口获取的DHCP IP地址信息。在接口配置模式下，使用以下命令：

`dhcp-client ip show`

配置路由优先级（管理距离）和路由权值

DHCP接口设置了默认路由后（`ip address dhcp setroute`），用户可以设置路由优先级（管理距离）和路由权值。在接口配置模式下，使用以下命令：

`dhcp-client route {distance value | weight value}`

- **distance value** – 指定路由优先级。范围是1到255，默认值是1。
- **weight value** – 指定路由权值。范围是1到255，默认值是1。

使用`no dhcp-client route {distance | weight}`命令恢复路由优先级和路由权值的默认值。

配置DHCP服务器功能

设备可以作为DHCP服务器为子网中DHCP客户端设备分配IP地址。DHCP服务器功能需要在DHCP服务器配置模式下进行。进入DHCP服务器配置模式，在全局配置模式下使用以下命令：

`dhcp-server pool pool-name`

- *pool-name* – 指定DHCP地址池名称。

执行该命令后，系统新建一个DHCP地址池，并且进入该地址池的DHCP服务器配置模式；如果指定的地址池名称已存在，则直接进入相应的DHCP服务器配置模式。

使用`no dhcp-server pool pool-name`命令删除指定的DHCP地址池。

用户在DHCP服务器配置模式下可操作的DHCP服务器功能配置包括：

- DHCP地址池基本配置
- 配置自动配置功能
- 为DHCP客户端配置DNS、WINS服务器和域名
- 为DHCP客户端配置SMTP、POP3和新闻服务器
- 配置中继代理IP地址
- IP-MAC地址绑定
- 配置DHCP选项

DHCP服务器地址池配置完毕，用户需要将配置的DHCP地址池绑定到接口，才能在接口开启DHCP服务器功能。具体命令描述请参考：

- 绑定地址池到接口

并且，用户可以通过相应的show随时查看系统的DHCP配置。

DHCP地址池基本配置

DHCP地址池的基本配置有：IP地址配置、保留地址池配置、网关配置、网络掩码配置以及DHCP租约配置。

IP地址配置

用户需要指定IP地址范围用来对外分配。指定地址池的IP地址范围，在DHCP服务器配置模式下，使用以下命令：

```
address start-ip-address [end-ip-address]
```

使用**no address** *start-ip-address*命令取消指定的IP地址范围。

保留地址池配置

保留地址池中的IP地址为地址池中的部分IP地址，作为DHCP服务器保留使用，不进行分配。配置保留地址池，在DHCP服务器配置模式下，使用以下命令：

```
exclude address start-ip-address [end-ip-address]
```

- *start-ip-address* – 指定保留地址池的起始IP地址。
- *end-ip-address* – 指定保留地址池的结束IP地址。

使用**no exclude address** *start-ip-address*命令取消指定的IP地址范围。

网关配置

该命令为客户端配置网关IP地址。在DHCP服务器配置模式下，使用以下命令：

```
gateway ip-address
```

- *ip-address* – 指定网关的IP地址。

使用**no gateway**命令取消网关IP地址的配置。

网络掩码配置

该命令为客户端配置网络掩码。在DHCP服务器配置模式下，使用以下命令：

netmask *netmask*

- *netmask* – 指定网络掩码，例如，255.255.255.0。

使用**no netmask**命令取消网络掩码的配置。

DHCP租约配置

租约为客户端从获得IP地址开始，能够使用该IP地址的时间，租约到期后，客户端需要重新向DHCP服务器申请IP地址。配置DHCP服务器的租约，在DHCP服务器配置模式下，使用以下命令：

lease *lease-time*

- *lease-time* – 指定租约时间，单位为秒。范围是300到1048575秒。默认是3600秒。

使用**no lease**命令恢复租约的默认值。

配置自动配置功能

自动配置功能在以下条件下能够起效：配置了DHCP服务器功能的设备上有另外一个接口启用了DHCP客户端功能。此时，配置了自动配置功能后，DHCP服务器（设备）如果没有配置DNS、WINS和域名，DHCP客户端（设备）会把从与自己相连的DHCP服务器上获取的DNS、WINS和域名信息下发给通过DHCP服务器（设备）获得信息的主机。但是，通过命令手工配置的DNS、WINS和域名具有高优先级。配置自动配置功能，在DHCP服务器配置模式下，使用以下命令：

auto-config interface *interface-name*

- *interface-name* – 同一台设备上开启了DHCP客户端功能的接口名称。

使用**no auto-config**命令取消自动配置功能。

为DHCP客户端配置DNS、WINS服务器和域名

为DHCP客户端配置DNS、WINS服务器和域名，在DHCP服务器配置模式下，使用以下命令：

dns *ip-address1* [*ip-address2*]

- *ip-address1* – 指定主DNS服务器的IP地址。
- *ip-address2* – 指定备用DNS服务器的IP地址。

wins *ip-address1* [*ip-address2*]

- *ip-address1* – 指定主WINS服务器的IP地址。
- *ip-address2* – 指定备用WINS服务器的IP地址。

domain *domain-name*

- *domain-name* – 指定域名。

使用以下命令取消DNS、WINS服务器以及域名的配置：

no dns

no wins

no domain

为DHCP客户端配置SMTP、POP3和新闻服务器

为DHCP客户端配置SMTP、POP3和新闻服务器，在DHCP服务器配置模式下，使用以下命令：

smtp *ip-address*

pop3 *ip-address*

news *ip-address*

使用以下命令取消SMTP、POP3和新闻服务器的配置：

no smtp

no pop3

no news

配置中继代理IP地址

当配有DHCP服务器功能的设备（设备1）与另一台配有DHCP中继代理功能的设备（设备2）相连，且PC通过设备2获得设备1的DHCP信息时，用户必须在设备1上配置中继代理IP地址和掩码，才能够成功传输DHCP信息到PC。在DHCP服务器配置模式下，使用以下命令：

relay-agent ip-address netmask

- *ip-address netmask* – 指定中继代理的IP地址和掩码，即设备2上启用中继代理功能的接口的IP地址和掩码。

使用**no relay-agent ip-address netmask**命令取消中继代理IP地址的配置。

IP-MAC地址绑定

用户可以手动将IP与MAC地址绑定，这样，绑定的IP地址只能分配该指定的MAC地址。配置IP-MAC绑定，在DHCP服务器配置模式下，使用以下命令：

ipmac-bind ip-address mac [description description]

- *ip-address* – 指定IP地址。IP地址必须是IP地址池中的地址。
- *mac* – 指定与IP地址绑定MAC地址。
- **description description** – 指定IP-MAC地址绑定的描述信息。范围是1到63个字符。

使用**no ipmac-bind ip-address**命令取消指定IP与MAC地址的绑定。

绑定地址池到接口

绑定地址池到接口后，接口会按照地址池中配置的参数值运行DHCP服务器功能。绑定地址池到接口，在接口配置模式下，使用以下命令：

dhcp-server enable pool pool-name

- *pool-name* – 指定已配置的地址池的名称。

使用**no dhcp-server enable**关闭接口的DHCP服务器功能。

配置DHCP选项

设备接口配置成DHCP服务器时，系统支持解析DHCP报文中的Option 60字段，Option 138字段,以及Option 49字段。

配置Option 49

通过配置Option49，DHCP客户端可以获取到运行X window System Display Manager的系统的IP地址列表。用户最多可配置6条IP地址。

配置Option 49，在DHCP服务器配置模式下，使用以下命令：

option 49 ip ip-address

- *ip-address* – 指定运行X window System Display Manager的系统的IP地址。

使用**no option 49 ip ip-address**取消Option 49的相关配置。

配置Option 60

Option 60 是由客户端设备在形成DHCP 报文时写入的，用以标识客户端的类型或配置。Option 60 包含n 字节的信息，这些信息是由DHCP 服务器解析的。设备供应商可以选择定义特定的VCI（Vendor Class Identifier）来传达特定的配置或其他客户端的识别信息。

用户可配置如下功能：

- 对客户端Option 60字段携带的VCI验证，通过验证后，下发IP地址等相关信息；
- 设置DHCP服务器Option 60字段携带的VCI。

验证客户端Option 60字段携带的VCI

用户可在DHCP服务器端验证客户端DHCP报文的Option 60字段携带的VCI。当DHCP报文的VCI与DHCP服务器指定的VCI验证字符串相同时，DHCP服务器下发IP地址等配置信息；不相同，DHCP服务器丢弃相关报文，不进行回复。当DHCP服务器不设置VCI验证字符串时，DHCP服务器将忽略客户端Option 60的属性值。为DHCP服务器设置VCI验证字符串，在DHCP服务器配置模式下，使用如下命令：

vci-match-string {ascii value| hex value}

- **ascii value** – 指定ASCII类型的VCI验证字符串。如果包含空格，需要用双引号包括此字符串。
- **hex value** – 指定十六进制类型的VCI验证字符串。

在每个指定DHCP服务器配置模式下，系统只支持设定一个VCI验证字符串，后续配置的VCI验证字符串将会自动覆盖之前配置的。

取消VCI验证字符串设置，使用**no vci-match-string**命令。

设置DHCP服务器Option 60字段携带的VCI

设置DHCP服务器Option 60字段携带的VCI后，DHCP服务器所发送的报文将携带此选项及VCI。设置DHCP服务器Option 60字段携带的VCI，在DHCP服务器配置模式下，使用如下命令：

option 60 {*ascii value* | *hex value*}

- *ascii value* – 指定ASCII类型的VCI。如果包含空格，需要用双引号包括此属性值。
- *hex value* – 指定十六进制类型的VCI。

取消Option 60携带的VCI设置，使用**no option 60**命令。

配置Option 138

DHCP服务器使用Option 138下发CAPWAP AC (Access Control)的列表给WTP（Wireless Terminal Point）。此列表包含一个或多个可用的CAPWAP AC的IP地址。WTP通过获取Option 138字段中的AC地址来查找并连接AC。

若DHCP服务器端未设置Option 138或DHCP客户端未进行请求，DHCP服务器端将不下发Option 138的信息。

配置Option 138添加CAPWAP AC的IP地址，在DHCP服务器配置模式下，使用如下命令：

option 138 ip *A.B.C.D*

- *A.B.C.D* – 指定CAPWAP AC的IP地址。

重复使用上述命令配置多个CAPWAP AC。每个DHCP Server最多支持设置4个CAPWAP AC。

取消CAPWAP AC的指定，使用**no option 138 ip** *A.B.C.D*命令。

查看DHCP配置信息

用户可以通过以下show命令查看DHCP地址池的绑定信息、配置信息或统计信息。

show dhcp-server {*binding* | *pool* | *statistics*} *pool-name*

- **binding** *pool-name* – 显示DHCP服务器的绑定信息。
- **statistics** *pool-name* – 显示DHCP服务器的统计信息。
- **pool** *pool-name* – 显示DHCP服务器的地址池信息。

配置DHCP中继代理功能

设备可以作为DHCP中继代理，接受DHCP客户端请求，并且将请求发送到DHCP服务器，然后将从DHCP服务器获得DHCP信息再返回给DHCP客户端。DHCP中继代理功能需要在接口配置模式下完成，包括：

- 指定DHCP服务器的IP地址
- 开启接口的DHCP中继代理功能

指定DHCP服务器的IP地址

指定DHCP服务器的IP地址，在接口配置模式下，使用以下命令：

```
dhcp-relay server ip-address
```

- *ip-address* – 指定DHCP服务器的IP地址。

使用**no dhcp-relay server** *ip-address*命令取消对DHCP服务器IP地址的配置。

开启接口的DHCP中继代理功能

开启接口的DHCP中继代理功能，在接口配置模式下，使用以下命令：

```
dhcp-relay enable
```

使用**no dhcp-relay enable**命令关闭接口的DHCP中继代理功能。

DDNS

DDNS是动态域名服务（Dynamic Domain Name Server）的缩写，可以实现固定域名到动态IP地址之间的解析。通常情况下，用户每次连接因特网时都会从ISP得到一个动态IP地址，即用户每次连接因特网得到的IP地址都不同。动态域名解析功能可以将域名绑定到用户的动态IP地址，每次当用户连接到因特网时，它都会自动更新自己的动态IP与域名的绑定。

在使用DDNS功能之前，用户需要在DDNS服务的提供商那里进行注册，以获取动态域名。设备支持以下三个动态域名服务提供商：

- 3322.org: <http://www.3322.org>
- Huagai.net: <http://www.ddns.com.cn>
- ZoneEdit.com: <http://www.zoneedit.com>

请访问相应的主页进行注册。

配置DDNS功能

当设备的外网接口IP地址发生变化后，设备会向DDNS服务器发送更新请求（HTTP方式），来更新IP地址与域名的绑定。用户可以在设备上配置不同的DDNS服务名称，然后为DDNS服务名称配置DDNS参数，例如更新方式、DDNS服务器和更新间隔时间等，最后将配置的DDNS服务名称绑定到接口上，从而启用DDNS功能。

- 配置DDNS服务名称
- 绑定DDNS服务名称到接口

配置DDNS服务名称

DDNS服务参数配置需要在DDNS服务名称配置模式下完成。在全局配置模式下，使用以下命令，用户可以创建一个DDNS服务名称、指定其更新类型并且进入指定的DDNS服务配置模式：

```
ddns name ddns-name type http
```

- *ddns-name* - 指定DDNS服务名称。
- *type http* - 指定DDNS服务的更新方式，即发送DDNS更新请求的方式，为HTTP。

运行该命令后，CLI进入该DDNS服务名称的配置模式，用户可以为该DDNS服务名称配置各种DDNS参数，包括DDNS服务器类型、DDNS服务器名称和端口号、最小更新间隔、最大更新间隔以及DDNS用户名称密码。

使用**no ddns name *ddns-name* type http**命令删除指定的DDNS服务名称。

指定DDNS服务器类型

设备支持通过五个DDNS服务商实现动态域名服务，分别是3322.org、Huagai.net、ZoneEdit.com、no-ip.com和dyndns.org。指定DDNS服务商，在DDNS服务名称配置模式下使用以下命令：

```
type {dyndns | huagai | no-ip | qdns | zoneedit}
```

- **dyndns** - 指定dyndns.org作为DDNS服务商。
- **huagai** - 指定Huagai.net作为DDNS服务商。
- **no-ip** - 指定no-ip.com作为DDNS服务商。

- **qdns** - 指定3322.org作为DDNS服务商。
- **zoneedit** - 指定ZoneEdit.com作为DDNS服务商。

使用**no type**命令取消对DDNS服务商的指定。

指定DDNS服务器名称和端口号

不同的DDNS服务器具有不同的服务器名称和端口号。指定DDNS服务器的名称和端口号，在DDNS服务名称配置模式下使用以下命令：

server name *server-name* **port** *port-number*

- *server-name* - 指定所配置DDNS服务器相应的服务器名称。
- *port-number* - 指定所配置DDNS服务器相应的服务器端口号。范围是1到65535。

使用**no server**命令取消DDNS服务器名称和服务器端口号的配置。



注意: 此处配置的名称和端口号必须为DDNS服务器相对应的名称和端口号。如果不知道确切信息，请勿配置该命令。与DDNS服务器连接成功后，服务器会自动将服务器名称和端口号信息一并返回。

指定最小更新间隔

启用DDNS功能的接口的IP地址发生变化后，设备需要向DDNS服务器发送更新请求。如果发送的请求没有响应，设备会根据此处配置的最小更新间隔再次发送请求。例如，设置最小更新间隔为5分钟，当第一次失败后，设备会在5分钟后发出第二次请求，如果再次失败，设备会在10（5x2）分钟后再次发出请求，再次失败，则在20（10x2）分钟后发出请求，以此类推，直到时间为120分钟后，不再增加时间，即以固定的每隔120分钟发出一次请求。配置最小更新间隔时间，在DDNS服务名称配置模式下使用以下命令：

minupdate interval *time-value*

- *time-value* - 指定最小更新间隔时间，单位为分钟。取值范围为5到120分钟。默认值为5分钟。

使用**no minupdate**恢复默认最小更新间隔时间。

指定最大更新间隔

最大更新间隔为在无IP地址变化的情况下，设备在多长时间后向DDNS服务器发出一次更新请求。配置DDNS最大更新间隔，在DDNS服务名称配置模式下使用以下命令：

maxupdate interval *time-value*

- *time-value* - 指定最大更新间隔时间，单位为小时。取值范围为24到8760小时。默认值为24小时。

使用**no maxupdate**恢复默认最大更新间隔时间。

指定DDNS用户

该命令指定的是在DDNS服务提供商处注册的用户信息。配置用户信息，在DDNS服务名称配置模式下使用以下命令：

user *user-name* **password** *user-password*

- *user-name* - 在DDNS服务提供商处注册的用户名称。
- *user-password* - 与用户名称相对应的密码。

使用**no user**命令取消用户信息的指定。

绑定DDNS服务名称到接口

只有把配置的DDNS服务名称绑定到接口上，当接口IP地址发生变化时，域名才能够按照配置的DDNS参数进行更新。绑定接口到DDNS服务名称，在全局配置模式下，使用以下命令：

ddns enable *ddns-name* **interface** *interface-name* **hostname** *host-name*

- *ddns-name* - 指定配置好的DDNS服务名称。
- *interface-name* - 指定要绑定的接口的名称。
- *host-name* - 指定在相应DDNS提供商处申请得到的域名。

使用**no ddns enable** *ddns-name* **interface** *interface-name*取消接口与DDNS服务名称的绑定。

显示DDNS信息

用户可以在任何模式下，通过show命令查看DDNS信息：

显示DDNS服务配置信息：**show ddns config** *ddns-name*

显示DDNS服务状态信息：**show ddns state** *ddns-name*

PPPoE

PPPoE是以太网上点对点协议（Point-to-Point Protocol over Ethernet）的缩写。PPPoE结合PPP协议和以太网，在分配IP地址的同时，可以对客户端进行接入控制、验证以及计费等。

PPPoE协议的实现包括两个阶段：发现阶段和PPP会话阶段。

- 发现阶段：在发现阶段，客户端确定一个PPPoE访问集中器（Access Concentrator），获得其以太网MAC地址并建立起一个PPPoE会话标识符Session ID。
- PPP会话阶段：客户端与在发现阶段确定的访问集中器进行PPP协商。这个协商过程与标准的PPP协商相同。

设备的接口可以配置成PPPoE客户端，进行PPPoE连接。

配置PPPoE

设备允许用户配置多个PPPoE实例，然后把配置好的PPPoE实例绑定到接口，配置接口为PPPoE方式获取IP地址后，接口会按照PPPoE实例中配置的参数，进行PPPoE连接。用户可配置的设备的PPPoE功能包括：

- 配置PPPoE实例
- 绑定PPPoE实例到接口
- 配置接口使用PPPoE方式获得IP地址
- 手动连接或者断开PPPoE连接
- 显示PPPoE配置信息

配置PPPoE实例

PPPoE实例中配置的是各种PPPoE参数，包括访问集中器、验证方式、PPPoE连接方式、网络掩码、路由距离和权值、服务、静态IP、PPPoE用户信息、时间表功能以及DNS服务器优先级。对PPPoE实例的配置，必须在PPPoE实例配置模式下进行。进入PPPoE实例配置模式，在全局配置模式下，使用以下命令：

pppoe-client group *group-name*

- *group-name* – 指定PPPoE实例的名称。执行该命令后，系统新建指定的PPPoE实例，并且进入该实例配置模式；如果指定的实例名称存在，则直接进入实例配置模式。

在全局配置模式下，使用**no pppoe-client group** *group-name*命令删除指定的PPPoE实例。

指定访问集中器

使用PPPoE连接，需要为设备指定访问集中器。指定访问集中器，在实例配置模式下，使用以下命令：

```
ac ac-name
```

- *ac-name* - 指定可使用的访问集中器的名称。

使用**no ac**命令取消对访问集中器的指定。

指定验证方式

设备与PPPoE服务器建立连接时，需要通过PPPoE验证。设备支持的验证方式有CHAP、PAP和Any三种。这里配置的验证方式必须与PPPoE服务器端的验证方式相同。指定验证方式，在实例配置模式下，使用以下命令：

```
authentication {chap | pap | any}
```

- **chap** - 指定验证方式为CHAP。
- **pap** - 指定验证方式为PAP。
- **any** - 指定验证方式为CHAP或者PAP任何一种。该选项为系统默认验证方式。

使用**no authentication**命令恢复默认验证方式。

配置PPPoE连接方式

PPPoE协议有两种连接方式，分别是：

- 自动连接方式：使用该方式，当PPPoE连接由于某些原因断开，且断开时间到达一定的时间，即为用户指定的自动连接时间，系统会自动重拨。
- 按需拨号方式：使用该方式，当PPPoE接口的空闲（无流量）时间到达一定的时间，即用户指定的空闲时间，系统会断开与因特网的连接；当产生上网需求时，系统会自动连接到因特网。

以上两种方式是互斥的。在未配置时间表功能的情况下，系统默认选用按需方式，而如果用户对两种方式都做了配置，系统会使用自动连接方式。

指定自动连接时间，在实例配置模式下，使用以下命令：

```
auto-connect time-value
```

- *time-value* - 指定自动连接的时间，单位为秒。范围是0到10000秒。默认值是0，表示关闭自动连接功能。

使用**no auto-connect**命令恢复默认自动连接值。

指定空闲时间，在实例配置模式下，使用以下命令：

idle-interval *time-value*

- *time-value* - 指定空闲时间，单位为分钟。范围是0到10000分钟。默认值是30分钟。

使用**no idle-interval**命令恢复默认空闲时间值。

指定网络掩码

用户可以为PPPoE方式获得的IP地址指定网络掩码。指定网络掩码，在实例配置模式下，使用以下命令：

netmask *netmask*

- *netmask* - 指定网络掩码，例如255.255.0.0。

使用**no netmask**命令取消网络掩码的指定，此时将使用系统默认掩码255.255.255.255。

指定路由距离和权值

指定路由距离和权值，在实例配置模式下，使用以下命令：

route {**distance** *value* | **weight** *value*}

- **distance** *value* - 指定路由距离。范围是1到255，默认值是1。
- **weight** *value* - 指定路由权值。范围是1到255，默认值是1。

使用**no route** {**distance** | **weight**} 命令恢复路由距离和权值的默认值。

指定服务

指定允许的服务，在实例配置模式下，使用以下命令：

service *service-name*

- *service-name* - 指定服务。此处指定的服务必须与PPPoE服务器端提供的服务相同。如果不指定服务，设备自动接受服务器返回的任何服务。

使用**no service**取消对服务的指定。

指定静态IP

用户可以指定一个静态的IP地址，并协商使用该静态IP地址。这样可以避免IP地址变化。指定静态IP地址，在实例配置模式下，使用以下命令：

```
static-ip ip-address
```

- *ip-address* – 指定静态IP地址。

使用**no static-ip**取消对静态IP地址的指定。

指定PPPoE用户信息

指定用户信息，在实例配置模式下，使用以下命令：

```
user user-name password password
```

- *user-name* – PPPoE用户名称。
- *password* – 与用户名称相对应的密码。

使用**no user**取消对用户信息的指定。

配置时间表功能

设备支持时间表功能，用户可以为PPPoE实例指定一个时间表条目，令PPPoE接口在指定的时间内保持与因特网的连接，在指定的时间断开连接。配置时间表功能，在实例配置模式下，使用以下命令：

```
schedule schedule-name [disconnect | sch-auto-connection time-value | sch-idle-timeout time-value]
```

- *schedule-name* – 指定时间表条目的名称。
- *disconnect* – 如果选择该关键字，系统将在时间表条目指定的时间内断开PPPoE连接。
- **sch-auto-connection** *time-value* – 如果选择该关键字，系统将在时间表条目指定的时间内使用自动连接的方式连接因特网。*time-value*指定自动连接的时间，单位为秒。范围是0到10000秒。默认值是0，表示关闭自动连接功能。
- **sch-idle-timeout** *time-value* – 如果选择该关键字，系统将在时间表条目指定的时间内使用按需拨号方式连接因特网。*time-value*指定空闲时间，单位为分钟。范围是0到10000分钟。默认值是30分钟。

使用**no schedule**取消时间表配置。



注意: 关于如何配置时间表, 请参阅“[配置时间表](#)”部分。

指定PPPoE服务器MAC地址

如果已知PPPoE服务器的MAC地址, 用户可以在设备上指定PPPoE服务器的MAC地址, 使设备能够迅速连接到PPPoE服务器。指定PPPoE服务器MAC地址, 在实例配置模式下, 使用以下命令:

```
mac mac-address
```

- *mac-address* – 指定PPPoE服务器的MAC地址。

在实例配置模式下使用该**no mac**命令取消对PPPoE服务器MAC地址的配置:

配置连接状态检测

为检查PPPoE连接状态, 用户可以进行配置, 让设备向PPPoE服务器发送LCP Echo请求, 如果在超时时间结束时, 仍未收到来自PPPoE服务器的LCP Echo回应, 则再次发送请求, 如果发送次数达到设置的重试次数, 都未收到回应, 系统则判断与PPPoE服务器断开连接。此时, 设备的PPPoE接口将显示为断开状态。

配置超时时间, 在实例配置模式下, 使用以下命令:

```
ppp lcp-echo-timeout timeout-value
```

- *timeout-value* – 指定超时时间, 单位为秒。取值范围是1到1000秒。默认值是180秒。

在实例配置模式下使用该命令**no**的形式恢复超时时间的默认值:

```
no ppp lcp-echo-timeout
```

配置重试次数, 在实例配置模式下, 使用以下命令:

```
ppp lcp-echo-retries times
```

- *times* – 指定重试次数。取值范围是1到30次。默认值是10次。

在实例配置模式下使用该命令**no**的形式恢复重试次数的默认值:

```
no ppp lcp-echo-retries
```

配置接口使用PPPoE方式获得IP地址

配置接口使用PPPoE方式获得IP地址，在接口配置模式下，为接口指定安全域后，使用以下命令指定PPPoE方式：

```
ip address pppoe [setroute]
```

- **setroute** – 将PPPoE服务器提供的网关信息设置为默认网关路由。

使用**no ip address pppoe**取消接口的PPPoE获取IP地址方式。

绑定PPPoE实例到接口

将配置好的PPPoE实例绑定到接口，接口会按照实例中配置的PPPoE参数进行PPPoE连接。绑定PPPoE实例到接口，在接口配置模式下，使用以下命令：

```
pppoe enable group group-name
```

- *group-name* – 指定PPPoE实例的名称。

使用命令**no pppoe enable group**取消PPPoE实例与接口的绑定。

手动连接或者断开PPPoE连接

用户可以在任何时候断开PPPoE连接或者进行PPPoE连接。在全局配置模式下，使用以下命令连接或者断开PPPoE连接：

```
pppoe-client group group-name {connect | disconnect}
```

- *group-name* – 指定PPPoE实例的名称。
- *connect* – 进行PPPoE连接。
- *disconnect* – 断开PPPoE连接。

显示PPPoE配置信息

用户可以通过show命令查看PPPoE实例的参数信息以及连接状态。显示PPPoE配置信息，在任何模式下，使用以下命令：

```
show pppoe-client {all | group group-name}
```


- **all** – 显示所有PPPoE实例的信息。
- **group group-name** – 显示指定PPPoE实例的信息。

虚拟交换机

由于实际应用的需要，设备会让部分接口之间的数据包在二层转发域中做二层转发（称作透明应用模式），部分接口之间的数据包做三层转发（称作路由应用模式）。为了使用户能够灵活地配置这种二、三层混合应用模式，系统引入了虚拟交换机即Virtual Switch（VSwitch）的概念。默认情况下，系统有一个VSwitch，称作VSwitch1。用户每新建一个VSwitch，系统都会为VSwitch自动生成一个VSwitch接口（VSwitchIF）。通过把接口绑定到安全域，再把安全域绑定到VSwitch，用户可以把接口绑定到VSwitch。

一个VSwitch就是一个二层转发域，每个VSwitch都有自己独立的MAC地址表，因此VSwitch中的接口之间的数据包会被按照二层转发规则进行转发。在VSwitch中，用户可以方便地配置策略规则。VSwitch接口相当于实际交换机的上连口，通过VSwitch接口，数据包可以实现二层与三层之间的转发。



注意: 关于如何创建VSwitch、如何把接口绑定到域以及如何把域绑定到VSwitch，请参阅“[接口](#)”部分。

VSwitch中的转发规则

在一个VSwitch，即一个二层转发域中，系统通过源地址学习建立MAC地址转发表。每个VSwitch都有自己的MAC地址转发表。系统根据数据包的类型（IP数据包、ARP包和非IP且非ARP包），分别进行不同的处理。

对于IP数据包，系统遵循以下转发规则：

1. 收到数据包。
2. 学习源地址，更新MAC地址转发表。
3. 如果目的MAC地址是单播地址，则根据目的MAC地址查找出接口。这时又有以下两种情况：
 - 如果目的MAC地址为VSwitch接口的MAC地址，并且VSwitch接口有IP地址，则按照路由转发规则进行转发；若VSwitch接口没有IP地址，则丢弃。
 - 根据目的MAC地址找到出接口。如果找到的出接口是数据包的源接口，则丢弃该数据报，否则从出接口继续转发数据包。

如果在MAC地址表中没有找到出接口（未知单播），直接跳到第6步。

4. 根据入接口和出接口确定源域和目的安全域。
5. 查找策略规则。如果策略规则允许则转发数据包；如果策略规则不允许，则丢弃数据包。
6. 如果在MAC地址转发表中没有找到出接口（未知单播），系统则尝试将数据包发给VSwitch中的所有其它二层接口，此时的操作流程为：把其它的每一个二层接口做为出接口，二层接口所在的二层安全域作为目的域，查询策略规则，如果策略允许，则在该二层接口转发数据包，如果策略不允许，则丢弃数据包。概括地说，对未知单播的转发即为策略限制下的广播。对于广播和多播IP包的处理类似于对未知单播的处理，不同的是广播和多播IP包会被同时拷贝一份进行三层处理。

对于ARP包，广播包和未知单播包转发到VSwitch中的其它所有接口，同时，复制一份由ARP模块进行处理。

对于非IP包且非ARP包，用户可以在全局配置模式下通过配置**l2-nonip-action**命令指定处理方式。

l2-nonip-action {drop | forward}

- **drop** – 丢弃。
- **forward** – 转发。

查看MAC表信息

通过系统CLI，用户可以查看所有VSwitch或者某个指定接口的MAC表项，用户还可以清除所有VSwitch或者某个指定接口的MAC表项。查看MAC表信息，请在任何模式下使用以下命令：

show mac [generic] | [interface interface-name]

- **generic** – 显示MAC表的统计信息，包括共有多少MAC表项以及多少MAC表项正在使用中。
- **interface interface-name** – 指定显示某个特定接口的MAC表项。

清除MAC表项，请在执行模式下使用以下命令：

clear mac [interface interface-name]

配置VSwitch

系统有一个默认VSwitch，即VSwitch1，VSwitch1不能被删除。用户可以根据需要创建新的VSwitch，也可以随时查看VSwitch的配置信息。

用户在新建一个VSwitch的同时，也新建了与VSwitch相对应的VSwitch接口。创建VSwitch，在全局配置模式下，使用以下命令：

vswitch vswitch *Number*

- *Number* – 指定VSwitch的数字标识。Number的取值范围根据平台不同而不同。例如，命令vswitch vswitch2创建了名为VSwitch2的VSwitch，同时也创建了VSwitchif2接口，并且进入VSwitch2的配置模式。如果指定的VSwitch名称已存在，则直接进入VSwitch配置模式。

在全局配置模式下，使用以上命令no的形式删除指定的VSwitch及其对应的VSwitch接口：

no vswitch vswitch *Number*

查看VSwitch配置信息，在任何模式下使用以下命令：

show vswitch [*vswitch-name*]

- *vswitch-name* – 显示指定VSwitch的信息。

透明模式下的VLAN透传

在透明模式下，设备的物理接口上承载很多VLAN时，通常需要配置相应的子接口和二层转发域（VSwitch），来实现不同VLAN数据包的传输。使用这种配置方式，用户可以基于VLAN做策略规则，对流量进行细致控制，可是，VLAN越多，配置就越复杂。为简化配置，系统提供VSwitch下的VLAN透传功能，即不需要配置子接口，使带有VLAN ID的数据包通过设备后仍保留原有VLAN ID。

默认情况下，VSwitch的VLAN透传功能为关闭状态。开启VSwitch的VLAN透传功能，在VSwitch配置模式下，使用以下命令：

forward-tagged-packet

在VSwitch配置模式下，使用该命令no的形式关闭VSwitch的VLAN透传功能：

no forward-tagged-packet

VSwitch支持对QinQ技术中双重VLAN ID数据包的透传。开启该功能，在VSwitch配置模式下，使用以下命令：

forward-double-tagged-packet

在VSwitch配置模式下，使用该命令no的形式关闭VSwitch对QinQ技术中双重VLAN ID数据包的透传功能：

no forward-double-tagged-packet



注意: 配置和使用VSwitch的VLAN透传功能时，

- 包含有子接口的VSwitch不能开启VLAN透传功能；
- 已经开启VLAN透传的VSwitch中的二层安全域不能绑定子接口；
- 经过透传的带有VLAN ID的数据包不支持三层混合模式传输。
- SG-6000-AX3200S、SG-6000-AX1200S、SG-6000-AX520S、SG-6000-AX320S、SG-6000-AX320S-GM、SG-6000-AX220S、SG-6000-AX120S和SG-6000-AX120S-GM设备不支持对 QinQ技术中双重VLAN ID数据包的透传。

透明模式下的ARP功能

在透明模式下，设备默认没有启用ARP学习功能。用户可以手动开启或关闭ARP学习，以获得IP-MAC的绑定信息。开启或关闭ARP功能，在VSwitch配置模式下，使用以下命令：

- 开启：**arp-l2mode**
- 关闭：**no arp-l2mode**

配置NAT

NAT规则基于VRouter创建并生效。用户可以在VRouter配置模式下，创建SNAT规则、修改SNAT规则排列以及删除SNAT规则等。为缺省VR即trust-vr配置NAT，也可以使用NAT模式（在全局配置模式下，使用nat命令进入NAT配置模式）。

进入VRouter配置模式，在全局配置模式下使用以下命令：

```
ip vrouter vrouter-name
```

- *vrouter-name* – 指定VRouter的名称。

创建SNAT规则

SNAT规则指定是否对符合条件的流量的源IP地址做NAT转换，如果需要转换，则同时指定转换的地址和方式。配置做NAT转换的SNAT规则，在VRouter配置模式下使用以下命令：

snatrule [**id** *id*] [**ingress-interface** *interface-name*] [**beforeid** | **afterid** | **top**] **from** *src-address* **to** *dst-address* [**service** *service-name*] [**EIF** *egress-interface* | **evr** *vrouter-name*] [**traffic-group** *traffic-group-name*] **trans-to** { {**ip** *ip-address*| **addressbook** *trans-to-address* | **EIF-ip** } } **mode** {**static** | **dynamicip** | **dynamicport** [**sticky**]} [**log**] [**group** *group-id*] [**disable**] [**track** *track-name*] [**description** *description*]

- **id** *id* – 为SNAT规则指定ID号。每一条SNAT规则都有一个唯一的ID。如果不指定，系统会自动分配。如果指定的ID为已有的SNAT规则的ID，已有的规则会被覆盖。
- **ingress-interface** *interface-name* – 指定匹配该SNAT规则的入接口。配置了入接口之后，只有从该接口进入的流量才会继续匹配这条SNAT规则，其他接口进入的流量不匹配。
- **before id** | **after id** | **top** – 指定规则所在的位置，可以是位于某个ID之前（**before id**）或者之后（**after id**），也可以是位于所有规则的首位（**top**）。如果不指定，该规则会处于所有SNAT规则的末尾。默认情况下，系统会将新创建的SNAT规则放到所有SNAT规则的末尾。
- **from** *src-address* **to** *dst-address* [**EIF** *egress-interface* | **evr** *vrouter-name*] – 指定该规则中流量应符合的条件。条件包括：
 - **from** *src-address* - 指定流量的源IP地址，*src-address*为IP地址（IPv4或IPv6）或者系统地址簿中指定的地址条目（IPv4或IPv6）。
 - **to** *dst-address* - 指定流量的目的IP地址，*dst-address*为IP地址（IPv4或IPv6）或者系统地址簿中指定的地址条目（IPv4或IPv6）。
 - **service** *service-name* – 指定流量的服务类型。*service-name*为服务簿中定义的服务。
 - **EIF** *egress-interface* | **evr** *vrouter-name* - 指定流量的出接口（**EIF** *egress-interface*）或者流量的下一跳VRouter（**evr** *vrouter-name*）。
- **ip** *ip-address*| **addressbook** *trans-to-address* | **EIF-ip** – 指定NAT转换地址。可以是IP地址或者系统地址簿中的地址，也可以是出接口的IP地址（**EIF-ip**）。
- **traffic-group** *traffic-group-name* - 指定已配置的流量组，即属于该流量组的流量才会匹配这条源NAT规则。若不指定，默认加入系统预定义的default流量组。
- **mode** {**static** | **dynamicip** | **dynamicport** [**sticky**]} – 指定转换模式。系统支持三种转换模式：static、dynamicip和dynamicport。具体描述请参阅下表：

模式	描述
static	静态源NAT转换即一对一的转换。该模式要求被转换到的地址条目（ trans-to-address ）包含的IP地址数与流量的源地址的地址条目（ src-address ）包含的IP地址数相同。
dynamic ip	动态源NAT转换即多对多的转换。该模式将源地址转换到指定的IP地址。每一个源地址会被映射到一个唯一的IP地址做转换，直到指定地址全部被占用。
dynamic port	即PAT。多个源地址将被转换成指定IP地址条目中的一个地址。如果不使用 sticky ，地址条目中的第一个地址将会首先被使用，当第一个地址的端口资源被用尽，第二个地址将会被使用。如果使用了 sticky ，每一个源IP产生的所有会话将被映射到同一个固定的IP地址。

- **log** – 使用该参数开启该SNAT规则的日志功能（当有流量匹配该地址转换规则时产生日志信息）。
- **group group-id** - 指定SNAT规则所属的HA组。如不指定该参数，创建的SNAT规则属于HA组0。
- **disable** – 如选择该选项，系统将禁用此SNAT规则。
- **track track-name** – 指定已创建的监测对象名称。配置该参数后，系统将对NAT转换后的公网地址是否有效进行监测，即以其作为源地址来监测到目标网站或主机的访问是否正常。可配置的监测对象包括Ping报文监测对象、HTTP报文监测对象、TCP报文监测对象。有关如何创建监测对象，请参阅“[配置监测对象](#)”部分。该功能仅支持动态端口模式（**dynamicport**），且NAT转换后的地址必须为IP地址或者地址簿中的地址（即**trans-to addressbook trans-to-address**）。系统优先使用监测成功的转换地址，当某个转换地址对目标网站或主机监测失败时，该地址被临时禁用，直至再次监测成功。当监测对象失败时，系统将在下个监测周期内禁用此地址并生成日志信息，不再转换私网地址为该公网地址，直到该地址被判定为可达。若SNAT规则的公网地址簿中地址全部被判定为不可达，系统将不禁用任何转换地址并发出日志信息。

- **description** *description* – 指定SNAT规则的描述信息。范围是1到63个字符。

例如，以下命令示例实现了untrust域中以太接口ethernet0/0的基于接口的NAT转换：

```
hostname(config)# ip vrouter trust-vr

hostname(config-vrouter)# snatrule from any to any eif ethernet0/0 trans-to eif-ip mode dynamicport

rule id=1
```

配置不做NAT转换的SNAT规则，在NAT配置模式下使用以下命令：

```
snatrule [id id] [before id | after id | top] from src-address to dst-address [eif egress-interface | evr vrouter-name] no-
trans [group group-id] [description description]
```

启用/禁用SNAT规则

在CLI的NAT配置模式下，用户可以通过使用以下命令启用或者禁用SNAT规则：

```
snatrule id id [enable | disable]
```

- **enable** – 启用指定ID的SNAT规则。
- **disable** – 禁用指定ID的SNAT规则。

修改SNAT规则排列顺序

每一条SNAT都有唯一一个ID号。流量进入设备时，设备对SNAT规则进行顺序查找，然后按照查找到的相匹配的第一条规则对流量的源IP做NAT转换。但是，ID的大小顺序并不是规则匹配顺序。使用show snat命令列出的规则顺序才是规则匹配顺序。用户可以移动已有的SNAT规则从而改变规则的排列顺序。改变规则的排列顺序，在VRouter配置模式下使用以下命令：

```
snatrule move id {before id | after id | top | bottom}
```

- **id** – 指定被移动的SNAT规则的ID号。
- **before id** – 将SNAT规则移动到某个ID之前。
- **after id** – 将SNAT规则移动到某个ID之后。

- **top** – 将SNAT规则移动到所有SNAT规则之首。
- **bottom** – 将SNAT规则移动到所有SNAT规则的末尾。

开启/关闭扩展PAT端口池功能

当SNAT的转换模式为dynamicport时，用户可以开启扩展PAT端口池功能，扩展NAT转换后的网络地址端口资源。默认情况下，该功能是关闭的。开启扩展PAT端口池功能，在全局模式下使用以下命令：

expanded-port-pool

在全局模式下，使用该命令no的形式关闭扩展PAT端口池功能：

no expanded-port-pool



注意：

- 设备的部分平台支持扩展PAT端口池功能，并且不同平台支持的扩展端口资源倍数不同。
- 该功能在配置SNAT规则前开启有效；如果在开启该功能前，系统中已配置SNAT规则，请重启设备使其生效。

删除SNAT规则

在CLI的NAT配置模式下，用户可以通过使用以下命令删除指定ID号的SNAT规则：

no snatrule id *id*

修改/删除SNAT描述信息

在CLI的NAT配置模式下，用户可以通过使用以下命令修改指定ID号的SNAT描述信息。

snatrule id *id* description *description*

- *id* – 指定要修改描述信息的SNAT规则ID号。
- **description *description*** – 指定SNAT规则的描述信息。范围是1到63个字符。

在CLI的NAT配置模式下，使用以下命令删除修改指定ID号的SNAT描述信息。


```
no snatrule id id description
```

显示SNAT配置信息

SNAT配置完毕，用户可以在任何CLI模式下通过使用以下命令查看系统中SNAT的配置信息：

```
show snat [resource] [id id] [vrouter vrouter-name]
```

```
show snat [vrouter vrouter-name] [src src-address] [dst dst-address] [service service-name] [trans-to trans-to-address]  
[description description]
```

- **id** – 显示指定ID号的SNAT规则信息。
- **resource** – 当SNAT的转换模式为dynamicport时，该参数用来指定显示源端口地址池中资源的利用情况。
- **vrouter** *vrouter-name* – 显示指定VRouter的SNAT配置信息。如果不指定该参数，系统将显示缺省VRouter（trust-vr）的SNAT规则。
- **src** *src-address* – 显示指定源地址的SNAT配置信息。
- **dst** *dst-address* – 显示指定目的地址的SNAT配置信息。
- **service** *service-name* – 显示指定服务的SNAT配置信息。
- **trans-to** *trans-to-address* - 显示指定转换后IP地址的SNAT配置信息。
- **description** *description* - 显示指定描述信息的SNAT配置信息。

查看监测失败的SNAT转换地址

查看监测失败的SNAT转换地址，在任何CLI模式下，使用以下命令：

```
show snat track-failed [vrouter vrouter-name] [slot slot-number] [cpu cpu-number]
```

- **track-failed** – 显示监测失败的SNAT转换地址。
- **vrouter** *vrouter-name* – 显示指定VRouter的监测失败的SNAT转换地址。如果不指定该参数，系统将显示缺省VRouter（trust-vr）的监测失败的SNAT转换地址。

- **slot slot-number** – 显示指定插槽的监测失败的SNAT转换地址。
- **cpu cpu-number** – 显示指定CPU的监测失败的SNAT转换地址。

创建DNAT规则

DNAT规则指定是否对符合条件的流量的目的IP地址做NAT转换。配置做NAT转换的DNAT规则，在VRouter配置模式下使用以下命令：

```
dnatrule [id id] [before id | after id | top] [ingress-interface interface] from src-address to dst-address [service service-name] [traffic-group traffic-group-name] trans-to trans-to-address [v4-mapped] [redirect] [port port] [load-balance] [track-tcp port] [track-ping] [log] [group group-id] [disable] [description description]
```

- **id id** – 为DNAT规则指定ID号。每一条DNAT规则都有一个唯一的ID。如果用户不指定，系统会为规则自动生成一个ID。如果指定的ID为已有的DNAT规则的ID，已有的规则会被覆盖。
- **before id** | **after id** | **top** – 指定规则所在的位置，可以是位于某个ID之前（**before id**）或者之后（**after id**），也可以是位于所有规则的首位（**top**）。如果不指定，该规则会处于所有DNAT规则的末尾。默认情况下，系统会将新创建的DNAT规则放到所有DNAT规则的末尾。流量进入设备时，设备对DNAT规则进行查找，然后按照查找到的相匹配的第一条规则对流量的目的IP做NAT转换。
- **ingress-interface interface** – 指定匹配该dnat规则的入接口。配置了入接口之后，只有从该接口进入的流量才会继续匹配这条DNAT规则，其他接口进入的流量不匹配。
- **from src-address to dst-address**[**service service-name**] – 指定该规则中流量应符合的条件。条件包括：
 - **from src-address** – 指定流量的源IP地址/掩码。*src-address*为IP地址/掩码或者系统地址簿中指定的地址条目。可以为IPv6/IPv4地址或IPv6/IPv4地址条目。
 - **to dst-address** – 指定流量的目的IP地址/掩码。*dst-address*为IP地址/掩码或者系统地址簿中指定的地址条目。可以为IPv6/IPv4地址或IPv6/IPv4地址条目。
 - **service service-name** – 指定流量的服务类型。如果需要一并转换端口号（通过**port port**参数指定），这里指定的服务就只能拥有一个协议和一个端口，例如TCP端口号可以是80，但不可以是80到100。
- **traffic-group traffic-group-name** - 指定已配置的流量组，即属于该流量组的流量才会匹配这条目的NAT规则。若不指定，默认加入系统预定义的default流量组。

- **trans-to** *trans-to-address* – 指定NAT转换地址。*trans-to-address*为IP地址/掩码或者系统地址簿中定义的地址条目。此处指定的NAT转换地址个数如果与流量目的IP地址（由命令的**to** *dst-address*参数指定）的个数不相同或者流量目的IP地址指定为**any**时，则需要为该条DNAT规则开启重定向功能（**redirect**）。如果为该条DNAT规则开启负载均衡功能（**load-balance**），也可以允许NAT转换地址个数与流量目的IP地址的个数不同，但是不允许流量目的IP地址为**any**。如果此处指定的NAT转换地址为包含DNS域名的地址簿条目，则需要为该条DNAT规则开启负载均衡功能（**load-balance**）。
- **v4-mapped** - 指定直接从报文的目的IPv6地址中抽取目的IPv4地址。
- **redirect** - 配置**redirect**参数为该条DNAT规则开启重定向功能，允许指定流量目的IP地址为**any**。
- **port** *port* – 内网服务器的端口号。
- **load-balance** – 配置**load-balance**参数为该条DNAT规则开启负载均衡功能，采用持续性算法分发流量，基于用户IP地址的散列值来选择服务器，均衡流量到不同的内网服务器。
- **track-tcp** *port* - 配置**track-tcp**参数并指定内网服务器端口号，系统会每隔3秒向内网服务器发送TCP报文，监控服务器的特定TCP端口是否可达。若连续三次发送报文均未收到响应，系统认为内网服务器出现故障。
- **track-ping** - 配置**track-ping**参数，系统会每隔3秒向内网服务器发送Ping报文，监控服务器是否可达。若连续三次发送报文均未收到响应，系统认为内网服务器出现故障。
- **log** – 使用该参数开启该DNAT规则的日志功能（当有流量匹配该地址转换规则时产生日志信息）。
- **group** *group-id* - 指定DNAT规则所属的HA组。如不指定该参数，创建的DNAT规则属于HA组0。
- **disable** – 如选择该选项，系统将禁用此DNAT规则。
- **description** *description* – 指定DNAT规则的描述信息。范围是1到63个字符。

例如，以下命令将任何到addr1的请求的IP转换成addr2的IP地址，并且不转换服务的端口号：

```
hostname(config-vrouter)# dnatrul from any to addr1 service any trans-to addr2
rule id=1
```

配置不做NAT转换的DNAT规则，在NAT配置模式下使用以下命令：

```
dnatrul [id id] [before id | after id | top] from src-address to dst-address [service service-name] no-trans [group group-id] [description description]
```

启用/禁用DNAT规则

在NAT配置模式下，用户可以通过使用以下命令启用或者禁用DNAT规则：

```
dnatrul rule id id [enable | disable]
```

- **enable** – 启用指定ID的DNAT规则。
- **disable** – 禁用指定ID的DNAT规则。

修改DNAT规则排列顺序

每一条DNAT都有唯一一个ID号。每一条DNAT都有唯一一个ID号。流量进入设备时，设备对DNAT规则进行顺序查找，然后按照查找到的相匹配的第一条规则对流量的目的IP做NAT转换。但是，ID的大小顺序并不是规则匹配顺序。使用**show dnaturul**命令列出的规则顺序才是规则匹配顺序。用户可以移动已有的DNAT规则从而改变规则的排列顺序。

修改DNAT规则排列顺序，请在NAT配置模式下使用以下命令：

```
dnatrul move id {before id | after id | top | bottom}
```

- *id* – 指定被移动的DNAT规则的ID号。
- **before** *id* – 将DNAT规则移动到某个ID之前。
- **after** *id* – 将DNAT规则移动到某个ID之后。
- **top** – 将DNAT规则移动到所有SNAT规则之首。
- **bottom** – 将DNAT规则移动到所有SNAT规则的末尾。

修改/删除DNAT描述信息

在NAT配置模式下，用户可以通过使用以下命令修改指定ID号的DNAT描述信息。

```
dnatrul id id description description
```

- *id* – 指定需修改描述信息的DNAT规则ID号。
- **description** *description* – 指定DNAT规则的描述信息。范围是1到63个字符。

在CLI的NAT配置模式下，使用以下命令删除修改指定ID号的DNAT描述信息。

no dnatrul id *id* description

删除DNAT规则

在NAT配置模式下，用户可以通过使用以下命令删除指定ID号的DNAT规则：

no dnatrul id *id*

显示DNAT配置信息

DNAT配置完毕，用户可以在任何CLI模式下通过使用以下命令查看系统中DNAT的配置信息：

show dnat [id *id* | [vrouter *vrouter-name*] [src *src-address*] [dst *dst-address*] [service *service-name*] [trans-to *trans-to-address*] [trans-port *port-number*] [description *description*]]

- **id** - 显示指定ID号的DNAT规则信息。
- **vrouter *vrouter-name*** - 显示指定VRouter的DNAT规则信息。如果不指定该参数，系统将显示缺省VRouter（trust-vr）的DNAT规则。
- **src *src-address*** - 显示指定源地址的DNAT配置信息。
- **dst *dst-address*** - 显示指定目的地址的DNAT配置信息。
- **service *service-name*** - 显示指定服务的DNAT配置信息。
- **trans-to *trans-to-address*** - 显示指定转换后IP地址的DNAT配置信息。
- **trans-port *port-number*** - 显示指定转换后端口号的DNAT配置信息。
- **description *description*** - 显示指定描述信息的DNAT配置信息。

显示内网服务器状态，请在任何模式下，使用以下命令：

show dnat server [*ip-address*] [vrouter *vrouter-name*] [tcp-port *port*] [ping]

- ***ip-address*** - 显示指定IP地址的内网服务器状态信息。
- **vrouter *vrouter-name*** - 显示指定VRouter的内网服务器状态信息。如果不指定该参数，系统将显示缺省VR即trust-vr的内网服务器状态信息。

- **tcp-port port** – 显示指定端口号的内网服务器状态信息。
- **ping** – 显示内网服务器的Ping监控状态信息。

DNS Rewrite

当客户端发起DNS请求，位于公网的DNS服务器返回DNS response报文时，安全设备将对报文中的IP地址进行重写，将其改为私网IP地址以保护和隐藏组网环境中的网络配置。配置该功能，在NAT配置模式下，输入以下命令：

```
dns-rewrite-rule [id id] dns-response {ip ip-address|address-book address -name} rewrite-to {ip ip-address|address-book address-name} [group group-id] dynamic-mapping
```

- **id id** – 指定该规则的ID。每一条规则都有一个唯一的ID。如果不指定，系统会自动分配。如果指定的ID为已有的规则的ID，已有的规则会被覆盖。
- **dns-response** {*ip ip-address*|**address-book** *address -name*} - 指定DNS response报文中的公网IP地址或地址簿名称。
- **rewrite-to** {*ip ip-address*|**address-book** *address-name*} – 指定设备重写后的私网IP地址或地址簿名称。
- **group group-id** – 指定该规则所属的HA组的组ID。

在任何模式下，使用**show dns-rewrite-rule** [*id id* | **vrouter** *vr-name*] **dynamic-mapping**查看DNS rewrite规则：

- **id id** | **vrouter vr-name** – 查看指定ID或VRouter下的DNS rewrite规则。

透明NAT

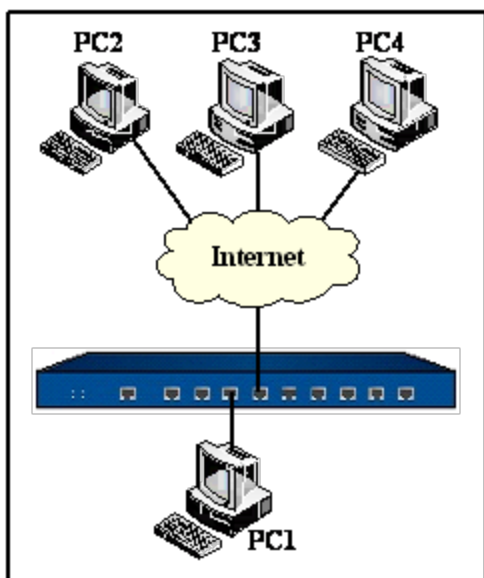
系统支持透明NAT功能，即设备在透明应用模式工作时支持NAT功能。默认情况下，透明NAT功能为关闭状态。在VSwitch配置模式下，使用以下命令开启或关闭透明NAT：

- **nat-enable**：开启透明NAT。
- **no nat-enable**：关闭透明NAT。

Full-cone NAT

Full-cone NAT也被称为一对一NAT、完全圆锥型NAT，指的是NAT设备将来自内网同一个IP和端口号的请求映射到同一个外网IP和端口号，之后任何外网主机都可以通过映射关系与该内网主机通讯。

如下图所示，假设内网的PC1经过NAT转换后与外网的PC2创建了连接，设备将PC1的内网IP地址和端口号（Private IP: Private port）转换为外网地址和端口号（Public IP: Public port）。由于已经创建了会话，PC2也可以通过会话匹配反向访问到PC1，而PC3和PC4即使能够找到PC1经过NAT转换后的公网IP（Public IP: Public port），由于无法找到会话匹配信息，默认仍无法与PC1进行通讯。在设备上启用Full-cone NAT后，设备会创建并维护一个Full-cone NAT表项，通过该表项对外公开PC1的内外网IP和端口的映射关系（Local IP:Local port <==> Public IP:Public port）。只要PC3和PC4能够访问PC1的公网IP（Public IP: Public port），就可以利用这个映射关系主动连接到PC1，从而实现穿越NAT设备。



启用Full-cone NAT功能，在全局配置模式下，使用以下命令：

```
nat type full-cone
```

使用该命令no的形式取消Full-cone NAT功能：

```
no nat type full-cone
```

指定开启Full-cone NAT功能的协议，在全局配置模式下，使用以下命令：

```
nat protocol {tcp | udp}
```

- **tcp** - 指定对TCP协议开启Full-cone NAT。
- **udp** - 指定对UDP协议开启Full-cone NAT。默认下系统只对UDP协议开启Full-cone NAT。

使用该命令no的形式取消上述配置：

```
no nat protocol {tcp | udp}
```

显示Full-cone NAT配置信息

显示Full-cone NAT配置信息，在任意模式下，使用以下命令：

```
show nat {configuration | generic | entry | control}
```

- **configuration** - 显示Full-cone NAT配置信息。
- **generic** - 显示Full-cone NAT表项概括信息。
- **entry** - 显示Full-cone NAT表项详细信息。
- **control** - 显示Full-cone NAT、扩展PAT端口池功能以及SNAT端口分割功能的启用状态。

IP包数据处理选项

为能够更好的传输数据信息，设备提供一些IP数据包处理选项，包括TCP MSS（Maximum Segment Size，最大分段大小）的配置、TCP序列号检查、TCP三次握手超时时间检查、TCP SYN包检查以及IP包分片处理相关配置等。

配置MSS值

MSS为TCP数据包每次能够传输的最大数据分段。用户可以通过命令，为所有的TCP SYN/ACK包或者IPSec VPN的TCP SYN/ACK包指定MSS值。合适的MSS值可以减少分片。指定MSS值，在全局配置模式下，使用以下命令：

```
tcp-mss {all | ipsec-vpn} size
```

- **all** - 为所有TCP SYN包指定MSS值。
- **ipsec-vpn** - 为IPSec VPN的TCP SYN包指定MSS值。
- **size** - 指定TCP SYN包的MSS值。范围是64到65535。所有TCP SYN/ACK包的默认MSS值为1448，IPSec VPN的TCP SYN/ACK包默认MSS值为1380。

在全局配置模式下，使用该命令no的形式，恢复默认MSS值：

```
no tcp-mss {all | ipsec-vpn}
```


TCP序列号检查

设备具有TCP包序列号检查功能。该功能检查TCP序列号，如果TCP序列号超出TCP窗口，该TCP包将会被丢弃。默认情况下，该功能为开启状态。配置TCP序列号检查功能，在全局配置模式下，使用以下命令：

- 关闭： `tcp-seq-check-disable`
- 开启： `no tcp-seq-check-disable`

TCP三次握手超时时间检查

设备可以对TCP三次握手建立的时间进行检查，如果在超时时间内，未完成三次握手，则断掉该连接。同时，用户可以指定超时时间。配置TCP三次握手超时时间检查，在全局配置模式下，使用以下命令：

`tcp-syn-check [timeout-value]`

- *timeout-value* – 指定三次握手的超时时间，单位为秒。范围是1到1800秒。默认值是20秒。

在全局配置模式下，使用该命令`no`的形式，关闭TCP三次握手超时时间检查功能：

`no tcp-syn-check`

TCP连接终止老化时间配置

在TCP连接终止的过程中，系统可以根据老化时间计算TCP连接在设备上的存活时间。如果在老化时间内，未收到刷新数据，系统将删除该连接。同时，用户可以指定TCP连接处于不同状态的老化时间，TCP连接进入对应的状态后，就使用该状态的老化时间。

在TCP连接终止的过程中，支持配置老化时间的状态有以下几种：

- ESTABLISHED状态
- FIN_WAIT_1状态
- FIN_WAIT_2状态
- TIME_WAIT状态

配置ESTABLISHED状态的老化时间，在全局配置模式下，使用以下命令：

`tcp-establish-check [timeout-value]`

- *timeout-value* – 指定TCP连接处于ESTABLISHED状态的老化时间，单位为秒。TCP三次握手建立后，进入ESTABLISHED状态，如果没有数据传输，TCP连接使用该状态的老化时间。取值范围是1到1800秒。默认值是300秒。

配置FIN_WAIT_1状态的老化时间，在全局配置模式下，使用以下命令：

tcp-fin-wait-1-check [*timeout-value*]

- *timeout-value* – 指定TCP连接处于FIN_WAIT_1状态的老化时间，单位为秒。范围是1到1800秒。默认值是120秒。

配置FIN_WAIT_2状态的老化时间，在全局配置模式下，使用以下命令：

tcp-fin-wait-2-check [*timeout-value*]

- *timeout-value* – 指定TCP连接处于FIN_WAIT_2状态的老化时间，单位为秒。范围是1到1800秒。默认值是120秒。

配置TIME_WAIT状态的老化时间，在全局配置模式下，使用以下命令：

tcp-time-wait-check [*timeout-value*]

- *timeout-value* – 指定TCP连接处于TIME_WAIT状态的老化时间，单位为秒。范围是1到1800秒。默认值是5秒。

TCP SYN包检查

系统支持TCP SYN包检查功能，在建立TCP连接时，设备将对收到的数据包进行检查：

- 当收到的包为TCP SYN包时，建立TCP连接。
- 当收到的包为TCP非SYN包时，按照指定动作对数据包进行处理。

默认情况下，该功能为开启状态。开启TCP SYN包检查功能并指定对TCP非SYN包的处理动作，在全局配置模式下，使用以下命令：

tcp-syn-bit-check {**drop** | **reset**}

- **drop** – 当收到的包为TCP非SYN包时，丢弃数据包。
- **reset** – 当收到的包为TCP非SYN包时，丢弃数据包并向对方设备发送RST报文。

在全局配置模式下使用**no tcp-syn-bit-check**命令关闭TCP SYN包检查功能。

查看TCP SYN包检查功能的配置信息，在任意模式下，使用以下命令：

```
show tcp-syn-bit-check
```

丢弃SYN包

系统支持在TCP会话延迟删除期间丢弃五元组相同的SYN包，即在TCP会话延迟删除期间，若系统收到五元组相同的SYN标记报文，会作丢弃处理。该功能开启后，可避免TCP会话在延迟删除期间匹配并转发SYN包，导致会话删除后新的数据报文无法匹配会话而出现丢包的现象。

默认情况下，该功能为禁用状态。

在全局配置模式下，使用**flow**命令进入Flow配置模式。启用或禁用丢弃SYN包功能，在Flow配置模式下，使用以下命令：

- **tcp-out-of-state-syn-drop** - 启用该功能。
- **no tcp-out-of-state-syn-drop** - 禁用该功能。

IP分片包处理

对于分片IP数据包，用户可以配置系统允许的每个IP包的最大分片数（超过该分片数值的IP数据包将会被丢弃）以及分片重组的超时时间（如果在指定的超时时间结束时设备仍未收到所有的分片包，数据包将会被丢弃）。

配置系统允许的每个IP的最大分片数，在全局配置模式下使用以下命令：

```
fragment chain number
```

- *number* – 指定系统允许的每个IP包的最大分片数，默认值为48。取值范围是1到1024。

在全局配置模式下使用**no fragment chain**命令恢复默认最大分片数。

配置分片重组超时时间，在全局配置模式下使用以下命令：

```
fragment timeout time
```

- *time* – 指定分片重组超时时间，默认值为2秒。取值范围是1到60秒。

在全局配置模式下使用**no fragment timeout**命令恢复默认超时时间。

逆向路由

逆向路由是指用于转发反向数据的路由。反向是相对于初始化数据流方向。启用或关闭逆向路由，在全局配置模式下使用以下命令：

reverse-route [**force** | **prefer**]

- **force** – 开启逆向路由。如果能找到逆向路由，则使用逆向路由转发反向数据。如果找不到逆向路由，则丢弃数据包。
- **prefer** – 优先使用逆向路由。如果能够找到逆向路由就使用逆向路由转发反向数据；如果找不到逆向路由则按原路径返回。

关闭逆向路由，在全局配置模式下使用命令 **no reverse-route**。关闭后，反向数据流到达设备后不进行逆向路由检查，原路返回。

应用层网关（ALG）

一些应用程序采用多通道数据传送，常见的如FTP，其控制通道和数据通道是分开的。在严格安全策略控制条件下的设备，对每种数据通道进行严格限制，例如只允许从内网到外网的FTP数据在知名的TCP 21号端口上进行传输，一旦FTP主动模式下，在公网上的FTP服务器试图主动连接内网主机的随机端口，设备就会进行拦截，此时FTP无法正常工作。这就要求设备足够智能以正确处理严格安全策略下合法应用的随机性。在FTP的实例中，设备通过分析FTP控制通道上传送的信息，得知服务器与客户端达成一致，服务器将主动连接客户端的某端口，设备就能临时的打开一条通道，使FTP正常工作。

系统采用最严格的NAT模式。一些VoIP应用在进行NAT穿越时，由于IP地址和端口号的改变可能导致VoIP无法正常工作，ALG技术在此时将保证NAT地址转换后，VoIP应用能够正常通信。因此，应用层网关提供以下功能：

- 在严格的安全策略规则下，利用应用层网关ALG技术，保证多通道应用程序正常的通信，如FTP。

配置ALG功能

系统可根据每种应用分别开启或关闭ALG控制功能。用户可在山石网科设备上配置以下应用的ALG控制功能：FTP、HTTP、MSRPC、PPTP、Q.931、RAS、RSH、RTSP、SIP、SQLNetV2、SUNRPC、TFTP、DNS、H323和XDMCP。用户可以开启或者关闭应用的ALG功能，也可以指定H323协议的超时时间。

开启或者关闭应用的ALG控制功能，在全局配置模式下使用以下命令：

开启：**alg** {**all** | **auto** | **TFTP** | **FTP** | **RSH** | ...}

关闭: **no alg** {**all** | **auto** | **TFTP** | **FTP** | **RSH** | ...}

- **all** - 开启或者关闭所有应用的ALG控制功能。
- **auto** - 根据应用识别的结果自动开启或关闭应用的ALG控制功能。
- **TFTP** | **FTP** | **RSH** | ... - 开启或者关闭指定应用的ALG控制功能。



注意: 如果关闭HTTP的ALG功能, 山石网科设备的HTTP内容阻断功能将失效。

ALG支持严格模式和非严格模式。严格模式创建的PINHOLE中所分配的SNAT端口和控制连接分配的SNAT端口一致。系统默认开启严格模式。开启ALG严格模式, 在全局配置模式下, 使用以下命令:

alg strict-mode

使用**no alg strict-mode**命令开启非严格模式。在如下场景中, 建议用户开启非严格模式, 避免影响数据流量:

- 存在第三方PINHOLE
- 配置了SNAT并开启了端口扩展
- 协商数据连接的PAYLOAD中的IP地址和端口号与控制连接的IP地址和端口号一致

指定H323协议的超时时间, 在全局配置模式下使用以下命令:

alg h323 session-time *time-value*

- *time-value* - 指定H323的超时时间。默认为60秒。范围是60到1800秒。

使用以上命令**no**的形式取消对H323超时时间的指定:

no alg h323 session-time

开启或者关闭对每秒处理SIP消息数目的限制功能, 在全局配置模式下使用以下命令:

开启: **alg sip-message-rate** *number*

- *number* - 指定每秒处理SIP消息数目的最大值。取值范围是1到65535。

关闭: **no alg sip-message-rate**

开启或者关闭对FTP PORT命令的异常检测功能, 在全局配置模式下, 使用以下命令:

开启: **alg ftp anomaly-detection**

关闭: **no alg ftp anomaly-detection**

开启或者关闭FTP的ALG功能, 在全局配置模式下, 使用以下命令:

开启: **alg ftp ftps-extension**

关闭: **no alg ftp ftps-extension**

开启或者关闭对所有的HTTP长连接请求记录日志, 在全局配置模式下, 使用以下命令:

开启: **alg http persistent connection**

关闭: **no alg http persistent connection**

用户可以在任意模式下使用show命令查看ALG控制功能的状态和配置:

- 查看是否对应用启用了ALG控制功能: **show alg**
- 查看SIP网关的ALG配置和状态: **show alg sip-capacity**

指定SIP代理模式

SIP是一个应用层的控制协议, 它通常用于多媒体会话, 例如Internet电话。SIP协议可以承载多种多媒体会话数据, 比如声音、影像、或者文本。

SIP服务器可以作为代理转发SIP客户端之间的通信。SIP客户端之间通信有两种模式, 一种是媒体数据经过SIP服务器进行代理, 另一种是媒体数据是不经过SIP服务器, SIP客户端之间直接通信。防火墙应该配合SIP客户端的通信模式, 选择与实际情况相同的模式, 如果不一致可能会导致通信问题。

在全局配置模式下, 使用以下命令使防火墙工作在客户端不经过SIP代理服务器而直接通信的模式下。防火墙默认使用这种模式, 它能保证不通过代理服务器的SIP客户端的通信正常。

no alg sip media-proxied-by-server

在全局配置模式下, 使用以下命令使防火墙工作在SIP服务器做代理的通信模式下。

alg sip media-proxied-by-server

查看ALG SIP信息

查看防火墙是否开启了SIP代理模式、每秒处理SIP消息数目的最大值、注册话机数量和正在进行通话的话机数量, SIP的在任意模式下, 使用以下命令:

show alg sip

第6章 路由

路由是将数据包从一个网络转发到另一个网络中的目的地址的过程。路由器是处在两个网络之间转发数据包的设备。路由器根据路由表中储存的各种传输路径传输数据包，每一个传输路径即为一个路由条目。

设备具有三层路由功能，通过VRouter，进行路由配置，对不同的数据包进行转发。

设备支持目的路由、ISP路由、源路由（Source-Based Routing，简称SBR）、源接口路由（Source-Interface-Based Routing，简称SIBR）、目的接口路由（Destination-Interface-Based Routing，简称DIBR）、策略路由（Policy-Based Routing，简称PBR）、动态路由（包括RIP、OSPF、OSPFv3和BGP）和等价多径路由（Equal Cost MultiPath Routing，简称ECMP）。

- [配置目的路由](#)：手工定义的路由条目，根据目的地址指定下一跳。
- [配置目的接口路由](#)：根据数据包的目的IP地址和入接口，选择路由，进行转发。
- [配置源路由](#)：根据数据包的源IP地址，选择路由，进行转发。
- [配置源接口路由（SIBR）](#)：根据数据包的源IP地址和入接口，选择路由，进行转发。
- [配置ISP信息](#)：添加ISP相关信息。
- [配置ISP路由](#)：根据不同的ISP确定下一跳。
- [配置策略路由（PBR）](#)：根据数据包的源IP地址、目的IP地址以及服务类型，选择路由，进行转发。
- [动态路由](#)：设备按照动态路由协议（配置[RIP](#)、[OSPF](#)、[OSPFv3](#)或者[BGP](#)）自动生成的动态路由表项对数据包进行路由选择并转发。
- [等价多径路由（ECMP）](#)：到达相同目的IP地址或网段的数据流量在多条相同管理距离的路径上进行负载均衡。

开启/关闭静态路由查询

对于策略路由、源接口路由和源路由，用户可以单独控制是否需要它们进行查询（系统要求必须进行目的路由查询）。默认情况下，策略路由、源接口路由和源路由查询为开启状态。开启/关闭策略路由、源接口路由和源路由查询，在全局配置模式下，使用以下命令（适用于所有VRouter）：

- 开启：**route enable** {pbr | sibr | sbr | dibr}
- 关闭：**route disable** {pbr | sibr | sbr | dibr}

开启/关闭会话重匹配路由

默认情况下，会话重匹配路由的功能是开启的。当用户添加、修改或删除路由时，会话会重新匹配最优路由。在会话重匹配路由的过程中，系统会根据情况对会话作出如下不同操作：

- 当会话之前匹配的路由被删除时：
 - 若会话保留功能（keep-session）关闭，则相匹配的会话将被删除。
 - 若会话保留功能（keep-session）开启，则相匹配的会话不会被删除，且会话的路由信息变为无效。当与会话之前匹配的路由被重新添加后，会话将重匹配路由：
 - 若重新匹配的路由的出接口未发生变化，则会话的路由信息变为有效，会话恢复可用状态。
 - 若重新匹配的路由的出接口发生变化，则会话将被删除。
- 当会话之前匹配的路由被修改或有新路由被添加时：
 - 若会话之前匹配的路由仍是最优路由，会话保持可用状态。
 - 若会话之前匹配的路由不是最优路由，但重新匹配的路由的出接口未发生变化，会话更新路由信息。
 - 若会话之前匹配的路由不是最优路由，且重新匹配的路由的出接口发生变化，会话将被删除。

在某些情况下（如添加或删除策略路由的应用类型），会话可能会被大量删除，导致流量异常。此时，需要关闭会话重新匹配功能。

在全局配置模式下，使用**flow**命令进入Flow配置模式。在Flow配置模式下，使用以下命令关闭或开启会话重匹配路由功能：

```
session rematch route {enable [ keep-session ] | disable}
```

- **enable** – 开启会话重匹配路由功能。
- **keep-session** – 会话保留功能。在开启会话重匹配路由功能且指定该参数后，即开启会话保留功能，当路由被删除时不删除相匹配的会话，且会话的路由信息变为无效。默认情况下，不指定该参数，会话保留功能为关闭状态。
- **disable** – 关闭会话重匹配路由功能。若会话保留功能是开启状态，也会被同时关闭。

关闭会话保留功能，在Flow配置模式下，使用**no session rematch route enable keep-session**命令。

目的路由

目的路由是手工定义的路由条目，根据目的地址指定下一跳。对外连接较少或者内网连接相对比较稳定的网络通常使用目的路由。用户可以根据需要确定是否添加默认路由条目。系统支持IPv4和IPv6两种类型的目的路由。

添加IPv4目的路由条目

用户可以为VRouter添加目的路由条目。但是，添加目的路由条目之前，需要进入VRouter配置模式。请在全局配置模式下使用以下命令：

```
ip vrouter vrouter-name
```

- *vrouter-name* – 指定VRouter的名称。

进入到VRouter配置模式下后，用户可以添加目的路由条目。在VRouter配置模式下使用以下命令：

```
ip route { A.B.C.D/M | A.B.C.D A.B.C.D } { null0 | A.B.C.D | interface-name [A.B.C.D] | vrouter  
vrouter-name } [distance-value] [weight weight-value] [description description] [schedule schedule-  
name][track track-name]
```

- *A.B.C.D/M* | *A.B.C.D A.B.C.D* – 指定目的地址。设备支持两种方式，*A.B.C.D/M*或者*A.B.C.D A.B.C.D*，例如1.1.1.0/24或者1.1.1.0 255.255.255.0。
- **null0** | *A.B.C.D* | *interface-name* [*A.B.C.D*] | **vrouter** *vrouter-name* – 指定下一跳。可以是Null0接口（即黑洞路由）、网关地址（*A.B.C.D*）、接口（*interface-name*）或者VRouter（**vrouter** *vrouter-name*）。当下一跳为接口时，用户可以选择Null0接口或者PPPoE接口。
- *distance-value* – 指定路由的管理距离大小。该参数设定路由的优先级，取值越小，优先级越高，而在有多条路由选择的时候，优先级高的路由会被优先使用。取值范围是1到255，默认值为1。当路由距离为255时，该路由无效。
- **weight** *weight-value* – 指定路由权值的大小。路由权值决定负载均衡中流量转发的比重。范围是1到255，默认值是1。
- **description** *description* – 指定路由的描述信息。范围是1到63个字符。

- **schedule** *schedule-name* – 指定时间表名称。该条配置将会在时间表指定的时间范围内生效。可配置多次该命令指定多个时间表（最多8个）。为避免产生不可预知的问题，建议用户不要配置时间重叠的时间表。
- **track** *track-name* - 指定已创建的监测对象名称。指定后，若针对该监测对象的监测失败，则该路由无效。

使用多条该命令添加多条静态路由条目。

使用以上命令no的形式删除指定的静态路由条目：

```
no ip route {A.B.C.D/M | A.B.C.D A.B.C.D} {null0 | A.B.C.D | interface-name A.B.C.D | interface-name [A.B.C.D] | vrouter vrouter-name} [description description]
```

添加IPv6目的路由条目

进入到VRouter配置模式下后，用户可以添加目的路由条目。在VRouter配置模式下使用以下命令：

```
ipv6 route ipv6-address/M {null0 | ipv6-address | vrouter vrouter-name | interface-name [ipv6-address]} [distance-value] [weight weight-value] [description description] [track track-name]
```

- *ipv6-address/M* – 指定目的地址网段。
- **null0** | *ipv6-address* | **vrouter** *vrouter-name* | *interface-name [ipv6-address]* – 指定下一跳。可以是Null0接口（即黑洞路由）、网关地址（*ipv6-address*）、VRouter（*vrouter vrouter-name*）或者接口（*interface-name*）。
- *distance-value* – 指定路由的管理距离大小。该参数设定路由的优先级，取值越小，优先级越高，而在有多条路由选择的时候，优先级高的路由会被优先使用。取值范围是1到255，默认值为1。当路由距离为255时，该路由无效。
- *weight-value* – 指定路由权值的大小。路由权值决定负载均衡中流量转发的比重。范围是1到255，默认值是1。
- **description** *description* - 指定路由的描述信息。范围是1到63个字符。
- **track** *track-name* – 指定已创建的监测对象名称。指定后，若针对该监测对象的监测失败，则该路由无效。

使用多条该命令添加多条目的路由条目。

使用以上命令no的形式删除指定的目的路由条目：

```
no ipv6 route ipv6-address/M { null0 | ipv6-address | vrouter vrouter-name | interface-name [ipv6-address] } [description description]
```

查看IPv4/IPv6目的路由信息

用户可以在任何模式下使用以下命令查看目的路由信息：

```
show {ip | ipv6} route static [vrouter vrouter-name]
```

- **ip** - 查看IPv4类型的目的路由信息。
- **ipv6** - 查看IPv6类型的目的路由信息。
- **vrouter-name** - 显示指定的VRouter的目的路由信息。

目的接口路由

目的接口路由（DIBR）根据数据包的目的IP地址和入接口，选择路由，进行转发。系统支持IPv4和IPv6两种类型的目的接口路由。

添加IPv4目的接口路由条目

目的接口路由的配置也需要在VRouter配置模式下完成。进入VRouter配置模式，在全局配置模式下，使用以下命令：

```
ip vrouter vrouter-name
```

进入到VRouter配置模式下后，用户可以添加目的接口路由条目。在VRouter配置模式下使用以下命令：

```
ip route in-interface interface-name { A.B.C.D/M | A.B.C.D A.B.C.D } { null0 | A.B.C.D | interface-name [A.B.C.D] | vrouter vrouter-name } [distance-value] [weight weight-value] [description description] [schedule schedule-name] [track track-name]
```

- **in-interface interface-name** - 指定路由条目的入接口。
- **A.B.C.D/M | A.B.C.D A.B.C.D** - 指定目的地址。设备支持两种方式，**A.B.C.D/M**或者**A.B.C.D A.B.C.D**，例如1.1.1.0/24或者1.1.1.0 255.255.255.0。

- **null0** | *A.B.C.D* | *interface-name* [*A.B.C.D*] | **vrouter** *vrouter-name* – 指定下一跳。可以是Null0接口（即黑洞路由）、网关地址（*A.B.C.D*）、接口（*interface-name*）或者VRouter（**vrouter** *vrouter-name*）。当下一跳为接口时，用户可以选择Null0接口或者PPPoE接口。
- *distance-value* – 指定路由的管理距离大小。该参数设定路由的优先级，取值越小，优先级越高，而在有多条路由选择的时候，优先级高的路由会被优先使用。取值范围是1到255，默认值为1。当路由距离为255时，该路由无效。
- **weight** *weight-value* – 指定路由权值的大小。路由权值决定负载均衡中流量转发的比重。范围是1到255，默认值是1。
- **description** *description* – 指定路由的描述信息。范围是1到63个字符。
- **schedule** *schedule-name* – 指定时间表名称。该条配置将会在时间表指定的时间范围内生效。可配置多次该命令指定多个时间表（最多8个）。为避免产生不可预知的问题，建议用户不要配置时间重叠的时间表。
- **track** *track-name* - 指定已创建的监测对象名称。指定后，若针对该监测对象的监测失败，则该路由无效。

使用多条该命令添加多条目的接口路由条目。

使用以上命令no的形式删除指定的目的接口路由条目：

```
no ip route in-interface interface-name { A.B.C.D/M | A.B.C.D A.B.C.D } { null0 | A.B.C.D | interface-name [A.B.C.D] | vrouter vrouter-name } [description description]
```

添加IPv6目的接口路由条目

在VRouter配置模式下，使用以下命令添加一条目的接口路由条目：

```
ipv6 route in-interface interface-name ipv6-address/M { null0 | ipv6-address | interface-name | vrouter vrouter-name } [distance-value] [weight weight-value] [description description] [track track-name]
```

- *interface-name* – 指定路由条目的入接口。
- *ipv6-address/M* – 指定目的地址网段。
- **null0** | *ipv6-address* | *interface-name* | **vrouter** *vrouter-name* - 指定下一跳。可以是Null0接口（即黑洞路由）、网关地址（*ipv6-address*）、VRouter（*vrouter* *vrouter-name*）或者接口（*interface-name*）。

- *distance-value* – 指定路由的管理距离大小。该参数设定路由的优先级，取值越小，优先级越高，而在有多条路由选择的时候，优先级高的路由会被优先使用。取值范围是1到255，默认值为1。当路由距离为255时，该路由无效。
- *weight-value* – 指定路由权值的大小。路由权值决定负载均衡中流量转发的权重。范围是1到255，默认值是1。
- **description** *description* - 指定路由的描述信息。范围是1到63个字符。
- **track** *track-name* – 指定已创建的监测对象名称。指定后，若针对该监测对象的监测失败，则该路由无效。

使用多条该命令添加多条目的接口路由条目。

使用以上命令no的形式删除指定的目的接口路由条目：

```
no ipv6 route in-interface interface-name ipv6-address/M { null0 | ipv6-address | interface-name | vrouter vrouter-name } [description description ]
```

查看IPv4/IPv6目的接口路由信息

用户可以在任何模式下使用以下命令查看目的接口路由信息：

```
show {ip | ipv6} route in-interface interface-name
```

- **ip** - 查看IPv4类型的目的接口路由信息。
- **ipv6** - 查看IPv6类型的目的接口路由信息。
- **in-interface** *interface-name* - 显示指定入接口的目的接口路由信息。

查看IPv6目的接口路由的FIB信息

用户可以在任何模式下使用以下命令查看目的接口路由的FIB信息：

```
show ipv6 fib in-interface interface-name
```

- **in-interface** *interface-name* - 显示指定入接口的目的接口路由的FIB信息。

源路由

源路由的配置需要在VRouter配置模式下完成。进入VRouter配置模式，在全局配置模式下，使用以下命令：

```
ip vrouter vrouter-name
```

添加IPv4源路由条目

在VRouter配置模式下，使用以下命令添加一条源路由条目：

```
ip route source { A.B.C.D/M | A.B.C.D A.B.C.D } { null0 | A.B.C.D | interface-name | vrouter  
vrouter-name } [distance-value] [weight weight-value] [schedule schedule-name] [description descrip-  
tion ] [track track-name]
```

- *A.B.C.D/M | A.B.C.D A.B.C.D* – 指定源路由条目的网络地址。设备支持两种方式，*A.B.C.D/M*或者*A.B.C.D A.B.C.D*，例如1.1.1.0/24或者1.1.1.0 255.255.255.0。
- *null0 | A.B.C.D | interface-name | vrouter vrouter-name* – 指定下一跳。可以是Null0接口（即黑洞路由）、网关地址（*A.B.C.D*）、接口（*interface-name*）或者VRouter（*vrouter vrouter-name*）。当下一跳为接口时，用户可以选择Null0接口或者PPPoE接口。
- *distance-value* – 指定路由的管理距离大小。该参数设定路由的优先级，取值越小，优先级越高，而在有多条路由选择的时候，优先级高的路由会被优先使用。取值范围是1到255，默认值为1。当路由距离为255时，该路由无效。
- *weight weight-value* – 指定路由权值的大小。路由权值决定负载均衡中流量转发的权重。范围是1到255，默认值是1。
- *schedule schedule-name* – 指定时间表名称。该条配置将会在时间表指定的时间范围内生效。可配置多次该命令指定多个时间表（最多8个）。为避免产生不可预知的问题，建议用户不要配置时间重叠的时间表。
- *description description* - 指定路由的描述信息。范围是1到63个字符。
- *track track-name* - 指定已创建的监测对象名称。指定后，若针对该监测对象的监测失败，则该路由无效。

使用以上命令no的形式删除指定的源路由条目：

```
no ip route source { A.B.C.D/M | A.B.C.D A.B.C.D } { null0 | A.B.C.D | interface-name | vrouter  
vrouter-name } [description description ]
```

添加IPv6源路由条目

在VRouter配置模式下，使用以下命令添加一条源路由条目：

```
ipv6 route source ipv6-address/M { null0 | ipv6-address / interface-name | vrouter vrouter-name } [distance-value] [name name] [weight weight-value] [description description] [track track-name]
```

- *ipv6-address/M* – 指定源地址网段。
- **null0** | *A.B.C.D* / *interface-name* | **vrouter** *vrouter-name* – 指定下一跳。可以是Null0接口（即黑洞路由）、网关地址（*ipv6-address*）、VRouter（*vrouter vrouter-name*）或者接口（*interface-name*）。
- *distance-value* – 指定路由的管理距离大小。该参数设定路由的优先级，取值越小，优先级越高，而在有多条路由选择的时候，优先级高的路由会被优先使用。取值范围是1到255，默认值为1。当路由距离为255时，该路由无效。
- *name* – 指定路由名称。
- *weight-value* – 指定路由权值的大小。路由权值决定负载均衡中流量转发的权重。范围是1到255，默认值是1。
- **description** *description* - 指定路由的描述信息。范围是1到63个字符。
- **track** *track-name* – 指定已创建的监测对象名称。指定后，若针对该监测对象的监测失败，则该路由无效。

使用多条该命令添加多条源路由条目。

使用以上命令no的形式删除指定的源路由条目：

```
no ipv6 route source ipv6-address/M { null0 | ipv6-address / interface-name | vrouter vrouter-name } [description description]
```

查看IPv4/IPv6源路由条目信息

用户可以在任何模式下通过show命令查看源路由条目信息。在任何模式下，使用以下命令：

```
show {ip | ipv6} route source [vrouter vrouter-name]
```

- **ip** - 查看IPv4类型的源路由信息。
- **ipv6** - 查看IPv6类型的源路由信息,。
- **vrouter-name** - 显示指定的VRouter的源路由信息。

源接口路由

源接口路由的配置也需要在VRouter配置模式下完成。进入VRouter配置模式，在全局配置模式下，使用以下命令：

```
ip vrouter vrouter-name
```

添加IPv4源接口路由条目

在VRouter配置模式下，使用以下命令添加一条源接口路由条目：

```
ip route source in-interface interface-name { A.B.C.D/M | A.B.C.D A.B.C.D } { null0 | A.B.C.D | interface-name | vrouter vrouter-name } [distance-value] [weight weight-value] [schedule schedule-name][description description][track track-name]
```

- *interface-name* - 指定路由条目的入接口。
- *A.B.C.D/M* | *A.B.C.D A.B.C.D* - 指定路由条目的源网络地址。设备支持两种方式，*A.B.C.D/M*或者*A.B.C.D A.B.C.D*，例如1.1.1.0/24或者1.1.1.0 255.255.255.0。
- **null0** | *A.B.C.D* | *interface-name* | **vrouter** *vrouter-name* - 指定下一跳。可以是Null0接口（即黑洞路由）、网关地址（*A.B.C.D*）、接口（*interface-name*）或者VRouter（**vrouter** *vrouter-name*）。
- *distance-value* - 指定路由的管理距离大小。该参数设定路由的优先级，取值越小，优先级越高，而在有多条路由选择的时候，优先级高的路由会被优先使用。取值范围是1到255，默认值为1。当路由距离为255时，该路由无效。
- **weight** *weight-value* - 指定路由权值的大小。路由权值决定负载均衡中流量转发的权重。范围是1到255，默认值是1。
- **schedule** *schedule-name* - 指定时间表名称。该条配置将会在时间表指定的时间范围内生效。可配置多次该命令指定多个时间表（最多8个）。为避免产生不可预知的问题，建议用户不要配置时间重叠的时间表。

- **description** *description* - 指定路由的描述信息。范围是1到63个字符。
- **track** *track-name* - 指定已创建的监测对象名称。指定后，若针对该监测对象的监测失败，则该路由无效。

使用以上命令no的形式删除指定的源接口路由条目：

```
no ip route source in-interface interface-name { A.B.C.D/M | A.B.C.D A.B.C.D } { null0 | A.B.C.D | interface-name | vrouter vrouter-name } [description description]
```

添加IPv6源接口路由条目

在VRouter配置模式下，使用以下命令添加一条源接口路由条目：

```
ipv6 route source in-interface interface-name ipv6-address/M { null0 | ipv6-address | interface-name | vrouter vrouter-name } [distance-value] [weight weight-value] [description description] [track track-name]
```

- *interface-name* - 指定路由条目的入接口。
- *ipv6-address/M* - 指定源地址网段。
- **null0** | *ipv6-address* | *interface-name* | **vrouter** *vrouter-name* - 指定下一跳。可以是Null0接口（即黑洞路由）、网关地址（*ipv6-address*）、VRouter（**vrouter** *vrouter-name*）或者接口（*interface-name*）。
- *distance-value* - 指定路由的管理距离大小。该参数设定路由的优先级，取值越小，优先级越高，而在有多条路由选择的时候，优先级高的路由会被优先使用。取值范围是1到255，默认值为1。当路由距离为255时，该路由无效。
- *weight-value* - 指定路由权值的大小。路由权值决定负载均衡中流量转发的权重。范围是1到255，默认值是1。
- **description** *description* - 指定路由的描述信息。范围是1到63个字符。
- **track** *track-name* - 指定已创建的监测对象名称。指定后，若针对该监测对象的监测失败，则该路由无效。

使用多条该命令添加多条源接口路由条目。

使用以上命令no的形式删除指定的源接口路由条目：

```
no ipv6 route source in-interface interface-name ipv6-address/M { null0 | ipv6-address | interface-name | vrouter vrouter-name } [description description]
```

查看IPv4/IPv6源接口路由条目信息

用户可以在任何模式下通过show命令查看源接口路由条目信息。在任何模式下，使用以下命令：

```
show {ip | ipv6} route source in-interface interface-name
```

IPv4 ISP路由

很多用户通常会申请多条线路进行流量负载均衡。然而，一般的均衡是不会根据流量的流向做均衡的，如果网通的服务器通过电信访问，网速就会很慢。设备针对该问题，提供ISP路由功能，使不同ISP流量走专有路由，从而提高网络速度。

配置IPv4 ISP路由，用户首先需要将子网条目添加到一个IPv4 ISP，然后才可以配置以ISP名称为目的地的IPv4 ISP路由。用户可以自定义IPv4类型的ISP信息，也可以上传包含不同ISP信息的配置文件。同时系统提供预定义IPv4 ISP配置文件包含三个ISP，分别是中国电信（China-telecom）、中国联通（China-unicom）和中国移动（China-mobile）。

配置ISP路由，用户需要进行的操作如下：

- 配置IPv4 ISP信息
- 配置IPv4 ISP路由
- 上传IPv4 ISP配置文件
- 查看IPv4 ISP路由配置信息
- 删除已上传的预定义IPv4 ISP配置文件

配置IPv4 ISP信息

在设备上配置IPv4 ISP信息，首先需要进入IPv4 ISP信息配置模式。在全局配置模式下，使用以下命令，创建IPv4 ISP名称并且进入IPv4 ISP信息配置模式：

```
isp-network isp-name
```

- *isp-name* – 指定ISP名称。

在全局配置模式下，使用该命令no的形式删除指定名称的IPv4 ISP：

```
no isp-network isp-name
```

添加IPv4子网条目

为IPv4 ISP添加子网条目，在IPv4 ISP信息配置模式下，使用以下命令：

```
subnet A.B.C.D/M
```

- *A.B.C.D/M* – 为IPv4 ISP指定子网，格式为IP地址/掩码，例如1.1.1.0/24，系统最多允许添加的子网条目数根据平台不同而不同，范围是1000-6000个。

在IPv4 ISP信息配置模式下配置多条该命令，为IPv4 ISP添加多个子网。

在IPv4 ISP信息配置模式下使用该命令no的形式删除指定的子网：

```
no subnet A.B.C.D/M
```

添加IPv4 ISP信息条目

为IPv4 ISP添加IPv4 ISP信息条目，即添加其他已配置的IPv4 ISP信息（预定义IPv4 ISP信息或自定义IPv4 ISP信息），在IPv4 ISP信息配置模式下，使用以下命令：

```
member isp-name
```

- *isp-name* – 指定IPv4 ISP名称。系统支持的IPv4 ISP嵌套层数最多为1层，并且不支持回环嵌套，IPv4 ISP信息不可以再嵌套它所属的IPv4 ISP信息。

在IPv4 ISP信息配置模式下配置多条该命令，为ISP添加多个IPv4 ISP信息条目。系统最多允许添加8个IPv4 ISP信息条目。

在IPv4 ISP信息配置模式下使用该命令no的形式删除指定嵌套的IPv4 ISP信息条目：

```
no member isp-name
```



注意：IPv4 ISP信息和IPv6 ISP信息不允许相互嵌套。

配置IPv4 ISP路由

IPv4 ISP路由需要在VRouter配置模式下进行配置。进入VRouter配置模式，在全局配置模式下使用以下命令：

ip vrouter *vrouter-name*

- *vrouter-name* – 指定VRouter的名称。

在VRouter配置模式，使用以下命令配置IPv4 ISP路由条目：

ip route *isp-name* { *A.B.C.D* | *interface-name* | **vrouter** *vrouter-name* } [*distance-value*] [**weight** *weight-value*] [**description** *description*] [**schedule** *schedule-name*]

- *isp-name* – 指定系统中已存在的IPv4 ISP名称作为路由的目的地址。
- *A.B.C.D* | *interface-name* | **vrouter** *vrouter-name* – 指定下一跳。可以是网关地址 (*A.B.C.D*)、接口 (*interface-name*) 或者VRouter (**vrouter** *vrouter-name*)。当下一跳为接口时，用户可以选择隧道接口名称、Null0接口或者PPPoE接口。
- *distance-value* – 指定路由的管理距离大小。该参数设定路由的优先级，取值越小，优先级越高，而在有多条路由选择的时候，优先级高的路由会被优先使用。取值范围是1到255，默认值为1。当路由距离为255时，该路由无效。
- **weight** *weight-value* – 指定路由权值的大小。路由权值决定负载均衡中流量转发的比重。范围是1到255，默认值是1。
- **description** *description* – 指定路由的描述信息。范围是1到63个字符。
- **schedule** *schedule-name* – 指定时间表名称。该条配置将会在时间表指定的时间范围内生效。可配置多次该命令指定多个时间表（最多8个）。为避免产生不可预知的问题，建议用户不要配置时间重叠的时间表。

使用多条该命令添加多条IPv4 ISP路由条目。

使用以上命令no的形式删除指定的IPv4 ISP路由条目：

no ip route *isp-name* { *A.B.C.D* | *interface-name* | **vrouter** *vrouter-name* } [*distance-value*] [**weight** *weight-value*] [**description** *description*] [**schedule** *schedule-name*]

查看IPv4 ISP路由配置信息

用户可以通过show命令查看IPv4 ISP路由配置信息。

- 查看预定义IPv4 ISP配置文件信息：
show pre-isp-network { **all** | *isp-name* }

- 查看自定义IPv4 ISP配置文件信息：

```
show isp-network {all | isp-name}
```

- 查看IPv4 ISP路由条目：

```
show ip route isp [isp-name | vrouter vrouter-name]
```

上传IPv4 ISP配置文件

设备支持两种IPv4 ISP配置文件，分别是用户自定义IPv4 ISP配置文件和系统预定义IPv4 ISP配置文件。

- 自定义IPv4 ISP配置文件：请按照下所示实例格式书写用户自定义配置文件，否则，即使文件上传成功，也不可以在系统中生效。用户自定义配置文件中包含的IPv4 ISP的个数最多为26个，也就是作为索引值的26个英文字母的个数。

```
# NOTICE: Keep the following comment lines intact!!!

E --- China-55

R --- China-66

# China-55

E:55.10.2.0/24

E:55.10.3.0/24

# China-66

R:66.20.2.0/24

R:66.20.3.0/24
```

- 预定义IPv4 ISP配置文件：系统预定义IPv4 ISP配置文件为加密形式，设备出厂时系统自带预定义ISP配置文件，在山石网科更新预定义IPv4 ISP配置文件版本后，用户可以通过上传至系统中实现升级。

用户可以通过FTP和TFTP服务器升级预定义IPv4 ISP配置文件或者上传自定义IPv4 ISP配置文件，在执行模式下，使用以下命令：

```
import ispfile from {ftp server ip-address [vrouter vrouter-name][user username password string] |
```

```
tftp server ip-address [vrouter vrouter-name][user username password string] | usb1} file-name
```

- **ftp server** *ip-address* - 指定FTP服务器的IP地址。
- **user** *username password string* - 指定FTP服务器的用户名和密码。
- **tftp server** *ip-address* - 指定TFTP服务器的IP地址。
- **vrouter** *vrouter-name* - 指定FTP/TFTP服务器所属的VRouter。
- **usb1** - 指定从U盘获取IPv4 ISP配置文件。
- *file-name* - 指定预定义IPv4 ISP配置文件的名称或者自定义IPv4 ISP配置文件名称。

删除已上传的预定义IPv4 ISP配置文件

如果已经上传过预定义IPv4 ISP配置文件，用户可以在执行模式下，通过使用以下命令将上传的预定义IPv4 ISP配置文件从系统中删除：

exec isp-network clear-predefine

执行该命令后，重启系统，系统将恢复使用原有的预定义IPv4 ISP配置文件（出厂时系统自带的预定义IPv4 ISP配置文件）。

IPv6 ISP路由

很多用户通常会申请多条线路进行流量负载均衡。然而，一般的均衡是不会根据流量的流向做均衡的，如果网通的服务器通过电信访问，网速就会很慢。设备针对该问题，提供ISP路由功能，使不同ISP流量走专有路由，从而提高网络速度。

配置IPv6 ISP路由，用户首先需要将子网条目添加到一个IPv6类型的ISP，然后才可以配置以ISP名称为目的地的IPv6 ISP路由。用户可以自定义IPv6 类型的ISP信息，也可以上传包含不同ISP信息的配置文件。同时系统提供预定义IPv6 ISP配置文件包含三个ISP，分别是中国电信（China-telecom-v6）、中国联通（China-unicom-v6）和中国移动（China-mobile-v6）。

配置ISP路由，用户需要进行的操作如下：

- 配置IPv6 ISP信息
- 配置IPv6 ISP路由
- 上传IPv6 ISP配置文件

- 查看IPv6 ISP路由配置信息
- 删除已上传的预定义IPv6 ISP配置文件

配置IPv6 ISP信息

在设备上配置IPv6 ISP信息，首先需要进入IPv6 ISP信息配置模式。在全局配置模式下，使用以下命令，创建IPv6 ISP名称并且进入IPv6 ISP信息配置模式：

```
isp-network isp-name ipv6
```

- *isp-name* - 指定IPv6 ISP名称，系统最多允许创建26个 IPv6 ISP信息。
- **ipv6** - 指定ISP信息类型为IPv6.

在全局配置模式下，使用该命令**no**的形式删除指定名称的IPv6 ISP：

```
no isp-network isp-name
```

添加IPv6子网条目

为IPv6 ISP添加子网条目，在IPv6 ISP信息配置模式下，使用以下命令：

```
subnet ipv6-address/prefix
```

- *ipv6-address/prefix* - 为IPv6 ISP指定子网，格式为IPv6地址/前缀长度，例如1::1/64，系统最多允许添加的子网条目数根据平台不同而不同，范围是1000-6000个。

在IPv6 ISP信息配置模式下配置多条该命令，为IPv6 ISP添加多个子网。

在IPv6 ISP信息配置模式下使用该命令**no**的形式删除指定的子网：

```
no subnet ipv6-address/prefix
```

添加IPv6 ISP信息条目

为IPv6 ISP添加IPv6 ISP信息条目，即添加其他已配置的IPv6 ISP信息（预定义IPv6 ISP信息或自定义IPv6 ISP信息），在IPv6 ISP信息配置模式下，使用以下命令：

```
member isp-name
```

- *isp-name* – 指定IPv6 ISP名称。系统支持的IPv6 ISP嵌套层数最多为1层，并且不支持回环嵌套，IPv6 ISP信息不可以再嵌套它所属的IPv6 ISP信息。

在IPv6 ISP信息配置模式下配置多条该命令，为IPv6 ISP添加多个IPv6 ISP信息条目。系统最多允许添加8个IPv6 ISP信息条目。

在IPv6 ISP信息配置模式下使用该命令no的形式删除指定嵌套的IPv6 ISP信息条目：

no member *isp-name*



注意: IPv6 ISP信息和IPv4 ISP信息不允许相互嵌套。

配置IPv6 ISP路由

IPv6 ISP路由需要在VRouter配置模式下进行配置。进入VRouter配置模式，在全局配置模式下使用以下命令：

ip vrouter *vrouter-name*

- *vrouter-name* – 指定VRouter的名称。

在VRouter配置模式，使用以下命令配置IPv6 ISP路由条目：

ipv6 route *isp-name* { *ipv6-address/prefix* | *interface-name* | **vrouter** *vrouter-name* } [*distance-value*]
[**weight** *weight-value*] [**description** *description*] [**schedule** *schedule-name*]

- *isp-name* – 指定系统中已存在的IPv6 ISP名称作为路由的目的地址。
- *ipv6-address/prefix* | *interface-name* | **vrouter** *vrouter-name* – 指定下一跳。可以是网关地址（*ipv6-address/prefix*）、接口（*interface-name*）或者VRouter（**vrouter** *vrouter-name*）。当下一跳为接口时，用户可以选择隧道接口名称、Null0接口或者PPPoE接口。
- *distance-value* – 指定路由的管理距离大小。该参数设定路由的优先级，取值越小，优先级越高，而在有多条路由选择的时候，优先级高的路由会被优先使用。取值范围是1到255，默认值为1。当路由距离为255时，该路由无效。
- **weight** *weight-value* – 指定路由权值的大小。路由权值决定负载均衡中流量转发的比重。范围是1到255，默认值是1。
- **description** *description* – 指定路由的描述信息。范围是1到63个字符。

- **schedule** *schedule-name* - 指定时间表名称。该条配置将会在时间表指定的时间范围内生效。可配置多次该命令指定多个时间表（最多8个）。为避免产生不可预知的问题，建议用户不要配置时间重叠的时间表。

使用多条该命令添加多条IPv6 ISP路由条目。

使用以上命令no的形式删除指定的IPv6 ISP路由条目：

```
no ipv6 route isp-name { ipv6-address/prefix | interface-name | vrouter vrouter-name } [distance-value] [weight weight-value] [description description] [schedule schedule-name]
```

查看IPv6 ISP信息

用户可以通过show命令查看IPv6 ISP配置文件信息，在任何模式下，使用以下命令：

- 查看预定义IPv6 ISP配置文件信息：
show ipv6 pre-isp-network {**all** | *isp-name*}
- 查看自定义IPv6 ISP配置文件信息：
show ipv6 isp-network {**all** | *isp-name*}

上传IPv6 ISP配置文件

设备支持两种IPv6 ISP配置文件，分别是用户自定义IPv6 ISP配置文件和系统预定义IPv6 ISP配置文件。用户仅可通过WebUI方式上传自定义IPv6 ISP配置文件。

用户可以通过FTP和TFTP服务器升级预定义IPv6 ISP配置文件，在执行模式下，使用以下命令：

```
import ispfile from {ftp server ip-address [vrouter vrouter-name] [user username password string] | tftp server ip-address [vrouter vrouter-name] [user username password string] | usb1} file-name
```

- **ftp server** *ip-address* - 指定FTP服务器的IP地址。
- **user** *username* **password** *string* - 指定FTP服务器的用户名和密码。
- **tftp server** *ip-address* - 指定TFTP服务器的IP地址。
- **vrouter** *vrouter-name* - 指定FTP/TFTP服务器所属的VRouter。
- **usb1** - 指定从U盘获取IPv6 ISP配置文件。
- *file-name* - 指定预定义IPv6 ISP配置文件的名称。

删除已上传的预定义IPv6 ISP配置文件

如果已经上传过预定义IPv6 ISP配置文件，用户可以在执行模式下，通过使用以下命令将上传的预定义IPv6 ISP配置文件从系统中删除：

```
exec isp-network clear-predefine ipv6
```

执行该命令后，重启系统，系统将恢复使用原有的预定义IPv6 ISP配置文件（出厂时系统自带的预定义IPv6 ISP配置文件）。



注意: 为保证预定义IPv6 ISP配置文件能够正常删除，请在删除已上传的预定义IPv6 ISP配置文件前，先删除嵌套的IPv6 ISP信息条目。

策略路由

策略路由功能检查数据包的源IP、目的IP和服务类型，对匹配策略的数据包的下一跳进行指定。

创建PBR策略

创建PBR策略，在全局配置模式下使用以下命令：

```
pbr-policy name
```

- *name* – 指定PBR策略名，名称范围是1到31个字符。如果该策略已经创建，则直接进入PBR策略配置模式。

使用**no pbr-policy name**删除指定的PBR策略。

创建PBR规则

进入PBR策略配置模式下，用户便可定义自己的PBR规则，系统支持配置IPv4和IPv6两种地址检测类型。在PBR策略配置模式下，使用以下命令创建PBR规则：

```
{match | match-v6} [id rule-id] [before rule-id | after rule-id | top] src-addr dst-addr service-name  
[application-name] nexthop {interface-name | A.B.C.D/X:X:X:X::X | vrouter vrouter-name | vsys  
vsys-name} [weight value] [track track-object-name]
```

- **match** - 指定创建的PBR规则检测的是IPv4类型的地址。
- **match-v6** - 指定创建的PBR规则检测的是IPv6类型的地址。
- **id rule-id** - 指定新建策略规则的ID，取值范围为1到255。如果不指定，系统将会为PBR规则自动分配一个ID。规则ID在该PBR策略中必须是唯一的。
- **before rule-id | after rule-id | top** - 指定PBR规则的位置，可以是某个规则之前（**before rule-id**）、某个规则之后（**after rule-id**）或者所有规则的首位（**top**）。默认情况下，系统会将新创建的策略规则放到所有规则的末尾。
- **src-addr** - 指定源地址，该地址为地址簿条目。
- **dst-addr** - 指定目的地址，该地址为地址簿条目。
- **service-name** - 指定服务名称。**service-name**为服务簿中定义的服务。
- **application-name** - 指定应用名称。**application-name**为应用簿中定义的应用。
- **nexthop { interface-name | A.B.C.D/X:X:X:X::X | vrouter vrouter-name | vsys vsys-name }** - 指定下一跳。**interface-name**为出接口的名称，**A.B.C.D/X:X:X:X::X**为下一跳的IPv4或IPv6地址，**vrouter vrouter-name**为VRouter，**vsys vsys-name**为虚拟系统。
- **weight value** - 指定下一跳的权重，取值范围是1到255，默认值是1。如果一条策略路由匹配多个下一跳，系统会按照权重值比例分配流量。
- **track track-object-name** - 指定下一跳的监测对象。如果监控对象失败，本条策略路由也会失败。关于如何配置监测对象，请参阅“系统管理”的“配置监测对象”部分。

使用该命令**no**的形式删除指定ID的规则。在PBR策略配置模式下，执行以下命令：

```
no { match | match-v6 } id rule-id
```

另外，用户还可以在PBR策略配置模式下使用以下命令，创建一个策略规则ID，并且进入PBR策略规则配置模式，再进一步配置其它策略规则相关参数：

```
{ match | match-v6 } [ id rule-id ] [ before rule-id | after rule-id | top ]
```

- **id id** - 指定PBR策略规则的ID。如果不指定，系统将会为策略规则自动分配一个ID。规则ID在整个系统中必须是唯一的。策略规则的ID大小并不表示策略规则的匹配先后顺序。

- **top** | **before rule-id** | **after rule-id** – 指定策略规则的位置，可以是某个规则ID之前（before id）、某个规则ID之后（after id）或者所有规则的首位（top）。默认情况下，系统会将新创建的策略规则放到所有规则的末尾。

编辑PBR策略规则

创建好的PBR策略规则可以通过编辑来修改不合适的参数值，但是修改工作必须在PBR策略规则配置模式下才可以进行。在CLI中进入PBR策略规则配置模式，请输入以下命令：

- **{match | match-v6} [id rule-id] [before rule-id | after rule-id | top]**
- **{match | match-v6} rule-id**（该命令适用于规则ID已存在的情况，并且用该命令no的形式，可以删除该条规则，即**no match id rule-id**）

进入PBR策略规则配置模式后，使用以下命令编辑策略规则：

- 添加地址簿条目类型源地址：**src-addr src-addr**
- 删除地址簿条目类型源地址：**no src-addr src-addr**
- 添加IPv4成员类型源地址：**src-ip {A.B.C.D/netmask | ipv4-address netmask}**
- 删除IPv4成员类型源地址：**no src-ip {A.B.C.D/netmask | ipv4-address netmask}**
- 添加IPv6成员类型源地址：**src-ip {X:X:X:X::X | ipv6-address/prefix}**
- 删除IPv6成员类型源地址：**no src-ip {X:X:X:X::X | ipv6-address/prefix}**
- 添加主机成员类型源地址：**src-host host-name**
- 删除主机成员类型源地址：**no src-host host-name**
- 添加IP地址范围类型源地址：**src-range min-ip [max-ip]**
- 删除IP地址范围类型源地址：**no src-range min-ip [max-ip]**
- 添加地址簿条目类型目的地址：**dst-addr dst-addr**
- 删除地址簿条目类型目的地址：**no dst-addr dst-addr**
- 添加IPv4成员类型目的地址：**dst-ip A.B.C.D/netmask**

- 删除IPv4成员类型目的地址: **no dst-ip** *A.B.C.D/netmask*
- 添加IPv6成员类型目的地址: **dst-ip** *ipv6-address/prefix*
- 删除IPv6成员类型目的地址: **no dst-ip** *ipv6-address/prefix*
- 添加主机成员类型目的地址: **dst-host** *host-name*
- 删除主机成员类型目的地址: **no dst-host** *host-name*
- 添加IP地址范围类型目的地址: **dst-range** *min-ip [max-ip]*
- 删除IP地址范围类型目的地址: **no dst-range** *min-ip [max-ip]*
- 添加角色类型源用户: **role** *role-name*
- 删除角色类型源用户: **no role** *role-name*
- 添加用户类型源用户: **user** *aaa-server-name user-name*
- 删除用户类型源用户: **no user** *aaa-server-name user-name*
- 添加用户组类型源用户: **user-group** *aaa-server-name user-group-name*
- 删除用户组类型源用户: **no user-group** *aaa-server-name user-group-name*
- 添加虚拟服务器类型: **virtual-server** *virtual-server-name*
- 删除虚拟服务器类型: **no virtual-server** *virtual-server-name*
- 添加域名簿类型: **host-book** *host-book-name*
- 删除域名簿类型: **no host-book** *host-book-name*
- 添加服务类型: **service** *service-name*
- 删除服务类型: **no service** *service-name*
- 添加应用类型: **application** *application-name*
- 删除应用类型: **no application** *application-name*

- 指定下一跳: **nexthop** {*interface-name* | *A.B.C.D/X:X:X:X::X* | *vrouter-name* | **vsys** *vsys-name*}
- 取消下一跳配置: **no nexthop**
- 配置时间表: **schedule** *schedule-name*
- 删除时间表: **no schedule**
- 添加规则描述: **description** *string*
- 删除规则描述: **no description**
- 开启日志记录功能: **log enable**
- 关闭日志记录功能: **no log enable**

启用/禁用PBR策略规则

默认情况下，配置好的PBR策略规则会在系统中立即生效。用户可以通过命令禁用某条策略规则，使其不对流量进行控制。禁用或者启用某条策略规则，在PBR策略规则配置模式下，使用以下命令：

- 禁用: **disable**
- 启用: **enable**

修改规则排列顺序

PBR策略中的规则通过ID进行唯一标识。流量进入设备时，设备对PBR策略规则进行顺序查找，然后按照查找到的相匹配的第一条规则对流量进行处理。但是，PBR策略规则ID的大小顺序并不是规则查找时的匹配顺序。使用**show pbr-policy**命令列出的规则顺序才是规则匹配顺序（系统将由上到下进行查找匹配）。用户在创建PBR策略规则时可以指定该规则的排列位置，也可以在PBR策略配置模式下修改其位置。PBR策略规则的排列位置可以是绝对位置，即处在首位（Top）或者处在末位（Bottom），也可以是相对位置，即位于某个ID之前或之后。修改规则排列顺序，在PBR策略配置模式下使用以下命令：

move *rule-id* {**top** | **bottom** | **before** *rule-id* | **after** *rule-id*}

配置目的路由优先查找

默认情况下，设备对进入的数据包进行转发时，按照这样的顺序选路：策略路由→源接口路由→源路由→目的路由，在某些情况下，用户需要使匹配PBR策略规则的数据包，转发时优先查找目的路由，即选路的顺序为：目的路由→策略路由。配置PBR策略规则的目的路由（DBR）优先查找，在PBR策略规则配置模式下，使用以下命令：

```
fib-lookup dbr-first
```

使用以上命令no的形式取消PBR策略规则的目的路由（DBR）优先查找：**no fib-lookup dbr-first**

应用PBR策略

可以通过绑定PBR策略到接口、安全域或者VRouter来实现PBR策略的应用。在接口配置模式、安全域配置模式或VRouter配置模式下，使用以下命令：

```
bind pbr-policy name
```

- *name* – 绑定指定的PBR策略到接口、安全域或者VRouter。

使用以上命令no的形式取消PBR策略在接口、安全域或者VRouter的绑定：

```
no bind pbr-policy
```

配置PBR策略全局匹配顺序

默认情况下，如果接口和其所在安全域或者VRouter绑定了PBR策略，流量匹配顺序为：接口->安全域->VRouter。用户可以根据需要自行配置PBR策略的全局匹配顺序，在全局配置模式下，使用以下命令：

```
pbr-match order index
```

- *index* – 为PBR策略指定全局匹配顺序的排序指数。包括1-6，顺序分别表示如下：
 - 1 - 接口->安全域->Vrouter。该排序指数为默认值。
 - 2 - 安全域->接口 ->Vrouter。
 - 3 - Vrouter ->安全域->接口。
 - 4 - 接口-> Vrouter ->安全域。

- 5 - Vrouter ->接口->安全域。
- 6 - 安全域-> Vrouter->接口。

使用**no pbr-match**恢复默认匹配顺序配置。

显示PBR策略全局匹配顺序

用户可以在任何模式下，通过show命令查看PBR策略规则的全局匹配顺序信息。具体命令以下：

```
show pbr-match order
```

策略路由规则支持配置TTL

用户可以在PBR规则中配置报文的TTL，符合条件的报文将被设备转发到特定的出口链路。配置TTL，请先执行以下命令进入PBR策略规则配置模式：

- {**match** | **match-v6**} [**id rule-id**] [**before rule-id** | **after rule-id** | **top**]
- {**match** | **match-v6**} **id rule-id**（该命令适用于规则ID已存在的情况）

在PBR策略规则配置模式下，输入以下命令：

```
ttl-range min-ttl max-ttl
```

- *min-ttl max-ttl* – 指定策略路由规则中报文的生存时间范围。*min-ttl*指定生存时间的最小值，取值范围为1到255；*max-ttl*指定生存时间的最大值，取值范围为1到255。

在PBR策略规则配置模式下，执行**no ttl-range**命令取消TTL范围的配置。

查看PBR策略规则信息

用户可以在任何模式下，通过show命令查看PBR策略规则的具体信息。具体命令以下：

```
show pbr-policy [name]
```

- *name* – 显示指定PBR策略的详细信息。如果不指定名称则显示所有PBR策略的详细信息。

动态路由

动态路由是根据网络系统的运行情况而自动调整的路由。设备根据路由协议自动调整动态路由表。系统支持RIP、OSPF、IS-IS和BGP三种动态路由协议。

RIP

RIP（Routing Information Protocol）是路由信息协议。它是一种在路由器之间交换路由信息的内部网关路由协议。目前，RIP有RIP-1和RIP-2两个版本，设备均支持。

对RIP协议的配置包括基本配置、引入路由、被动接口、邻居、网络和距离。另外，RIP参数配置完成后，用户还需要在不同的接口上配置RIP参数，包括指定接口接收和发送更新的RIP版本号、水平分割以及接口的RIP认证。

基本配置

RIP协议的基本配置包括指定RIP版本号、指定缺省度量、指定缺省距离、配置缺省信息发布以及配置定时器（时间间隔、失效时间、保持时间和清除时间）。用户可以为不同的VRouter分别配置RIP协议。对RIP协议的基本配置需要在RIP路由模式下进行。进入RIP路由模式，请在全局配置模式下，使用以下命令：

ip vrouter *vrouter-name* （进入VRouter配置模式）

router rip （进入RIP路由模式，同时开启设备的RIP功能）

在VRouter配置模式下，使用**no router rip**关闭RIP功能。

指定版本号

设备支持RIP-1和RIP-2两个版本。RIP-1以广播方式传输报文；而RIP-2使用组播方式。指定RIP协议版本号，在RIP路由模式使用以下命令：

version *version-number*

- *version-number* – 指定版本号，1（RIP-1）或者2（RIP-2）。默认为2。

使用**no version**命令恢复默认版本配置。

指定缺省度量

RIP协议使用跳数来衡量到达目的网络的距离，称为度量。路由器到与它直接相连网络的度量为1，通过一个路由器可达的网络的度量为2，依此类推，度量的最大值可以到15，度量大于15的网络为不可达网络。缺省度量在引入路由时生效。指定RIP的缺省度量，在RIP路由配置模式下使用以下命令：

default-metric *value*

- *value* – 指定缺省度量值。范围是1到15，默认值是1。

使用**no default-metric**命令恢复缺省度量值。

指定缺省距离

指定RIP路由的缺省距离，在RIP路由配置模式下使用以下命令：

distance *distance-value*

- *distance-value* – 指定缺省管理距离。范围是1到255，默认值是120。

使用**no distance**命令恢复缺省距离值。

配置缺省信息发布

用户可以指定是否默认路由发布到其它使用RIP协议的路由器。默认情况下，RIP协议不发送默认路由。配置缺省信息发布，在RIP路由配置模式下使用以下命令：

发送：**default-information originate**

不发送：**no default-information originate**

配置定时器

RIP可配置的定时器分别是时间间隔（Interval）、失效时间（Invalid）、保持时间（Holddown）和清除时间（Flush）。具体描述如下：

- 时间间隔：每次向所有邻居发送全部RIP路由所间隔的时间。默认是30秒。
- 失效时间：如果一条路由在失效时间内一直没有被更新，该路由的度量就会被标记为16，表示为不可达路由。默认的失效时间是180秒。
- 保持时间：如果一条更新后的路由的度量变大，例如，从2更新到4，该路由会被赋予一个保持时间，路由在保持时间内，不接受任何更新。默认的保持时间是180秒。
- 清除时间：度量被标记为16的不可达路由会一直被发布到其它RIP协议路由，直到清除时间结束；如果该路由仍没有被更新，清除时间结束后，将会被从RIP路由信息数据库中删除。默认的清除时间是240秒。

用户可以修改以上四个定时器的时间值。配置定时器，在RIP路由配置模式下使用以下命令：

timers basic *interval-time invalid-time holddown-time flush-time*

- *interval-time* – 指定发送更新的时间间隔，单位为秒。范围是0到16777215秒。默认值是30秒。
- *invalid-time* – 指定路由的失效时间，单位为秒。范围是1到16777215秒。默认值是180秒。

- *holddown-time* – 指定路由的保持时间，单位为秒。范围是1到16777215秒。默认值是180秒。
- *flush-time* – 指定路由的清除时间，单位为秒。范围是1到16777215秒。默认值是240秒。

使用**no timers basic**命令恢复定时器的默认值。

引入路由

RIP协议允许用户将设备上其它路由协议（BGP、直连、静态和OSPF）的路由信息引入到RIP中，并向外发布。同时，用户可以设置被引入路由的度量。配置引入路由，在RIP路由配置模式下使用以下命令：

redistribute {bgp | connected | static | ospf} [metric value]

- **bgp | connected | static | ospf** – 指定引入路由的类型，可以是BGP（**bgp**）、直连路由（**connected**）、静态路由（**static**）或者OSPF（**ospf**）。
- **metric value** – 指定引入路由的度量。范围是1到15。如果不指定该数值，系统会使用RIP的缺省度量（通过**default-metric value**配置）。

用户可以配置多条该命令引入不同类型的路由。

使用**no redistribute {bgp | connected | static | ospf}**命令取消指定类型路由的引入。

配置被动接口

用户可以将一些接口配置为只接收更新但是不发送，这种只接收更新的接口就是被动接口。配置被动接口，在RIP路由配置模式下使用以下命令：

passive-interface interface-name

- *interface-name* – 指定接口的名称作为被动接口。

用户可以配置多条该命令添加多个被动接口。

使用**no passive-interface interface-name**命令取消被动接口的配置。

配置邻居

用户可以指定一些邻居，使邻居和设备之间能够允许点到点（非广播）的RIP信息交换。指定邻居，在RIP路由配置模式下使用以下命令：

neighbor *ip-address*

- *ip-address* – 指定邻居的IP地址。

用户可以配置多条该命令添加多个邻居。

使用**no neighbor** *ip-address*命令删除指定的邻居。

配置网络

用户需要配置一些网络，只有在指定网络中的接口才能接收和发送RIP更新。配置网络，在RIP路由配置模式下使用以下命令：

network *ip-address/netmask*

- *ip-address/netmask* – 指定网络的IP地址，例如10.200.0.0/16。

用户可以配置多条该命令添加多个网络。

使用**no network** *ip-address/netmask*命令删除指定的网络。

配置距离

用户可以为从一些指定网络得到的路由指定管理距离。配置距离，在RIP路由配置模式下使用以下命令：

distance *distance-value ip-address/netmask*

- *distance-value* – 指定管理距离。范围是1到255。用该命令指定的距离优先级高于RIP基本配置中的缺省距离（通过**distance** *distance-value*指定）。
- *ip-address/netmask* – 指定网络的IP地址，例如10.200.0.0/16。

用户可以配置多条该命令为从不同的网络更新的路由指定距离。

使用**no distance** *ip-address/netmask*命令删除指定的管理距离。

RIP数据库

设备运行RIP协议，就拥有一个RIP路由数据库，该数据库中储存了所有可达目的网络的路由条目。路由条目包含的信息有目的地址、下一跳、度量、来源以及定时器信息。用户可以在任何模式下，通过以下命令，随时查看RIP数据库的信息：

```
show ip rip database [A.B.C.D/M] [vrouter vrouter-name]
```

- *A.B.C.D/M* – 显示指定目的IP地址的RIP信息。
- **vrouter vrouter-name** – 显示指定VRouter的RIP信息。系统目前只支持trust-vr一个VRouter。

配置接口的RIP功能

RIP功能在设备接口上的配置包括：认证方式、发送和接收的RIP版本号以及水分割功能。接口的RIP功能配置需要在接口配置模式下完成。

配置RIP报文认证

只有RIP-2支持RIP报文认证。认证方式有两种，分别是明文认证和MD5密文认证。明文认证不能提供安全保障。未加密的认证字随RIP报文一同传送，所以明文认证不能用于安全性要求较高的情况。默认为明文认证。用户需要配置RIP报文的认证方式和认证码。在接口配置模式下，使用以下命令：

- 方式：**ip rip authentication mode {md5 | text}**
- 认证码：**ip rip authentication stringstring**

使用以上两个命令no的形式可以取消对认证方式和认证码的指定：

- **no ip rip authentication mode**
- **no ip rip authentication string**

配置发送和接收的RIP版本号

默认情况下，接口发送RIP-2信息。指定接口发送RIP信息的版本号，在接口配置模式下，使用以下命令：

```
ip rip send version [1][2]
```

- 1 – 指定只发送RIP-1的RIP信息。
- 2 – 指定只发送RIP-2的RIP信息。

使用**no ip rip send version**命令恢复默认版本号。

默认情况下，接口接收RIP-2信息。指定接口接收RIP信息的版本号，在接口配置模式下，使用以下命令：

ip rip receive version [1][2]

- 1 – 指定只接收RIP-1的RIP信息。
- 2 – 指定只接收RIP-2的RIP信息。

使用**no ip rip receive version**命令恢复默认版本号。

配置水平分割

水平分割是指不从本接口发送从该接口学到的路由。它可以在一定程度上避免产生路由环，保证路由的正确传播。配置水平分割功能，在接口配置模式下，使用以下命令：

- 开启水平分割：**ip rip split-horizon**
- 关闭水平分割：**no ip rip split-horizon**

显示系统RIP信息

用户可以通过show命令随时查看系统的RIP信息。查看RIP信息，在任何模式下使用以下命令：

show ip rip

OSPF

OSPF是开放式最短路径优先协议（Open Shortest Path First）的缩写。它是IETF组织开发的一个基于链路状态的内部网关协议。当前的OSPF版本为版本2（RFC2328）。OSPF适应各种规模的网络，快速收敛特性能够在网络拓扑结构发生变化后立即发送更新报文，并且其算法本身决定了不会生成路由环路。OSPF还具有以下特性：

- 区域划分：将自治系统的网络划分成区域来管理，从而减少了协议对CPU和内存的占用，提高性能。
- 无类路由：无类路由特性允许可变长子网掩码的使用。

- 等价路由：支持等价路由，提高多条路由的利用率。
- 组播发送：支持组播地址发送，减少对非OSPF设备的影响。
- 支持验证：支持基于接口的报文验证以保证路由计算的安全性。



注意：“自治系统”是处于一个管理机构控制之下的路由器和网络群组。一个自治系统中的所有路由器必须运行相同的路由协议。

OSPF协议配置

用户可以为不同的VRouter分别配置OSPF协议。OSPF协议配置包括以下各项：

- 配置Router ID
- 配置区域认证
- 配置接口的网络类型
- 配置区域的路由聚合
- 配置区域的缺省花费
- 配置区域的虚拟链路
- 配置stub区域
- 配置NSSA区域
- 配置OSPF的引用带宽
- 配置缺省度量
- 配置缺省信息发布
- 配置缺省距离
- 配置OSPF定时器
- 指定运行OSPF协议的接口网络
- 引入路由

- 配置路由映射表
- 匹配多条路由匹配规则
- 修改引入路由属性
- 配置路由访问控制列表
- 配置距离
- 配置被动接口

OSPF协议的基本配置需要在OSPF路由模式下进行。进入OSPF路由模式，请在VRouter配置模式下，使用以下命令：

ip vrouter *vrouter-name* （进入VRouter配置模式）

router ospf [*process-id*] （进入OSPF路由模式，同时开启设备的OSPF功能）

- *process-id* – 指定OSPF的进程ID。默认值是1，取值范围是1到65535。每个OSPF进程相互独立，有各自的链路状态数据库和对应的OSPF路由表信息。每一个VRouter支持最多4个OSPF进程，多个进程共同维护一个VRouter的路由表。

在指定OSPF进程ID时，注意如下事项：

- 每个OSPF进程中运行OSPF协议的接口网络不能重叠。
- 当多个OSPF进程中存在相同前缀的路由条目时，首先比较各个路由条目的管理距离，管理距离低的将被优先加入到VRouter的路由表中；管理距离相同时，优先发现的的路由条目将被加入到VRouter的路由表中。
- 当其他路由协议引入OSPF路由时，将默认引入进程ID为1的OSPF路由信息。如果此进程不存在，将无法引入OSPF路由。

在VRouter配置模式下，使用**no router ospf** [*process-id*]关闭OSPF功能。

配置Router ID

每一台运行OSPF协议的路由器都必须拥有一个Router ID。Router ID是每个路由器在整个OSPF域中唯一标识，使用IP地址的形式表示。为设备的OSPF协议配置Router ID，在OSPF路由模式下，使用以下命令：

router-id *A.B.C.D* [*local*]

- *A.B.C.D* – 指定OSPF协议使用的Router ID，为IP地址形式。
- *local* - 指定OSPF协议的Router ID为本地配置，该配置适用于HA A/A工作模式，并且不进行HA配置同步。
默认情况下，Router ID为非本地配置。

配置接口的网络类型

OSPF协议的接口的网路类型有以下三种：广播、点到点（Point-to-point）以及点到多点（Point-to-multipoint）网络类型。默认情况下，接口的网络类型为广播类型。配置接口的网络类型，在接口配置模式下，使用以下命令：

```
ip ospf network {point-to-point | point-to-multipoint}
```

- **point-to-point** – 指定接口网络类型为点到点网络类型。
- **point-to-multipoint** -指定接口网络类型为点到多点网络类型。

在隧道接口配置模式下，使用该命令**no**的形式恢复接口网络类型为广播类型：

```
no ip ospf network
```

配置区域的路由聚合

路由聚合是指将具有相同前缀的路由信息通过ABR聚合在一起，只发布一条路由到其它区域。一个区域可以配置多条聚合网段，这样OSPF可以对多个网段进行聚合。默认情况下，区域的路由聚合功能是关闭的。配置区域的路由聚合，在OSPF路由模式下，使用以下命令：

```
area {id | A.B.C.D} range {A.B.C.D/M} [advertise | not-advertise]
```

- *id | A.B.C.D* – 指定需要进行路由聚合的区域ID。区域ID用32比特数来表示，可以是数字形式，也可以是IP地址形式。
- **range {A.B.C.D/M}** – 指定被聚合的网段。
- **advertise** – 指定将这一网段的路由聚合并通告聚合后的路由。
- **not-advertise** – 指定将这一网段的路由聚合且不通告聚合后的路由。

路由聚合功能仅对区域边界路由（连接骨干区域和非骨干区域的路由器，简称为ABR）有效。

使用**no area {id | A.B.C.D} range {A.B.C.D/M} [advertise | not-advertise]**命令取消路由聚合的配置。

配置区域的缺省花费

区域的缺省花费是指将报文发送到stub区域的缺省路由花费。指定区域的缺省花费，在OSPF路由模式下，使用以下命令：

```
area {id | A.B.C.D} default-cost cost-value
```

- *id | A.B.C.D* – 指定需要指定缺省花费的区域ID。区域ID用32比特数来表示，可以是数字形式，也可以是IP地址形式。
- *cost-value* – 指定花费值。默认值是1。范围是0到16777214。

使用**no area {id | A.B.C.D} default-cost**命令恢复缺省花费的配置。



注意: 该命令仅对NSSA区域有效。

配置区域的虚拟链路

虚拟链路（Virtual Links）用来连接不连续的骨干区域，使他们能够保持逻辑上的连续性。配置虚拟链路以及定时器参数，在OSPF路由模式下，使用以下命令：

```
area {id | A.B.C.D} virtual-link A.B.C.D [hello-interval interval-value] [retransmit-interval interval-value] [transmit-delay interval-value] [dead-interval interval-value]
```

- *id | A.B.C.D* – 需要做虚拟链路进行连接的区域ID。区域ID用32比特数来表示，可以是数字形式，也可以是IP地址形式。
- **virtual-link A.B.C.D** – 指定作为虚拟链路路由器的Router ID。
- **hello-interval interval-value** – 指定接口发送Hello报文的时间间隔，单位为秒，默认值是10秒。范围是1到65535秒。
- **retransmit-interval interval-value** – 一台路由器向它的邻居发送一条LSA后需要获得对方的确认报文。若在指定的时间内没有收到对方的确认报文，就会向邻居重传这条LSA。该参数用来指定邻接路由器之间重传LSA的时间间隔，单位为秒，默认值是5秒。范围是3到65535秒。
- **transmit-delay interval-value** – 指定更新包的延迟时间，单位为秒，默认值是1秒。范围是1到65536秒。

- **dead-interval** *interval-value* – 如果路由器在一定的时间内都没有收到对方的Hello报文，则认为对端路由器失效，这个一定的时间就是相邻路由器间的失效时间。该参数指定失效时间值，单位为秒，默认值是40秒。范围是1到655635秒。

使用**no area {id | A.B.C.D} virtual-link A.B.C.D [hello-interval] [retransmit-interval] [transmit-delay] [dead-interval]**命令恢复定时器的默认时间值。

用户可以配置虚拟链路的认证方式。在OSPF路由模式下，使用以下命令：

area {id | A.B.C.D} virtual-link A.B.C.D authentication [message-digest] [authentication-key string] [message-digest-key IDmd5 string] [null]

- **id | A.B.C.D** – 需要做虚拟链路进行连接的区域ID。区域ID用32比特数来表示，可以是数字形式，也可以是IP地址形式。
- **virtual-link A.B.C.D** – 指定作为虚拟链路路由器的Router ID。
- **message-digest** – 指定使用MD5认证。
- **authentication-key string** – 指定明文认证的认证密码。
- **message-digest-key IDmd5 string** – 指定MD5认证的认证ID和密码。
- **null** – 不使用认证。

使用**no area {id | A.B.C.D} virtual-link A.B.C.D authentication [message-digest] [authentication-key string] [message-digest-key ID]**命令取消认证配置。

配置stub区域

stub区域是不收发Type-5的LSA（AS-external-LSAs）区域。对于产生大量Type-5 LSA的网络，这种处理方式能够有效减小stub区域内路由器的LSDB规模，并缓解SPF计算对路由器资源的占用。stub区域通常位于自治系统边界。配置OSPF的stub区域，在OSPF路由模式下，使用以下命令：

area {id | A.B.C.D} stub [no-summary]

- **id | A.B.C.D** – 指定stub区域的区域ID。区域ID用32比特数来表示，可以是数字形式，也可以是IP地址形式。
- **no-summary** – 阻止ABR向stub区域发送3类或4类汇总LSA。

使用**no area {id | A.B.C.D} stub [no-summary]**命令取消stub区域的配置。

配置NSSA区域

Stub区域不能引入外部路由，为了在允许将自治系统外部路由通告到OSPF路由域内部的同时，保持其余部分的Stub区域的特征，网络管理员可以将区域配置为NSSA区域。配置OSPF的NSSA区域，在OSPF路由模式下，使用以下命令：

```
area {id | A.B.C.D} nssa [no-summary | no-redistribution | default-information-originate]
```

- *id* | *A.B.C.D* – 指定NSSA区域的区域ID。区域ID用32比特数来表示，可以是数字形式，也可以是IP地址形式。
- **no-summary** | **no-redistribution** | **default-information-originate** – **no-summary**参数只用于NSSA区域的ABR，配置后，NSSA ABR只通过Type-3的Summary-LSA向区域内发布一条缺省路由，不再向区域内发布任何其它Summary-LSAs（这种区域又称为Totally NSSA区域）。**no-redistribution**参数用于禁止将AS外部路由以Type-7 LSA的形式引入到NSSA区域中，这个参数通常只用在既是NSSA区域的ABR，也是OSPF自治系统的ASBR的路由器上，以保证所有外部路由信息能正确地进入OSPF路由域。**default-information-originate**参数只用于NSSA区域的ABR或ASBR，配置后，对于ABR，不论本地是否存在缺省路由，都将生成一条Type-7 LSA向区域内发布缺省路由；对于ASBR，只有当本地存在缺省路由时，才产生Type-7 LSA向区域内发布缺省路由。

使用**no area** {*id* | *A.B.C.D*} **nssa** [**no-summary** | **no-redistribution** | **default-information-originate**]命令取消NSSA区域的配置。

配置OSPF的引用带宽

OSPF可以根据接口的带宽计算接口发送OSPF报文的花费。配置OSPF的引用带宽，在OSPF路由模式下，使用以下命令：

```
auto-cost reference-bandwidth bandwidth
```

- *bandwidth* – 指定带宽值，单位为Mbps，默认值是100。范围是1到4294967。

使用**no auto-cost reference-bandwidth**命令使OSPF根据接口的类型计算接口发送OSPF报文的花费。

指定缺省度量

此处配置的OSPF协议的缺省度量在引入路由时生效。指定OSPF的缺省度量，在OSPF路由配置模式下使用以下命令：

```
default-metric value
```

- *value* – 指定缺省度量值。范围是1到16777214。

使用**no default-metric**命令恢复缺省度量的默认值。

配置缺省信息发布

用户可以指定是否将默认路由发布到其它使用OSPF协议的路由器。默认情况下，是不发送默认路由的。配置缺省信息发布，在OSPF路由配置模式下使用以下命令：

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

- **always** – OSPF无条件产生并发送默认路由。
- **type {1 | 2}** – 指定与发送到OSPF路由域的默认路由相关联的外部路由的类型。1指type1外部路由，2指type2外部路由。
- **metric value** – 指定发送默认路由的度量。如果不使用该命令配置度量并且也没有使用**default-metric value**配置默认度量，其默认度量将会是20。范围是0到16777214。

使用**no default-information originate**命令恢复默认值。

指定缺省距离

指定OSPF路由的缺省距离，在OSPF路由配置模式下使用以下命令：

distance distance-value

- **distance-value** – 指定缺省管理距离。范围是1到255，默认值是110。

使用**no distance**命令恢复缺省距离的默认值。

配置OSPF定时器

用户可以指定以下两个OSPF协议的定时器：OSPF收到更新后在多长时间内进行重新计算以及OSPF两次计算的时间间隔。配置OSPF定时器，在OSPF路由配置模式下使用以下命令：

timers spf delay1 delay2

- **delay1** – 收到更新后，在该指定时间内进行重新计算，单位为秒。范围是0到65535，默认值是5秒。
- **delay2** – 指定两次计算的时间间隔，单位为秒。范围是0到65535，默认值是10秒。

使用**no timers spf**命令恢复默认值。

指定运行OSPF协议的接口网络

指定运行OSPF协议的接口网络并且将网络配置到指定的区域中，在OSPF路由配置模式下使用以下命令：

```
network A.B.C.D/Marea {id | A.B.C.D}
```

- *A.B.C.D/M* – 指定运行OSPF协议的接口网络。
- **area {id | A.B.C.D}** – 指定将网络添加到的区域ID。区域ID用32比特数来表示，可以是数字形式，也可以是IP地址形式。

使用**no network A.B.C.D/Marea {id | A.B.C.D}**命令取消对网络的指定。

引入路由

OSPF协议允许用户引入其他OSPF进程路由信息以及其它路由协议（BGP、IS-IS、直连、静态和RIP）的路由信息，并向外发布。用户可以设置被引入路由的度量以及外部路由的类型，还可以引用路由映射表对路由信息进行过滤，仅允许引入或拒绝引入特定的路由信息。配置引入路由，在OSPF路由配置模式下使用以下命令：

```
redistribute {bgp | connected | isis | ospf process-id | static | rip} [type {1 | 2}] [metric value]  
[route-map name]
```

- **bgp | connected | isis | ospf process-id | static | rip** – 指定引入路由的类型，可以是BGP (**bgp**)、ISIS(**isis**)、指定的OSPF进程 (**ospf process-id**)、直连路由 (**connected**)、静态路由 (**static**) 或者RIP (**rip**)。
- **type {1 | 2}** – 指定外部路由的类型。1指type1外部路由，2指type2外部路由。
- **metric value** – 指定引入路由的度量。范围是0到16777214。如果不指定该数值，系统会使用OSPF的缺省度量（通过**default-metric value**配置）。
- **route-map name** – 指定用于过滤引入路由信息的路由映射表。有关路由映射表的更多信息，请参考“[配置路由映射表](#)”。

用户可以配置多条该命令引入不同类型的路由。

使用**no redistribute {bgp | connected | static | rip}**命令取消指定类型路由的引入。

配置路由映射表

默认情况下系统会引入所有的路由信息。用户可以引用路由映射表对引入的路由信息进行过滤。路由映射表主要由路由匹配规则和匹配成功后所执行操作（允许或拒绝）两部分组成。如果引入的路由信息命中了任何路由匹配规则，系统就会执行对应的操作，允许或拒绝引入这些路由信息。



注意:

- 如果用户设置的操作是允许，匹配成功后系统仅允许引入匹配的路由信息，拒绝引入所有未匹配的路由信息。
- 如果用户设置的操作是拒绝，匹配成功后系统会拒绝引入匹配的路由信息，但仍允许引入未匹配的路由信息。

用户可通过以下步骤配置路由映射表，实现对引入路由信息的过滤：

1. 创建路由映射表并在表中创建路由匹配规则。不同的匹配规则通过序列号区分。序列号越小，匹配优先级越高。默认情况下，引入的路由信息命中任何路由匹配规则，系统将不再继续匹配后续的规则；如果引入的路由信息没有命中任何匹配规则，系统将执行拒绝操作。
2. 在路由匹配规则中配置匹配条件。匹配条件可以是引入路由的度量值、目的地址、下一跳地址或下一跳接口。一条路由匹配规则中可以包含多个匹配条件，这些匹配条件之间是与（AND）关系，即引入的路由信息必须满足匹配规则中的所有匹配条件才会认定为命中了该条规则。
3. 如果匹配条件为路由的目的地址或下一条地址，配置匹配时所引用的路由访问控制列表。有关路由访问控制列表的更多信息，请参考“[配置路由访问控制列表](#)”。
4. 如有需要，设置系统在命中一条路由匹配规则后继续匹配其他规则。
5. 如有需要，修改引入路由的部分属性后再对外发布

创建路由映射表并在表中配置路由匹配规则，在全局配置模式下，使用以下命令：

```
route-map name {deny | permit} sequence
```

- **route-map** *name* - 指定路由映射表名称，并进入路由映射表配置模式。取值范围是1到31个字符。如果该名称已经存在，则直接进入路由映射表配置模式。

- **deny** | **permit** – 指定对匹配的路由信息所执行的操作。deny为拒绝，permit为允许。
- *sequence* – 指定该路由映射表下路由匹配规则的序列号。取值范围是1到65535。

使用该命令no的形式删除路由映射表：

```
no route-map name [sequence]
```

- *sequence* – 仅删除路由映射表中指定的匹配规则。

配置路由匹配规则中的匹配条件，在路由映射表配置模式下，使用以下命令：

```
match {as-path access-list-number | community {community-list-name | community-list-number}  
[exact-match] | metric metric-value | interface interface-name | ip address access-list | ip next-hop  
access-list}
```

- **as-path** *access-list-number* – 匹配路由的AS路径。*access-list-number*为用户配置的AS路径访问控制列表号。如果路由的AS路径匹配该访问控制列表中允许的AS路径，则认为匹配成功。有关AS路径访问控制列表配置的更多信息，请参考“[配置AS路径访问控制列表](#)”。
- **community** {*community-list-name* | *community-list-number*} [*exact-match*] – 匹配路由的团体属性。*community-list-name*为团体属性列表名称；*community-list-number*为团体属性列表号；*exact-match*指定对团体属性进行精确匹配。有关团体属性列表列表配置的更多信息，请参考“[配置团体属性列表](#)”。
- **metric** *metric-value* – 匹配路由的度量值。取值范围是0到4294967295。
- **interface** *interface-name* – 匹配路由的下一跳接口。
- **ip address** *access-list* – 匹配路由的目的地址。*access-list*为用户配置的路由访问控制列表。如果路由的目的地址属于该访问控制列表中允许的地址，则认为匹配成功。有关访问控制列表配置的更多信息，请参考“[配置路由访问控制列表](#)”。
- **ip next-hop** *access-list* – 匹配路由的下一跳地址。*access-list*为用户配置的路由访问控制列表。如果路由的下一跳地址属于该访问控制列表中允许的地址，则认为匹配成功。有关访问控制列表配置的更多信息，请参考“配置路由访问控制列表”。

重复以上命令向路由匹配规则中添加多个匹配条件。使用该命令no的形式删除匹配条件：

```
no match {metric | interface | ip address | ip next-hop}
```




注意: 如果用户仅创建了路由映射表但没有在映射表中配置任何路由匹配规则，系统默认会认为引入的路由信息匹配成功。

例如，设置OSPF协议仅引入BGP协议中下一跳接口为eth0/1且度量值为50的路由信息，命令行如下：

```
hostname(config)# route-map test permit 10
hostname(config-route-map)# match interface ethernet0/1
hostname(config-route-map)# match metric 50
hostname(config-route-map)# exit
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# router ospf
hostname(config-router)# redistribute bgp route-map test
hostname(config-router)# end
```

匹配多条路由匹配规则

默认情况下，如果引入的路由信息命中任何路由匹配规则，系统将不再继续匹配后续的规则。用户可以要求系统在命中一条规则后仍继续匹配其他规则，以实现更精细的控制。设置系统在匹配成功后继续匹配其他规则，在路由映射表配置模式下，使用以下命令：

continue [*sequence*]

- *sequence* – 指定继续匹配的规则序列号。取值范围是1到65535。该序列号必须大于当前规则的序列号。如果没有指定此参数，系统在当前规则匹配成功后会继续匹配下一条规则。

使用该命令no的形式取消继续匹配其他规则：

no continue

例如，也可以通过以下命令行设置OSPF协议仅引入BGP协议中下一跳接口为eth0/1且度量值为50的路由信息：

```
hostname(config)# route-map test permit 10
hostname(config-route-map)# match interface ethernet0/1
hostname(config-route-map)# continue 20
```

```
hostname(config-route-map)# exit

hostname(config)# route-map test permit 20

hostname(config-route-map)# match metric 50

hostname(config-route-map)# exit

hostname(config)# ip vrouter trust-vr

hostname(config-vrouter)# router ospf

hostname(config-router)# redistribute bgp route-map test

hostname(config-router)# end
```

修改引入路由属性

对于满足匹配条件的引入路由，用户可以在修改路由的部分属性后再对外发布。修改引入路由的属性，在路由映射表配置模式下，使用以下命令：

```
set {metric metric-value | metric-type {type-1 | type-2}}
```

- **metric *metric-value*** – 修改引入路由的度量值。取值范围是取值范围是0到4294967295。
- **metric-type {type-1 | type-2}** – 修改外部路由的度量类型。**type-1**指type1类型外部路由度量，**type-2**指type2类型外部路由度量。

使用该命令**no**的形式取消对路由属性的修改并还原到引入路由时的设置：

```
no set {metric | metric-type}
```

配置路由访问控制列表

路由匹配规则中的目的地址和下一跳地址匹配是通过引用路由访问控制列表实现的。路由访问控制列表主要由IP地址匹配规则和匹配成功后所执行操作（允许或拒绝）两部分组成。如果目的地址或下一跳地址匹配指定的IP地址，系统会继续执行指定的操作。一个路由访问控制列表中可以包含多条IP地址匹配规则，系统按照添加时间顺序依次匹配，命中任何一条规则会立即结束匹配；如果匹配失败，系统会执行拒绝操作。

配置路由访问控制列表，在全局配置模式下，执行以下命令：

```
access-list route name {deny | permit} {A.B.C.D/M [exact-match] | any}
```

- *name* – 指定路由访问控制列表的名称并进入路由访问控制列表配置模式。取值范围是1到31个字符。如果该名称已经存在，则直接进入路由访问控制列表配置模式。
- **deny** | **permit** – 指定对匹配的IP地址所执行的操作。deny为拒绝，permit为允许。
- *A.B.C.D/M* – 指定需要匹配的IP地址或IP地址前缀（不包括掩码）。
- **exact-match** – 对IP地址前缀进行精确匹配（包括掩码）。
- **any** – 匹配任意IP地址。

使用该命令no的形式删除路由访问控制列表：

```
no access-list route name [{deny | permit} {A.B.C.D/M [exact-match] | any}]
```

如果指定了具体的IP地址匹配规则，该命令只从路由访问控制列表中删除对应的规则而不会删除整个访问控制列表。

对路由访问控制列表添加描述信息，在全局配置模式下，使用以下命令：

```
access-list route name description description
```

- *name* – 指定路由访问控制列表的名称。取值范围是1到31个字符。
- *description* – 指定描述信息。取值范围是1到31个字符。

使用该命令no的形式删除描述信息：

```
no access-list route name description
```

例如，设置OSPF协议拒绝引入BGP协议中下一跳地址为192.168.1.1和192.168.2.0网段中IP地址和的路由信息，命令行如下：

```
hostname(config)# route-map test deny 10
hostname(config-route-map)# match ip next-hop access_list
hostname(config-route-map)# exit
hostname(config)# access-list route access_list permit 192.168.1.1/32
hostname(config)# access-list route access_list permit 192.168.2.0/24
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# router ospf
hostname(config-router)# redistribute bgp route-map test
```

```
hostname(config-router)# end
```

配置距离

用户可以根据路由类型指定管理距离。配置距离，在OSPF路由配置模式下使用以下命令：

```
distance ospf {intra-area distance-value | inter-area distance-value | external distance-value}
```

- **intra-area distance-value** – 指定区域内路由的管理距离。默认值是110。范围是1到255。
- **inter-area distance-value** – 指定区域间路由的管理距离。默认值是110。范围是1到255。
- **external distance-value** – 指定外部type5类型路由的管理距离。默认值是110。范围是1到255。

使用**no distance ospf**命令恢复距离的默认值。

配置被动接口

用户可以将一些接口配置为只接收更新但是不发送，这种只接收更新的接口就是被动接口。配置被动接口，在OSPF路由配置模式下使用以下命令：

```
passive-interface interface-name
```

- *interface-name* – 指定接口的名称作为被动接口。

用户可以配置多条该命令添加多个被动接口。

使用**no passive-interface interface-name**命令取消被动接口的配置。

配置接口OSPF功能

接口的OSPF功能配置需要在接口配置模式下完成。OSPF协议在设备接口上的配置包括：

- 配置接口的OSPF认证
- 指定接口的链路花费
- 配置接口定时器
- 指定接口路由器优先级
- 配置接口的网络类型

配置接口的OSPF认证

接口的OSPF认证优先于区域OSPF认证。设备支持明文认证和MD5认证。默认情况下，接口的OSPF认证是关闭的。开启或者关闭接口的OSPF认证功能，在接口配置模式下使用以下命令：

ip ospf authentication

no ip ospf authentication

配置明文认证的认证密码，在接口配置模式下，使用以下命令：

ip ospf authentication-key *string*

- *string* – 指定认证密码（最多为8个字符）。

使用**no ip ospf authentication-key**命令取消密码配置。

配置MD5认证ID和密码，在接口配置模式下，使用以下命令：

ip ospf message-digest-key *ID* md5 *string*

- *ID* – 指定认证ID。
- *string* – 指定认证密码。

使用**no ip ospf message-digest-key *ID***命令取消密码配置。

指定接口的链路花费

指定接口的链路花费，在接口配置模式下，使用以下命令：

ip ospf cost *cost-value* [*local*]

- *cost-value* – 指定接口的链路花费。取值范围是1到65535。
- **local** – 指定接口的链路花费为local。当设备处于HA AA模式时，配置此参数，该接口的链路花费值将不会同步到备份设备，从而使两台设备具有不同的链路花费值，避免出现非对称OSPF路由。

使用**no ip ospf cost [*local*]**命令取消对所需花费的指定。

配置接口定时器

接口的定时器有以下四个：接口发送Hello包的时间间隔、接口相邻路由器的失效时间、接口重传LSA的时间间隔以及接口更新包的延迟时间。

指定接口发送Hello包的时间间隔，在接口配置模式下，使用以下命令：

ip ospf hello-interval *interval*

- *interval* – 指定接口发送Hello包的时间间隔，单位为秒。默认值是10秒。范围是1到65535秒。

使用**no ip ospf hello-interval**恢复默认时间间隔。

如果接口在一定的时间内都没有收到对方的Hello报文，则认为对端路由器失效，这个一定的时间就是相邻路由器间的失效时间。指定接口的相邻路由失效时间，在接口配置模式下，使用以下命令：

ip ospf dead-interval *interval*

- *interval* – 指定接口的相邻路由失效时间，单位为秒。默认值是40秒（发送Hello包时间间隔的4倍）。范围是1到65535秒。

使用**no ip ospf dead-interval**恢复默认失效时间。

指定接口重传LSA的时间间隔，在接口配置模式下，使用以下命令：

ip ospf retransmit-interval *interval*

- *interval* – 指定接口重传LSA的时间间隔，单位为秒。默认值是5秒。范围是3到65535秒。

使用**no ip ospf retransmit-interval**恢复默认时间间隔。

指定接口更新包的延迟时间，在接口配置模式下，使用以下命令：

ip ospf transmit-delay *interval*

- *interval* – 指定接口更新包的延迟时间，单位为秒。默认值是1秒。范围是1到65535秒。

使用**no ip ospf transmit-delay**恢复默认延迟时间。

指定接口路由器优先级

路由器的优先级用来决定使用哪个路由器作为指定路由器。指定路由器用来接收网络中所有其它路由器的链路信息，并将收到的链路信息广播出去。指定接口路由器的优先级，在接口配置模式下，使用以下命令：

ip ospf priority *level*

- *level* – 指定路由器的优先级。默认值是1。范围是0到255。优先级为0的路由器不会被选中作为指定路由器。当同一个网络的两个路由器都可作为指定路由器时，优先级高的路由器会被选中；如果优先级也相同，Router ID高的会被选中。

使用**no ip ospf priority**命令恢复默认优先级。

配置接口的网络类型

OSPF协议的接口的网路类型有以下三种：广播、点到点（Point-to-point）以及点到多点（Point-to-multipoint）网络类型。默认情况下，接口的网络类型为广播类型。配置接口的网络类型，在接口配置模式下，使用以下命令：

```
ip ospf network {point-to-point | point-to-multipoint}
```

- **point-to-point** - 指定接口网络类型为点到点网络类型。
- **point-to-multipoint** - 指定接口网络类型为点到多点网络类型。

在隧道接口配置模式下，使用该命令no的形式恢复接口网络类型为广播类型：

```
no ip ospf network
```

显示OSPF信息

显示OSPF路由信息，在任何模式下使用以下命令：

```
show ip route ospf [vrouter vrouter-name]
```

- *vrouter-name* - 显示指定的VRouter的OSPF路由信息。

显示设备的OSPF信息，在任何模式下使用以下命令：

```
show ip ospf [vrouter vrouter-name] [process process-id]
```

- *vrouter-name* - 指定VRouter名称。
- **process process-id** - 指定OSPF进程ID。

显示设备OSPF协议的数据库信息，在任何模式下使用以下命令：

```
show ip ospf database {asbr-summary | external | nssa-external | network | router | summary}  
[A.B.C.D] [{adv-router A.B.C.D} | self-originate] [vrouter vrouter-name] [process process-id]
```

- **asbr-summary** - 显示自制系统边界路由LSAs。
- **external** - 显示外部路由LSAs。
- **nssa-external** - 显示NSSA的外部LSA的有关信息。
- **network** - 显示网络LSAs。

- **router** - 显示路由LSAs。
- **summary** - 显示汇总LSAs。
- *A.B.C.D* - 链路状态ID，以IP地址形式表示。
- **adv-router***A.B.C.D* - 显示指定路由器的LSAs。
- **self-originate** - 只显示自己产生的LSA（从本地路由器）。
- *vrouter-name* - 指定VRouter名称。
- **process***process-id* - 指定OSPF进程ID。

show ip ospf database [**max-age** | **self-originate**] [**vrouter** *vrouter-name*] [**process** *process-id*]

- **max-age** - 指定最大老化时间。
- **self-originate** - 只显示自己产生的LSA（从本地路由器）。
- *vrouter-name* - 指定VRouter名称。
- **process** *process-id* - 指定OSPF进程ID。

显示OSPF接口信息，在任何模式下使用以下命令：

show ip ospf interface [*interface-name*] [**vrouter** *vrouter-name*] [**process** *process-id*]

显示OSPF虚拟链路信息，在任何模式下使用以下命令：

show ip ospf virtual-links [**vrouter** *vrouter-name*] [**process** *process-id*]

显示OSPF邻居信息，在任何模式下使用以下命令：

show ip ospf neighbor [*A.B.C.D* | **detail**] [**vrouter** *vrouter-name*] [**process** *process-id*]

显示OSPF路由信息，在任何模式下使用以下命令：

show ip ospf route [*A.B.C.D*] [**vrouter** *vrouter-name*] [**process** *process-id*]

显示路由映射表信息，在任何模式使用以下命令：

show route-map [*name*]

显示路由访问控制列表信息，在任何模式使用以下命令：

show access-list route [*name*]

OSPFv3

OSPFv3是OSPF（Open Shortest Path First，开放式最短路径优先）的第3个版本，主要提供对IPv6的支持。

OSPFv3和OSPFv2在很多方面是相同的：

- Router ID，Area ID仍然是32位的。
- 相同类型的报文：Hello报文，DD（Database Description，数据库描述）报文，LSR（Link State Request，链路状态请求）报文，LSU（Link State Update，链路状态更新）报文和LSAck（Link State Acknowledgment，链路状态确认）报文。
- 相同的邻居发现机制和邻接形成机制。
- 相同的LSA扩散机制和老化机制。

OSPFv3和OSPFv2的不同主要有：

- OSPFv3是基于链路（Link）运行，OSPFv2是基于网段（Network）运行。
- OSPFv3在同一条链路上可以运行多个实例。
- OSPFv3是通过Router ID来标识邻接的邻居。OSPFv2则是通过IP地址来标识邻接的邻居。

用户可以为不同的VRouter分别配置OSPFv3协议。OSPFv3协议配置包括以下各项：

- 配置Router ID
- 配置区域的虚拟链路
- 配置缺省度量
- 配置缺省管理距离
- 配置缺省路由发布
- 指定接口区域及实例
- 配置引入路由
- 配置被动接口
- 配置OSPFv3接口定时器

- 指定接口路由器优先级
- 指定接口的链路花费
- 关闭/开启OSPFv3协议
- 配置接口MTU匹配检查

OSPFv3协议的基本配置需要在OSPFv3路由模式下进行。进入OSPFv3路由模式，请在配置模式下，使用以下命令：

ip vrouter vrouter-name （进入VRouter配置模式）

ipv6 router ospf [process-id] （进入OSPFv3路由模式，并创建OSPFv3进程。每个OSPFv3进程之间相互独立，每个虚拟路由器可以创建一个OSPFv3进程。）

- *process-id* – 指定OSPFv3的进程ID。若不指定，默认为进程1。每个OSPFv3进程相互独立，有各自的链路状态数据库和对应的OSPFv3路由表信息。每个VRouter最多可创建4个OSPFv3进程，多个进程共同维护一个VRouter的路由表。每个OSPFv3进程都可以引入其它OSPFv3进程的OSPFv3路由，也可以引入其它IPv6路由（静态、直连、IPv6BGP、RIPng、ISISv6）。

在配置OSPFv3多进程时，注意如下事项：

- 多进程OSPFv3生成相同目的网络，当管理距离和度量值都相同时，先生成路由的进程会优先被选择。多个OSPFv3进程之间不进行等价路由。
- 当其他路由协议引入OSPFv3路由时，只能引入进程ID为1的OSPFv3路由信息。

在VRouter配置模式下，使用**no ipv6 router ospf**关闭OSPFv3进程。

配置Router ID

每一台运行OSPFv3协议的路由器都必须拥有一个Router ID。Router ID是每个路由器在整个OSPFv3自治系统中唯一标识，使用IP地址的形式表示。为设备的OSPFv3协议配置Router ID，在OSPFv3路由模式下，使用以下命令：

router-id A.B.C.D [local]

- **A.B.C.D** – 指定OSPFv3协议使用的Router ID，为IP地址形式。
- **local** - 指定OSPFv3协议的Router ID为本地配置，即该配置不在设备间同步。默认情况下，Router ID为非本地配置。

配置区域的虚拟链路

非骨干区域之间的路由信息必须通过骨干区域来转发。对此，OSPFv3有两个规定：

- 所有非骨干区域必须与骨干区域保持连通；
- 骨干区域自身也必须保持连通。

但在实际应用中，可能会因为各方面条件的限制，无法满足这个要求。这时可以通过配置OSPF虚连接（Virtual Link）予以解决。虚拟链路用来保持非骨干区域与骨干区域的连通，以及保持骨干区域自身的连通。虚链路总是建立在两台区域边界路由器(ABR)之间，且必须在两端同时配置才能生效。其中至少一台ABR属于骨干区域。配置虚拟链路，在OSPFv3路由模式下，使用以下命令：

```
area { id | A.B.C.D } virtual-link A.B.C.D
```

- *id* | *A.B.C.D* – 指定虚拟链路穿过的区域ID。区域ID用32比特数来表示，可以是数字形式，也可以是IP地址形式。
- *A.B.C.D* – 指定虚拟链路对端ABR的Router ID。

在OSPFv3路由模式下，使用**no area { *id* | *A.B.C.D* } virtual-link *A.B.C.D***命令取消配置。

指定缺省度量

指定OSPFv3协议的缺省度量。如果引入路由时没有配置度量值，则指定的缺省度量在引入路由时生效。指定OSPFv3的缺省度量，在OSPFv3路由配置模式下使用以下命令：

```
default-metric value
```

- *value* – 指定缺省度量值。范围是1到16777214。

在OSPFv3路由模式下，使用**no default-metric**命令恢复缺省度量的默认值。

配置缺省管理距离

用户可以根据路由类型指定管理距离。配置距离，在OSPFv3路由配置模式下使用以下命令：

```
distance { distance-value | ospf [intra-area distance-value | inter-area distance-value] external distance-value }
```

- *distance-value* – 指定所有路由的管理距离。默认值是110。范围是1到255。
- *intra-area distance-value* – 指定区域内路由的管理距离。默认值是110。范围是1到255。
- *inter-area distance-value* – 指定区域间路由的管理距离。默认值是110。范围是1到255。
- *external distance-value* – 指定外部类型路由的管理距离。默认值是110。范围是1到255。

在OSPFv3路由模式下，使用**no distance [ospf]**命令恢复距离的默认值。

配置缺省路由发布

用户可以指定是否将缺省路由通告到本区域内其他的路由器。配置缺省路由发布，在OSPF路由配置模式下使用以下命令：

default-information originate [always] [type {1 | 2}] [metric value]

- **always** – 指定always参数时，当前路由器产生并通告默认路由。如果当前路由器不存在缺省路由，会引入一条缺省路由并通告出去。这条缺省路由的下一跳指向当前路由器。当不指定always参数时，如果当前路由器不存在缺省路由，将不会通告缺省路由。
- **type {1 | 2}** – 指定与发送到OSPF路由域的缺省路由相关联的外部路由的类型。1指type1外部路由，这类路由的可信程度较高，并且和OSPFv3自身路由的开销具有可比性，所以到第一类外部路由的开销等于当前路由器到相应的ASBR的开销与ASBR到该路由目的地址的开销之和。2指type2外部路由，这类路由的可信度比较低，所以OSPF协议认为从ASBR到自治系统之外的开销远远大于在自治系统之内到达ASBR的开销。所以计算路由开销时将主要考虑前者，即到第二类外部路由的开销等于ASBR到该路由目的地址的开销。如果计算出开销值相等的两条路由，再考虑本路由器到相应的ASBR的开销。
- **metric value** – 指定缺省路由的度量。范围是0到16777214。如果不使用该命令配置度量并且也没有使用**default-metric value**配置默认度量，其默认度量将会是20。

在OSPFv3路由模式下，使用**no default-information originate**命令恢复默认值。

指定接口区域及实例

在接口配置模式下，指定接口所属的OSPFv3区域及实例。

ipv6 ospf process-id area { A.B.C.D | id} {instance id}

- *process-id* – 指定接口所属OSPFv3的进程ID，默认值是1。
- **area { A.B.C.D | id }** – 指定接口所属区域的ID。区域ID用32比特数来表示，可以是数字形式，也可以是IP地址形式。
- **instance id** – 指定接口所属的实例ID。建立邻居关系的接口必须属于相同的实例。取值范围是0到255。默认值是0。

在接口配置模式下，使用**no ipv6 ospf area { A.B.C.D | id }**取消接口上的区域及实例配置。

配置引入路由

OSPFv3协议允许用户引入其它路由协议（BGP、直连、ISIS、静态和RIPng）的路由信息，并向外发布。同时，用户可以设置被引入路由的度量以及外部路由的类型。配置引入路由，在OSPF路由配置模式下使用以下命令：

redistribute { bgp | connected | isis | static | ripng | ospfv3 } [type { 1 | 2 }] [metric value]

- **bgp | connected | isis | static | ripng | ospfv3** – 指定引入路由的类型，可以是BGP（bgp）、直连路由（connected）、ISIS（isis）、静态路由（static）、RIPng（ripng）或者OSPFv3路由。
- **type { 1 | 2 }** – 指定外部路由的类型。1指type1外部路由，2指type2外部路由。
- **metric value** – 指定引入路由的度量。范围是0到16777214。如果不指定该数值，系统会使用OSPF的缺省度量（通过**default-metric value**配置）。

用户可以配置多条该命令引入不同类型的路由。

在OSPFv3路由模式下，使用**no redistribute { bgp | connected | isis | static | ripng }**命令取消指定类型路由的引入。

配置被动接口

用户可以将一些接口配置为只接收更新但是不发送，这种只接收更新的接口就是被动接口。配置被动接口，在接口配置模式下使用以下命令：

ipv6 ospf passive

用户可以配置多条该命令添加多个被动接口。

在接口配置模式下，使用**no ipv6 ospf passive**命令取消被动接口的配置。

配置OSPFv3接口定时器

接口的定时器有以下四个：接口发送Hello包的时间间隔、接口相邻路由器的失效时间、接口重传LSA的时间间隔以及接口更新包的延迟时间。

指定接口发送Hello包的时间间隔，在接口配置模式下，使用以下命令：

ipv6 ospf hello-interval interval

- *interval* – 指定接口发送Hello包的时间间隔，单位为秒。默认值是10秒（若OSPFv3接口选择点到多点的网络类型，则默认值是30秒）。范围是1到65535秒。

在接口配置模式下，使用**no ipv6 ospf hello-interval**恢复默认时间间隔。

如果接口在一定的时间内都没有收到邻居的Hello报文，则认为邻居路由器失效，这个一定的时间就是相邻路由器间的失效时间。指定接口的相邻路由失效时间，在接口配置模式下，使用以下命令：

ipv6 ospf dead-interval interval

- *interval* – 指定接口的相邻路由器失效时间，单位为秒。默认值是40秒（发送Hello包时间间隔的4倍），若OSPFv3接口选择点到多点的网络类型，则默认值是120秒。范围是1到65535秒。

在接口配置模式下，使用**no ipv6 ospf dead-interval**恢复默认失效时间。

ipv6 ospf retransmit-interval interval

- *interval* – 指定接口重传LSA的时间间隔，单位为秒。默认值是5秒。范围是3到65535秒。

使用**no ipv6 ospf retransmit-interval**恢复默认时间间隔。

ipv6 ospf transmit-delay interval

- *interval* – 指定接口更新包的延迟时间，单位为秒。默认值是1秒。范围是1到65535秒。

在接口配置模式下，使用**no ipv6 ospf transmit-delay**恢复默认延迟时间。

指定接口路由器优先级

路由器的优先级用来决定使用哪个路由器作为指定路由器。指定路由器用来接收网络中所有其它路由器的链路信息，并将收到的链路信息广播出去。指定接口路由器的优先级，在接口配置模式下，使用以下命令：

ipv6 ospf priority level

- *level* – 指定路由器的优先级。默认值是1。范围是0到255。优先级为0的路由器不会被选中作为指定路由器。当同一个网络的两个路由器都可作为指定路由器时，优先级高的路由器会被选中；如果优先级也相同，Router ID高的会被选中。

在接口配置模式下，使用**no ipv6 ospf priority**命令恢复默认优先级。

配置接口的链路花费

OSPF有两种方式来配置接口的花费：

- 在接口配置模式下直接配置花费；
- 配置接口的带宽参考值，OSPFv3根据带宽参考值自动计算接口的花费。

指定接口的花费，在接口配置模式下，使用以下命令：

ipv6 ospf cost *cost-value*

- *cost-value* – 指定接口的花费。取值范围是1到65535。

在接口配置模式下，使用**no ipv6 ospf cost**命令取消对所需花费的指定。

OSPFv3可以根据接口的带宽计算接口发送OSPFv3报文的花费。指定接口带宽值，在OSPFv3路由模式下，使用以下命令：

auto-cost reference-bandwidth *bandwidth*

- *bandwidth* – 指定接口带宽值，单位为Mbps，默认值是100。范围是1到4294967。

在OSPFv3路由模式下，使用**no auto-cost reference-bandwidth**命令恢复默认的带宽值。

配置接口MTU匹配检查

OSPFv3通过DBD报文检查邻居间的接口MTU设置是否匹配。如果相邻的OSPFv3路由器接口之间的MTU不匹配，则他们之间不能建立邻接关系。为了用户可通过修改接口的MTU来解决此问题。但是，有些接口无法修改MTU。用户可对OSPFv3进行配置，使OSPFv3忽略对MTU匹配的检查。

使OSPFv3忽略对MTU匹配的检查，在接口配置模式下，使用如下命令：

ipv6 ospf mtu-ignore

在接口配置模式下，使用**no ipv6 ospf mtu-ignore**命令恢复对邻居间接口MTU匹配的检查。

关闭/开启OSPFv3协议

在接口上正常关闭OSPFv3协议，在接口配置模式下，使用**ipv6 ospf shutdown**命令。

在接口上重新开启OSPFv3协议，在接口配置模式下，使用**no ipv6 ospf shutdown**命令。

查看OSPFv3信息

显示OSPFv3路由信息，在任何模式下使用以下命令：

show ipv6 ospf [**vrouter** *vrouter-name*] [**process** *process-id*]

- *vrouter-name* - 显示指定的VRouter的OSPF路由信息。若不指定vr，则只显示trust-vr协议信息。
- *process-id* - 显示指定进程的process id OSPFv3协议的信息。不指定process id的情况下，显示该VR内所有的OSPFv3进程的协议信息。

显示OSPFv3协议的数据库信息，在任何模式下使用以下命令：

show ipv6 ospf database {**inter-router** | **external** | **network** | **router** | **inter-prefix** | **link** | **intra-prefix**} [*A.B.C.D*] [{**adv-router** *A.B.C.D*} | **self-originate**] [**vrouter** *vrouter-name*] [**process** *process-id*]

- **inter-router** - 此类型LSA显示到本自治系统内的ASBR的路由。该LSA由ABR生成，在与该LSA相关的区域内传播。每一条inter-router类型的LSA描述了一条到达本自治系统内的ASBR（Autonomous System Border Router，自治系统边界路由器）的路由。
- **external** - 此类型LSA显示到自治系统系统外部的路由。由ASBR生成，描述到达其它AS（Autonomous System，自治系统）的路由，传播到整个AS（Stub区域除外）。
- **network** - 此类型LSA的链路状态显示本网段接口的链路状态。由广播网络和NBMA（Non-Broadcast Multi-Access）网络的DR（Designated Router，指定路由器）生成，描述本网段接口的链路状态，只在DR所处区域内传播。
- **router** - 此类型LSA由每个路由器生成，描述本路由器的链路状态和开销，只在路由器所处区域内传播。
- **inter-prefix** - 该类型LSA显示到本自治系统内其他区域的IPv6地址前缀的路由。该LSA由ABR（Area Border Router，区域边界路由器）生成，在与该LSA相关的区域内传播。每一条inter-prefix LSA描述了一条到达本自治系统内其他区域的IPv6地址前缀（IPv6 Address Prefix）的路由。

- **link** - 路由器为每一条链路生成一个link类型的LSA，在本地链路范围内传播。每一个Link类型的LSA描述了该链路上所连接的IPv6地址前缀及路由器的Link-local地址。
- **intra-prefix** - 每个该类型LSA包含路由器上的IPv6前缀信息，Stub区域信息或穿越区域（Transit Area）的网段信息，该LSA在区域内传播。由router类型LSA和network类型LSA不再包含地址信息，导致了intra-prefix类型LSA的引入。
- **A.B.C.D** - 链路状态ID，以IP地址形式表示。
- **adv-router A.B.C.D** - 显示指定路由器的LSAs。
- **self-originate** - 只显示自己产生的LSA（从本地路由器）。
- **vrouter-name** - 指定VRouter名称。若不指定vr，只显示trust-vr内所有OSPFv3进程的数据库信息。
- **process process-id** - 显示指定进程的process id OSPFv3协议的数据库信息。不指定process id时，则显示该VR内所有的OSPFv3进程的数据库信息。

显示OSPF接口信息，在任何模式下使用以下命令：

```
show ipv6 ospf interface [interface-name] [vrouter vrouter-name] [process process-id]
```

显示OSPF邻居信息，在任何模式下使用以下命令：

```
show ip ospf neighbor [A.B.C.D | detail] [vrouter vrouter-name] [process process-id]
```

显示OSPF边界路由器信息，在任何模式下使用以下命令：

```
show ipv6 ospf border-routers [A.B.C.D] [vrouter vrouter-name] [process process-id]
```

显示OSPF路由信息，在任何模式下使用以下命令：

```
show ip ospf route [X:X:X:X::X/M] [vrouter vrouter-name] [process process-id]
```

显示OSPFv3虚拟链路信息，在任何模式下使用以下命令：

```
show ip ospf virtual-links [vrouter vrouter-name] [process process-id]
```

IS-IS

IS-IS（Intermediate System-to-Intermediate System）最初是ISO为CLNP（Connection-Less Network Protocol）设计的一种动态路由协议。为了提供对IP的路由支持，IETF（Internet Engineering Task Force）在RFC 1195中对IS-IS进行了扩充和修改，使它能够同时应用在TCP/IP和OSI环境中，称为集

成化IS-IS（Integrated IS-IS或Dual IS-IS）。IS-IS属于IGP（Interior Gateway Protocol），用于自治系统内部。IS-IS是一种链路状态协议，使用SPF（Shortest Path First）算法进行路由计算。

系统支持应用在TCP/IP网络环境中的IS-IS动态路由协议。

用户可以为不同的VRouter分别配置IS-IS动态路由协议。IS-IS协议配置包括以下各项：

- 指定路由器类型
- 使能接口IS-IS
- 配置接口IS-IS类型
- 配置网络类型为点对点类型
- 配置NET地址
- 配置管理距离
- 配置度量类型
- 配置接口度量值
- 引入路由
- 发布缺省路由
- 配置Hello报文发送时间间隔
- 配置Hello报文失效乘数
- 配置Hello报文填充功能
- 配置被动接口
- 配置DIS选举优先级
- 配置LSP生成时间间隔
- 配置LSP最大生存时间
- 配置LSP刷新时间
- 配置SPF计算时间间隔
- 配置过载标志位

- 配置主机名映射
- 配置认证
- 配置接口认证模式

IS-IS基本配置

IS-IS动态路由协议的基本配置需要在IS-IS路由配置模式下进行。进入IS-IS路由配置模式，依次使用以下命令：

ip vrouter vrouter-name - 在全局配置模式下执行此命令，进入VRouter配置模式。

router isis - 进入IS-IS路由配置模式，同时在此VRouter创建一个IS-IS进程。每个VRouter的IS-IS进程之间相互独立。

需要关闭IS-IS进程时，在VRouter配置模式下，使用**no router isis**。

指定路由器类型

路由器类型包括：Level-1路由器，Level-2路由器，以及Level-1-2路由器。指定路由器类型，在IS-IS路由配置模式下，使用如下命令：

is-type [level-1 | level-1-2 | level-2-only]

- **level-1 | level-1-2 | level-2-only** - 指定路由器类型为Level-1路由器 (**level-1**)，Level-2路由器(**level-2**)，Level-1-2路由器 (**level-1-2**)。路由器默认类型为Level-1-2类型。只有当路由器类型为Level-1-2时，用户可对接口的类型进行指定。

取消路由器类型配置，在IS-IS路由配置模式下，使用**no is-type**命令。

使能接口IS-IS

默认情况下，IS-IS功能在接口上处于关闭状态。在当前路由器上创建IS-IS进程后，需要在接口上使能IS-IS。在接口配置模式下，使用如下命令：

isis enable

使用**no isis enable**命令在接口上关闭IS-IS功能。

配置接口IS-IS类型

当路由器类型是Level-1时，接口的邻接类型只能为Level-1；当路由器类型是Level-2时，接口的邻接类型只能为Level-2；当路由器类型是Level-1-2时，接口的邻接类型默认为level-1-2类型。配置接口的邻接类型，在接口配置模式下，使用如下命令：

```
isis circuit-type [level-1 | level-1-2 | level-2-only]
```

- **level-1 | level-1-2 | level-2-only** – 指定接口类型为level-1邻接类型接口（**level-1**）， level-2邻接类型接口（**level-2-only**）或者level-1-2邻接类型接口（**level-1-2**）。

配置网络类型为点对点类型

当只有两台设备接入到广播网络时，可以配置接口所在链路的类型为点对点链路类型。对于点对点链路类型，IS-IS不进行DIS选举和CSNP泛洪。在接口配置模式下，使用如下命令：

```
isis network point-to-point
```

使用**no isis network point-to-point**命令取消点对点链路类型设置。

IS-IS路由信息配置

配置NET地址

NET（Network Entity Title，网络实体名称）指示的是IS本身的网络层信息，不包括传输层信息，可以看作是一类特殊的NSAP，即SEL为0的NSAP地址。NET地址用来标识开启IS-IS进程的设备。一个IS-IS进程的设备最多可以配置3个NET地址。这三个NET地址的区域地址可以不同，但是System ID必须相同。指定设备的NET地址，在IS-IS路由配置模式下，使用如下命令：

```
net net [local]
```

- **net** – 指定NET地址。在建立Level-1邻居时，区域地址必须相同，否则无法建立邻居。在建立Level-2邻居时，不检查区域地址是否相同。
- **local** - 指定NET地址为本地配置，即该配置不会在设备间同步。默认情况下，NET地址为非本地配置。

使用**no net net [local]**命令取消对NET地址的设置。

配置管理距离

指定IS-IS路由的管理距离，在IS-IS路由配置模式下，使用以下命令：

distance *distance-value*

- *distance-value* – 为IS-IS路由指定管理距离。范围是1到255，默认值是115。

使用**no distance**命令恢复缺省管理距离。

配置度量类型

当度量类型为**narrow**时，路由器只生成和接收metric field的类型为**narrow**类型的报文。接口度量值的取值范围为0到63。对于大型网络，路由的最大度量值为1023。当路由度量值大于1023时，认为目标不可达。当度量类型为**wide**时，路由器仅生成和接收metric field的类型为**wide**类型的报文。接口度量值的取值范围为0到16777215。当度量类型为**transition**时，路由器既可以接收/发送**narrow**类型的报文，也可以接收/发送**wide**类型的报文。配置度量类型，在IS-IS路由配置模式下，使用如下命令：

metric-style {**wide** | **narrow** | **transition**}

- **wide** – 路由器仅生成和接收metric field的类型为**wide**类型的报文。
- **narrow** – 路由器只生成和接收metric field的类型为**narrow**类型的报文。默认为**narrow**。
- **transition** – 路由器既可以接收/发送**narrow**类型的报文，也可以接收/发送**wide**类型的报文。

使用**no metric-style**恢复默认度量类型。

配置接口度量值

度量值用来计算经过此链路到达网络目的地址的链路开销。配置接口所在链路的度量值，在接口配置模式下，使用如下命令：

isis metric value [**level-1** | **level-2**]

- *value* – 指定接口所在链路的度量值。取值范围为1到16777214。默认值为10。当接口的度量类型为**narrow**时，度量值不能超过63。
- **level-1** | **level-2** – 使用**level-1**参数指定Level-1 路由信息的度量值。使用**level-2**参数指定Level-2 路由信息的度量值。不指定**level-1**和**level-2**参数时，设置的度量值将会同时对Level-1 和Level-2路由信息生效。

使用**no isis metric**命令恢复接口度量值的默认值。

引入路由

IS-IS协议允许用户将设备上其它路由协议（直连、静态、OSPF、BGP和RIP）的路由信息引入到IS-IS中，并向外发布。同时，用户可以设置被引入路由的度量。配置引入路由，在IS-IS路由配置模式下使用以下命令：

```
redistribute {connected | static | ospf | bgp | rip} [level-1 | level-1-2 | level-2] [metric value] [metric-type {external | internal}]
```

- **connected | static | ospf | bgp | rip** - 指定引入路由的类型，可以是直连路由（**connected**）、静态路由（**static**）、OSPF（**ospf**），BGP（**bgp**）或者RIP（**rip**）。
- **level-1 | level-1-2 | level-2** - 指定引入路由的级别，可以作为Level-1路由（**level-1**）、Level-2路由（**level-2**）或者同时作为Level-1和Level-2路由（**level-1-2**）。默认值为level-2。
- **metric value** - 指定引入路由的度量。范围是0到4294967295。默认值为0。当路由器的度量类型为narrow时，引入路由的度量值不能超过63。
- **metric-type {external | internal}** - 当指定metric类型为external时，metric值为使用命令metric value中配置的值加64；当指定metric类型为internal时，metric值为命令metric value中配置的数值。默认类型为internal。

使用**no redistribute {connected | static | ospf | bgp | rip} [level-1 | level-1-2 | level-2]**命令取消指定类型路由的引入。

发布缺省路由

对于引入其他协议的路由信息时所存在的缺省路由，不会被路由器引入并使用。如果需要在路由域中发布缺省路由，在IS-IS路由配置模式下使用以下命令：

```
default-information originate
```

当配置了此命令的路由器的路由表中存在一条缺省路由，IS-IS将只通过Level-2 LSP通告此路由。

使用**no default-information originate**命令取消发布缺省路由。

IS-IS网络优化

配置Hello报文发送时间间隔

配置接口发送Hello报文的时间间隔，在接口配置模式下，使用如下命令：

```
isis hello-interval value [level-1 | level-2]
```

- *value* – 接口发送Hello报文的时间间隔。取值范围为1到600。单位为秒。默认值为3秒。
- **level-1 | level-2** – 使用**level-1**参数指定Level-1 Hello报文的发送时间间隔。使用**level-2**参数指定Level-2 Hello报文的发送时间间隔。默认为Level-2 和Level-1Hello报文。

使用**no isis hello-interval**命令将Hello报文发送时间间隔恢复为默认值。

配置Hello报文失效乘数

在指定抑制时间内，如果路由器没有收到来自邻居的Hello报文，将宣告邻居失效。抑制时间等于Hello报文失效乘数与Hello报文发送时间间隔的乘积，。配置Hello报文失效乘数，在接口配置模式下，使用如下命令：

isis hello-multiplier *value* [level-1** | **level-2**]**

- *value* – 指定Hello报文失效乘数。取值范围为2到100。默认值为10。
- **level-1 | level-2** – 使用**level-1**参数指定Level-1 Hello报文的失效乘数。使用**level-2**参数指定Level-2 Hello报文的失效乘数。默认为Level-1和Level-2 Hello报文。

使用**no isis hello-multiplier**命令恢复报文失效乘数的默认值。

配置Hello报文填充功能

使用Hello报文填充功能将Hello报文填充到接口MTU大小。配置Hello报文填充功能，在接口配置模式下，使用如下命令：

isis hello padding

使用**no isis hello padding**命令取消Hello报文填充功能。

配置DIS选举优先级

在广播类型网络中，通过指定接口的DIS(Designated IS)优先级，影响DIS选举结果。在DIS选举中，接口的DIS优先级高的IS被选举为DIS。当DIS优先级相同时，则MAC地址最大的接口所属的IS被选举为DIS。配置接口的DIS选举优先级，在接口配置模式下，使用如下命令：

isis priority *value* [level-1** | **level-2**]**

- *value* – 指定DIS选举优先级。取值范围为0到127。默认值为64。
- **level-1 | level-2** – 使用**level-1**参数指定Level-1接口的DIS选举优先级。使用**level-2**参数指定Level-2 接口的DIS选举优先级。默认为Level-1和Level-2接口设置相同的DIS选举优先级。

使用 **no isis priority** [*level-1* | *level-2*] 命令恢复指定级别接口的DIS选举优先级。

配置被动接口

如果把接口配置为被动接口，则此被动接口不向外发送和接受IS-IS报文，并且此接口不与相邻路由器建立邻居关系。但仍然可以把该接口直连网络的路由信息放在LSP中从其他接口宣告出去。配置被动接口，在接口配置模式下，使用如下命令：

isis passive

使用 **no isis passive** 命令取消被动接口设置。

配置LSP生成时间间隔

为了防止网络拓扑频繁变化而导致LSP频繁重新生成，用户可配置LSP生成时间间隔，以抑制网络变化频繁导致占用过多的带宽资源和路由器资源。配置LSP生成时间间隔，在IS-IS路由配置模式下，使用如下命令：

lsp-gen-interval *value* [*level-1* | *level-2*]

- *value* – 指定LSP生成时间间隔。取值范围为1到120。默认值为30。单位为秒。
- **level-1** | **level-2** – 选择**level-1**仅为Level-1 LSPs指定生成时间间隔；选择**level-2**仅为level-2 LSPs指定生成时间间隔。不指定参数时，配置的生成时间间隔适用于Level-1 LSP和Level-2 LSP。

使用 **no lsp-gen-interval** 命令恢复默认值。

配置LSP最大生存时间

为LSP配置最大生存时间。当LSP的最大生存时间递减为0时，IS-IS协议将在LSDB中把此LSP继续保持60秒。若还未收到此LSP的更新，则删除此LSP。配置LSP最大生存时间，在IS-IS路由配置模式下，使用如下命令：

max-lsp-lifetime *value*

- *value* – 指定LSP的最大生存时间。取值范围为350到65535。默认值为1200。单位为秒。

使用 **no max-lsp-lifetime** 命令恢复默认值。

配置LSP刷新时间

每一个LSP都有一个最大生存时间，因此每个路由器必须定时刷新自己生成的LSP，以防止LSP的最大生存时间减小至0。用户可对LSP的刷新周期进行配置。配置LSP刷新时间，在IS-IS路由配置模式下，

使用如下命令：

lsp-refresh-interval *value*

- *value* – 指定LSP的刷新时间。取值范围为1到65535。默认值为900。单位为秒。需要确保刷新时间比LSP最大生存时间少300秒以上，使刷新后的LSP可以在原LSP过期前到达区域内的设备。

使用**no lsp-refresh-interval**命令恢复默认值。

配置SPF计算时间间隔

当LSDB发生变化时需要进行路由计算。计算SPF的时间间隔可以由用户根据需要进行配置。配置SPF计算时间间隔，在IS-IS路由配置模式下，使用如下命令：

spf-interval *value* [**level-1** | **level-2**]

- *value* – 指定计算SPF的时间间隔。取值范围为1到120。默认值为10。单位为秒。
- **level-1** | **level-2** – 选择**level-1**仅为Level-1 SPF指定计算时间间隔；选择**level-2**仅为level-2 SPF指定计算时间间隔。不指定参数时，配置的计算时间间隔适用于Level-1 SPF和Level-2 SPF的计算。

使用**no spf-interval**命令恢复默认值。

配置过载标志位

当路由器因资源不足而导致LSDB不完整或不准确时，会在通告的LSPs中设置过载标志位。其它路由器在收到此类型LSPs后，就不会再利用这台路由器转发需要经过它传送的数据，但到此路由器直连地址的报文仍然可以被转发给此路由器。为路由器手工配制过载标志位，在IS-IS路由配置模式下，使用如下命令：

set-overload-bit

使用**no set-overload-bit**命令取消配置过载标志位。

配置主机名映射

在IS-IS路由域中，System ID作为NET地址的一部分，用来在区域内唯一标识主机或路由器。主机名映射可以将System ID映射到主机名。IS-IS的路由器维护一个主机名到System ID的映射关系表。配置主机名映射，在IS-IS路由配置模式下，使用如下命令：

hostname dynamic

使用**no hostname dynamic**取消主机名映射配置。

IS-IS网络安全性

配置认证

对路由器之间所发送的LSP报文，CSNP报文，PSNP报文进行认证配置。认证配置只影响路由信息的学习，不影响邻居的建立。认证方式有两种，分别是明文认证和MD5密文认证。明文认证不能提供安全保障。未加密的认证字随报文一同传送。默认为明文认证。配置验证方式，在IS-IS路由配置模式下，使用如下命令：

```
authentication {md5 | text} [level-1 | level-2]
```

- **md5 | text** – 使用MD5认证方式（**md5**）或明文认证（**text**）。
- **level-1 | level-2** – 使用**level-1**参数为Level-1路由器之间的报文指定认证方式。使用**level-2**参数为Level-2路由器之间的报文指定认证方式。通过配置Level-1路由器之间的认证，可以防止将从不可信任的路由器学习到的路由信息加入到Level-1的LSDB中。同一区域内的Level-1路由器必须配置相同的认证方式和认证密码。通过配置Level-2路由器间的认证，可以防止将不可信的路由信息注入Level-2路由器。同一路由域中所有Level-2路由器必须配置相同的认证方式和认证密码。

取消认证配置，在IS-IS路由配置模式下，使用**no authentication mode**。

指定认证方式后，需要继续指定认证所使用的密钥。为Level-1路由器之间报文的认证方式指定密钥，使用如下命令：

```
area-password word
```

- **word** – 指定认证所使用的密钥。密钥的最大长度为32字符。

删除指定的密钥，使用**no area-password**命令。

为Level-2路由器之间报文的认证方式指定密钥，使用如下命令：

```
domain-password word
```

- **word** – 指定认证所使用的密钥。密钥的最大长度为32字符。

删除指定的密钥，使用**no domain-password**命令。

配置接口认证模式

接口认证用来确认邻居的合法性，防止与无法信任的路由器形成邻居。配置接口认证后，认证密码将会封装到Hello报文中。通过检查才会形成邻居关系，否则将不会形成邻居关系。两台路由器要形成邻

居关系必须配置相同的认证模式和认证密码。配置接口认证模式，在接口配置模式下，使用如下命令：

```
isis authentication {md5 | text} [level-1 | level-2]
```

- **md5 | text** – 使用MD5认证方式（**md5**）或明文认证（**text**）。
- **level-1 | level-2** – 使用**level-1**参数为Level-1路由器之间的Hello报文指定认证方式。使用**level-2**参数为Level-2路由器之间的Hello报文指定认证方式。

使用**no isis authentication**命令取消接口认证。

配置接口认证模式后，需要继续指定认证所使用的密钥。在接口配置模式下，使用如下命令：

```
isis password word [level-1 | level-2]
```

- **word** – 指定认证所使用的密钥。密钥的最大长度为32字符。
- **level-1 | level-2** – 使用**level-1**参数为Level-1路由器之间的Hello报文认证指定密码。使用**level-2**参数为Level-2路由器之间的Hello报文认证指定密码。

使用**no isis password**命令取消指定的密钥。

查看IS-IS信息

显示IS-IS进程信息及相关配置，在任何模式下使用以下命令：

```
show isis [vrouter vrouter-name]
```

- **vrouter-name** - 显示指定的VRouter的IS-IS进程信息及相关配置。

显示IS-IS链路状态数据库，任何模式下使用以下命令：

```
show isis database [detail] [vrouter vrouter-name]
```

- **detail** – 显示链路状态数据库的详细信息。
- **vrouter-name** - 显示指定的VRouter的链路状态数据库信息。

显示IS-IS接口信息，在任何模式下使用以下命令：

```
show isis interface [interface-name]
```

显示IS-IS邻居信息，在任何模式下使用以下命令：

```
show isis neighbor [detail] [vrouter vrouter-name]
```

显示动态主机名配置，在任何模式下使用以下命令：

```
show isis hostname [vrouter vrouter-name]
```

显示IS-IS路由信息，在任何模式下使用以下命令：

```
show isis route [A.B.C.D/M] [vrouter vrouter-name]
```

显示路由引入信息，在任何模式下使用以下命令：

```
show isis route redistribute [level-1 | level-2] [A.B.C.D/M] [vrouter vrouter-name]
```

BGP

BGP是边界网关协议（Border Gateway Protocol）的缩写。它是在自治系统（“自治系统”是处于一个管理机构控制之下的路由器和网络群组。一个自治系统中的所有路由器必须运行相同的路由协议）之间动态交换路由信息的路由协议，也是ISP之间使用的协议。BGP使用TCP传输协议，端口号为179，并且支持无类别域间选路（CIDR）。BGP有两种运行方式：当BGP运行在自治系统之间时，为EBGP，而当BGP运行在自治系统之内时，为IBGP。BGP具有以下特点：

- 首次建立TCP连接后，BGP邻居之间交换整个BGP路由表，之后仅交换更新路由信息。
- 周期性发送KEEPALIVE报文校验TCP的连通性。
- BGP路由器仅选择最优路径发布到BGP邻居。
- BGP是一种距离矢量的路由协议，从设计上避免了环路的发生。

发送BGP消息的路由器称为BGP发言人，它接收或产生新的路由信息，并发布给其它BGP发言人。当BGP发言人收到来自其它自治系统的新路由时，如果该路由比当前已知路由更优、或者当前还没有该路由，它就把这条路由发布给所有其它BGP发言人。相互交换消息的BGP发言人之间互称对等体（peer），多个相关的对等体可以构成对等体组（peer group）。对等体组的作用是简化配置，不影响实际的对等体关系的建立与路由的传递。

BGP有4种类型的报文，分别为OPEN、UPDATE、NOTIFICATION和KEEPALIVE。BGP对等体间通过发送OPEN报文来交换各自的版本、自治系统号、保持时间、BGP标识符等信息，进行协商。OPEN报文主要用于建立邻居（BGP对等体）关系，它是BGP路由器之间的初始握手消息，应该发生在任何通告消息之前。对等体在收到OPEN消息之后，即以KEEPALIVE消息作为响应。一旦握手成功，则这些BGP邻居就可以进行UPDATE（更新）、KEEPALIVE（保持激活）以及NOTIFICATION（通知）等消息的交换操作。UPDATE报文携带的是路由更新信息，其中包括撤销路由信息和可达路

由信息及其路径属性。当BGP检测到差错（连接中断、协商出错、报文差错等）时，发送NOTIFICATION 报文，关闭同对等体的连接。KEEPALIVE报文在BGP对等体间周期性发送，以确保连接有效。

BGP协议配置

用户可以为不同的VRouter分别配置BGP协议。BGP协议配置包括以下各项：

- 进入BGP配置模式
- 指定Router ID
- 创建聚合路由
- 添加静态BGP路由
- 配置定时器
- 指定BGP路由管理距离
- 指定缺省度量
- 创建BGP对等体组
- 添加BGP对等体到对等体组
- 配置BGP对等体
- 配置BGP MD5认证
- 激活BGP连接
- 配置缺省信息发布
- 配置描述信息
- 配置BGP对等体定时器
- 配置下一跳为自身
- 配置EBGP多跳
- 关闭对等体或者对等体组

- 重置BGP连接
- 配置AS路径访问控制列表
- 配置团体属性列表
- 引入路由
- 配置路由映射表
- 修改引入路由属性
- 配置基于AS路径访问控制列表的路由过滤
- 配置向对等体或者对等体组发送团体属性
- 配置基于路由映射表的路由过滤
- 等价负载均衡

进入BGP配置模式

对BGP协议的配置需要在BGP路由模式下进行。进入BGP路由模式，在VRouter配置模式下，使用以下命令：

ip vrouter vrouter-name （从全局模式进入VRouter配置模式）

router bgp number

- *number* – 指定自治系统的编号。范围是1到4294967295。

运行该命令后，系统的BGP路由功能被开启，为指定的自治系统创建BGP实例，并且进入BGP实例配置模式。

在VRouter配置模式下，使用**no router bgp number**删除BGP实例。

指定Router ID

每一台运行BGP协议的路由器都必须拥有一个Router ID。Router ID是每个路由器在整个BGP域中的唯一标识，使用IP地址的形式表示。如果不指定Router ID，系统会将设备上回环接口的最大IP地址设置为Router ID，如果没有回环接口或者回环接口未配置IP地址，则选择其他接口的最大IP作为Router ID。指定Router ID，在BGP实例配置模式下，使用以下命令：

router-id A.B.C.D

- *A.B.C.D* – 指定BGP协议使用的Router ID，为IP地址形式。

在BGP实例配置模式下，使用该命令no的形式取消Router ID的指定：

```
no router-id
```

创建聚合路由

用户可以将BGP路由表内的路由条目进行聚合。创建聚合路由，在BGP实例配置模式下，使用以下命令：

```
aggregate-address {A.B.C.D/M | A.B.C.D A.B.C.D} [as-set] [summary-only]
```

- *A.B.C.D/M* | *A.B.C.D A.B.C.D* – 指定聚合网络地址。设备支持两种方式，*A.B.C.D/M*或者*A.B.C.D A.B.C.D*，例如1.1.1.0/24或者1.1.1.0 255.255.255.0。
- **as-set** – 如果指定该参数，系统会将聚合路由的路径信息作为自己的路径信息发布给其它路由器。
- **summary-only** – 如果指定该参数，系统将只发布聚合路由。

在BGP实例配置模式下，使用该命令no的形式取消聚合路由的指定：

```
no aggregate-address {A.B.C.D/M | A.B.C.D A.B.C.D}
```

添加静态BGP路由

向BGP路由表中添加静态BGP路由条目，在BGP实例配置模式下，使用以下命令：

```
network {A.B.C.D/M | A.B.C.D A.B.C.D}
```

- *A.B.C.D/M* | *A.B.C.D A.B.C.D* – 指定BGP静态路由条目信息。设备支持两种方式，*A.B.C.D/M*或者*A.B.C.D A.B.C.D*，例如1.1.1.0/24或者1.1.1.0 255.255.255.0。

在BGP实例配置模式下使用该命令no的形式删除指定的静态路由条目：

```
no network {A.B.C.D/M | A.B.C.D A.B.C.D}
```

配置定时器

用户可以配置两个BGP定时器，分别是KEEPALIVE（保持激活）和HOLDDOWN（保持时间），描述如下：

- **KEEPALIVE**（保持激活）：系统向BGP对等体发送保持激活信息的频率。默认为每隔60秒发送一次。
- **HOLDDOWN**（保持时间）：如果本地路由器在保持时间结束后仍没有收到某对等体的保持激活信息，则判断为该对等体老化。默认为180秒。

配置定时器，在BGP实例配置模式下，使用以下命令：

timers *keepalive holddown*

- *keepalive* – 指定发送保持激活信息的频率，单位为秒。默认是60秒。取值范围是0到65535，且小于或者等于HOLDDOWN/3的值，如果大于HOLDDOWN/3，实际生效的时间将为HOLDDOWN/3。参数值为0表示不发送KEEPALIVE信息。
- *holddown* – 指定保持时间，单位为秒。默认是180秒。取值范围是0或者3到65535。参数值为0表示不检查保持时间。

在BGP实例配置模式下使用该命令**no**的形式恢复定时器的默认值：

no timers

指定BGP路由管理距离

用户可以为从其它对等体获得的BGP路由以及本地BGP路由指定管理距离。指定BGP路由管理距离，在BGP实例配置模式下，使用以下命令：

distance *ebgp-distance ibgp-distance local-distance*

- *ebgp-distance* – 指定EBGP路由管理距离。默认值为20。取值范围是1到255的整数。
- *ibgp-distance* – 指定IBGP路由管理距离。默认值为200。取值范围是1到255的整数。
- *local-distance* – 指定本地路由管理距离。默认值为200。取值范围是1到255的整数。

在BGP实例配置模式下使用该命令**no**的形式恢复默认BGP路由管理距离：

no distance

指定缺省度量

默认情况下，引入的IGP路由的度量保持不变，引入的直连路由的度量为0。用户可以为引入路由指定缺省度量。指定引入路由的缺省度量，在BGP实例配置模式下，使用以下命令：

default-metric *value*

- *value* – 指定缺省度量值。范围是1到4294967295。

在BGP实例配置模式下使用该命令no的形式恢复默认情况：

```
no default-metric
```

创建BGP对等体组

使用BGP对等体组，可以简化配置，也可以使信息更新更为有效。创建BGP对等体组，在BGP实例配置模式下，使用以下命令：

```
neighbor peer-group-name peer-group
```

- *peer-group-name* – 指定将要创建的对等体组的名称。

在BGP实例配置模式下使用该命令no的形式删除已创建的BGP对等体组：

```
no neighbor peer-group-name peer-group
```

添加BGP对等体到对等体组

添加BGP对等体到对等体组，在BGP实例配置模式下，使用以下命令：

```
neighbor A.B.C.D peer-group peer-group-name
```

- *A.B.C.D* – 指定将要添加的BGP对等体的IP地址。
- *peer-group-name* – 指定系统中已创建的对等体组的名称。

在BGP实例配置模式下使用该命令no的形式将BGP对等体从对等体组中删除：

```
no neighbor A.B.C.D peer-group peer-group-name
```

配置BGP对等体

用户需要为当前设备指定BGP对等体（对等体组），交换BGP路由信息。配置BGP对等体（对等体组），在BGP实例配置模式下，使用以下命令：

```
neighbor {A.B.C.D | peer-group} remote-as number
```

- *A.B.C.D* | *peer-group* – 指定对等体IP地址或者对等体组的名称。
- *number* – 指定所配置对等体或者对等体组所在的自治区域的编号。

在BGP实例配置模式下使用该命令no的形式取消BGP对等体或者对等体组的指定：

```
no neighbor {A.B.C.D | peer-group} remote-as
```

配置BGP MD5认证

为提高BGP的安全性，用户可以配置BGP对等体或者对等体组在建立TCP连接时进行MD5认证，认证通过后才可建立TCP连接。配置BGP MD5认证，在BGP实例配置模式下，使用以下命令：

```
neighbor {A.B.C.D | peer-group} password password
```

- *A.B.C.D | peer-group* – 指定对等体IP地址或者对等体组的名称。
- *password password* – 指定MD5密码串，范围是1到32个字符。

在BGP实例配置模式下使用该命令no的形式取消BGP MD5认证的配置：

```
no neighbor {A.B.C.D | peer-group} password
```



注意：参与MD5认证的对等体或者对等体组的密码必须一样。

激活BGP连接

默认情况下，已配置的BGP对等体或者对等体组与当前设备的BGP连接是激活的。用户可以关闭连接也可以重新激活BGP连接。激活BGP连接，在BGP实例配置模式下，使用以下命令：

```
neighbor {A.B.C.D | peer-group} activate
```

- *A.B.C.D | peer-group* – 指定对等体IP地址或者对等体组的名称。

在BGP实例配置模式下使用该命令no的形式关闭指定对等体或者对等体组的BGP连接：

```
no neighbor {A.B.C.D | peer-group} activate
```

配置缺省信息发布

用户可以指定当前设备是否将默认路由发布到其它BGP对等体或者对等体组。默认情况下，不发送默认路由。

配置缺省信息发布到BGP对等体或者对等体组，在BGP实例配置模式下，使用以下命令：

```
default-information originate
```

如果路由表中没有默认路由，系统将不会发布默认路由。

在BGP实例配置模式下，使用该命令no的形式取消缺省信息发布：

no default-information originate

配置缺省信息发布到BGP对等体或者对等体组，在BGP实例配置模式下，使用以下命令：

neighbor {A.B.C.D | peer-group} default-originate

- *A.B.C.D | peer-group* – 指定对等体IP地址或者对等体组的名称。

如果路由表中没有默认路由，系统将会构造一条默认路由发布到BGP对等体或者对等体组。

在BGP实例配置模式下使用该命令no的形式取消缺省信息发布：

no neighbor {A.B.C.D | peer-group} default-originate

配置描述信息

为对等体或者对等体组配置描述信息，在BGP实例配置模式下，使用以下命令：

neighbor {A.B.C.D | peer-group} description description

- *A.B.C.D | peer-group* – 指定对等体IP地址或者对等体组的名称。
- *description* – 指定描述信息。范围是1到80个字符。

在BGP实例配置模式下使用该命令no的形式取消对等体或者对等体组的描述信息：

no neighbor {A.B.C.D | peer-group} description

配置BGP对等体定时器

默认情况下，在整个BGP系统中，BGP对等体或对等体组之间的定时器按照timer keepalive holddown设置的值生效，用户可以为某个特定的BGP对等体或者对等体组指定不同的定时器数值，该数值优先级高于timer keepalive holddown设置的值。为BGP对等体或者对等体组指定定时器数值，在BGP实例配置模式下，使用以下命令：

neighbor {A.B.C.D | peer-group} timers keepalive holddown

- *A.B.C.D | peer-group* – 指定对等体IP地址或者对等体组的名称。
- *keepalive* – 指定发送保持激活信息的频率，单位为秒。默认是60秒。取值范围是0到65535，且小于或者等于HOLDDOWN/3的值，如果大于HOLDDOWN/3，实际生效的时间将为HOLDDOWN/3。参数值为0表示不发送KEEPALIVE信息。

- *holddown* – 指定保持时间，单位为秒。默认是180秒。取值范围是0或者3到65535。参数值为0表示不检查保持时间。

在BGP实例配置模式下使用该命令no的形式取消对BGP对等体或对等体组定时器的指定：

```
no neighbor {A.B.C.D | peer-group} timers
```

配置下一跳为自身

配置该功能后，路由器将通告对等体或者对等体组BGP路由的下一跳为该路由器自身。配置下一跳路由为自身，在BGP实例配置模式下，使用以下命令：

```
neighbor {A.B.C.D | peer-group} next-hop-self
```

- *A.B.C.D | peer-group* - 指定对等体IP地址或者对等体组的名称。

在BGP实例配置模式下使用该命令no的形式取消下一跳为自身的指定：

```
no neighbor {A.B.C.D | peer-group} next-hop-self
```

配置EBGP多跳

对于运行在自治系统之间的BGP（即EBGP），如果BGP对等体或对等体组没有直接连接，用户需要配置EBGP多跳才能在设备之间创建邻居关系。配置EBGP多跳，在BGP实例配置模式下，使用以下命令：

```
neighbor {A.B.C.D | peer-group} ebgp-multihop [ttl]
```

- *A.B.C.D | peer-group* - 指定对等体IP地址或者对等体组的名称。
- *ttl* - 指定到对等体IP地址或者对等体组的最大下一跳数。取值范围是1到255，默认值是255。如果在达到最大下一跳数后仍无法找到指定的对等体或对等体组，系统会认为创建邻居关系失败。

在BGP实例配置模式下使用该命令no的形式取消EBGP多跳：**no neighbor {A.B.C.D | peer-group} ebgp-multihop**

关闭对等体或者对等体组

用户可以关闭指定的对等体或者对等体组。关闭对等体或者对等体组后，所有与被关闭对等体或者对等体组相关的会话都会被中断，所有相关的路由信息也会被删除。关闭对等体或者对等体组，在BGP实例配置模式下，使用以下命令：

```
neighbor {A.B.C.D | peer-group} shutdown
```

- *A.B.C.D* | *peer-group* – 指定对等体IP地址或者对等体组的名称。

在BGP实例配置模式下使用该命令no的形式开启对等体或者对等体组：

```
no neighbor {A.B.C.D | peer-group} shutdown
```

重置BGP连接

重置BGP连接，在执行模式下，使用以下命令：

```
clear ip bgp {* | A.B.C.D | external | peer-group peer-group-name | number} [vrouter vrouter-name]
```

- * - 重置当前所有BGP会话连接。
- *A.B.C.D* – 重置指定对等体的BGP连接。
- external – 重置所有EBGP连接。
- peer-group *peer-group-name* – 重置指定BGP对等体组的连接。
- *number* – 重置指定自治系统中的BGP连接。
- vrouter *vrouter-name* – 指定需重置连接所在的VRouter。

配置AS路径访问控制列表

AS路径是路由在到达目的网络之前所经过的AS号码序列。在到达目的网络之前，BGP路由每经过一个AS，在出AS时就会将AS号码添加到AS路径中。

用户可以通过AS路径访问控制列表实现路由过滤。AS路径访问控制列表主要由正则表达式和匹配成功后所执行操作（允许或拒绝）两部分组成。如果正则表达式匹配路由的AS路径，系统会继续执行指定的操作；如果匹配失败，系统会执行拒绝操作。系统最多允许配置64个AS路径访问控制列表，每个AS路径访问控制列表最多允许配置8条正则表达式。

配置AS路径访问控制列表，在全局配置模式下使用以下命令：

```
ip as-path access-list access-list-number {deny | permit} regular-expression
```

- *access-list-number* – 指定AS路径访问控制列表号。范围为1到500。
- deny | permit – 指定对匹配的路由所执行的操作。deny为拒绝，permit为允许。

- *regular-expression* – 指定用于匹配AS路径的正则表达式。系统支持PCRE（Perl Compatible Regular Expressions）正则表达式语法。

在全局配置模式下使用该命令no的形式删除AS路径访问控制列表：

```
no ip as-path access-list access-list-number [{deny | permit} regular-expression]
```

例如，配置序号为1的AS路径控制列表，拒绝经过AS 31的路由，但允许其他路由，请输入以下命令：

```
hostname(config)# ip as-path access-list 1 deny _31_  
hostname(config)# ip as-path access-list 1 permit .*  
hostname(config)#
```

开启/关闭EBGP的multipath-relax功能

对于EBGP在通过不同AS路径去往同一个目的网络，系统支持开启EBGP的multipath-relax功能，从而使EBGP在不同AS路径上实现负载均衡。在BGP实例配置模式下，使用以下命令：

- **best-path as-h path multipath-relax** - 开启该功能。
- **no best-path as-h path multipath-relax** - 关闭该功能。

配置团体属性列表

在BGP中，团体属性标识一组具有相同特征的路由信息，与其所在的IP子网和AS无关。除用户自定义的团体属性外，系统支持如下的公认团体属性：

- No-export：带有这一团体属性值的路由不能通告给AS之外的对等体。
- No-adverties：带有这一团体属性值的路由不能通告给任何BGP对等体。
- Local-as：带有这一团体属性值的路由可以通告给本地AS内的其他对等体，不能通告到本地AS以外的对等体。
- Internet：带有这一团体属性值的路由可以通告给任何BGP邻居。默认情况下所有路由都携带该属性。

团体属性列表主要由团体属性和匹配成功后所执行操作（允许或拒绝）两部分组成。如果引入路由的团体属性匹配指定的团体属性，系统会继续执行指定的操作；如果匹配失败，系统会执行拒绝操作。系统最多允许配置128个团体属性列表，每个团体属性列表最多允许配置一条Permit规则和一条Deny规则。

配置团体属性列表，在全局配置模式下使用以下命令：

```
ip community-list {standard community-list-name | community-list-number} {deny | permit} {[internet] [local-as] [no-advertise] [no-export] [community-number]}
```

- **standard community-list-name** – 指定团体属性列表名称。为1到31个字符的字符串。
- **community-list-number** – 指定团体属性列表号。范围为1到99。
- **deny | permit** – 指定对匹配的路由所执行的操作。**deny**为拒绝，**permit**为允许。
- **[internet] [local-as] [no-advertise] [no-export] [community-number]** – 指定团体属性，可以同时指定多个团体属性，不同团体属性间用空格隔开。**community-number**为1到4294967295之间的数字。

在全局配置模式下使用该命令**no**的形式删除团体属性列表：

```
no ip community-list {standard community-list-name | community-list-number}
```

引入路由

BGP协议允许用户引入其它路由协议（OSPF、直连、静态和RIP）的路由信息，并向外发布。同时，用户可以设置被引入路由的度量，还可以引用路由映射表对路由信息进行过滤，仅允许引入或拒绝引入特定的路由信息。配置引入路由，在BGP实例配置模式下使用以下命令：

```
redistribute {ospf | connected | static | rip} [metric value] [route-map name]
```

- **ospf | connected | static | rip** – 指定引入路由的类型，可以是OSPF（**ospf**）、直连路由（**connected**）、静态路由（**static**）或者RIP（**rip**）。
- **metric value** – 指定引入路由的度量。范围是0到4294967295。如果不指定该数值，系统会使用BGP的缺省度量（通过**default-metric value**配置）。
- **route-map name** – 指定用于过滤引入路由信息的路由映射表。有关路由映射表的更多信息，请参考“[配置路由映射表](#)”。

用户可以配置多条该命令引入不同类型的路由。

使用**no redistribute {ospf | connected | static | rip}**命令取消指定类型路由的引入。

配置路由映射表

默认情况下系统会引入所有的路由信息。用户可以引用路由映射表对引入的路由信息进行过滤。路由映射表主要由路由匹配规则和匹配成功后所执行操作（允许或拒绝）两部分组成。如果引入的路由信息命中了任何路由匹配规则，系统就会执行对应的操作，允许或拒绝引入这些路由信息。

**注意:**

- 如果用户设置的操作是允许，匹配成功后系统仅允许引入匹配的路由信息，拒绝引入所有未匹配的路由信息。
- 如果用户设置的操作是拒绝，匹配成功后系统会拒绝引入匹配的路由信息，但仍允许引入未匹配的路由信息。

用户可通过以下步骤配置路由映射表，实现对引入路由信息的过滤：

1. 创建路由映射表并在表中创建路由匹配规则。不同的匹配规则通过序列号区分。序列号越小，匹配优先级越高。默认情况下，引入的路由信息命中任何路由匹配规则，系统将不再继续匹配后续的规则；如果引入的路由信息没有命中任何匹配规则，系统将执行拒绝操作。
2. 在路由匹配规则中配置匹配条件。匹配条件可以是引入路由的AS路径、团体属性、度量值、目的地址或下一跳地址。一条路由匹配规则中可以包含多个匹配条件，这些匹配条件之间是与（AND）关系，即引入的路由信息必须满足匹配规则中的所有匹配条件才会认定为命中了该条规则。
3. 如有需要，可以设置系统在命中一条路由匹配规则后继续匹配其他规则。有关匹配多条路由匹配规则配置的更多信息，请参考“[匹配多条路由匹配规则](#)”。
4. 如有需要，修改引入路由的部分属性后再对外发布。

创建路由映射表并在表中配置路由匹配规则，在全局配置模式下，使用以下命令：

```
route-map name {deny | permit} sequence
```

- **route-map** name – 指定路由映射表名称，并进入路由映射表配置模式。取值范围是1到31个字符。如果该名称已经存在，则直接进入路由映射表配置模式。
- **deny | permit** – 指定对匹配的路由信息所执行的操作。deny为拒绝，permit为允许。
- **sequence** – 指定该路由映射表下路由匹配规则的序列号。取值范围是1到65535。

使用该命令no的形式删除路由映射表：

```
no route-map name [sequence]
```

- **sequence** – 仅删除路由映射表中指定的匹配规则。

配置路由匹配规则中的匹配条件，在路由映射表配置模式下，使用以下命令：


```
match {as-path access-list-number | community {community-list-name | community-list-number}
[exact-match] | metric metric-value | ip address access-list | ip next-hop access-list}
```

- **as-path** *access-list-number* – 匹配路由的AS路径。*access-list-number*为用户配置的AS路径访问控制列表号。如果路由的AS路径匹配该访问控制列表中允许的AS路径，则认为匹配成功。有关AS路径访问控制列表配置的更多信息，请参考“[配置AS路径访问控制列表](#)”。
- **community** {*community-list-name* | *community-list-number*} [*exact-match*] – 匹配路由的团体属性。*community-list-name*为团体属性列表名称；*community-list-number*为团体属性列表号；*exact-match*指定对团体属性进行精确匹配。有关团体属性列表配置的更多信息，请参考“[配置团体属性列表](#)”。
- **metric** *metric-value* – 匹配路由的度量值。取值范围是0到4294967295。
- **ip address** *access-list* – 匹配路由的目的地址。*access-list*为用户配置的路由访问控制列表。如果路由的目的地址属于该访问控制列表中允许的地址，则认为匹配成功。有关访问控制列表配置的更多信息，请参考“[配置路由访问控制列表](#)”。
- **ip next-hop** *access-list* – 匹配路由的下一跳地址。*access-list*为用户配置的路由访问控制列表。如果路由的下一跳地址属于该访问控制列表中允许的地址，则认为匹配成功。有关访问控制列表配置的更多信息，请参考“[配置路由访问控制列表](#)”。

重复以上命令向路由匹配规则中添加多个不同类型的匹配条件。使用该命令no的形式删除匹配条件：

```
no match {as-path | community | metric | ip address | ip next-hop}
```



注意: 如果用户仅创建了路由映射表但没有在映射表中配置任何路由匹配规则，系统默认会认为引入的路由信息匹配成功。

修改引入路由属性

对于满足匹配条件的引入路由，用户可以在修改路由的部分属性后再对外发布。修改引入路由的属性，在路由映射表配置模式下，使用以下命令：

```
set {as-path prepend as-number | commu-list {community-list-name | community-list-number} delete
| community {[internet] [local-AS] [no-advertise] [no-export] [community-list-number]} [additive] |
ip next-hop ip-address | local-preference value | metric metric-value | origin {egp | igp | incomplete}}
```

- **as-path prepend** *as-number* – 在引入路由的AS路径后添加新的AS路径。取值范围为1到65535之间的数字，多个数字之间用空格隔开。
- **commu-list** { *community-list-name* | *community-list-number* } **delete** – 指定团体属性列表名称（*community-list-name*）或者团体属性列表号（*community-list-number*），删除匹配的团体属性。
- **community** { [internet] [local-AS] [no-advertise] [no-export] [*community-list-number*] } [**additive**] – 修改引入路由的团体属性。**additive**为在引入路由的团体属性中添加新的团体属性。
- **ip next-hop** *ip-address* – 修改引入路由的下一跳地址。
- **local-preference** *value* – 修改引入路由的本地优先属性。取值范围是0到4294967295。
- **metric** *metric-value* – 修改引入路由的度量值。取值范围是0到4294967295。
- **origin** { **igp** | **egp** | **incomplete** } – 修改引入路由的来源属性。**igp**为路由起始于AS内部；**egp**为路由通过EGP获得；**incomplete**为路由通过其他方法获得。

使用该命令no的形式取消对路由属性的修改并还原到引入路由时的设置：

```
no set {as-path prepend | commu-list | community | ip next-hop | local-preference | origin | metric | metric-type}
```

配置基于AS路径访问控制列表的路由过滤

BGP协议支持通过AS路径访问控制列表对对等体（对等体组）引入的路由或者向外发布的路由进行过滤。配置基于AS路径访问控制列表的路由过滤，在BGP实例配置模式下，使用以下命令：

```
neighbor {A.B.C.D | peer-group} filter-list access-list-number {in | out}
```

- *A.B.C.D* | *peer-group* – 指定BGP对等体的IP地址或者对等体组的名称。
- *access-list-number* – 指定AS路径访问控制列表号。有关AS路径访问控制列表的更多信息，请参考“[配置AS路径访问控制列表](#)”。
- **in** | **out** – 指定对引入的路由（in）或者向外发布的路由（out）进行过滤。

使用该命令no的形式取消基于AS路径访问控制列表的路由过滤配置：

```
no neighbor {A.B.C.D | peer-group} filter-list {in | out}
```

配置向对等体或者对等体组发送团体属性

配置向对等体（对等体组）发送团体属性，在BGP实例配置模式下，使用以下命令：

```
neighbor {A.B.C.D | peer-group} send-community {standard | extended | both}
```

- *A.B.C.D* | *peer-group* – 指定BGP对等体的IP地址或者对等体组的名称。
- **standard** | **extended** | **both** – 指定发送团体属性的类别，可以是标准团体属性（**standard**），扩展团体属性（**extended**），或者标准团体属性和扩展团体属性（**both**）。

使用该命令no的形式取消发送团体属性配置：

```
no neighbor {A.B.C.D | peer-group} send-community
```

配置基于路由映射表的路由过滤

BGP协议支持通过路由映射表对对等体（对等体组）引入的路由或者向外发布的路由进行过滤。配置基于路由映射表的路由过滤，在BGP实例配置模式下，使用以下命令：

```
neighbor {A.B.C.D | peer-group} route-map {in | out}
```

- *A.B.C.D* | *peer-group* – 指定BGP对等体的IP地址或者对等体组的名称。
- **in** | **out** – 指定对引入的路由（**in**）或者向外发布的路由（**out**）进行过滤。

使用该命令no的形式取消基于路由映射表的路由过滤配置：

```
no neighbor {A.B.C.D | peer-group} route-map {in | out}
```

等价负载均衡

配置BGP负载均衡的最大路径数，在BGP实例配置模式下，使用以下命令：

```
maximum-paths {ebgp | ibgp} maximum-number
```

- *maximum-number* – 指定EBGP/IBGP最大ECMP路径数。配置路径数后，若存在多条等价路径，多条路径均会被加入到路由表中。这样即可使BGP在多条路径上实现负载均衡。取值范围是1到8，默认值是1。

在BGP实例配置模式下，使用该命令no的形式取消等价负载均衡：

```
no maximum-paths {ebgp | ibgp}
```



注意: 配置该功能前，用户需先开启ECMP功能。如何开启ECMP，请参阅[“等价多径路由 \(ECMP\)”](#)。

查看BGP信息

显示BGP路由信息，在任何模式下使用以下命令：

```
show ip route bgp [vrouter vrouter-name]
```

- *vrouter-name* - 显示指定VRouter的BGP路由信息。

显示整个BGP路由表的路由信息，在任何模式下使用以下命令：

```
show ip bgp [A.B.C.D | A.B.C.D/M] [vrouter vrouter-name]
```

- *A.B.C.D* | *A.B.C.D/M* - 显示到指定网络的BGP路由信息。
- *vrouter-name* - 显示指定VRouter的BGP路由信息。

显示BGP数据库中存储的所有自治系统路径信息，在任何模式下使用以下命令：

```
show ip bgp paths [vrouter vrouter-name]
```

- *vrouter-name* - 显示指定的VRouter的自治系统路径信息。

显示所有BGP连接的状态参数，包括前缀、路径和属性信息等，在任何模式下使用以下命令：

```
show ip bgp summary [vrouter vrouter-name]
```

- *vrouter-name* - 显示指定VRouter的BGP连接状态参数。

显示BGP对等体状态，在任何模式下使用以下命令：

```
show ip bgp neighbor [A.B.C.D] [vrouter vrouter-name]
```

- *A.B.C.D* - 显示指定对等体的状态。
- *vrouter-name* - 显示指定VRouter的BGP对等体的状态。

显示BGP团体属性列表信息，在任何模式下使用以下命令：

```
show ip community [community-list-name]
```

- *community-list-name* – 显示指定名称或者序号的团体属性列表信息。如不输入该参数，则显示所有团体属性列表信息。

show ip as-path-access-list [*access-list-number*]

- *access-list-number* – 显示指定序号的AS路径访问控制列表信息。如不输入该参数，则显示所有AS路径访问控制列表信息。

等价多径路由（ECMP）

等价多径路由（ECMP）是对经过安全设备的数据流量在多条等价路径（同协议）上进行负载均衡转发的方法。

配置ECMP功能

默认情况下，系统的ECMP功能为开启状态，并允许最多40条等价路由条目进行负载均衡。在VRouter配置模式下，使用以下命令开启或关闭ECMP功能：

ecmp enable *ecmp-route-num*

- *ecmp-route-num* – 系统允许的最大ECMP路由条目数。取值范围为1到1000。当取值为1时表示不使用ECMP功能。

配置ECMP选路方式

在全局配置模式下，使用以下命令配置ECMP选路方式：

ecmp-route-select {*by-5-tuple* | *by-src* | *by-src-and-dst*}

- **by-5-tuple** – 基于五元组（源IP地址、目的IP地址、源端口、目的端口和服务类型）进行选路。
- **by-src** – 基于源IP地址进行选路。
- **by-src-and-dst** – 基于源IP地址和目的IP地址进行选路。该方式为系统默认选路方式。

静态组播路由

组播是将数据从一个源点传送到多个目的节点的一种通信方式。发送数据的源点称为组播源，接收数据的多个节点构成组播组。组播源将数据发送至目的地址，其地址范围是224.0.0.0至239.255.255.255

之间的D类地址，称为组播地址。

互联网内任意一台主机均可作为组播源，源点只发送一份数据至组播地址，组内的所有接收者均可接收到相同的数据。应用组播方式传递信息，能够有效的节约网络带宽；如果接入网络用户数量增加，不会增大发送数据主机的负担，降低了网络负荷。

用户可以通过手工配置组播路由规则来实现将数据从组播源传送给组播成员。组播路由规则需要定义以下信息：

- 组播源和组播地址：即组播源IP和目的IP。
- 入接口和出接口：匹配对应组播源和组播地址的数据从组播路由规则中指定的入接口进，从指定的出接口出。

开启/关闭组播路由功能

系统支持IPv4和IPv6两种类型的组播路由功能。默认情况下，组播路由功能为关闭状态。在VRouter配置模式下，使用以下命令开启或关闭组播路由功能：

- **{ip | ipv6 } multicast-routing**
 - **ip** - 开启IPv4类型的组播路由功能。
 - **ipv6** - 开启IPv6类型的组播路由功能。
- **no {ip | ipv6 } multicast-routing**
 - **ip** - 关闭IPv4类型的组播路由功能。
 - **ipv6** - 关闭IPv6类型的组播路由功能。

配置静态组播路由

配置IPv4静态组播路由

在VRouter配置模式下，使用以下命令创建静态组播路由：

```
ip mroute A.B.C.D A.B.C.D [iif interface-name] [oif interface-name]
```

- *A.B.C.D A.B.C.D* – 指定组播源和组播地址。第一个A.B.C.D为组播源IP地址；第二个A.B.C.D为组播地址，其地址范围是224.0.0.0 至 239.255.255.255 之间。
- **iif** *interface-name* – 指定入接口名称。在此命令中，最多允许用户指定2个入接口名称。
- **oif** *interface-name* – 指定出接口名称。在此命令中，最多允许用户指定4个出接口名称。

在VRouter配置模式下，使用该命令的no形式删除静态组播路由：

```
no ip mroute A.B.C.D A.B.C.D [iif interface-name] [oif interface-name]
```

指定入接口/出接口

用户可以为已创建的静态组播路由条目配置入接口或出接口。系统允许为每条组播路由条目最多配置2个入接口，32个出接口。入接口或出接口的配置需要在静态组播路由配置模式下进行。进入静态组播路由配置模式，在VRouter配置模式下，使用以下命令：

```
ip mroute A.B.C.D A.B.C.D
```

- *A.B.C.D A.B.C.D* – 指定组播源和组播地址。第一个A.B.C.D为组播源IP地址；第二个A.B.C.D为组播地址。

为已创建的静态组播路由条目指定入接口或出接口名称，在静态组播路由配置模式下，使用以下命令：

- 指定入接口名称：**iif** *interface-name*
- 指定出接口名称：**oif** *interface-name*

多次执行以上命令配置多个入接口或出接口。

配置IPv6静态组播路由

在VRouter配置模式下，使用以下命令创建静态组播路由：

```
ipv6 mroute X:X:X:X::X X:X:X:X::X [iif interface-name] [oif interface-name]
```

- *X:X:X:X::X X:X:X:X::X* – 指定组播源和组播地址。第一个X:X:X:X::X为组播源IP地址；第二个X:X:X:X::X为组播地址。
- **iif** *interface-name* – 指定入接口名称。在此命令中，最多允许用户指定2个入接口名称。
- **oif** *interface-name* – 指定出接口名称。在此命令中，最多允许用户指定4个出接口名称。

在VRouter配置模式下，使用该命令的no形式删除静态组播路由：

```
no ipv6 mroute X:X:X:X::X X:X:X:X::X [iif interface-name] [oif interface-name]
```

指定入接口/出接口

用户可以为已创建的静态组播路由条目配置入接口或出接口。系统允许为每条组播路由条目最多配置2个入接口，32个出接口。入接口或出接口的配置需要在静态组播路由配置模式下进行。进入静态组播路由配置模式，在VRouter配置模式下，使用以下命令：

```
ipv6 mroute X:X:X:X::X X:X:X:X::X
```

- `X:X:X:X::X X:X:X:X::X` - 指定组播源和组播地址。第一个X:X:X:X::X为组播源IP地址；第二个X:X:X:X::X为组播地址。

为已创建的静态组播路由条目指定入接口或出接口名称，在静态组播路由配置模式下，使用以下命令：

- 指定入接口名称：**iif** *interface-name*
- 指定出接口名称：**oif** *interface-name*

多次执行以上命令配置多个入接口或出接口。

为已创建的IPv6静态组播路由条目删除已指定的入接口或出接口，可以在VRouter配置模式下，使用**no ipv6 mroute** `X:X:X:X::X X:X:X:X::X` [**iif** *interface-name*] [**oif** *interface-name*]命令；或者在IPv6静态组播路由配置模式下，使用以下命令：

- 删除入接口：**iif** *interface-name*
- 删除出接口：**oif** *interface-name*

显示组播路由信息

用户可以在任何模式下，随时使用show命令查看IPv4组播路由信息。命令如下：

```
show ip mroute [A.B.C.D A.B.C.D | static | summary] [vrouter vr-name]
```

- **show ip mroute** - 显示全部IPv4组播路由信息。
- `A.B.C.D A.B.C.D` - 通过指定组播源地址和组播地址，显示其组播路由信息。第一个A.B.C.D为组播源地址，第二个A.B.C.D为组播地址。

- **static** - 显示静态组播路由信息。
- **summary** - 显示组播路由的摘要信息。
- **vrouter** *vr-name* - 显示指定VRouter下的IPv4组播路由信息。

用户可以在任何模式下，随时使用show命令查看IPv6组播路由信息。命令如下：

show ipv6 mroute [*X:X:X:X::X X:X:X:X::X* | **summary**] [**vrouter** *vr-name*]

- **show ipv6 mroute** - 显示全部IPv6组播路由信息。
- *X:X:X:X::X X:X:X:X::X* - 通过指定组播源地址和组播地址，显示其组播路由信息。第一个*X:X:X:X::X*为组播源地址，第二个*X:X:X:X::X*为组播地址。
- **summary** - 显示组播路由的摘要信息。
- **vrouter** *vr-name* - 显示指定VRouter下的IPv6组播路由信息。

显示组播FIB信息

用户可以在任何模式下，使用以下命令查看IPv4组播FIB信息：

show mfib [*A.B.C.D A.B.C.D* | **summary**] [**vrouter** *vr-name*]

- **show mfib** - 显示所有IPv4组播FIB信息。
- *A.B.C.D A.B.C.D* - 通过指定组播源地址和组播地址，显示其组播FIB信息。第一个*A.B.C.D*为组播源地址，第二个*A.B.C.D*为组播地址。
- **summary** - 显示IPv4组播FIB的摘要信息。
- **vrouter** *vr-name* - 显示指定VRouter下的IPv4组播FIB信息。

用户可以在任何模式下，使用以下命令查看IPv6组播FIB信息：

show ipv6 mfib [*X:X:X:X::X X:X:X:X::X* | **summary**] [**vrouter** *vr-name*]

- **show ipv6 mfib** - 显示所有IPv6组播FIB信息。
- *X:X:X:X::X X:X:X:X::X* - 通过指定组播源地址和组播地址，显示其组播FIB信息。第一个*X:X:X:X::X*为组播源地址，第二个*X:X:X:X::X*为组播地址。

- **summary** – 显示IPv6组播FIB的摘要信息。
- **vrouter vr-name** – 显示指定VRouter下的IPv6组播FIB信息。

互联网组管理协议

互联网组管理协议IGMP（Internet Group Message Protocol）是用于在主机和路由器之间建立并维护组播成员关系的协议。通过IGMP协议，主机向路由器报告组成员的加入和离开，路由器周期性地发送查询报文查看是否有组成员处于活动状态，如果未收到组播成员的报告报文，则认为该组播组中已无组成员。

当前版本的系统支持IGMPv1（由RFC1112定义）和、IGMPv2（由RFC2236定义）和IGMPv3（由RFC3376定义）。并且支持IGMP Proxy（工作在应用层）和IGMP Snooping（工作在链路层）两个功能。

IGMP Proxy

IGMP Proxy靠代理拦截主机和路由器之间的IGMP报文来建立组播路由表项，进行组播数据的转发。IGMP Proxy在安全设备的两个接口上分别实现不同的功能。上联到组播路由器的上行接口代理实现主机的功能，响应来自路由器的查询。当组播组新增一个成员或者最后一个成员退出时，安全设备通过上行接口主动发送成员报告报文或者离开报文。下联到用户主机的下行接口代理实现路由器的功能，进行组成员的登记、查询和删除工作。

配置IGMP代理，请按照以下步骤进行操作：

1. 启用组播路由功能。具体操作，请参阅“开启/关闭组播路由功能开启/关闭组播路由功能”。
2. 启用IGMP代理功能。
3. 配置上行接口为主机模式，代理主机功能。
4. 配置下行接口为路由器模式，代理IGMP路由器功能。
5. 配置策略规则。

启用IGMP代理

在VRouter配置模式下，使用以下命令启用或禁用IGMP代理功能：

- 启用IGMP代理: **ip igmp-proxy enable**
- 禁用IGMP代理: **no ip igmp-proxy enable**

在全局配置模式下, 使用以下命令进入VRouter配置模式:

ip vrouter *vrouter-name*

- *vrouter-name* - 指定VRouter的名称。如果指定的名称已存在, 则直接进入VRouter配置模式。

配置接口的IGMP代理模式

在接口配置模式下, 用户可使用以下命令配置接口的IGMP代理模式, 使它处于主机模式或路由器模式:

ip igmp-proxy {**router-mode** | **host-mode**} [*A.B.C.D*] [**v2** | **v3**]

- **router-mode** - 配置下行接口的IGMP代理模式为路由器模式。
- **host-mode** - 配置上行接口的IGMP代理模式为主机模式。
- [*A.B.C.D*] - 指定组播组地址。配置组播地址后, 系统认为IGMP代理模式仅对此组播地址有效。
- **v2** - 指定接口发送的IGMP报文的协议版本为IGMPv2。默认情况下, 使用IGMPv2协议。
- **v3** - 指定接口发送的IGMP报文的协议版本为IGMPv3。

在接口配置模式下, 使用该命令**no**的形式取消指定接口的IGMP代理模式:

no ip igmp-proxy {**router-mode** | **host-mode**} [*A.B.C.D*]

查看IGMP Proxy信息

用户可以在任何模式下, 随时使用show命令查看IGMP Proxy信息。命令如下:

show ip igmp-proxy [*A.B.C.D*] [**vrouter** *vrouter-name*]

- **show ip igmp-proxy** - 查看系统中全部IGMP Proxy信息。
- [*A.B.C.D*] - 查看指定的组播组地址的IGMP Proxy信息。
- [**vrouter** *vrouter-name*] - 查看指定的VRouter下的IGMP Proxy信息。

IGMP Snooping

IGMP Snooping是通过监听主机和路由器之间的IGMP报文，在二层设备上建立针对某个组播地址的组播路由表项。开启IGMP Snooping功能后，安全设备根据组播路由表项转发组播数据，有效的减少了组播通信的开销。如果没有开启IGMP Snooping功能，安全设备只能广播组播数据。

配置IGMP Snooping，请按照以下步骤进行操作：

1. 开启组播路由功能。具体操作，请参阅“开启/关闭组播路由功能开启/关闭组播路由功能”。
2. 开启IGMP Snooping功能。
3. 配置IGMP Snooping。
4. 配置策略规则。

启用IGMP Snooping

在VSwitch配置模式下，使用以下命令启用或禁用IGMP Snooping功能：

- 启用IGMP Snooping功能：**ip igmp-snooping enable**
- 禁用IGMP Snooping功能：**no ip igmp-snooping enable**

在全局配置模式下，使用以下命令创建或进入VSwitch配置模式：

vswitch vswitchNumber

- *Number* – 指定VSwitch的数字标识。Number的取值范围根据平台不同而不同。例如，命令**vswitch vswitch2**创建了名为VSwitch2的VSwitch，同时也创建了VSwitchif2接口，并且进入VSwitch2的配置模式。如果指定的VSwitch名称已存在，则直接进入VSwitch配置模式。

配置IGMP Snooping

在接口配置模式下，使用以下命令配置IGMP Snooping功能：

ip igmp-snooping {router-mode [A.B.C.D] | host-mode [A.B.C.D] | disable | auto}

- **router-mode** – 配置下行接口的IGMP Snooping模式为路由器模式。
- **host-mode** – 配置上行接口的IGMP Snooping模式为主机模式。

- `[A.B.C.D]` – 指定组播组地址。
- **disable** – 禁用接口的IGMP Snooping功能。
- **auto** – 指定该参数，系统通过IGMP报文自动确定接口的模式。

在接口配置模式下，使用该命令**no**的形式取消配置IGMP Snooping功能：

```
no ip igmp-snooping {router-mode A.B.C.D | host-mode A.B.C.D}
```

未知组播丢弃

默认情况下，未知组播丢弃功能为关闭状态。开启该功能后，安全设备将丢弃发往未知组播组的报文，从而节省带宽。在VSwitch配置模式下，使用以下命令开启未知组播丢弃功能：

```
unknown-multicast drop
```

在VSwitch配置模式下，使用该命令**no**的形式关闭未知组播丢弃功能：

```
no unknown-multicast drop
```

查看IGMP Snooping信息

用户可以在任何模式下，随时使用**show**命令查看IGMP Snooping信息。命令如下：

```
show ip igmp-snooping [A.B.C.D] [vswitch name]
```

- **show ip igmp-snooping** - 显示全部IGMP Snooping信息。
- `[A.B.C.D]` – 查看指定的组播组地址的IGMP Snooping信息。
- `[vswitch name]` – 查看指定的VSwitch下的IGMP Snooping信息。

协议无关组播（PIM）

协议无关组播PIM（Protocol Independent Multicast），表示为IP组播提供路由信息的可以是静态路由或任意单播路由协议（如RIP、OSPF、IS-IS、BGP等）。组播路由和所采用的单播路由协议无关，只要是能够通过单播路由协议产生相应的组播路由表项即可。

根据机制的不同，PIM分为以下两种模式：

- PIM-DM (Protocol Independent Multicast-Dense Mode)：协议无关组播—密集模式，适用于小规模、接收者分布较为密集的情况。
- PIM-SM (Protocol Independent Multicast-Sparse Mode)：协议无关组播—稀疏模式，适用于大规模、接收者分布较为稀疏的情况。

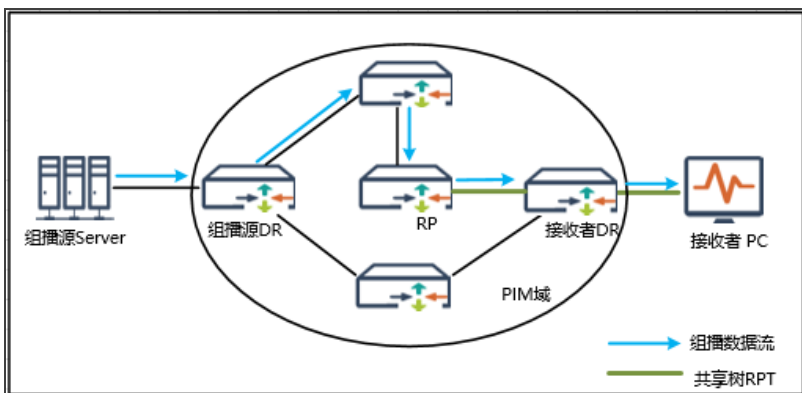
目前设备系统版本仅支持PIM-SM模式。

PIM-SM基本原理

PIM-SM (Protocol Independent Multicast-Sparse Mode，协议无关组播-稀疏模式)可以有效解决大型网络且用户分布比较分散的场景中，“点到多点”的数据传输问题，使用户能够按需接收数据。

PIM-SM假设网络中所有主机都不需要接收组播数据，只有在主机明确提出需要接收组播数据时，PIM设备才会向该主机转发组播数据。

PIM-SM通过配置的RP (Rendezvous Point，汇聚点)和BSR (Bootstrap Router，自举路由器)，向PIM域中的PIM设备发送组播信息，从而构建RPT (Rendezvous Point Tree，共享树)，组播数据通过RP沿着RPT转发给接收者。



PIM-SM相关概念如下：

- **PIM域**: 由PIM设备所组成的PIM网络。
- **DR (Designated Router)**: 称为指定路由器，在PIM域中，包括两种DR:
 - **组播源DR**: 组播源DR是与组播源直接相连且负责向RP发送注册报文的PIM设备。
 - **接收者DR**: 与组播组成员（通常为接收者主机）直接相连且负责向该组成员转发组播数据的PIM设备。

- **RP (Rendezvous Point)**：称为汇聚点，是PIM域的转发核心，分为静态PR和动态PR。PIM-SM中建立的RPT (Rendezvous Point Tree)，就是一棵以RP为根，以存在组播数据接收者的PIM设备为叶子的共享树。
- **BSR (Bootstrap Router)**：称为自举路由器，负责收集和分发网络内的RP信息。
- **RPT (Rendezvous Point Tree)**：称为共享树。以RP (Rendezvous Point) 为根，组播组成员为叶子的组播分发树称为RPT。
- **SPT (Shortest Path Tree)**：称为最短路径树。以组播源为根，组播组成员为叶子的组播分发树称为SPT。

配置PIM-SM

对PIM-SM的配置包括基本配置以及在不同的接口上配置PIM-SM功能。



注意: PIM-SM功能与静态组播路由功能、IGMP Proxy功能均是互斥的，不能同时配置。

PIM-SM的基本配置

PIM-SM的基本配置包括：

- 开启/关闭组播路由功能（具体请参阅“静态组播路由>开启/关闭组播路由功能”章节）
- 开启/关闭PIM-SM功能
- 配置候选RP
- 配置候选BSR
- 配置静态RP
- 指定关闭RPT向SPT切换

用户可以为不同的VRouter分别配置PIM-SM。对PIM-SM的基本配置需要在PIM-SM模式下进行。进入PIM-SM配置模式，请在全局配置模式下，使用以下命令：

ip vrouter vrouter-name （进入VRouter配置模式）

router pim （进入PIM-SM配置模式）

开启/关闭PIM-SM功能

默认情况下，PIM-SM功能为关闭状态。在PIM-SM配置模式下，使用以下命令开启或关闭PIM-SM功能：

- 开启PIM-SM: **pim-sm enable**
- 关闭PIM-SM: **no pim-sm enable**

配置候选RP

在PIM-SM域内选择几台PIM设备配置候选RP（Rendezvous Point, 汇聚点），从候选RP中选举产生RP。必须同时配置候选BSR，由候选BSR（Bootstrap Router, 自举路由器）选举产生BSR，BSR负责收集并发布网络中的RP信息。

配置候选RP，在PIM-SM配置模式下，使用以下命令：

rp-candidate *interface-name* [**interval** *interval-time*] [**priority** *level*]

- *interface-name* – 指定候选RP所在接口，该接口必须开启PIM-SM功能。
- *interval-time* – 指定发送候选RP消息的时间间隔，单位是秒。范围是1到16383秒。默认值是60秒。
- **priority level** – 指定优先级（数值越小，优先级越高）。在RP选举中，优先级较高的候选RP优先被选举为RP。范围是0到255，默认值为0。

在PIM-SM配置模式下，使用以上命令**no**的形式删除配置的候选RP：

no rp-candidate



注意: 当配置候选RP时，无需指定组播地址，默认组播地址为224.0.0.0/4。

配置候选BSR

在一个PIM-SM域中，需要配置一个或多个候选BSR，候选BSR之间通过自动选举，产生BSR，BSR负责收集并发布RP信息。

配置候选BSR，在PIM-SM配置模式下，使用以下命令：

bsr-candidate *interface-name* [**priority** *level*]

- *interface-name* – 指定候选BSR所在接口，该接口必须开启PIM-SM功能。
- **priority** *level* – 指定优先级（数值越大，优先级越高）。如果在PIM-SM域中，只有一个候选BSR，即被选为BSR；如果存在多个候选BSR，在BSR选举中，优先级较高的候选BSR优先被选举为BSR。范围是0到255，默认值为0。

在PIM-SM配置模式下，使用以上命令**no**的形式删除配置的候选BSR：

no bsr-candidate



注意: 当使用动态RP时，候选RP必须配置，同时，在PIM-SM域中至少配置一个候选BSR。

配置静态RP

当网络内仅有一个RP时，用户可以配置静态RP，这样可以避免候选RP和BSR之间频繁的信息交互占用带宽。PIM-SM域内所有设备都必须配置完全相同的静态RP。

指定静态RP地址，在PIM-SM配置模式下，使用以下命令：

rp-address *A.B.C.D* [*A.B.C.D/M*]

- *A.B.C.D* – 指定静态RP所在接口IP地址。
- *A.B.C.D/M* – 指定组播地址。

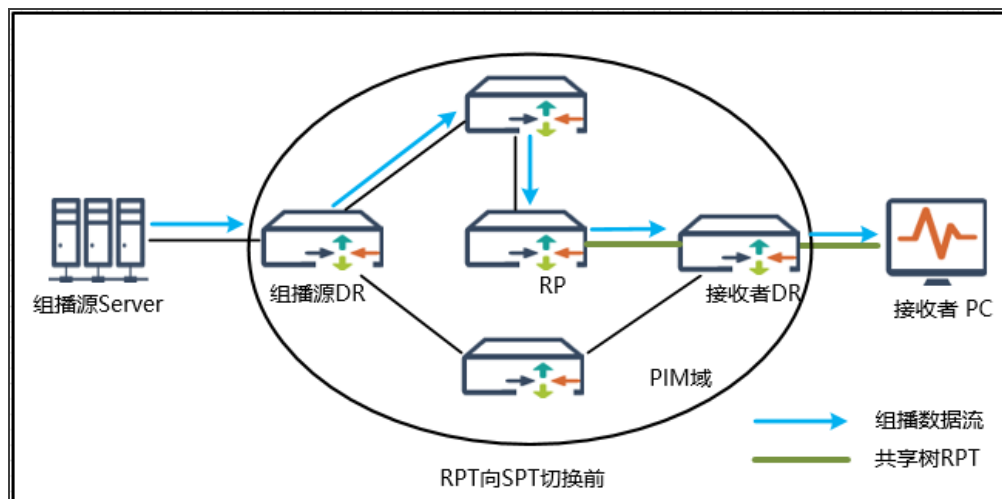
在PIM-SM配置模式下，使用以上命令**no**的形式删除配置的静态RP地址：

no rp-address *A.B.C.D* [*A.B.C.D/M*]

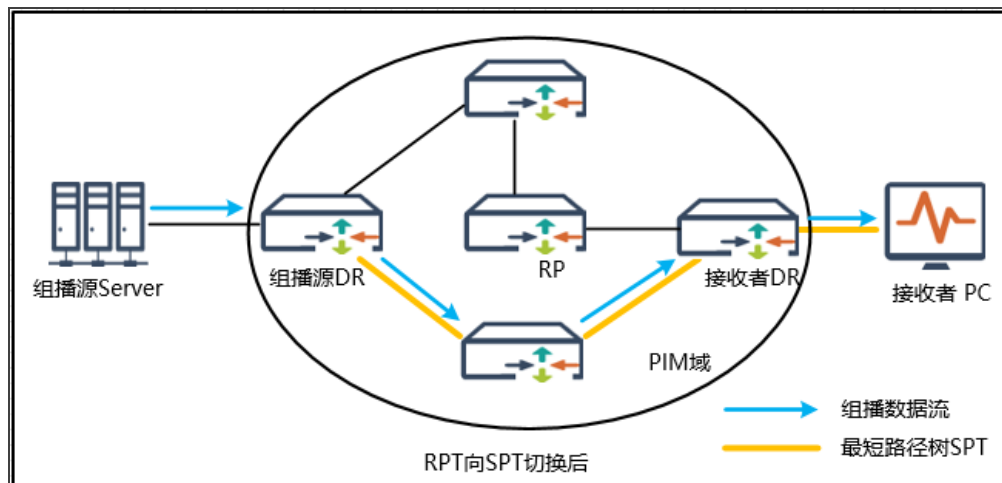
指定关闭RPT向SPT切换

由于PIM-SM域中已构建的RPT（Rendezvous Point Tree, 共享树）不一定是路径最短的树，因此当组播数据流量变大时，RP可能会成为故障点。为了解决这个问题，在默认情况下，RPT可以向SPT（Shortest Path Tree, 最短路径树）切换，切换到SPT后，组播数据将直接从组播源沿着SPT发送到接收者。用户可以根据需要，指定关闭RPT向SPT切换。

RPT向SPT切换前示意图：



RPT向SPT切换后示意图：



指定关闭RPT向SPT切换，在PIM-SM配置模式下，使用以下命令：

spt-threshold {0 | infinity}

- 0 - 指定RPT向SPT切换。该选项为默认选项。
- **infinity** - 关闭RPT向SPT切换。

在PIM-SM配置模式下，使用以上命令no的形式恢复默认向SPT切换：

no spt-threshold

配置接口的PIM-SM功能

配置接口的PIM-SM功能包括：

- 开启/关闭接口的PIM-SM功能
- 配置DR优先级
- 指定接口的Hello报文发送间隔
- 指定发送IGMP通用查询报文间隔
- 指定IGMP通用查询超时时间
- 指定IGMP通用查询最大响应时间

开启/关闭接口的PIM-SM功能

默认情况下，接口的PIM-SM功能为关闭状态。用户可以在接口配置模式下，使用以下命令，开启或关闭指定接口的PIM-SM功能：

- 开启指定接口的PIM-SM功能：**ip pim sparse-mode**
- 关闭指定接口的PIM-SM功能：**no ip pim sparse-mode**



注意：仅支持三层接口上开启PIM-SM功能。

配置DR优先级

DR（Designated Router）的优先级用来决定使用哪个路由器作为指定路由器（DR）。指定DR的优先级，在接口配置模式下，使用以下命令：

ip pim dr-priority *level*

- *level* – 指定DR的优先级（数值越大，优先级越高）。默认值是1。范围是0到4294967294。PIM-SM域中的路由器都可指定作为DR，优先级高的路由器会被选中；如果优先级也相同，IP地址大的会被选中。

使用**no ip pim dr-priority**命令恢复默认优先级。

指定接口的Hello报文发送间隔

接口开启PIM-SM功能后，会定期发送Hello报文。用户可以根据需要，指定接口的Hello报文的发送间隔，在接口配置模式下，使用以下命令：

```
ip pim query-interval interval
```

- *interval* – 指定接口的Hello报文发送间隔。范围是0到65535秒，默认值是30秒。

使用**no ip pim query-interval**命令恢复默认发送间隔值。

指定发送IGMP通用查询报文间隔

接收者主机所在的网络可能同时连接多台组播路由器。这些组播路由器之间通过自动选举，选举出一台路由器作为查询器，负责维护接口上的IGMP组成员关系。对于Hillstone设备，在接口开启PIM-SM功能后，查询器会主动发送的IGMP通用查询报文，来了解组播组成员的加入和离开。

指定发送IGMP通用查询报文间隔，在接口配置模式下，使用以下命令：

```
ip pim igmp-query-interval interval
```

- *interval* – 指定接口发送IGMP通用查询报文间隔时间。范围是1到18000秒，默认值是60秒。

使用**no ip pim igmp-query-interval**命令恢复默认值。

指定IGMP通用查询超时时间

如果网络内的组播路由器在指定超时时间内，未收到IGMP通用查询报文，组播路由器之间将会重新进行查询器的选举。

指定IGMP通用查询超时时间，在接口配置模式下，使用以下命令：

```
ip pim igmp-query-timeout timeout-value
```

- *timeout-value* – 指定IGMP通用查询超时时间。范围是3到300秒，默认值是120秒。

使用**no ip pim igmp-query-timeout**命令恢复超时时间默认值。

指定IGMP通用查询最大响应时间

用户可以指定接收者主机接受到通用查询报文后的最大响应时间。当查询器发送2次IGMP通用查询报文后，如果在指定的最大响应时间内，未收到接收者主机的响应，那么系统将会在组播路由表中删除该接收者。

指定IGMP通用查询最大响应时间，在接口配置模式下，使用以下命令：

```
ip pim igmp-query-max-response-time response-time
```

- *response-time* - 指定IGMP通用查询最大响应时间。范围是1到25秒，默认值是10秒。

使用**no ip pim igmp-query-max-response-time**命令恢复超时时间默认值。

显示PIM-SM信息

显示BSR信息，在任何模式下使用以下命令：

```
show ip pim bsr-route [vrouter vrouter-name]
```

- *vrouter-name* - 显示指定VRouter的BSR信息。

显示配置PIM-SM功能接口信息，在任何模式下使用以下命令：

```
show ip pim interface [interface-name]
```

- *interface-name* - 显示指定接口的PIM信息。

显示PIM邻居信息，在任何模式下使用以下命令：

```
show ip pim neighbor [vrouter vrouter-name]
```

- *vrouter-name* - 显示指定VRouter的PIM邻居信息。

显示RP信息，在任何模式下使用以下命令：

```
show ip pim rp [vrouter vrouter-name | mapping [vrouter vrouter-name]]
```

- *vrouter-name* - 显示指定VRouter的RP信息。
- **mapping** [**vrouter** *vrouter-name*] - 显示指定VRouter的所有RP映射信息。

显示RPF信息，在任何模式下使用以下命令：

show ip pim rpf source-address [**vrouter** *vrouter-name*]

- *source-address* – 显示指定组播源IP地址的RPF信息。
- *vrouter-name* – 显示指定VRouter下的组播源IP的RPF信息。

显示IGMP组播组信息，在任何模式下使用以下命令：

show ip pim igmp groups [*group-address* [**vrouter** *vrouter-name*]]

- *group-address* – 显示指定IP地址的IGMP组播组信息。
- **vrouter** *vrouter-name* – 显示指定VRouter下的IGMP组播组信息。

显示IGMP接口信息，在任何模式下使用以下命令：

show ip pim igmp interfaces [*interface-name*]

- *interface-name* – 显示指定接口（已开启PIM-SM功能）的IGMP信息。

PIM-SSM

使用PIM-SM模式实现组播数据传输需要在网络中维护RP（Rendezvous Point，汇聚点），当网络中的接收者已经知道了组播源的具体位置，希望直接向组播源请求组播数据时，PIM-SSM（Protocol Independent Multicast-Source-Specific Multicast，协议无关组播－指定源组播）可为指定源组播提供解决方案，通过IGMPv3来维护主机与路由器之间的关系，实现组播组成员的快速加入，直接在组播源和组成员之间建立SPT（Shortest Path Tree，最短路径树），无需维护RP，组播数据沿着SPT转发给接收者。

配置PIM-SSM

PIM-SSM的基本配置包括：

- 开启/关闭组播路由功能（具体请参阅“静态组播路由>开启/关闭组播路由功能”章节）
- 配置PIM-SSM组播组地址范围



注意: PIM-SSM是在PIM-SM基础上实现的，在配置PIM-SSM之前，请先配置PIM-SM功能（具体请参阅“协议无关组播（PIM）> [配置PIM-SM](#)”章节）。

配置PIM-SSM组播组地址范围

默认情况下，PIM-SSM组播地址范围是232.0.0.0/8。用户可以根据需要，配置PIM-SSM组播组地址范围，须确保网络内所有PIM设备配置的PIM-SSM组地址范围一致。在配置PIM-SSM组播组地址范围后，PIM-SSM功能将会被同时开启。

配置PIM-SSM组播组地址范围，在PIM-SM配置模式下，使用以下命令：

```
pim-ssm {default | group-prefix/Mask }
```

- **default** - 指定使用默认的PIM-SSM组播组地址范围232.0.0.0/8。
- *group-prefix/Mask* - 指定特定的PIM-SSM组播组地址范围。

在PIM-SM配置模式下，使用以上命令no的形式删除配置的PIM-SSM组播组地址范围：

```
no pim-ssm
```

配置IGMP报文过滤功能

用户可以通过配置该功能，对开启PIM-SM/PIM-SSM功能的接口收到的IGMP报文进行过滤，允许/拒绝接收指定协议版本的IGMP报文中的组播源或组播组。默认情况下，允许接口接收所有IGMP报文。

指定接口允许/拒绝接收IGMPv1/IGMPv2报文中的组播组，在接口配置模式下，使用以下命令：

```
ip pim igmp {permit | deny} group-prefix/Mask
```

- **permit** - 指定该接口允许接收IGMPv1/IGMPv2报文中的组播组。
- **deny** - 指定该接口拒绝接收IGMPv1/IGMPv2报文中的组播组。
- *group-prefix/Mask* - 指定组播组地址范围。

在接口配置模式下，使用以上命令no的形式恢复默认值：

```
no ip pim igmp {permit | deny}
```

指定接口允许/拒绝接收IGMPv3报文中的组播源和组播组，在接口配置模式下，使用以下命令：

```
ip pim igmpv3 {permit | deny} {any | source-prefix/Mask} {any | group-prefix/Mask}
```

- **permit**-指定该接口允许接收IGMPv3报文中的组播源和组播组。
- **deny**-指定该接口拒绝接收IGMPv3报文中的组播源和组播组。
- **any | source-prefix/Mask**-指定组播源地址范围。**any**为任意组播源地址。
- **any | group-prefix/Mask**-指定组播组地址范围。**any**为任意组播组地址。

在接口配置模式下，使用以上命令no的形式恢复默认值：

```
no ip pim igmpv3 {permit | deny}
```

BFD

BFD（Bidirectional Forwarding Detection，双向转发检测）是一套全网统一的检测机制，用于快速检测、监控网络中链路或者IP路由的转发连通状况，为了提升现有网络性能，协议邻居之间必须能快速检测到通信故障，从而更快的建立起备用通道恢复通信。

BFD在两台路由器上建立会话，用来监测两台路由器间的双向转发路径，为上层协议服务，如路由协议。BFD本身并没有发现机制，而是靠被服务的上层协议通知其该与谁建立会话，会话建立后如果在检测时间内没有收到对端的BFD报文则认为发生故障，通知被服务的上层协议，上层协议进行相应的处理。

当前版本的系统支持BFD与静态路由、OSPF、BGP路由协议联动。实现在运行静态路由、OSPF、BGP路由协议的链路上进行转发连通状况检测。

BFD工作模式

BFD会话建立有两种模式：主动模式和被动模式。目前只支持主动模式，不支持被动模式。

- 主动模式：在建立会话前不管是否收到对端发来的BFD控制报文，都会主动发送BFD控制报文。
- 被动模式：在建立会话前不会主动发送BFD控制报文，直到收到对端发送来的控制报文。在会话初始化过程中，通信双方至少要有一个运行在主动模式才能成功建立起会话。

BFD会话建立后有两种检测模式：异步模式和查询模式。通信双方要求运行在相同的模式。

- 异步模式：以异步模式运行的设备周期性地发送BFD控制报文，如果在检测时间内对端没有收到BFD控制报文，则认为会话down。

- 查询模式：假定有一个独立的方法，确认自己和对端系统的连通性。这样，BFD会话建立后，会停止周期发送BFD控制报文，除非需要显式地验证连接性。

BFD Echo功能

BFD Echo功能即BFD回声功能，本端设备周期性地发送BFD Echo报文，远端设备不对报文进行处理，只通过转发通道将报文返回到本端。通过Echo功能，可以更快的检测到故障。

Echo功能可以和两种检测模式配合使用，如果在异步模式下启用Echo功能，可以减少控制报文的发送；如果在查询模式下启用Echo功能，在BFD会话建立后可以取消发送BFD控制报文。



注意: 如果需要使用Echo功能，在本端设备开启Echo功能的基础上，对端设备必须能够对Echo报文进行转发，否则功能不生效。

配置BFD基本功能

BGP基本功能的配置包括以下各项：

- 配置BFD检测模式
- 配置BFD会话参数
- 开启/关闭Echo功能
- 指定接收Echo报文时间间隔
- 配置Echo报文的源IP地址

配置BFD检测模式

BFD会话建立后有两种检测模式：异步模式和查询模式。通信双方要求运行在相同的模式。默认情况下，BFD会话的检测模式为异步模式。用户可以根据需要指定BFD会话检测模式为查询模式，在接口配置模式下，使用以下命令：

bfd demand enable

在接口配置模式下使用该命令no的形式恢复默认为异步模式：

no bfd demand enable

配置BFD会话参数

在BFD会话建立之后，用户可以根据需要修改发送或接收BFD会话报文的最小时间间隔以及检测时间倍数。配置BFD会话检测参数，在接口配置模式下，使用以下命令：

```
bfd min-tx min-tx-value min-rx min-rx-value detect-multiplier value
```

- *min-tx-value* – 指定发送BFD报文的最小时间间隔，单位是毫秒。默认值为100，取值范围为100到1000。
- *min-rx-value* – 指定接收BFD报文的最小时间间隔，单位是毫秒。默认值为100，取值范围为100到1000。
- *value* – 指定检测时间倍数，用来计算检测超时时间。

使用**no bfd min-tx min-rx detect-multiplier**恢复默认BFD会话参数。



注意：检测超时时间计算方法如下：

- 异步模式：超时时间 = $\max(\text{本端配置的 min-tx-value}, \text{对端配置的 min-rx-value}) \times \text{对端检测时间倍数}$ 。
- 查询模式下并开启Echo功能：超时时间 = $\max(\text{本端配置的 min-tx-value}, \text{对端配置的接收Echo报文时间间隔}) \times \text{本端检测时间倍数}$ 。
- 异步模式下并开启echo功能：超时时间 = $\max(\text{本端配置的 min-tx-value}, \text{对端配置的接收Echo报文时间间隔}) \times \text{对端检测时间倍数}$ 。
- 关于如何配置接收Echo报文时间间隔，请参阅 [“指定接收Echo报文时间间隔”](#)

开启/关闭Echo功能

默认情况下，Echo功能是关闭的，启用此功能，在接口配置模式下，使用以下命令：

```
bfd echo enable
```

在接口配置模式下，用该命令no的形式关闭此功能：

```
no bfd echo enable
```

指定接收Echo报文时间间隔

指定接收BFD Echo报文时间间隔，在接口配置模式下，使用以下命令：

```
bfd min-echo-rx value
```

- *value* – 指定接收BFD Echo报文时间间隔，单位为毫秒。取值范围是100到1000毫秒。默认为0，即表示不接收BFD Echo报文。

在接口配置模式下，使用**no bfd min-echo-rx**命令恢复默认值。

配置Echo报文的源IP地址

为了避免对端发送大量的ICMP重定向报文造成网络拥塞，用户需要配置Echo报文的源IP地址，在接口配置模式下，使用以下命令：

```
bfd echo-source-ip echo-src-address
```

- *echo-src-address* – 指定BFD Echo报文的源IP地址。

在接口配置模式下，使用**no bfd echo-source-ip**命令删除Echo报文的源IP地址。



注意：

- Echo报文的源IP地址用户可以任意指定。建议用户配置Echo报文的源IP地址不属于该设备任何一个接口所在网段。
- 本端发送Echo报文的目的地址使用本端接口地址。

配置BFD多跳检测

BFD会话分为单跳检测和多跳检测，用户可以根据会话的组网环境选择不同的检测方式：

- 单跳检测：指对两个直连设备进行IP连通性检测。
- 多跳检测：指BFD可以检测两个设备间任意路径的链路连通性情况。



注意:

- 目前系统仅支持BFD多跳会话检测与BGP进行联动。
- BFD多跳会话检测仅支持异步模式，不支持查询模式和Echo功能。

创建BFD多跳检测模板

BFD多跳检测模板用于指定BFD控制报文的加密认证方式、发送或接收BFD多跳会话报文的最小时间间隔以及检测时间倍数。创建BFD多跳检测模板，在全局配置模式下使用以下命令：

bfd template *template-name* **multi-hop**

- *template-name* - 指定所创建的BFD多跳检测模板的名称，并且进入该BFD多跳检测模板配置模式。如果指定名称已存在，则直接进入BFD多跳检测模板配置模式。

使用**no bfd template** *template-name*删除指定的BFD多跳检测模板。

指定BFD控制报文的加密认证方式

随着网络跳数的增多，BFD控制报文可能更加容易被篡改，在BFD多会话中，支持对BFD控制报文进行加密认证。指定BFD控制报文的加密认证方式，在BFD多跳检测模板配置模式下，使用以下命令：

authentication-type {**m-md5** | **m-sha1** | **md5** | **sha1** | **simple**} *key-id* {**plain** *plain-string*}

- **m-md5** | **m-sha1** | **md5** | **sha1** | **simple** - 指定所采用的认证算法：Meticulous MD5算法（**m-md5**）、Meticulous SHA1算法（**m-sha1**）、MD5算法（**md5**）、SHA1算法（**sha1**）以及简单认证（**simple**）。
- *key-id* - 指定认证ID。
- **plain** *plain-string* - 以明文的方式指定密钥。

在BFD多跳检测模板配置模式下，使用**no authentication-type**删除配置的BFD控制报文加密方式。

配置BFD多跳会话参数

在BFD多跳会话建立之后，用户可以根据需要修改发送或接收BFD多跳会话报文的最小时间间隔以及检测时间倍数。配置BFD会话检测参数，在BFD多跳检测模板配置模式下，使用以下命令：

interval min-tx min-tx-value min-rx min-rx-value detect-multiplier value

- *min-tx-value* – 指定发送BFD多跳会话报文的最小时间间隔，单位是毫秒。默认值为100，取值范围为100到1000。
- *min-rx-value* – 指定接收BFD多跳会话报文的最小时间间隔，单位是毫秒。默认值为100，取值范围为100到1000。
- **detect-multiplier value** – 指定检测时间倍数，用来计算检测超时时间。默认值为3，取值范围是3到50。
- 在BFD多跳检测模板配置模式下，使用**no interval min-tx min-rx detect-multiplier**恢复默认BFD多跳会话参数。



注意：BFD多跳检测超时时间计算方法如下：

- 异步模式：超时时间 = $\max(\text{本端配置的min-tx-value}, \text{对端配置的min-rx-value}) \times \text{对端检测时间倍数}$ 。

配置BFD与路由协议联动

BFD与路由协议联动的配置包括以下各项：

- 配置BFD与静态路由联动
- 配置BFD与OSPF联动
- 配置BFD与BGP联动

配置BFD与静态路由联动

由于静态路由没有发现邻居机制，BFD与静态路由联动，如果BFD会话检测到故障，则表明该静态路由下一跳不可达，即不会添加此路由到路由表中，从而实现快速路由选路。

配置BFD与静态路由联动，对指定的静态路由下一跳开启BFD检测功能，在VRouter配置模式下，使用以下命令：

```
ip route {A.B.C.D/M | A.B.C.D A.B.C.D} interface-name A.B.C.D bfd
```

- *A.B.C.D/M | A.B.C.D A.B.C.D* – 指定静态路由条目的网络地址。安全网关支持两种方式，*A.B.C.D/M*或者 *A.B.C.D A.B.C.D*，例如1.1.1.0/24或者1.1.1.0 255.255.255.0。
- *interface-name A.B.C.D* – 指定下一跳接口地址。
- **bfd** – 对指定下一跳开启BFD检测功能。

在VRouter配置模式下，使用以上命令no的形式取消BFD与指定静态路由联动：

```
no ip route {A.B.C.D/M | A.B.C.D A.B.C.D} interface-name A.B.C.D bfd
```

配置BFD与 OSPF联动

通过BFD与OSPF联动，实现优于OSPF协议Hello检测机制的快速链路检测，从而提高OSPF协议的收敛性能。

配置BFD与OSPF联动，对指定的OSPF相关接口上开启BFD检测功能，在接口配置模式下，使用以下命令：

```
ip ospf bfd
```

在接口配置模式下，使用以上命令no的形式取消BFD与OSPF联动：

```
no ip ospf bfd
```

配置BFD与 BGP联动

配置BFD与BGP联动，对指定的BGP邻居开启BFD检测功能，在BGP实例配置模式下，使用以下命令：

```
neighbor A.B.C.D fall-over bfd
```

- *A.B.C.D* – 指定BGP对等体的IP地址。

在BGP实例配置模式下，使用以上命令no的形式取消BFD与指定BGP邻居联动：

```
no neighbor A.B.C.D fall-over bfd
```

显示BFD会话信息

显示BFD会话信息，在任何模式下使用以下命令：

```
show bfd session [neighbor A.B.C.D | detail]
```

- *A.B.C.D* – 指定相邻路由器的ID。
- **detail** – 显示所有路由器的BFD会话详细信息。

第7章 用户认证

对用户和主机进行识别，即为“认证”，认证是产品的一个重要功能。开启了认证功能的网络能够允许或拒绝用户和主机对网络进行访问。从用户的角度出发，认证可以分为：

- 位于企业内网的用户通过认证访问互联网（通常使用AAA服务器进行认证）。
- 位于互联网的用户访问内网的资源（通常使用VPN）。

AAA简介

AAA是Authentication（认证）、Authorization（授权）和Accounting（计费）的简称。具体内容如下：

- 认证：验证用户身份。
- 授权：根据配置对用户授予一定权限。
- 计费：记录用户使用网络资源应付的费用。

设备支持以下认证方式：

- 本地认证：将用户信息（包括用户名称、密码和各种属性）配置在设备上。本地认证速度快，可以降低运营成本，但是存储信息量受设备硬件条件的限制。默认情况下，设备使用本地认证的方式对用户进行认证。
- 外部认证：支持通过RADIUS、LDAP、AD、TACACS+协议和微信公众平台进行外部认证。将用户信息储存在外部RADIUS、LDAP、AD、TACACS+服务器和微信公众平台上，通过外部服务器对设备的用户进行认证。

系统支持以下授权方式：

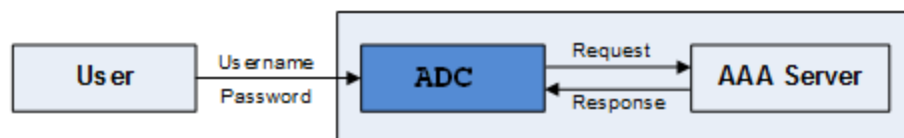
- 本地授权：根据设备上为本地用户帐号配置的相关属性进行授权。
- 外部服务器认证成功后授权：RADIUS/LDAP/AD/TACACS+协议的认证和授权绑定在一起。

系统支持以下计费方式：

- 不计费：不记录用户使用网络资源的费用。
- 外部服务器计费：使用RADIUS服务器对通过认证的用户进行计费。

设备外部认证流程

当用户通过终端与设备建立连接从而获得访问或管理设备的权利时，设备可以基于配置的RADIUS/LDAP/AD/TACACS+服务器来认证用户。下图为设备外部认证流程图：



如图所示，设备的外部认证流程为：

1. 用户将名称和密码发给设备。
2. 设备接收用户名称和口令，并向RADIUS/LDAP/AD/TACACS+服务器发送认证请求。
3. RADIUS/LDAP/AD/TACACS+服务器收到合法请求后，进行验证。如果认证通过，RADIUS/LDAP/AD/TACACS+服务器会把用户的配置信息返回给设备，否则，返回拒绝信息。设备和RADIUS/TACACS+服务器之间的安全由共享的密钥（密钥或者密文）来保证。

配置AAA服务器

AAA服务器是认证服务器，存储用户信息（包括用户名称、密码和各种属性），在用户请求访问网络时，提供认证功能。

- [创建AAA服务器](#)
- [配置本地服务器认证参数](#)
- [配置RADIUS服务器认证参数](#)
- [配置RADIUS服务器的计费功能](#)
- [配置LDAP服务器认证参数](#)
- [配置Active-Directory服务器认证参数](#)
- [配置TACACS+服务器认证参数](#)

创建AAA服务器

对AAA的各项配置需要在AAA服务配置模式下进行。在全局配置模式下使用以下命令创建AAA服务器：

aaa-server *aaa-server-name* [**type** {**local** | **radius** | **ldap** | **tacacs+**}]

- *aaa-server-name* - 指定AAA服务实例的名称，为1到31个字符的字符串，区分大小写。
- **type** {**local** | **radius** | **ldap** | **tacacs+**} - 指定所创建AAA服务器的类型，可以是本地（local）、RADIUS、LDAP或者TACACS+类型的服务器。若不指定，默认创建RADIUS类型的AAA服务器。

执行该命令后，系统创建指定名称的AAA服务实例，并且进入AAA服务配置模式；如果指定的名称已存在，则直接进入AAA服务配置模式。在全局配置模式下使用该命令**no**的形式删除指定的AAA服务器：

no aaa-server *aaa-server-name*

配置本地服务器认证参数

在全局配置模式下执行**aaa-server** *aaa-server-name* **type local**命令可以进入指定名称的本地服务器配置模式。用户可配置的本地服务器认证参数包括：

- 配置密码控制
- 配置角色映射规则
- 配置用户黑名单
- 配置备份认证服务器

配置密码控制

为了提高用户密码的安全性以防止出现安全问题，系统提供密码控制功能。对于密码控制功能的配置，必须在密码控制配置模式下进行。进入密码控制配置模式，在本地服务器配置模式下，使用以下命令：

password-control

系统支持的密码控制功能包括：

- 允许本地用户修改密码
- 配置密码过期时间及密码到期提醒功能
- 配置历史密码检查功能
- 配置密码复杂度
- 开启/关闭首次登录强制修改密码功能

允许本地用户修改密码

系统支持本地用户通过认证后，在认证登录成功页面修改自己的用户密码。默认情况下，该功能为关闭状态。在密码控制配置模式下，使用以下命令开启或关闭允许本地用户修改登录密码功能：

- 开启：**allow-pwd-change**
- 关闭：**no allow-pwd-change**

配置密码过期时间及密码到期提醒功能

配置密码的过期时间并配置密码到期提醒功能，即在过期前n天提醒用户修改密码。还可以配置历史密码检查功能，新密码不能与前n次历史密码重复。

配置密码的过期时间及密码到期提醒，在密码控制配置模式下，使用以下命令：

aging aging-day [alert-before-expire alert-day]

- *aging-day* – 指定密码的过期时间。取值范围是1-365天，默认值是90。
- *alert-day* – 指定在密码过期前提醒用户修改密码的天数。取值范围是1-30天，例如在密码前15天提醒用户修改密码，默认值是7。

使用**no aging**取消密码过期时间及密码到期提醒的配置。

配置历史密码检查功能

配置历史密码检查功能，在修改密码时，进行历史密码的校验，新密码不能与前n次历史密码重复，在密码控制配置模式下，使用以下命令：

history-check count

- *count* – 指定新密码不能与前n次历史密码重复。取值范围是1-5，默认值是3。

使用**no history-check**取消历史密码检查的配置。

配置密码复杂度

密码的复杂度越低，其被破解的可能性就越大，比如包含用户名、密码长度短等。出于安全性的考虑，用户可以开启密码复杂度的配置功能并配置密码复杂度的要求，以确保用户的密码具有较高的复杂度。

开启密码复杂度配置功能，在密码控制配置模式下，使用以下命令：

complexity enable

使用`no complexity enable`命令关闭密码复杂度配置功能。

配置密码复杂度，在密码控制配置模式下，使用以下命令：

```
complexity {capital - letters letters | small-letters length | min - length length | no-include -username | non-alpha-numeric-letters length | numeric-characters length}
```

- `capital - letters letters` - 指定密码包含的大写字母的最小长度，范围是0-16，默认值是0。
- `small-letters length` - 指定密码包含的小写字母的最小长度，范围是0-16，默认值是0。
- `min - length length` - 指定密码最小长度，范围是1-16，默认值是1。
- `no-include -username` - 指定密码不能包含用户名。
- `non-alphanumeric-letters length` - 指定密码包含特殊字符（即非数字的字符）的最小长度，范围是0-16，默认值是0。
- `numeric-characters length` - 指定密码包含的数字的最小长度，范围是0-16，默认值是0。

使用`no complexity {capital - letters | small-letters | min - length | no-include -username | non-alphanumeric-letters | numeric-characters }`命令恢复密码复杂度的默认值。

开启/关闭首次登录修改密码功能

默认情况下，首次登录修改密码功能是关闭状态。在开启首次登录修改密码功能后，当用户首次登录进行Web认证或SSL VPN时，系统将会提示用户“首次登录，请修改密码”强制用户按照已配置的密码复杂度进行修改密码。

开启/关闭首次登录修改密码功能，在密码控制配置模式下，使用以下命令：

- 开启：`first-login-check`
- 关闭：`no first-login-check`



注意：只有在开启允许本地用户修改登录密码功能后，才可以开启首次登录修改密码功能。

配置角色映射规则

为本地服务器指定角色映射规则后，系统将会为通过该服务器认证的用户按照指定角色映射规则分配角色。

为本地服务器指定角色映射规则，在本地服务器配置模式下，使用以下命令：

```
role-mapping-rule rule-name
```

- *rule-name* – 指定系统中已经配置的角色映射规则的名称。

在本地服务器配置模式下，使用该命令no的形式取消角色映射规则的指定：

```
no role-mapping-rule
```

配置用户黑名单

为本地服务器配置用户黑名单后，系统将会禁止通过该服务器认证的黑名单用户访问任何网络资源。配置用户黑名单，在本地服务器配置模式下，使用以下命令：

```
user-black-list username user-name
```

- *user-name* – 指定黑名单中的用户名。取值范围是1到63个字符。

在本地服务器配置模式下，使用该命令no的形式删除黑名单用户：

```
no user-black-list username user-name
```

配置备份认证服务器

为本地服务器配置备份认证服务器后，当主服务器出现问题或者用户在主服务器认证失败时，备份认证服务器发挥身份认证的作用。备份认证服务器可以与主服务器为不同类型。系统中已配置的本地、Active-Directory、RADIUS或者LDAP服务器均可作为备份认证服务器。为本地服务器配置备份认证服务器，在本地服务器配置模式下，使用以下命令：

```
backup-aaa-server aaa-server-name
```

- *aaa-server-name* – 指定系统中已经配置的AAA服务器的名称。

在本地服务器配置模式下，使用该命令no的形式取消备份认证服务器的配置：

```
no backup-aaa-server
```



注意:

- 备份认证服务器和主认证服务器必须处于相同VSYs。关于VSYs的详细信息，请参阅[虚拟系统](#)。
- 备份认证服务器不能嵌套备份认证服务器。
- 删除AAA服务器之前，请确保该服务器未被指定为备份认证服务器。

配置防暴力破解功能

为了防止非法用户通过暴力方法获取用户名和密码，可以通过配置基于用户名或基于IP地址的防暴力破解功能，即在指定时间内，若用户连续输错指定次数的用户名和密码，系统将会按照指定的锁定时间锁定该用户或IP地址。防暴力破解功能的配置包括：

- 开启或关闭防暴力破解功能
- 配置尝试次数
- 配置锁定时间
- 查看锁定列表信息
- 解除用户/IP地址的锁定

开启或关闭防暴力破解功能

防暴力破解功能默认情况下是关闭的。开启防暴力破解功能，在本地服务器配置模式下使用以下命令：

- 启用：`lockout {ip | user} enable`
- 关闭：`lockout {ip | user} disable`

配置尝试次数

配置尝试次数，即在指定时间内，允许用户连续输错用户名和密码的次数，在本地服务器配置模式下使用以下命令：

```
lockout {ip | user} failed-attempts number interval interval
```

- **failed-attempts** *number* – 指定时间内允许输错用户名和密码的次数，基于用户名配置时，取值范围是1-32，默认值是5次；基于IP地址配置时，取值范围是1-2048，默认值是64次。
- **interval** *interval* – 指定连续输错用户名和密码的时间范围，单位是秒，取值范围是1-180秒，默认值是60秒。

在本地服务器配置模式下，使用**no logout {ip | user} failed-attempts**命令恢复默认值。

配置锁定时间

在指定时间内，若用户连续输错指定次数的用户名和密码，系统将会按照指定的锁定时间锁定该用户或IP地址。配置锁定时间，在本地服务器配置模式下使用以下命令：

logout {ip | user} logout-time time

- **logout-time** *time* – 指定锁定时间，单位是秒，取值范围是30-1800秒，基于用户名配置时，默认值是600秒；基于IP地址配置时，默认值是60秒。

在本地服务器配置模式下，使用**no logout {ip | user} logout-time**命令恢复默认值。

查看锁定列表信息

查看被锁定的用户信息、被锁定的IP地址信息，在任何模式下，使用以下命令：

show aaa-server aaa-server-name logout {user [username] | ip [ip-address vr_id number]}

- *aaa-server-name* - 指定AAA服务器名称。
- **user** [username] - 查看指定名称的锁定用户信息。
- **ip** [ip-address vr_id number] - 查看指定IP地址和VRouter ID的锁定IP信息。

解除用户/IP地址的锁定

解除对指定用户/IP地址的锁定并且从锁定列表中删除，在任何模式下，使用以下命令：

exec aaa aaa-server-name logout delete {user [username] | ip [ip-address vr_id number]}

- *aaa-server-name* - 指定AAA服务器名称。
- **user** [username] - 解除对指定名称的用户的锁定。
- **ip** [ip-address vr_id number] - 解除对指定IP地址和VRouter ID的锁定。

配置RADIUS服务器认证参数

在全局配置模式下执行`aaa-server aaa-server-name type radius`命令可以进入指定名称的RADIUS服务器配置模式。用户可配置的RADIUS服务器认证参数包括：

- 配置认证主服务器的IP地址或域名
- 配置备份服务器1的IP地址或域名
- 配置备份服务器2的IP地址或域名
- 配置RADIUS服务器端口号
- 配置RADIUS服务器的共享密钥秘密
- 配置重试次数
- 配置超时时间
- 配置角色映射规则
- 配置用户黑名单
- 配置备份认证服务器
- 添加字典文件
- 配置防暴力破解功能
- 启用/禁用授权策略
- 添加授权策略到聚合策略
- 配置SM4国密加密算法

配置认证主服务器的IP地址或域名

配置认证主服务器的IP地址或域名以及所属的VRouter，在RADIUS服务器配置模式下，使用以下命令：

```
host { ip-address | host-name } [vrouter vrouter-name]
```

- *ip-address* | *host-name* – 指定认证主服务器的IP地址（可以为IPv4或IPv6 地址）或者域名。
- **vrouter** *vrouter-name* – 指定认证主服务器所属的VRouter。默认为系统缺省VR即trust-vr。

在RADIUS服务器配置模式下，使用该命令no的形式取消认证主服务器的IP地址或者域名配置：

```
no host
```

配置备份服务器1的IP地址或域名

该参数为可选配置。备份服务器是与主服务器相同类型服务器。在当通过主服务器进行认证失败时，依次启用备份服务器1和2进行认证。配置备份服务器1的IP地址或域名以及所属的VRouter，在RADIUS服务器配置模式下，使用以下命令：

```
backup1 {ip-address | host-name} [vrouter vrouter-name]
```

- *ip-address | host-name* – 指定备份服务器1的IP地址（可以为IPv4或IPv6 地址）或者域名。
- **vrouter** *vrouter-name* – 指定认证主服务器所属的VRouter。默认为系统缺省VR即trust-vr。

在RADIUS服务器配置模式下，使用该命令no的形式取消备份服务器1的IP地址或者域名配置：

```
no backup1
```

配置备份服务器2的IP地址或域名

该参数为可选配置。备份服务器是与主服务器相同类型服务器。在当通过主服务器进行认证失败时，依次启用备份服务器1和2进行认证。配置备份服务器2的IP地址或域名以及所属的VRouter，在RADIUS服务器配置模式下，使用以下命令：

```
backup2 {ip-address | host-name} [vrouter vrouter-name]
```

- *ip-address | host-name* – 指定备份服务器2的IP地址（可以为IPv4或IPv6 地址）或者域名。
- **vrouter** *vrouter-name* – 指定备份服务器所属的VRouter。默认为系统缺省VR即trust-vr。

在RADIUS服务器配置模式下，使用该命令no的形式取消备份服务器2的IP地址或者域名配置：

```
no backup2
```

配置RADIUS服务器端口号

配置RADIUS服务器端口号，在RADIUS服务器配置模式下，使用以下命令：

```
port port-number
```

- *port-number* – 指定RADIUS服务器的端口号。默认值是1812。取值范围是1024到65535。

在RADIUS服务器配置模式下，使用该命令no的形式恢复端口号的默认值：

no port

配置RADIUS服务器的共享密钥秘密

配置RADIUS服务器的共享密钥秘密，在RADIUS服务器配置下，使用以下命令：

secret secret

- *secret* – 指定RADIUS服务器的共享密钥秘密字符串。字符串范围为1到31个字符。

在RADIUS服务器配置模式下，使用该命令no的形式取消对RADIUS服务器共享密钥秘密的配置：

no secret

配置重试次数

重试次数指设备向AAA服务器在没有收到服务器回应时重新发送认证报文的次数。配置重试次数，在RADIUS服务器配置模式下，使用以下命令：

retries times

- *times* – 指定重传次数。取值范围是1到10次。默认为3次。

在RADIUS服务器配置模式下使用该命令no的形式恢复重传次数的默认值：

no retries

配置超时时间

超时时间指AAA服务器的应答超时时间。如果在超时时间结束时设备仍未收到服务器的应答，则会重新发送认证报文。重新发送报文的次数由**retries times**命令配置。配置超时时间，在RADIUS服务器配置模式下，使用以下命令：

timeout time-value

- *time-value* – 指定超时时间，单位为秒。取值范围是1到30秒。默认为3秒。

在RADIUS服务器配置模式下使用该命令no的形式恢复超时时间的默认值：

no timeout

指定角色映射规则

为RADIUS服务器指定角色映射规则后，系统将会为通过该服务器认证的用户按照指定角色映射规则分配角色。为RADIUS服务器指定角色映射规则，在RADIUS服务器配置模式下，使用以下命令：

role-mapping-rule *rule-name*

- *rule-name* – 指定系统中已配置的映射规则的名称。

在RADIUS服务器配置模式下，使用该命令**no**的形式取消角色映射规则的指定：

no role-mapping-rule

配置用户黑名单

为RADIUS服务器配置用户黑名单后，系统将会禁止通过该服务器认证的黑名单用户访问任何网络资源。配置用户黑名单，在RADIUS服务器配置模式下，使用以下命令：

user-black-list username *user-name*

- *user-name* – 指定黑名单中的用户名。取值范围是1到63个字符。

在RADIUS服务器配置模式下，使用该命令**no**的形式删除黑名单用户：

no user-black-list username *user-name*

配置备份认证服务器

为RADIUS服务器配置备份认证服务器后，当主服务器出现问题或者用户在主服务器认证失败时，备份认证服务器发挥身份认证的作用。备份认证服务器可以与主服务器为不同类型。系统中已配置的本地、RADIUS均可作为备份认证服务器。为RADIUS服务器配置备份认证服务器，在RADIUS服务器配置模式下，使用以下命令：

backup-aaa-server *aaa-server-name*

- *aaa-server-name* – 指定系统中已经配置的AAA服务器的名称。

在RADIUS服务器配置模式下，使用该命令**no**的形式取消备份认证服务器的配置：

no backup-aaa-server



注意:

- 备份认证服务器不能嵌套备份认证服务器。
- 删除AAA服务器之前，请确保该服务器未被指定为备份认证服务器。
- 如果为同一RADIUS服务器配置了备份服务器1（**backup1**）、备份服务器2（**backup2**）和备份认证服务器（**backup-aaa-server**），当用户在主服务器认证无响应时，系统会按照这样的顺序对该用户再次进行认证：备份服务器1→备份服务器2→备份认证服务器；当用户在主服务器认证失败时，系统会先通过备份服务器1和2进行认证，如果备份服务器1和2认证失败，再通过备份认证服务器对该用户再次进行认证。

添加字典文件

对于RADIUS服务器来说，厂商的属性以字典文件的方式来定义。山石的字典文件名为dictionary.hillstone。RADIUS服务器管理员通过修改服务器的主字典文件的方式，将dictionary.hillstone文件引用进来。

dictionary.hillstone字典文件定义了以下属性：

属性	说明
Hillstone-user-type	用户类型。 admin type=16 PnPVPN=4 all=31 其他类型用户不检查此值。
Hillstone-user-vsys-id	VSYS ID值。 管理员必须配置此参数。目前仅支持ID等于0。
Hillstone-user-admin-privilege	读写权限。 读写=4294967295 只读=0
Hillstone-user-login-type	管理员登录类型。 telnet=2 SSH=4

属性	说明
	CONSOLE=1 HTTP=8 HTTPS=16 all=31 任意组合等于数值相加的值（如telnet+SSH=6）。

配置防暴力破解功能

为了防止非法用户通过暴力方法获取用户名和密码，可以通过配置基于用户名或基于IP地址的防暴力破解功能，即在指定时间内，若用户连续输错指定次数的用户名和密码，系统将会按照指定的锁定时间锁定该用户或IP地址。防暴力破解功能的配置包括：

- 开启或关闭防暴力破解功能
- 配置尝试次数
- 配置锁定时间

开启或关闭防暴力破解功能

防暴力破解功能默认情况下是关闭的。开启防暴力破解功能，请在RADIUS服务器配置模式下使用以下命令：

- 启用：**lockout {ip | user} enable**
- 关闭：**lockout {ip | user} disable**

配置尝试次数

配置尝试次数，即在指定时间内，允许用户连续输错用户名和密码的次数，请在RADIUS服务器配置模式下使用以下命令：

lockout {ip | user} failed-attempts *number* interval *interval*

- **failed-attempts *number*** – 指定时间内允许输错用户名和密码的次数，基于用户名配置时，取值范围是1-32，默认值是5次；基于IP地址配置时，取值范围是1-2048，默认值是64次。

- **interval** *interval* – 指定连续输错用户名和密码的时间范围，单位是秒，取值范围是1-180秒，默认值是60秒。

在RADIUS服务器配置模式下，使用**no logout {ip | user} failed-attempts**命令恢复默认值。

配置锁定时间

在指定时间内，若用户连续输错指定次数的用户名和密码，系统将会按照指定的锁定时间锁定该用户或IP地址。配置锁定时间，请在RADIUS服务器配置模式下使用以下命令：

logout {ip | user} logout-time *time*

- **logout-time** *time* – 指定锁定时间，单位是秒，取值范围是30-1800秒，基于用户名配置时，默认值是600秒；基于IP地址配置时，默认值是60秒。

在Radius服务器配置模式下，使用**no logout {ip | user} logout-time**命令恢复默认值。

查看锁定列表信息

查看被锁定的用户信息、被锁定的IP地址信息，在任何模式下，使用以下命令：

show aaa-server *aaa-server-name* **logout** {**user** [*username*] | **ip** [*ip-address* **vr_id** *number*]}

- *aaa-server-name* - 指定AAA服务器名称。
- **user** [*username*] - 查看指定名称的锁定用户信息。
- **ip** [*ip-address* **vr_id** *number*] - 查看指定IP地址和VRouter ID的锁定IP信息。

解除用户/IP地址的锁定

解除对指定用户/IP地址的锁定并且从锁定列表中删除，在任何模式下，使用以下命令：

exec aaa *aaa-server-name* **logout delete** {**user** [*username*] | **ip** [*ip-address* **vr_id** *number*]}

- *aaa-server-name* - 指定AAA服务器名称。
- **user** [*username*] - 解除对指定名称的用户的锁定。
- **ip** [*ip-address* **vr_id** *number*] - 解除对指定IP地址和VRouter ID的锁定。

启用/禁用授权策略

用户通过RADIUS服务器认证时，当用户认证成功后，RADIUS服务器会为认证用户创建一条包含目的网段、目的端口、协议以及行为的安全策略，该策略被称为授权策略。系统支持“认证时授权策略”和“动态授权策略”两种授权策略，用户可以启用授权策略功能，使系统能够从RADIUS服务器获取该授权策略，并加入到系统的策略列表中，使其生效。当认证用户断开连接后，授权策略将会被自动删除。

默认情况下，授权策略为禁用状态。启用或禁用授权策略，在RADIUS服务器配置模式下，使用以下命令：

- 启用：**authorization-policy enable**
- 禁用：**authorization-policy disable**



注意：如果需要获取通过RADIUS CoA报文动态修改后的动态授权策略，请先配置RADIUS动态授权功能。关于RADIUS动态授权功能的配置方法，请参阅“[RADIUS动态授权](#)”。

添加授权策略到聚合策略

启用RADIUS服务器的授权策略后，用户可以指定将获取到的授权策略添加到系统已创建的聚合策略中，作为聚合策略成员排列在聚合策略的末尾，更便于用户统一管理授权策略。如果未添加到聚合策略，授权策略将会默认加入到系统策略列表的末尾。

添加授权策略到聚合策略，在RADIUS服务器配置模式下，使用以下命令：

authorization-policy associated-aggregate-rule *rule-name*

- *rule-name* - 指定需要添加到的聚合策略名称。

在RADIUS服务器配置模式下，使用该命令no的形式取消添加：

no authorization-policy associated-aggregate-rule

配置SM4国密加密算法

RADIUS服务器支持使用SM4国密加密算法对密码进行加密存储以及加密传输。为RADIUS服务器配置SM4国密加密算法，需要在扩展配置模式下使用相关命令进行配置。

进入扩展配置模式，在RADIUS服务器配置模式下，使用以下命令：

extend-option

为RADIUS服务器配置SM4国密加密算法，在扩展配置模式下，使用以下命令：

encryption-algorithm SM4

- **SM4** 指定SM4国密加密算法。SM4不区分大小写。

在扩展配置模式下，使用**no encryption-algorithm**命令删除国密加密算法的配置。

配置RADIUS服务器的计费功能

系统支持对使用RADIUS服务器认证的用户进行计费。在全局配置模式下执行**aaa-server aaa-server-name type radius**命令可以进入指定名称的RADIUS服务器配置模式。用户可配置的RADIUS服务器计费功能的参数包括：

- 开启或关闭计费功能
- 配置计费主/备份服务器的IP地址或域名
- 配置计费服务器的端口号
- 配置计费服务器的共享密钥

开启或关闭计费功能

在RADIUS服务器配置模式下，输入以下命令开启或关闭该RADIUS服务器的计费功能：

- 开启：**accounting enable**
- 关闭：**no accounting enable**

当计费功能开启后，用户可以继续对计费功能的其他参数进行配置。

配置计费主/备份服务器的IP地址或域名

配置计费主/备份服务器的IP地址或域名，在RADIUS服务器配置模式下，使用以下命令：

```
accounting {host {ip-address | host-name} | backup1 {ip-address | host-name} | backup2 {ip-address | host-name}}  
[vrouter vrouter]
```


- **host** {*ip-address* | *host-name*} - 指定主服务器的IP地址或者域名。
- **backup1** {*ip-address* | *host-name*} - 指定备份服务器1的IP地址或者域名。
- **backup2** {*ip-address* | *host-name*} - 指定备份服务器2的IP地址或者域名。
- **vrouter** *vrouter* - 指定计费主/备服务器所属的VRouter。默认为系统缺省VR即trust-vr。

在RADIUS服务器配置模式下，使用该命令no的形式取消计费主/备份服务器的IP地址或者域名配置：

```
no accounting {host | backup1 | backup2}
```

配置计费服务器端口号

配置计费服务器端口号，在RADIUS服务器配置模式下，使用以下命令：

```
accounting port port-number
```

- *port-number* - 指定计费服务器的端口号。默认值是1813。取值范围是1024到65535。

在RADIUS服务器配置模式下，使用该命令no的形式恢复端口号的默认值：

```
no accounting port
```

配置计费服务器的共享密钥

配置计费服务器的共享密钥，在RADIUS服务器配置下，使用以下命令：

```
accounting secret secret
```

- *secret* - 指定计费服务器的共享密钥字符串。字符串范围为1到31个字符。

在RADIUS服务器配置模式下，使用该命令no的形式取消对计费服务器共享密钥的配置：

```
no accounting secret
```

配置LDAP服务器认证参数

在全局配置模式下执行**aaa-server** *aaa-server-name* **type ldap**命令可以进入指定名称的LDAP服务器配置模式。用户可配置的LDAP服务器认证参数包括：

- 配置认证主服务器的IP地址或域名
- 配置备份服务器1的IP地址或域名
- 配置备份服务器2的IP地址或域名
- 配置服务器端口号
- 配置服务器认证或同步方法
- 指定更新服务器连接
- 指定Base-DN
- 指定登录DN
- 指定Authid属性值
- 指定登录密码
- 指定名称属性
- 指定Group-class
- 指定成员属性名
- 配置角色映射规则
- 配置用户黑名单
- 配置用户自动同步
- 配置用户过滤功能
- 配置同步的工作模式
- 配置备份认证服务器
- 配置防暴力破解功能

配置认证主服务器的IP地址或域名

配置认证主服务器的IP地址或域名以及所属的VRouter，在LDAP服务器配置模式下，使用以下命令：

```
host {ip-address | host-name} [vrouter vrouter-name]
```

- *ip-address* | *host-name* – 指定认证主服务器的IP地址（IPv4地址或IPv6地址）或者域名。
- **vrouter** *vrouter-name* – 指定认证主服务器所属的VRouter。默认为系统缺省VR即trust-vr。

在LDAP服务器配置模式下，使用该命令no的形式取消认证主服务器的IP地址或者域名配置：

```
no host
```

配置备份服务器1的IP地址或域名

该参数为可选配置。备份服务器是与主服务器相同类型服务器。在当通过主服务器进行认证失败时，依次启用备份服务器1和2进行认证。配置备份服务器1的IP地址或域名以及所属的VRouter，在LDAP服务器配置模式下，使用以下命令：

```
backup1 {ip-address | host-name} [vrouter vrouter-name]
```

- *ip-address* | *host-name* – 指定备份服务器1的IP地址（IPv4地址或IPv6地址）或者域名。
- **vrouter** *vrouter-name* – 指定认证主服务器所属的VRouter。默认为系统缺省VR即trust-vr。

在LDAP服务器配置模式下，使用该命令no的形式取消备份服务器1的IP地址或者域名配置：

```
no backup1
```

配置备份服务器2的IP地址或域名

该参数为可选配置。备份服务器是与主服务器相同类型服务器。在当通过主服务器进行认证失败时，依次启用备份服务器1和2进行认证。配置备份服务器2的IP地址或域名以及所属的VRouter，在LDAP服务器配置模式下，使用以下命令：

```
backup2 {ip-address | host-name} [vrouter vrouter-name]
```

- *ip-address* | *host-name* – 指定备份服务器2的IP地址（IPv4地址或IPv6地址）或者域名。
- **vrouter** *vrouter-name* – 指定认证主服务器所属的VRouter。默认为系统缺省VR即trust-vr。

在LDAP服务器配置模式下，使用该命令no的形式取消备份服务器2的IP地址或者域名配置：

```
no backup2
```

配置服务器端口号

配置LDAP服务器端口号，在LDAP服务器配置模式下，使用以下命令：

```
port port-number
```

- *port-number* – 指定LDAP服务器的端口号。默认值是389。取值范围是1到65535。

在LDAP服务配置模式下，使用该命令no的形式恢复端口号的默认值：

```
no port
```

配置服务器认证或同步方法

LDAP服务器和系统之间可以使用明文和MD5摘要两种方法进行用户认证或用户同步。配置LDAP服务器认证或同步方法，在LDAP服务器配置模式下，使用以下命令：

```
auth-method {plain | digest-md5}
```

- **plain** – 指定使用明文的方法来认证或同步用户。
- **digest-md5** – 指定使用MD5摘要的方法来认证或同步用户。该方法为系统默认认证方法。

在LDAP服务配置模式下，使用该命令no的形式恢复默认认证或同步方法：

```
no auth-method
```



注意: 如果指定使用MD5摘要方法后没有配置Authid属性值，那么从服务器同步用户的过程中将使用明文方法，认证用户的过程中将使用MD5摘要方法。

指定Base-DN

指定Base-DN，Base-DN是指当LDAP服务器收到一个认证请求时，目录查询的起始点。在LDAP服务器配置模式下，使用以下命令：

```
base-dn string
```

- *string* – 指定Base-DN的具体内容，如dc=hillstonenet。

在LDAP服务配置模式下，使用该命令no的形式取消Base-DN的指定：

no base-dn

指定登录DN

如果使用明文方法来认证或同步用户，系统会使用登录DN和登录密码到服务器进行认证，从而能够连接服务器进行用户认证或同步。指定登录DN（通常为LDAP服务器预设的具有查询权限的用户账号），在LDAP服务器配置模式下，使用以下命令：

login-dn *string*

- *string* – 指定登录DN的具体内容，为1到255个字符的字符串，不区分大小写。

在LDAP服务配置模式下，使用该命令no的形式取消登录DN的指定：

no login-dn

指定Authid属性值

如果使用MD5摘要方法来认证或同步用户，系统会使用Authid属性值和登录密码到服务器进行认证，从而能够连接服务器进行用户认证或同步。配置Authid属性值，在LDAP服务器配置模式下，使用以下命令：

login-dn authid *string*

- *string* – 指定Authid的值，为1到63个字符的字符串，区分大小写。

在LDAP服务配置模式下，使用该命令no的形式取消Authid的指定：

no login-dn authid

指定登录密码

指定登录密码，此处的登录密码即为登录DN所对应的密码。在LDAP服务器配置模式下，使用以下命令：

login-password *string*

- *string* – 指定登录密码的具体内容。

在LDAP服务配置模式下，使用该命令no的形式取消登录密码的指定：

no login-password

指定名称属性

名称属性是指LDAP服务器上唯一标识名称的字符串。在LDAP服务器配置模式下，使用以下命令来指定名称属性：

naming-attribute *string*

- *string* – 指定名称属性的具体内容，为1到63个字符的字符串。该字符串通常为uid（User ID）或cn（Common Name），默认值为uid。

在LDAP服务配置模式下，使用该命令no的形式恢复默认情况：

no naming-attribute

指定用户组名称属性

用户组名称属性是指LDAP服务器上唯一标识用户组名称的字符串。在LDAP服务器配置模式下，使用以下命令来指定用户组名称属性：

group-naming-attribute *string*

- *string* – 指定名称属性的具体内容，为1到63个字符的字符串。该字符串通常为uid（User ID）或cn（Common Name），默认值为uid。

在LDAP服务配置模式下，使用该命令no的形式恢复默认情况：

no group-naming-attribute

指定Group-class

指定组对象objectClass的值，在LDAP服务器配置模式下，使用以下命令：

group-class *string*

- *string* – 指定Group-class的具体内容为1到63个字符的字符串，默认值为groupOfUniqueNames。

在LDAP服务配置模式下，使用该命令no的形式恢复默认情况：

no group-class

指定成员属性名

指定组对象中成员属性的名称，在LDAP服务器配置模式下，使用以下命令：

member-attribute *string*

- *string* – 指定成员属性名的具体内容，为1到63个字符的字符串，默认值为uniqueMember。

在LDAP服务配置模式下，使用该命令no的形式恢复默认情况：

no member-attribute

指定角色映射规则

为LDAP服务器指定角色映射规则后，系统将会为通过该服务器认证的用户按照指定角色映射规则分配角色。

为LDAP服务器指定角色映射规则，在LDAP服务器配置模式下，使用以下命令：

role-mapping-rule *rule-name*

- *rule-name* – 指定系统中已配置的映射规则的名称。

在LDAP服务器配置模式下，使用该命令no的形式取消角色映射规则的指定：

no role-mapping-rule

配置用户黑名单

为LDAP服务器配置用户黑名单后，系统将会禁止通过该服务器认证的黑名单用户访问任何网络资源。配置用户黑名单，在LDAP服务器配置模式下，使用以下命令：

user-black-list username *user-name*

- *user-name* – 指定黑名单中的用户名。取值范围是1到63个字符。

在LDAP服务器配置模式下，使用该命令no的形式删除黑名单用户：

no user-black-list username *user-name*

配置用户同步功能

用户同步指的是完成LDAP服务器配置后，系统将认证服务器上的用户信息同步到本地的功能，默认情况下系统每隔30分钟同步一次。

启用/禁用用户同步功能

在进行用户同步前，需要先启用用户同步功能。默认情况下，用户同步功能是启用的。启用或禁用用户同步功能，在LDAP服务器配置模式下，使用以下命令：

- 启用：**sync enable**
- 禁用：**sync disable**

配置用户同步方式

系统支持多种用户同步方式，包括手动同步和自动同步。

手动同步

更新LDAP服务器连接，手动同步用户信息。在LDAP服务器配置模式下，使用以下命令：

manual-sync

执行一次该命令即进行一次同步，如果同步过程中再次执行该命令，系统将清除原有用户同步信息，重新进行同步。

自动同步

自动同步方式包括三种：按时间间隔同步、每天同步和一次性同步。配置自动同步方式，在LDAP服务器配置模式下，使用以下命令：

auto-sync {periodically interval | daily HH:MM | once}

- *interval* – 指定为按时间间隔同步，并配置自动同步的间隔时间。取值范围为30到1440，单位为分钟，默认值为30。
- *HH:MM* – 指定为每天同步，并配置每天执行自动同步的时间点。HH和MM分别代表小时和分钟。
- **once** – 指定为一次性同步，当LDAP服务器配置信息有更改时，系统将会自动同步。首次配置该命令后，系统会执行一次同步。

恢复默认自动同步方式，即每隔30分钟进行一次同步。在LDAP服务器配置模式下，使用以下命令：

no auto-sync

配置用户过滤功能

在配置LDAP服务器认证参数时，通过指定用户过滤条件，使得在同步LDAP服务器上的用户时只有符合过滤条件的用户信息才被同步到设备中，或者只允许上述用户在登录时进行认证。配置用户过滤功能，必须先进入AAA认证服务器配置模式。在全局配置模式下执行**aaa-server** *aaa-server-name* **type ldap**命令可以进入指定名称的LDAP服务器配置模式。

配置用户过滤功能，在LDAP服务器配置模式下，使用以下命令：

user-filter *filter-string*

- filter-string - 指定用户过滤条件，为0到120个字符的字符串。例如，配置LDAP服务器时，filter-string设置为“（|（objectclass=inetOrgperson）（objectclass=person））”，表明只同步或认证所有被定义为inetOrgperson或者person的用户。

常用的操作符如下：

操作符	描述
=	相等
&	条件与
	条件或
!	条件非
*	通配符，代替0个或多个字符
~=	类似（用于模糊查询）
>=	字典序大于等于
<=	字典序小于等于



注意：

- 设备支持LDAP服务器支持的所有操作符。
- 如果用户输入的格式不符合LDAP服务器的规定，可能会导致用户同步或认证失败。

在LDAP服务器配置模式下，使用**no user-filter**命令取消用户过滤功能，即同步所有的用户，并且对所有的用户进行认证。

配置同步的工作模式

系统支持通过两种工作模式从LDAP服务器同步组织结构和用户信息到本地：按OU(OrganizationUnit)同步和按Group同步，从而管理员可以通过OU和Group类型的用户组进行安全策略控制。默认情况下，系统会按Group同步用户信息到本地。

配置用户同步的工作模式，在LDAP服务器配置模式下，使用以下命令：

sync-type {ou | group}

- **ou** – 指定按OU组织结构同步用户到本地。
- **group** – 指定按Group同步用户到本地。

在LDAP服务器配置模式下，使用**no sync-type**命令取消配置。

如果以OU模式来同步用户信息，可以配置要同步的OU组织结构的最大深度。在LDAP服务器配置模式下，使用以下命令：

sync-ou-depth *depth-value*

- *depth-value* – 指定同步OU组织结构的最大深度。取值范围为1到12，默认值为12。超过最大深度的OU组织结构不会被同步，但是超过最大深度的所有用户会被同步，并且被同步到其所属最大限制深度的OU中。需要注意的是，如果各层级OU的名称总长度（包括“OU=”和标点符号）大于128个字符，那么超过此长度的OU信息将不会被同步。

在LDAP服务器配置模式下，使用**no sync-ou-depth**命令恢复默认值。

配置备份认证服务器

为LDAP服务器配置备份认证服务器后，当主服务器出现问题或者用户在主服务器认证失败时，备份认证服务器发挥身份认证的作用。备份认证服务器可以与主服务器为不同类型。系统中已配置的本地、Active-Directory、RADIUS或者LDAP服务器均可作为备份认证服务器。为LDAP服务器配置备份认证服务器，在LDAP服务器配置模式下，使用以下命令：

backup-aaa-server *aaa-server-name*

- `aaa-server-name` – 指定系统中已经配置的AAA服务器的名称。

在LDAP服务器配置模式下，使用该命令`no`的形式取消备份认证服务器的配置：

no backup-aaa-server



注意:

- 备份认证服务器和主认证服务器必须处于相同VSYS。关于VSYS的详细信息，请参阅[虚拟系统](#)。
- 备份认证服务器不能嵌套备份认证服务器。
- 删除AAA服务器之前，请确保该服务器未被指定为备份认证服务器。
- 如果为同一LDAP服务器配置了备份服务器1（**backup1**）、备份服务器2（**backup2**）和备份认证服务器（**backup-aaa-server**），当用户在主服务器认证无响应时，系统会按照这样的顺序对该用户再次进行认证：备份服务器1→备份服务器2→备份认证服务器；当用户在主服务器认证失败时，系统会先通过备份服务器进行认证，如果备份服务器认证失败再通过备份认证服务器对该用户再次进行认证

配置防暴力破解功能

为了防止非法用户通过暴力方法获取用户名和密码，可以通过配置基于用户名或基于IP地址的防暴力破解功能，即在指定时间内，若用户连续输错指定次数的用户名和密码，系统将会按照指定的锁定时间锁定该用户或IP地址。防暴力破解功能的配置包括：

- 开启或关闭防暴力破解功能
- 配置尝试次数
- 配置锁定时间

开启或关闭防暴力破解功能

防暴力破解功能默认情况下是关闭的。开启防暴力破解功能，请在LDAP服务器配置模式下使用以下命令：

- 启用：**lockout {ip | user} enable**
- 关闭：**lockout {ip | user} disable**

配置尝试次数

配置尝试次数，即在指定时间内，允许用户连续输错用户名和密码的次数，在LDAP服务器配置模式下使用以下命令：

lockout {**ip** | **user**} **failed-attempts** *number* **interval** *interval*

- **failed-attempts** *number* – 指定时间内允许输错用户名和密码的次数，基于用户名配置时，取值范围是1-32，默认值是5次；基于IP地址配置时，取值范围是1-2048，默认值是64次。
- **interval** *interval* – 指定连续输错用户名和密码的时间范围，单位是秒，取值范围是1-180秒，默认值是60秒。

在LDAP服务器配置模式下，使用**no lockout** {**ip** | **user**} **failed-attempts**命令恢复默认值。

配置锁定时间

在指定时间内，若用户连续输错指定次数的用户名和密码，系统将会按照指定的锁定时间锁定该用户或IP地址。配置锁定时间，在LDAP服务器配置模式下使用以下命令：

lockout {**ip** | **user**} **lockout-time** *time*

- **lockout-time** *time* – 指定锁定时间，单位是秒，取值范围是30-1800秒，基于用户名配置时，默认值是600秒；基于IP地址配置时，默认值是60秒。

在LDAP服务器配置模式下，使用**no lockout** {**ip** | **user**} **lockout-time**命令恢复默认值。

查看锁定列表信息

查看被锁定的用户信息、被锁定的IP地址信息，在任何模式下，使用以下命令：

show aaa-server *aaa-server-name* **lockout** {**user** [*username*] | **ip** [*ip-address* **vr_id** *number*]}

- *aaa-server-name* - 指定AAA服务器名称。
- **user** [*username*] - 查看指定名称的锁定用户信息。
- **ip** [*ip-address* **vr_id** *number*] - 查看指定IP地址和VRouter ID的锁定IP信息。

解除用户/IP地址的锁定

解除对指定用户/IP地址的锁定并且从锁定列表中删除，在任何模式下，使用以下命令：

exec aaa *aaa-server-name* **lockout delete** {**user** [*username*] | **ip** [*ip-address* **vr_id** *number*]}

- *aaa-server-name* - 指定AAA服务器名称。
- **user** [*username*] - 解除对指定名称的用户的锁定。
- **ip** [*ip-address* **vr_id** *number*] - 解除对指定IP地址和VRouter ID的锁定。

配置Active-Directory服务器认证参数

在全局配置模式下执行**aaa-server** *aaa-server-name* **type active-directory**命令可以进入指定名称的Active-Directory服务器配置模式。用户可配置的Active-Directory服务器认证参数包括：

- 配置认证主服务器的IP地址或域名
- 配置备份服务器1的IP地址或域名
- 配置备份服务器2的IP地址或域名
- 配置服务器端口号
- 配置服务器认证或同步方法
- 指定更新服务器连接
- 指定Base-DN
- 指定登录DN
- 指定sAMAccountName属性值
- 指定登录密码
- 配置角色映射规则
- 配置用户黑名单
- 配置服务器监控功能
- 配置用户自动同步
- 配置用户过滤功能
- 配置同步的工作模式
- 配置备份认证服务器

- 配置仅同步Base-DN下用户组
- 配置防暴力破解功能

配置认证主服务器的IP地址或域名

配置认证主服务器的IP地址或域名以及所属的VRouter，在Active-Directory服务器配置模式下，使用以下命令：

```
host {ip-address | host-name} [vrouter vrouter-name]
```

- *ip-address | host-name* – 指定认证主服务器的IP地址（IPv4地址或IPv6地址）或者域名。
- **vrouter** *vrouter-name* – 指定认证主服务器所属的VRouter。默认为系统缺省VR即trust-vr。

在Active-Directory服务器配置模式下，使用该命令no的形式取消认证主服务器的IP地址或者域名配置：

```
no host
```

配置备份服务器1的IP地址或域名

该参数为可选配置。备份服务器是与主服务器相同类型服务器。在当通过主服务器进行认证失败时，依次启用备份服务器1和2进行认证。配置备份服务器1的IP地址或域名以及所属的VRouter，在Active-Directory服务器配置模式下，使用以下命令：

```
backup1 {ip-address | host-name} [vrouter vrouter-name]
```

- *ip-address | host-name* – 指定备份服务器1的IP地址（IPv4地址或IPv6地址）或者域名。
- **vrouter** *vrouter-name* – 指定认证主服务器所属的VRouter。默认为系统缺省VR即trust-vr。

在Active-Directory服务器配置模式下，使用该命令no的形式取消备份服务器1的IP地址或者域名配置：

```
no backup1
```

配置备份服务器2的IP地址或域名

该参数为可选配置。备份服务器是与主服务器相同类型服务器。在当通过主服务器进行认证失败时，依次启用备份服务器1和2进行认证。配置备份服务器2的IP地址或域名以及所属的VRouter，在Active-Directory服务器配置模式下，使用以下命令：

```
backup2 {ip-address | host-name} [vrouter vrouter-name]
```

- *ip-address | host-name* – 指定备份服务器2的IP地址（IPv4地址或IPv6地址）或者域名。
- **vrouter** *vrouter-name* – 指定认证主服务器所属的VRouter。默认为系统缺省VR即trust-vr。

在Active-Directory服务器配置模式下，使用该命令no的形式取消备份服务器2的IP地址或者域名配置：

no backup2

配置服务器端口号

配置Active-Directory服务器端口号，在Active-Directory服务器配置模式下，使用以下命令：

port *port-number*

- *port-number* – 指定Active-Directory服务器的端口号。默认值是389。取值范围是1到65535。

在Active-Directory服务配置模式下，使用该命令no的形式恢复端口号的默认值：

no port

配置服务器认证或同步方法

Active-Directory服务器和系统之间可以使用明文和MD5摘要两种方法进行用户认证或用户同步。配置Active-Directory服务器认证或同步方法，在Active-Directory服务器配置模式下，使用以下命令：

auth-method {**plain** | **digest-md5**}

- **plain** – 指定使用明文的方法来认证或同步用户。
- **digest-md5** – 指定使用MD5摘要的方法来认证或同步用户。该方法为系统默认认证方法。

在Active-Directory服务配置模式下，使用该命令no的形式恢复默认认证或同步方法：

no auth-method



注意：如果指定使用MD5摘要方法后没有配置sAMAccountName属性值，那么从服务器同步用户的过程中将使用明文方法，认证用户的过程中将使用MD5摘要方法。

指定Base-DN

指定Base-DN，Base-DN是指当Active-Directory服务器收到一个认证请求时，目录查询的起始点。在Active-Directory服务器配置模式下，使用以下命令：

base-dn *string*

- *string* – 指定Base-DN的具体内容，如dc=hillstonenet。

在Active-Directory服务配置模式下，使用该命令no的形式取消Base-DN的指定：

no base-dn

指定同步Base-DN

Base-DN是指Active-Directory服务器目录查询的起始点。指定同步Base-DN后，该Base-DN路径下的所有用户及用户组将同步到本地。指定同步Base-DN，在Active-Directory服务器配置模式下，使用以下命令：

sync-base-dn *string*

- *string* – 指定同步Base-DN的具体内容，如OU=A，dc=hillstonenet。

在Active-Directory服务配置模式下，使用该命令no的形式取消同步Base-DN的指定：

no sync-base-dn

指定认证Base-DN

Base-DN是指Active-Directory服务器目录查询的起始点。指定认证Base-DN后，该Base-DN路径下的所有用户（包括用户组中的直属用户）将允许通过认证。指定认证Base-DN，在Active-Directory服务器配置模式下，使用以下命令：

auth-base-dn *string*

- *string* – 指定认证Base-DN的具体内容，如OU=A，dc=hillstonenet。

在Active-Directory服务配置模式下，使用该命令no的形式取消认证Base-DN的指定：

no auth-base-dn

指定登录DN

如果使用明文方法来认证或同步用户，系统会使用登录DN和登录密码到服务器进行认证，从而能够连接服务器进行用户认证或同步。指定登录DN（通常为AD服务器预设的具有查询权限的用户账号），在Active-Directory服务器配置模式下，使用以下命令：

```
login-dn string
```

- *string* – 指定登录DN的具体内容，为1到255个字符的字符串，不区分大小写。

在Active-Directory服务配置模式下，使用该命令no的形式取消登录DN的指定：

```
no login-dn
```

指定sAMAccountName属性值

如果使用MD5摘要方法来认证或同步用户，系统会使用sAMAccountName属性值和登录密码到服务器进行认证，从而能够连接服务器进行用户认证或同步。配置sAMAccountName属性值，在Active-Directory服务器配置模式下，使用以下命令：

```
login-dn sAMAccountName string
```

- *string* – 指定sAMAccountName的值，为1到63个字符的字符串，区分大小写。

在Active-Directory服务配置模式下，使用该命令no的形式取消sAMAccountName的指定：

```
no login-dn sAMAccountName
```

指定登录密码

指定登录密码，此处的登录密码即为登录DN所对应的密码。在Active-Directory服务器配置模式下，使用以下命令：

```
login-password string
```

- *string* – 指定登录密码的具体内容。

在Active-Directory服务配置模式下，使用该命令no的形式取消登录密码的指定：

```
no login-password
```

指定角色映射规则

为Active-Directory服务器指定角色映射规则后，系统将会为通过该服务器认证的用户按照指定角色映射规则分配角色。为Active-Directory服务器指定角色映射规则，在Active-Directory服务器配置模式下，使用以下命令：

```
role-mapping-rule rule-name
```

- *rule-name* – 指定系统中已配置的映射规则的名称。

在Active-Directory服务器配置模式下，使用该命令no的形式取消角色映射规则的指定：

```
no role-mapping-rule
```

配置用户黑名单

为Active-Directory服务器配置用户黑名单后，系统将会禁止通过该服务器认证的黑名单用户访问任何网络资源。配置用户黑名单，在Active-Directory服务器配置模式下，使用以下命令：

```
user-black-list username user-name
```

- *user-name* – 指定黑名单中的用户名。取值范围是1到63个字符。

在Active-Directory服务器配置模式下，使用该命令no的形式删除黑名单用户：

```
no user-black-list username user-name
```

配置服务器监控功能

通过服务器监控功能，系统能够从Active-Directory服务器上获取域用户的用户名和IP地址对应关系信息，从而允许用户访问网络资源，实现单点认证。另外，利用所获取的用户名和IP地址对应关系信息，系统还可以实现基于用户的安全统计、日志记录、行为审计等。

实现Active-Directory服务器监控功能，需要在Active-Directory服务器或者域内其他PC上安装并运行服务器监控软件AD Agent。AD Agent可在以下操作系统中运行：Windows Server 2003（32/64位）、Windows Server 2008（32/64位，Windows Server 2008 R2 64位）。安装并成功运行AD Agent后，当域用户从Active-Directory服务器登录或者注销时，AD Agent会记录该用户的用户名、IP地址、当前时间等信息，并将用户名和IP地址对应关系信息发送到系统。这样，系统就可以获得每个在线用户的IP地址信息。

开启/关闭服务器监控功能

开启Active-Directory服务器监控功能，在Active-Directory服务器配置模式下，使用以下命令：

agent

在Active-Directory服务器配置模式下，使用该命令no的形式关闭Active-Directory服务器监控功能：

no agent

指定监听端口及用户绑定信息删除超时时间

系统通过监听端口与AD Agent建立通信连接，获取域用户的用户名和IP地址对应关系信息。当通信连接断开时，如果在指定的用户绑定信息删除超时时间内，未重新建立通信连接，系统则会删除已获取的用户名和IP地址对应关系信息。指定监听端口和用户绑定信息删除超时时间，在Active-Directory服务器配置模式下，使用以下命令：

agent [port port-number] [disconn-del-timeout time]

- **port port-number** – 指定监听端口号。AD Agent通过该端口与系统建立通信连接。取值范围为1025到65535。系统默认为6666。该端口号必须和系统中AD服务器设置的监听端口号一致，否则无法通信。
- **disconn-del-timeout time** – 指定用户绑定信息删除超时时间。取值范围为0到1800，单位为秒。若不指定，系统默认超时时间为300秒。0表示永不超时。

在Active-Directory服务器配置模式下，使用该命令no的形式取消已指定的监听端口号和用户绑定信息删除超时时间：

no agent

显示监控用户信息

在任何模式下，使用以下命令查看当前在线的服务器监控用户信息：

show auth-user agent [interface interface-name | vrouter vrouter-name | slot slot-no]

踢出用户映射信息

踢出某指定IP的用户和IP的映射信息。在任意模式下，使用以下命令：

exec user-mapping agent kickout ip ip-address vrouter vrouter-name

配置用户同步功能

用户同步指的是完成Active-Directory服务器配置后，系统将认证服务器上的用户信息同步到本地的功能，默认情况下系统每隔30分钟同步一次。

启用/禁用用户同步功能

在进行用户同步前，需要先启用用户同步功能。默认情况下，用户同步功能是启用的。启用或禁用用户同步功能，在Active-Directory服务器配置模式下，使用以下命令：

- 启用：`sync enable`
- 禁用：`sync disable`

配置用户同步方式

系统支持多种用户同步方式，包括手动同步和自动同步。

手动同步

更新Active-Directory服务器连接，手动同步用户信息。在Active-Directory服务器配置模式下，使用以下命令：

manual-sync

执行一次该命令即进行一次同步，如果同步过程中再次执行该命令，系统将清除原有用户同步信息，重新进行同步。

自动同步

自动同步方式包括三种：按时间间隔同步、每天同步和一次性同步。配置自动同步方式，在Active-Directory服务器配置模式下，使用以下命令：

auto-sync {periodically *interval* | daily *HH:MM* | once}

- *interval* – 指定为按时间间隔同步，并配置自动同步的间隔时间。取值范围为30到1440，单位为分钟，默认值为30。
- *HH:MM* – 指定为每天同步，并配置每天执行自动同步的时间点。HH和MM分别代表小时和分钟。
- *once* – 指定为一次性同步，当Active-Directory服务器配置信息有更改时，系统将会自动同步。首次配置该命令后，系统会执行一次同步。

恢复默认自动同步方式，即每隔30分钟进行一次同步。在Active-Directory服务器配置模式下，使用以下命令：

no auto-sync

配置用户过滤功能

在配置Active-Directory服务器认证参数时，通过指定用户过滤条件，使得在同步Active-Directory服务器上的用户时只有符合过滤条件的用户信息才被同步到设备中，或者只允许上述用户在登录时进行认证。配置用户过滤功能，必须先进入AAA认证服务器配置模式。在全局配置模式下执行**aaa-server** *aaa-server-name* **type active-directory**命令可以进入指定名称的Active-Directory服务器配置模式。

配置用户过滤功能，在Active-Directory服务器配置模式下，使用以下命令：

user-filter *filter-string*

- filter-string* - 指定用户过滤条件，为0到120个字符的字符串。例如，配置Active-Directory服务器时，*filter-string*设置为“memberOf=CN=Admin,DC=test,DC=com”，表明只同步或认证DN为“CN=Admin,DC=test,DC=com”的Group中的用户。

常用的操作符如下：

操作符	描述
=	相等
&	条件与
	条件或
!	条件非
*	通配符，代替0个或多个字符
~=	类似（用于模糊查询）
>=	字典序大于等于
<=	字典序小于等于



注意：

- Hillstone设备支持Active-Directory服务器支持的所有操作符。
- 如果用户输入的格式不符合Active-Directory服务器的规定，可能会导致用户同步或认证失败。
- 删除AAA服务器之前，请确保该服务器未被指定为备份认证服务器。



- 如果为同一RADIUS服务器配置了备份服务器1（backup1）、备份服务器2（backup2）和备份认证服务器（backup-aaa-server），当用户在主服务器认证无响应时，系统会按照这样的顺序对该用户再次进行认证：备份服务器1→备份服务器2→备份认证服务器；当用户在主服务器认证失败时，系统会先通过备份服务器1和2进行认证，如果备份服务器1和2认证失败，再通过备份认证服务器对该用户再次进行认证。

在Active-Directory服务器配置模式下，使用**no user-filter**命令取消用户过滤功能，即同步所有的用户，并且对所有的用户进行认证。

配置同步的工作模式

系统支持通过两种工作模式从Active-Directory服务器同步组织结构和用户信息到本地：按OU(OrganizationUnit)同步和按Group同步，从而管理员可以通过OU和Group类型的用户组进行安全策略控制。默认情况下，系统会按Group同步用户信息到本地。

配置用户同步的工作模式，在Active-Directory服务器配置模式下，使用以下命令：

sync-type {ou | group}

- **ou** - 指定按OU组织结构同步用户到本地。
- **group** - 指定按Group同步用户到本地。

在Active-Directory服务器配置模式下，使用**no sync-type**命令取消配置。

如果以OU模式来同步用户信息，可以配置要同步的OU组织结构的最大深度。在Active-Directory服务器配置模式下，使用以下命令：

sync-ou-depth depth-value

- **depth-value** - 指定同步OU组织结构的最大深度。取值范围为1到12，默认值为12。超过最大深度的OU组织结构不会被同步，但是超过最大深度的所有用户会被同步，并且被同步到其所属最大限制深度的OU中。需要注意的是，如果各层级OU的名称总长度（包括“OU=”和标点符号）大于128个字符，那么超过此长度的OU信息将不会被同步。

在Active-Directory服务器配置模式下，使用**no sync-ou-depth**命令恢复默认值。

配置备份认证服务器

为Active-Directory服务器配置备份认证服务器后，当主服务器出现问题或者用户在主服务器认证失败时，备份认证服务器发挥身份认证的作用。备份认证服务器可以与主服务器为不同类型。系统中已配置的本地、Active-Directory、RADIUS或者LDAP服务器均可作为备份认证服务器。为Active-Directory服务器配置备份认证服务器，在Active-Directory服务器配置模式下，使用以下命令：

```
backup-aaa-server aaa-server-name
```

- *aaa-server-name* – 指定系统中已经配置的AAA服务器的名称。

在Active-Directory服务器配置模式下，使用该命令no的形式取消备份认证服务器的配置：

```
no backup-aaa-server
```



注意：

- 备份认证服务器和主认证服务器必须处于相同VSYS。关于VSYS的详细信息，请参阅[虚拟系统](#)。
- 备份认证服务器不能嵌套备份认证服务器。
- 删除AAA服务器之前，请确保该服务器未被指定为备份认证服务器。
- 如果为同一Active-Directory服务器配置了备份服务器1（backup1）、备份服务器2（backup2）和备份认证服务器（backup-aaa-server），当用户在主服务器认证无响应时，系统会按照这样的顺序对该用户再次进行认证：备份服务器1→备份服务器2→备份认证服务器；当用户在主服务器认证失败时，系统会先通过备份服务器进行认证，如果备份服务器认证失败再通过备份认证服务器对该用户再次进行认证。

配置仅同步Base-DN下用户组

在同步AD服务器用户时，可以根据需要，启用或禁用仅同步Base-DN下的用户组功能，在Active-Directory服务器配置模式下，使用以下命令：

- 启用：`sync-group-under-basedn enable`
- 禁用：`no sync-group-under-basedn enable`

配置防暴力破解功能

为了防止非法用户通过暴力方法获取用户名和密码，可以通过配置基于用户名或基于IP地址的防暴力破解功能，即在指定时间内，若用户连续输错指定次数的用户名和密码，系统将会按照指定的锁定时间锁定该用户或IP地址。防暴力破解功能的配置包括：

- 开启或关闭防暴力破解功能
- 配置尝试次数
- 配置锁定时间
- 查看锁定列表信息
- 解除用户/IP地址的锁定

开启或关闭防暴力破解功能

防暴力破解功能默认情况下是关闭的。开启防暴力破解功能，在Active-Directory服务器配置模式下使用以下命令：

- 启用：`lockout {ip | user} enable`
- 关闭：`lockout {ip | user} disable`

配置尝试次数

配置尝试次数，即在指定时间内，允许用户连续输错用户名和密码的次数，在Active-Directory服务器配置模式下使用以下命令：

`lockout {ip | user} failed-attempts number interval interval`

- **failed-attempts number** – 指定时间内允许输错用户名和密码的次数，基于用户名配置时，取值范围是1-32，默认值是5次；基于IP地址配置时，取值范围是1-2048，默认值是64次。
- **interval interval** – 指定连续输错用户名和密码的时间范围，单位是秒，取值范围是1-180秒，默认值是60秒。

在Active-Directory服务器配置模式下，使用`no lockout {ip | user} failed-attempts`命令恢复默认值。

配置锁定时间

在指定时间内，若用户连续输错指定次数的用户名和密码，系统将会按照指定的锁定时间锁定该用户或IP地址。配置锁定时间，在Active-Directory服务器配置模式下使用以下命令：

```
lockout {ip | user} lockout-time time
```

- **lockout-time time** - 指定锁定时间，单位是秒，取值范围是30-1800秒，基于用户名配置时，默认值是600秒；基于IP地址配置时，默认值是60秒。

在Active-Directory服务器配置模式下，使用**no lockout {ip | user} lockout-time**命令恢复默认值。

查看锁定列表信息

查看被锁定的用户信息、被锁定的IP地址信息，在任何模式下，使用以下命令：

```
show aaa-server aaa-server-name lockout {user [username] | ip [ip-address vr_id number]}
```

- *aaa-server-name* - 指定AAA服务器名称。
- **user [username]** - 查看指定名称的锁定用户信息。
- **ip [ip-address vr_id number]** - 查看指定IP地址和VRouter ID的锁定IP信息。

解除用户/IP地址的锁定

解除对指定用户/IP地址的锁定并且从锁定列表中删除，在任何模式下，使用以下命令：

```
exec aaa aaa-server-name lockout delete {user [username] | ip [ip-address vr_id number]}
```

- *aaa-server-name* - 指定AAA服务器名称。
- **user [username]** - 解除对指定名称的用户的锁定。
- **ip [ip-address vr_id number]** - 解除对指定IP地址和VRouter ID的锁定。

配置TACACS+服务器认证参数

在全局配置模式下执行**aaa-server aaa-server-name type tacacs+**命令可以进入指定名称的TACACS+服务器配置模式。用户可配置的TACACS+服务器认证参数包括：

- 配置认证主服务器的IP地址或域名
- 配置备份服务器1的IP地址或域名
- 配置备份服务器2的IP地址或域名
- 配置TACACS+服务器端口号
- 配置TACACS+服务器的共享密钥
- 配置TACACS+服务器

配置认证主服务器的IP地址或域名

配置认证主服务器的IP地址或域名以及所属的VRouter，在TACACS+服务器配置模式下，使用以下命令：

```
host { ip-address | host-name } [vrouter vrouter-name]
```

- *ip-address* | *host-name* – 指定认证主服务器的IP地址或者域名。
- **vrouter** *vrouter-name* – 指定认证主服务器所属的VRouter。默认为系统缺省VR即trust-vr。

在TACACS+服务器配置模式下，使用该命令no的形式取消认证主服务器的IP地址或者域名配置：

```
no host
```

配置备份服务器1的IP地址或域名

该参数为可选配置。备份服务器是与主服务器相同类型服务器。在当通过主服务器进行认证失败时，依次启用备份服务器1和2进行认证。配置备份服务器1的IP地址或域名以及所属的VRouter，在TACACS+服务器配置模式下，使用以下命令：

```
backup1 { ip-address | host-name } [vrouter vrouter-name]
```

- *ip-address* | *host-name* – 指定备份服务器1的IP地址或者域名。
- **vrouter** *vrouter-name* – 指定认证主服务器所属的VRouter。默认为系统缺省VR即trust-vr。

在TACACS+服务器配置模式下，使用该命令no的形式取消备份服务器1的IP地址或者域名配置：

```
no backup1
```

配置备份服务器2的IP地址或域名

该参数为可选配置。备份服务器是与主服务器相同类型服务器。在当通过主服务器进行认证失败时，依次启用备份服务器1和2进行认证。配置备份服务器2的IP地址或域名以及所属的VRouter，在TACACS+服务器配置模式下，使用以下命令：

```
backup2 {ip-address | host-name} [vrouter vrouter-name]
```

- *ip-address | host-name* – 指定备份服务器2的IP地址或者域名。
- **vrouter** *vrouter-name* – 指定备份服务器所属的VRouter。默认为系统缺省VR即trust-vr。

在TACACS+服务器配置模式下，使用该命令no的形式取消备份服务器2的IP地址或者域名配置：

```
no backup2
```

配置TACACS+服务器端口号

配置TACACS+服务器端口号，在TACACS+服务器配置模式下，使用以下命令：

```
port port-number
```

- *port-number* – 指定TACACS+服务器的端口号。默认值是49。

在TACACS+服务器配置模式下，使用该命令no的形式恢复端口号的默认值：

```
no port
```

配置TACACS+服务器的共享密钥

配置TACACS+服务器的共享密钥，在TACACS+服务器配置下，使用以下命令：

```
secret secret
```

- *secret* – 指定TACACS+服务器的共享密钥秘密字符串。字符串范围为1到31个字符。

在TACACS+服务器配置模式下，使用该命令no的形式取消对TACACS+服务器共享密钥秘密的配置：

```
no secret
```

指定系统管理员认证服务器

AAA认证服务器的认证参数配置完成后，用户需要指定某个服务器作为设备系统管理员使用的认证服务器。默认情况下，系统使用“Local”作为系统管理员认证服务器。用户不可以删除“Local”。指定系统管理员认证服务器，在全局配置模式下输入以下命令：

```
admin auth-server server-name
```

- *server-name* - 指定认证服务器的名称。

使用**no admin auth-server**命令恢复使用默认系统认证服务器“Local”。

用户可以根据需要，指定优先使用本地服务器对Console方式访问的管理员进行认证，如果所配置的本地服务器不可达或认证服务器不可用时，系统会使用默认Radius服务器进行系统管理员认证。指定Console方式访问的管理员优先使用本地服务器认证，在全局配置模式下，使用以下命令：

```
admin console local-auth-prior
```

使用**no admin console local-auth-prior**命令取消优先使用本地认证服务器“Local”。

默认情况下，如果所配置的外部服务器不可达或认证服务不可用，系统会使用默认本地服务器“Local”进行系统管理员认证。当使用Radius服务器作为认证服务器时，用户可以选择关闭“Local”服务器认证，即当指定的Radius服务器不可达或者认证服务器不可用时，禁止使用“Local”进行系统管理员认证。

使用Radius服务器进行认证时，关闭/开启“Local”服务器认证，在全局配置模式下，使用以下命令：

- 关闭“Local”服务器认证：**admin auth-server radius-server-name disable-retry-local**
- 开启“Local”服务器认证：**admin auth-server radius-server-name**

显示优先使用本地服务器认证启用状态

显示优先使用本地服务器认证功能启用状态，在任何模式下使用以下命令：

```
show admin console local-auth-prior
```

Radius动态授权

Radius 动态授权功能，包含以下两点内容：

- 当用户认证成功后，Radius服务器可以发送Radius CoA（Change of Authorization）请求消息将认证用户的权限下发到设备，设备自动生成该用户的安全策略规则，当该用户下线时，设备将会自动删除该用户的安全策略规则。

开启/关闭RADIUS动态授权功能

默认情况下，RADIUS动态授权功能是关闭的。开启或关闭RADIUS动态授权功能，在全局配置模式下，使用以下命令：

- 开启：`radius-server dynamic-authorization enable`
- 关闭：`no radius-server dynamic-authorization enable`



注意：如果需要使用RADIUS动态授权功能，请先开启并配置RADIUS服务器的计费功能。具体配置方法，请参阅“[配置RADIUS服务器的计费功能](#)”。

配置RADIUS动态授权服务器

配置用来发送动态授权请求的RADIUS授权服务器信息，在全局配置模式下，使用以下命令：

```
radius-server dynamic-authorization {server-ip ip-address [destination-ip destination-ip]} {secret key-string}
```

- `server-ip ip-address` - 指定RADIUS授权服务器的IP地址（IPv4地址或IPv6地址）。
- `destination-ip destination-ip` - 指定授权请求的目的IP地址，该选项为选配项。
- `secret key-string` - 指定Radius授权服务器的共享密钥，字符串范围为1到31个字符。

在全局配置模式下，使用该命令`no`的形式删除RADIUS授权服务器配置：

```
no radius-server dynamic-authorization server-ip ip-address
```

配置动态授权端口号

配置动态授权的端口号，在全局配置模式下，使用以下命令：

```
radius-server dynamic-authorization port port-number
```

- `port-number` - 指定动态授权的端口号，默认值是3799。取值范围是1024到65535。

在全局配置模式下，使用该命令`no`的形式恢复端口号的默认值：

```
no radius-server dynamic-authorization port
```

查看RADIUS授权服务器配置信息

查看RADIUS授权服务器配置信息，在任意模式下，使用以下命令：

```
show radius-server dynamic-authorization
```

认证与授权的显示与调试

配置完毕，在任何模式下执行show命令可以查看配置后的运行情况，用户可以通过查看显示信息验证配置的效果。在任何模式下执行debug aaa命令可以对AAA进行调试。

查看AAA服务器的配置信息，请输入以下命令：

```
show aaa-server [server-name]
```

显示用户黑名单的配置信息，请输入以下命令：

```
show user-black-list
```

显示AAA的调试信息，请输入以下命令：

```
debug aaa[accounting | authentication | authorization | internal | radius | user]
```

- **accounting** - 显示AAA计费的调试信息。
- **authentication** - 显示AAA认证的调试信息。
- **authorization** - 显示AAA授权的调试信息。
- **internal** - 显示本地用户通过AAA本地认证方式访问设备时的调试信息。
- **radius** - 显示RADIUS认证的调试信息。
- **user** - 显示本地用户属性变化时的调试信息。

单点登录

单点登录（SSO，Single Sign-On）指用户通过一次认证之后，系统通过某种方式获取其认证信息，之后该用户不需要再次在设备上认证，即用户可以实现“免认证”上网。

单点登录有多种实现方式，互相独立，均可实现“免输入”（不输入用户名、密码）认证。

SSO Radius单点登录

接收Radius计费报文

设备可接收符合Radius标准协议的计费报文，并根据报文内容，生成对应的用户认证信息并加入认证用户表、重置用户保活定时器以及删除已认证用户。

使设备接收Radius计费报文、分析报文内容以及采取相应动作，需要进行如下配置：

在全局配置模式下，使用如下命令，进入SSO-Radius配置模式：

```
user-sso server sso-radius default
```

在sso-radius配置模式下，使用如下命令：

```
enable
```

关闭设备接收Radius计费报文功能，在SSO-Radius配置模式下，使用`no enable`。

指定AAA服务器

指定用户所属的AAA服务器。指定AAA服务器，在SSO-Radius配置模式下，使用以下命令：

```
aaa-server aaa-server-name
```

- *aaa-server-name* – 指定AAA服务器的名称。AAA服务器支持选择Local、AD或者LDAP类型的服务器。选择AAA服务器后，系统可以在引用的AAA服务器上查询在线用户的用户名对应的用户组和角色信息，从而实现基于用户组和角色的策略控制。

在SSO-Radius配置模式下使用该命令`no`的形式取消对AAA服务器的指定：

```
no aaa-server
```

指定设备接收Radius报文的端口号

指定设备接收Radius报文的端口号（不可在非根VSYS中配置端口），在SSO-Radius配置模式下，使用如下命令：

```
port port
```

- *port* – 指定端口号。取值范围1~65535。默认端口号1813。

使用**no port**命令恢复默认端口号。

配置Radius客户端

指定Radius客户端的IP地址。最多支持指定8条记录。指定IP地址后，进入SSO Radius客户端配置模式。指定SSO Radius客户端的IP地址并进入SSO Radius客户端配置模式，在SSO-Radius配置模式下，使用如下命令：

client {any | A.B.C.D}

- **any** – 接收任意SSO Radius客户端发送的报文。
- **A.B.C.D** – 接收指定IP地址的SSO Radius客户端发送的报文。

删除所设置的SSO Radius客户端，在全局配置模式下，使用**no client {any | A.B.C.D}** 命令。

配置共享密钥

设备使用共享密钥校验报文，校验成功后，才会对报文进行解析，否则丢弃报文。SSO Radius客户端需要配置与设备相同的共享密钥，或者SSO Radius客户端和设备都不配置共享密钥，报文才能通过校验。配置共享密钥，在SSO Radius客户端配置模式下，使用如下命令：

shared-secret key-value

- *key-value* – 指定共享密钥。长度1-31个字符。

清除共享密钥，使用**no shared-secret**命令。

显示SSO Radius配置信息

显示SSO Radius配置信息，在任意模式下，使用如下命令：

show user-sso server sso-radius default

查看用户映射信息

查看SSO Radius的用户名和IP映射信息。在任意模式下，使用以下命令：

show user-mapping user-sso sso-radius default

查看认证用户表

设备生成的用户认证信息保存在用户认证表。在任意模式下，使用以下命令：

```
show auth-user sso-radius [interface interface-name] [vrouter vrouter-name]
```

踢出用户映射信息

踢出某指定IP的用户和IP的映射信息。在任意模式下，使用以下命令：

```
exec user-mapping user-sso sso-radius kickout ip ip-address vrouter vrouter-name
```

AD Scripting单点登录

AD Scripting单点登录使用户通过Active-Directory服务器认证的同时，即可自动通过设备认证。目前只支持Active-Directory服务器的AD Scripting功能。

Hillstone提供脚本程序“Logonscript.exe”，用户只需将脚本文件添加到Active-Directory服务器的登录/注销脚本中即可实现AD Scripting功能。



注意：将脚本程序“Logonscript.exe”添加到AD服务器的方法，请参考[AD Scripting单点登录配置举例](#)。

进入AD Scripting配置模式

进入AD Scripting配置模式，在全局配置模式下，使用以下命令：

```
user-sso server ad-scripting default
```

开启/关闭AD Scripting功能

默认情况下，系统的AD Scripting功能是关闭的。在安全网关上开启或者关闭AD Scripting功能，在AD-Scripting配置模式下，使用以下命令：

- 启用：enable
- 关闭：no enable

指定AAA服务器

指定用户所属的AAA服务器，在AD-Scripting配置模式下，使用以下命令：

```
aaa-server aaa-server-name
```

- *aaa-server-name* – 指定AAA服务器的名称。AAA服务器支持选择Local、AD或者LDAP类型的服务器。选择AAA服务器后，系统可以在引用的AAA服务器上查询在线用户的用户名对应的用户组和角色信息，从而实现基于用户组和角色的策略控制。

在AD-Scripting配置模式下使用该命令no的形式取消对AAA服务器的指定：

```
no aaa-server
```

配置空闲超时时间

空闲超时时间指认证用户在无流量状态下保持认证状态的最长时间，超出空闲超时时间后，设备删除用户认证信息。配置空闲超时时间，在AD-Scripting配置模式下，使用以下命令：

```
idle-timeout timeout
```

- *timeout* – 指定空闲超时时间，单位为分钟。取值范围是1到60*24分钟。

默认情况下，在无流量状态下认证用户永不超时。在AD-Scripting配置模式下使用该命令no的形式恢复空闲超时时间的默认值：

```
no idle-timeout
```

拒绝同名用户登录

AD-Scripting的用户同名登录功能为关闭状态时，如果开启拒绝同名用户登录功能，同一用户再次登录的信息会替换掉已登录的信息，系统自动断开已登录的连接。如果关闭拒绝同名用户登录功能，则系统允许同一用户再次登录。在AD-Scripting配置模式下，输入以下命令开启此功能：

- 开启拒绝同名用户登录（默认设置）：**auto-kickout**
- 关闭拒绝同名用户登录：**no auto-kickout**

显示AD Scripting配置信息

在任意模式下，使用以下命令查看AD Scripting配置信息：

```
show user-sso server ad-scripting default
```

查看用户映射信息

查看AD Scripting的用户名和IP映射信息。在任意模式下，使用以下命令：

```
show user-mapping user-sso ad-scripting default
```

查看认证用户表

设备生成的用户认证信息保存在用户认证表。在任意模式下，使用以下命令：

```
show auth-user ad-scripting [interface interface-name] [vrouter vrouter-name]
```

踢出用户映射信息

踢出某指定IP的用户和IP的映射信息。在任意模式下，使用以下命令：

```
exec user-mapping user-sso ad-scripting kickout ip ip-address vrouter vrouter-name
```

AD Polling单点登录

创建AD Polling Profile

创建AD Polling profile并进入AD-Polling配置模式，在全局配置模式下，输入以下命令：

```
user-sso client ad-polling profile-name
```

- *profile-name* - 指定所创建的AD Polling profile的名称。执行该命令后，系统将创建指定名称的AD Polling profile，并进入AD-Polling配置模式；如果指定的名称已存在，则直接进入AD-Polling配置模式。

在全局配置模式下使用该命令的no形式删除指定的AD Polling profile：

```
no user-sso client ad-polling name
```

开启/关闭AD Polling功能

启用AD Polling功能后，系统定时查询并获取AD服务器上的上线用户信息，并定时探测在线用户是否下线。开启AD Polling功能，在AD-Polling配置模式下，使用以下命令：

enable

关闭AD Polling功能，在AD-Polling配置模式下，使用以下命令：

no enable

指定认证服务器

指定域内认证AD服务器，在AD-Polling配置模式下，使用以下命令：

host ip-address [vrouter vrouter-name]

- *ip-address* - 指定域内认证AD服务器的IP地址。此处仅支持AD服务器。指定认证AD服务器后，当域用户从该AD服务器登录时，AD服务器会产生登录日志。
- *vrouter-name* - 指定AD服务器所属的虚拟路由器。

在AD-Polling配置模式下，使用该命令no的形式删除域内认证服务器：

no host

指定AAA服务器

指定系统引用的AAA服务器，在AD-Polling配置模式下，使用以下命令：

aaa-server server-name

- *server-name* - 指定引用的AAA服务器的名称。AAA服务器支持选择Local、AD或者LDAP类型的服务器，建议用户直接选择配置的认证AD服务器。选择AAA服务器后，系统可以在引用的AAA服务器上查询在线用户的用户名对应的用户组和角色信息，从而实现基于用户组和角色的策略控制。

在AD-Polling配置模式下，使用该命令no的形式删除AAA服务器：

no aaa-server

指定账户

指定一个域用户的用户名，用于登录AD服务器。在AD-Polling配置模式下，使用以下命令：

account *username*

- *username* - 指定域用户的用户名。格式为domain\username，范围是1到63个字符。要求该用户具有读取AD服务器上的安全日志的权限，例如AD服务器上权限是Domain Admins的默认用户Administrator。

在AD-Polling配置模式下，使用该命令no的形式删除账户：

no account

指定密码

指定与域用户名对应的密码，在AD-Polling配置模式下，使用以下命令：

password *password*

- *password* - 指定与域用户名对应的密码。范围是1到31个字符。

在AD-Polling配置模式下，使用该命令no的形式删除密码：

no password

指定AD Polling间隔

指定AD Polling定时探测的时间间隔，在AD-Polling配置模式下，使用以下命令：

ad-polling-interval *interval*

- *interval* - 指定AD Polling定时探测的时间间隔。系统每隔时间间隔去AD服务器查询上线用户信息。取值范围为1到3600秒，默认为2秒。为保证获取的用户上线信息的实时性，建议配置2到5秒。

在AD-Polling配置模式下，使用该命令no的形式恢复AD Polling定时探测的时间间隔默认值：

no ad-polling-interval

指定客户端探测间隔

指定客户端定时探测的间隔，在AD-Polling配置模式下，使用以下命令：

client-probing-interval *time*

- *time* – 指定客户端定时探测的时间间隔。系统每隔时间间隔会通过WMI探测已上线用户是否在线，如果探测不到，则踢出用户。取值范围为0到1440分钟，默认为0分钟，即关闭该功能。如果对用户下线要求不高，建议配置较大探测间隔，节省系统性能。

在AD Polling配置模式下，使用该命令no的形式恢复客户端探测时间间隔的默认值：

no client-probing-interval

指定强制超时时间

指定强制下线时间，在AD-Polling配置模式下，使用以下命令：

force-timeout *time*

- *time* - 指定强制下线时间。当用户在线时长超过配置的强制超时时间后，系统会提出用户，强制用户下线。取值范围是0到144000分钟，默认为600分钟。如果设置为0分钟，则关闭该功能。

在AD-Polling配置模式下，使用该命令no的形式恢复强制超时时间的默认值：

no force-timeout

查看AD Polling配置

查看系统所有或者指定名称的AD Polling配置，包括名称、状态、AAA服务器，客户端探测间隔等。在任意模式下，使用以下命令：

show user-sso client ad-polling [*profile-name*]

- *profile-name* – 指定AD Polling profile的名称。此时显示指定AD Polling的配置信息。

查看用户映射信息

查看指定名称的AD Polling的用户名/IP绑定信息。在任意模式下，使用以下命令：

show user-mapping user-sso ad-polling *profile-name*

查看认证用户表

设备生成的用户认证信息保存在用户认证表。在任意模式下，使用以下命令：

```
show auth-user ad-polling [interface interface-name] [vrouter vrouter-name]
```

踢出用户映射信息

踢出某指定IP的用户和IP的映射信息。在任意模式下，使用以下命令：

```
exec user-mapping user-sso ad-polling kickout ip ip-address vrouter vrouter-name
```

SSO Monitor单点登录

创建SSO Monitor Profile

创建SSO Monitor profile并进入SSO-Monitor配置模式，在全局配置模式下，输入以下命令：

```
user-sso client sso-monitor profile-name
```

- *profile-name* - 指定所创建的SSO Monitor profile的名称。执行该命令后，系统将创建指定名称的SSO Monitor profile，并进入SSO-Monitor配置模式；如果指定的SSO Monitor profile名称已存在，则直接进入SSO-Monitor配置模式。

在全局配置模式下使用该命令的no形式删除指定的SSO Monitor profile：

```
no user-sso client sso-monitor name
```

开启/关闭SSO Monitor功能

启用SSO Monitor功能后，系统通过SSO-Monitor协议与第三方认证服务器建立连接并获取用户在线状态及所属用户组信息，并实时更新在线用户的用户名/IP绑定信息。开启SSO Monitor功能，在SSO-Monitor配置模式下，使用以下命令：

```
enable
```

关闭SSO Monitor功能，在SSO-Monitor配置模式下，使用以下命令：

```
no enable
```

指定认证服务器

指定第三方认证服务器，在SSO-Monitor配置模式下，使用以下命令：

```
host ip-address [vrouter vrouter-name]
```

- *ip-address* - 指定第三方认证服务器的名称或者IP地址。第三方自定义认证服务器需要支持SSO-Monitor协议。指定认证服务器后，当用户从该服务器登录时，服务器会保存用户认证信息。
- *vrouter-name* - 指定认证服务器所属的虚拟路由器。

在SSO-Monitor配置模式下，使用该命令no的形式删除第三方认证服务器：

```
no host
```

指定AAA服务器

指定系统引用的AAA服务器，在SSO-Monitor配置模式下，使用以下命令：

```
aaa-server server-name
```

- *server-name* - 指定引用的AAA服务器的名称。AAA服务器支持选择Local、AD或者LDAP类型的服务器。选择AAA服务器后，系统可以在引用的AAA服务器上查询在线用户的用户名对应的用户组和角色信息，从而实现基于用户组和角色的策略控制。

在SSO-Monitor配置模式下，使用该命令no的形式删除AAA服务器：

```
no aaa-server
```

指定端口

指定第三方认证服务器的端口号，系统通过该端口号获取认证用户信息。默认为6666。在SSO-Monitor配置模式下，使用以下命令：

```
port number
```

- *number* - 指定第三方认证服务器的端口号，系统通过该端口号获取认证用户信息。默认为6666，取值范围为1024到65535。

在SSO-Monitor配置模式下，使用该命令no的形式恢复默认端口号：

```
no port
```

指定组织同步模式

指定组织同步模式，在SSO-Monitor配置模式下，使用以下命令：

```
org-source {aaa-server | message}
```


- **aaa-server** – 指定组织同步模式为AAA服务器。系统采用AAA服务器中的用户组织结构作为用户所属组，一般用于第三方认证服务器通过AAA服务器进行认证，且用户组织结构保存在AAA服务器的场景。
- **message** -指定组织同步模式为消息。系统采用认证消息中的用户组作为用户所属组，一般用于第三方认证服务器保存用户组的场景。

默认情况下，组织同步模式为消息。在SSO-Monitor配置模式下，恢复默认情况，使用以下命令

```
no org-source
```

指定重连超时时间

指定连接超时时间，在SSO-Monitor配置模式下，使用以下命令：

```
disconn-del-timeout timeout
```

- *timeout* - 设置连接超时时间。系统和第三方认证服务器超时断开后，系统等待连接超时时间，如果超时时间内仍然连接失败，则删除在线用户。范围是0到1800秒，默认值为300。0表示用户认证信息永不超时。

在SSO Monitor配置模式下，使用该命令no的形式恢复SSO-Monitor重连超时时间为默认值：

```
no disconn-del-timeout
```

查看SSO Monitor配置

查看系统所有或者指定名称的SSO Monitor配置，包括名称、状态、AAA服务器，客户端探测间隔等。在任意模式下，使用以下命令：

```
show user-ss client sso-monitor [profile-name]
```

- *profile-name* – 指定SSO Monitor profile的名称。此时显示指定SSO Monitor的配置信息。

查看用户映射信息

查看SSO Monitor的用户名和IP映射关系。在任意模式下，使用以下命令：

```
show user-mapping user-ss sso-monitor profile-name
```

查看认证用户表

设备生成的用户认证信息保存在认证用户表。在任意模式下，使用以下命令查看认证用户表：

```
show auth-user sso-monitor [interface interface-name] [vrouter vrouter-name]
```

踢出用户映射信息

踢出某指定IP的用户和IP的映射信息。在任意模式下，使用以下命令：

```
exec user-mapping user-sso sso-monitor kickout ip ip-address vrouter vrouter-name
```

TS Agent单点登录

在Windows服务器上安装并运行Hillstone Terminal Service Agent软件。启用TS Agent功能后，当用户通过远程桌面服务登录Windows服务器时，Hillstone Terminal Service Agent为用户分配端口段，并将端口段和用户信息发送给设备，设备创建基于流量IP、端口段和用户的映射信息，实现用户的“免登录”。

使用TS Agent实现单点登录，包含以下两个步骤：

- TS Agent服务器端配置，即在Windows服务器上安装并运行Hillstone Terminal Service Agent。
- TS Agent客户端配置，即在ADC上配置TS Agent功能。



注意：本节主要对如何在ADC上进行TS Agent功能配置及查看的命令进行介绍。在Windows服务器上安装并运行Hillstone Terminal Service Agent软件的方法，请参考[TS Agent单点登录配置举例](#)。

创建TS Agent Profile

创建TS Agent profile并进入TS-Agent配置模式，在全局配置模式下，输入以下命令：

```
user-sso client ts-agent profile-name
```

- *profile-name* - 指定所创建的TS Agent profile的名称。执行该命令后，系统将创建指定名称的TS Agent profile，并进入TS-Agent配置模式；如果指定的TS Agent profile名称已存在，则直接进入TS-Agent配置模式。

在全局配置模式下使用该命令的no形式删除指定的TS Agent profile：

```
no user-sso client ts-agent profile-name
```

开启/关闭TS Agent功能

启用TS Agent功能后，系统与Hillstone Terminal Service Agent建立SSL连接并获取用户及端口段信息，并实时更新在线用户的流量IP、端口段和用户名的映射信息。

开启TS Agent功能，在TS-Agent配置模式下，使用以下命令：

enable

关闭TS Agent功能，在TS-Agent配置模式下，使用以下命令：

no enable

指定TS Agent服务器

指定TS Agent服务器，在TS-Agent配置模式下，使用以下命令：

host {*domain-name* | *ip-address*} [**vrouter** *vrouter-name*]

- *domain-name* | *ip-address* - 指定TS Agent服务器的管理地址，支持域名、IPv4及IPv6地址。
- **vrouter** *vrouter-name* - 指定TS Agent服务器所属的虚拟路由器。

在TS-Agent配置模式下，使用该命令no的形式删除TS Agent服务器：

no host

指定TS Agent服务器端口

指定TS Agent服务器端口号，在TS-Agent配置模式下，使用以下命令：

port *port-number*

- *port-number* - 指定TS Agent服务器的端口号。取值范围为1025到65534，默认值为5019。该端口号必须和Hillstone Terminal Service Agent中设置的监听端口一致，否则无法通信。

在TS-Agent配置模式下，使用该命令no的形式恢复默认端口号：

no port

指定AAA服务器

指定系统引用的AAA服务器，在TS-Agent配置模式下，使用以下命令：

aaa-server *server-name*

- *server-name* - 指定引用的AAA服务器的名称。AAA服务器支持选择Local、AD或者LDAP类型的服务器。选择AAA服务器后，系统可以在引用的AAA服务器上查询在线用户的用户名对应的用户组和角色信息，从而实现基于用户组和角色的策略控制。

在TS-Agent配置模式下，使用该命令no的形式删除AAA服务器：

no aaa-server

指定断开超时时间

指定断开超时时间，在TS-Agent配置模式下，使用以下命令：

disconnection-timeout *timeout*

- *timeout* - 设置断开超时时间。当ADC和Hillstone Terminal Service Agent的连接断开时，如果在指定的断开超时时间内仍然连接失败，则删除在线用户信息。范围是0到1800秒，默认值为300。0表示立即删除在线用户信息。

在TS-Agent配置模式下，使用该命令no的形式恢复断开超时时间为默认值：

no disconnection-timeout

指定流量IP

指定流量IP，在TS-Agent配置模式下，使用以下命令：

traffic-ip *ip-address*

- *ip-address* - 指定流量IP地址，即TS Agent服务器网络接口（网卡）的IP地址。支持IPv4地址和IPv6地址，最多可以指定4个IP地址。

在TS-Agent配置模式下，使用该命令no的形式删除指定的流量IP地址：

no traffic-ip *ip-address*

查看TS Agent配置

查看系统所有或者指定名称的TS Agent配置，包括名称、启用状态、TS Agent服务器、AAA服务器、断开超时时间、流量IP等。在任意模式下，使用以下命令：

`show user-sso client ts-agent [profile-name]`

- *profile-name* – 指定TS Agent profile的名称。此时显示指定TS Agent的配置信息。

查看TS Agent状态信息

查看TS Agent的状态信息，包括连接状态、用户分配端口范围，用户端口段大小，每用户最多端口段，心跳时间间隔、心跳超时时间等。在任意模式下，使用以下命令：

`show user-sso client ts-agent profile-name status`

查看TS Agent用户映射信息

查看TS Agent的用户映射关系。在任意模式下，使用以下命令：

`show user-mapping user-sso ts-agent profile-name`

查看认证用户表

设备生成的用户认证信息保存在认证用户表。在任意模式下，使用以下命令查看认证用户表：

`show auth-user ts-agent [port-range range | vrouter vrouter-name]`

踢出用户映射信息

踢出用户映射信息，支持踢出指定IP和端口范围映射的用户映射信息，以及踢出指定用户名的用户映射信息。在任意模式下，使用以下命令：

`exec user-mapping user-sso ts-agent kickout {ip ip-address vrouter vrouter-name port-range range | username user-name auth-server server-name}`

单点登录配置举例

TS Agent单点登录配置举例

以下为使用TS Agent实现单点登录配置举例。在Windows服务器上安装并运行Hillstone Terminal Service Agent。启用TS Agent功能后，当用户通过远程桌面服务登录Windows服务器时，Hillstone Terminal Service Agent为用户分配端口段，并将端口段和用户信息发送给设备，设备创建基于流量IP、端口段和用户的映射信息，实现用户的“免登录”。

使用TS Agent实现单点登录，包含以下两个步骤：

- TS Agent服务器端配置，即在Windows服务器上安装并运行Hillstone Terminal Service Agent。
- TS Agent客户端配置，即在StoneOS上配置TS Agent功能。

第一步：在Windows服务器上安装并运行Hillstone Terminal Service Agent。

1. 点击链接<http://swupdate.hillstonenet.com:1337/sslvpn/download?os=windows-tsagent>下载Hillstone Terminal Service Agent安装程序。下载完成后，将其拷贝到Windows Server服务器上。



注意:

- 目前支持Windows Server 2008 R2，Windows Server 2016和Windows Server 2019。Windows Server 2008 R2必须装有Windows Server 2008 R2 Service Pack 1以及KB3033929。
- 建议先关闭杀毒软件，再进行Hillstone Terminal Service Agent的安装。

2. 双击Hillstone Terminal Service Agent安装程序HSTSAgent.exe，按照安装向导提示逐步安装直至完成。
3. 双击Hillstone Terminal Service Agent快捷方式，弹出Hillstone Terminal Service Agent对话框。
4. 点击<监听配置>标签页，进行如下配置：
 - 监听地址IPv4：0.0.0.0
 - 监听端口（1025-65534）：5019
 - 心跳时间间隔（1-30秒）：5
 - 心跳超时时间（10-300秒）：60点击“保存”按钮，保存配置。

5. 点击<端口配置>标签页，进行如下配置：

- 用户分配端口范围（1025-65534）：20000-39999
 - 用户端口段大小（20-2000）：200
 - 每用户最多端口段（1-256）：1
 - 用户端口耗尽时允许系统分配端口：勾选
- 点击“保存”按钮，保存配置。

第二步：在StoneOS上配置TS Agent功能。

```
host-name(config)# user-sso client ts-agent tsagent1

host-name(config-ts-agent)# host 10.1.1.1

host-name(config-ts-agent)# aaa-server local

host-name(config-ts-agent)# traffic-ip 10.1.1.1

host-name(config-ts-agent)# enable

host-name(config-ts-agent)# exit

hostname(config)#
```

PKI

PKI（Public Key Infrastructure）即公钥基础设施，是提供公钥加密和数字签名服务的系统，目的是为了自动管理密钥和证书，保证网上数据信息传输的机密性、真实性、完整性和不可否认性。PKI采用证书进行公钥管理，通过第三方的可信任机构，把用户的公钥和用户的其它标识信息捆绑在一起，从而在网上验证用户的身份。一个PKI系统由公钥密码技术（Public Key Cryptography）、证书认证机构（CA）、注册机构（RA）、数字证书（Digital Certificate）和相应的PKI存储库组成。

以下介绍几个PKI相关的术语：

- 公钥密码技术：用户使用公钥密码技术产生密钥对，分别为公钥（public key）和私钥（private key），公钥向外界公开，私钥则自己保留。公钥与私钥互为补充，被一个密钥加密的数据，只可以用相匹配的另外一个密钥解密。
- 认证机构（CA）：是一个向个人、计算机或任何其它实体颁发证书的可信实体。CA受理证书服务申请，根据证书管理策略验证申请方的信息，然后用其私钥对证书进行签名，并颁发该证书给申请方。

- 注册机构（RA）：RA是CA的延伸，RA向CA转发证书服务申请，也向目录服务器转发CA颁发的数字证书和证书撤销列表，以提供目录浏览和查询服务。
- 证书撤销列表（CRL）：证书具有一定的使用期限，但是由于密钥被泄露、业务终止等原因，CA可通过撤销证书缩短证书的使用期限。一个证书一旦被撤销，证书中心就要公布CRL来声明该证书是无效的，并列出不能再使用的证书的序列号。

系统在以下功能模块中可以使用PKI认证方式：

- HTTPS/SSH：使用HTTPS或者SSH方式访问设备时，支持PKI认证。

配置PKI

系统的PKI配置包括：

- 创建和删除PKI密钥对
- 配置PKI信任域
- 配置在线证书状态协议
- 导入CA证书
- 导入密钥
- 导入加密密钥对
- 生成证书服务请求
- 安装本地证书
- 下载证书撤销列表
- 导出和导入PKI信任域
- 导出和导入本地证书
- 证书链

创建和删除PKI密钥对

系统有一个默认PKI密钥对，名为“Default-Key”。创建PKI密钥对，在全局配置模式下，使用以下命令：


```
pki key generate {rsa | dsa | ecc | sm2} [label key-name] [modulus size][ec-group {prime256 | prime384 | prime521}]  
[noconfirm]
```

- **rsa | dsa | ecc** - 指定密钥对的类型，包括RSA、DSA、ECC和SM2。
- **label key-name** - 指定密钥对的名称。该名称在系统中必须是唯一的。如没有指定该参数，系统将选择默认的密钥对Default-Key。
- **modulus size** - 指定密钥对的模长，单位为比特。可选项有1024（系统默认值）、2048、512和768。仅当密钥对类型为RSA或DSA时，该参数有效。
- **ec-group {prime256 | prime384 | prime521}** - 指定椭圆曲线组，包含 P-256、P-384、P-521椭圆曲线。
- **noconfirm** - 禁止关于该密钥对的提示信息。例如，创建的密钥对如果在系统中存在同名密钥对，如果不配置该参数，系统将提示是否覆盖已有同名密钥对，如果配置该参数，系统将直接拒绝创建同名密钥对。另外，用户可以使用命令**pki key zeroize noconfirm**禁止所有密钥对的提示信息。

删除已有的PKI密钥，在全局配置模式下，使用以下命令：

```
pki key zeroize {default | label key-name} [noconfirm]
```

- **default | label key-name** - 指定被删除密钥。**default**为删除系统默认密钥（Default-Key），**label key-name**为删除指定名称的密钥。
- **noconfirm** - 禁止该密钥对的提示信息。

配置PKI信任域

PKI信任域包含申请PKI本地证书所需的配置信息，例如密钥对、证书申请方式以及证书主题内容等。配置PKI信任域，首先需要进入PKI信任域配置模式。进入PKI信任域配置模式，在全局配置模式下使用以下命令：

```
pki trust-domain trust-domain-name
```

- **trust-domain-name** - 指定PKI信任域的名称。执行该命令后，系统生成指定名称的PKI信任域并且进入PKI信任域配置模式；如果指定的名称已存在，则直接进入PKI信任域配置模式。

在全局配置模式下，使用**no pki trust-domain trust-domain-name**命令删除指定的PKI信任域。

进入PKI信任域后，用户可以做以下配置：

- 指定证书获得方法
- 指定密钥对
- 配置主题内容
- 配置证书撤销列表

指定证书获得方法

为PKI信任域指定证书获得方法，在PKI信任域配置模式，使用以下命令：

```
enrollment {self | terminal}
```

- **self** – 使用自签名的获得方法。
- **terminal** – 使用终端（剪切和粘贴）的获得方法。

在PKI信任域配置模式下使用**no enrollment**命令取消证书获得方法的配置。



注意: 该命令没有默认值，因此，用户必须使用该命令指定一个证书获得方法。

指定密钥对

为PKI信任域指定密钥对，在PKI信任域配置模式，使用以下命令：

```
keypair key-name
```

- *key-name* – 指定密钥对的名称。

在PKI信任域配置模式使用**no keypair**命令取消密钥对的指定。

配置主题内容

为PKI信任域配置主题内容，在PKI信任域配置模式，使用以下命令：

- 配置普通名称：**subject commonName** *string*
- 配置国家名称（可选）：**subject country** *string*



注意: 国家名称只能包含两个字符。

- 配置所在位置（可选）：**subject localityName** *string*
- 配置州或省名称（可选）：**subject stateOrProvinceName** *string*
- 配置机构名称（可选）：**subject organization** *string*
- 配置机构单元（可选）：**subject organizationUnit** *string*

使用以上命令no的形式取消相关配置：

- **no subject commonName**
- **no subject country**
- **no subject localityName**
- **no subject stateOrProvinceName**
- **no subject organization**
- **no subject organizationUnit**

配置证书撤销列表

证书撤销列表帮助用户检查一个有效期内证书是否被它的CA撤销。配置CRL的检查方式，在PKI信任域配置模式，使用以下命令：

crl {nocheck | optional | required}

- **nocheck** – 安全设备不检查CRL。该选项为默认选项。
- **optional** – 即使CRL不可用，山石网科设备仍然可以接受对端的认证。
- **required** – 只有CRL可用时，才可以接收对端认证。

另外，用户可以配置获得CRL信息的URL。该配置需要在CRL配置模式下进行。进入CRL配置模式，在PKI信任域配置模式，使用以下命令：

crl configure

在CRL配置模式下，使用以下命令配置获得CRL信息的URL：

url index {url-http | url-ldap [username user-name password password auth-method auth-method]} [vrouter vrouter-name]

- **index** – 为URL指定排序指数。系统最多支持3个URL，并且最先使用指数为1的URL。
- **url-http** – 指定通过HTTP方式获得CRL信息，并指明获得CRL信息的URL。输入的URL必须以“http://”开头，为1到255个字符的字符串。
- **url-ldap** – 指定通过LDAP方式获得CRL信息，并指明获得CRL信息的URL。输入的URL必须以“ldap://”开头，为1到255个字符的字符串。
- **username user-name password password auth-method auth-method** – 指定通过LDAP方式获得CRL信息时的用户名（**username user-name**）、密码（**password password**）和认证方式（**auth-method auth-method**）。如不配置，系统默认通过匿名方式获得CRL信息。
- **username user-name** - 用户名为LDAP服务器的登录DN（通常为LDAP服务器预设的具有查询权限的用户账号）。
- **password password** – 密码为登录DN所对应的密码。
- **auth-method auth-method** -指定LDAP服务器的认证方式，支持明文认证（plain）。
- **vrouter vrouter-name** – 指定获取CRL信息的VRouter。默认为系统缺省VR即trust-vr。

配置在线证书状态协议

在线证书状态协议（Online Certificate Status Protocol，简称为OCSP），其作用与CRL相同，即获得数字证书的撤销状态。与CRL相比，OCSP可实现证书状态的在线查询，具有更强的时效性。CRL和OCSP可以共同配置使用，其中任何一种方法验证证书失败，系统都会判断证书为不可用。

在PKI信任域配置模式下，使用以下命令启用/关闭OCSP证书状态检查功能：

- 启用：**ocsp required**
- 关闭：**ocsp nocheck**

OCSP相关参数配置需要在OCSP配置模式下进行。进入OCSP配置模式，在PKI信任域配置模式下，执行**ocsp configure**命令。OCSP相关配置参数包括：

- 指定OCSP响应器
- 配置OCSP请求随机数
- 指定OCSP响应信息失效时间

指定OCSP响应器

指定OCSP响应器，在OCSP配置模式下，使用以下命令：

url *url*

- *url* – 指定OCSP响应器的URL，以“http://”开头。

使用该命令**no**的形式取消URL的指定，即**no url**。

配置OCSP请求随机数

设备发送OCSP请求时，用户可指定在请求中增加随机数，以此来增强设备与OCSP响应器之间通信的安全性。配置OCSP请求随机数，在OCSP配置模式下，使用以下命令：

- 使用随机数（默认状态）：**nonce enable**
- 不使用随机数：**nonce disable**

指定OCSP响应信息失效时间

系统提供OCSP响应信息缓存功能，用来提高证书认证效率。用户可根据需要指定缓存在设备中的OCSP响应信息的失效时间（失效的响应信息将会被从缓存中清除）。指定失效时间，在OCSP配置模式下，使用以下命令：

response-cache-refresh-interval *time*

- *time* - 指定缓存的OCSP响应信息的失效时间，单位为分钟，取值范围为0到1440。0表示不缓存，即每次获得证书认证请求时，系统都会向OCSP响应器发出请求，询问证书状态；当取值为1到1440之间的任意数值时，缓存的响应信息的失效时间由“当前系统时间+*time*”的时间与响应信息本身的next update时间相比较而得出，哪个时间近，哪个时间即为失效时间。

在OCSP配置模式下，使用**no response-cache-refresh-interval**命令取消失效时间的配置。此时OCSP响应信息的失效时间即为OCSP响应信息自身的next update时间（系统默认状态）。

导入CA证书

导入CA证书，在全局配置模式下，使用以下命令：

pki authenticate *trust-domain-name*

- *trust-domain-name* – 指定PKI信任域的名称。

执行该命令后，系统提示用户将证书内容拷贝到指定的位置，回车后输入句点（.），之后再次敲回车。系统将开始导入CA证书。

导入密钥

导入密钥到PKI信任域，请在全局配置模式下使用以下命令：

```
pki key import {rsa | dsa | ecc | sm2} [label label-name]
```

- **rsa** - 指定导入RSA类型的密钥到PKI。
- **dsa** - 指定导入DSA类型的密钥到PKI。
- **ecc** - 指定导入ECC类型的密钥到PKI。
- **sm2** - 指定导入SM2类型的密钥到PKI。
- **label-name** - 指定密钥对的名称。该名称在系统中必须是唯一的。如没有指定该参数，系统将选择默认的密钥对Default-Key。

导入加密密钥对

用户需在导入时指定签名密钥对用于解密。被导入的加密密钥对是指将签名密钥对用数字信封的方式进行保护。导入国密标准的加密密钥对到PKI信任域，请在执行模式下使用以下命令：

```
import pki key key-name enc-key sig-key-name from {ftp server ip-address [vrouter VR-name] [user user-name password password] file-name | tftp server ip-address [vrouter VR-name] file-name}
```

- **key-name** - 指定导入后的加密密钥对的名字。
- **enc-key** - 指定密钥的类型为国密标准定义的加密密钥类型的。
- **sig-key-name** - 指定用于解密的签名密钥对。
- **ftp | tftp** - 指定上传的方式，通过FTP上传或TFTP上传。
- **server ip-address** - 指定FTP服务器或TFTP服务器的IP地址。
- **vrouter VR-name** - 指定所属VRouter的名称。

- **user** *user-name* **password** *password* – 指定服务器的用户名和密码。
- *file-name* – 指定导入的本地加密密钥对文件名称。

生成证书服务请求

PKI信任域配置完成后，用户需要根据PKI信任域的内容，生成证书服务请求，然后将生成的服务请求发送到CA服务器，申请得到相应的本地证书。生成证书服务请求，在全局配置模式下，使用以下命令：

```
pki enroll trust-domain-name
```

- *trust-domain-name* – 指定PKI信任域的名称，生成相应的证书服务请求。

安装本地证书

从CA服务器获得本地证书后，用户需要将本地证书安装到山石网科设备上。安装本地证书，在全局配置模式下，使用以下命令：

```
pki import trust-domain-name certificate
```

- *trust-domain-name* – 指定PKI信任域的名称，安装相应的本地证书。

执行该命令后，系统提示用户将证书内容拷贝到指定的位置，然后输入句点（.）并敲回车。系统将开始安装证书。

下载证书撤销列表

为PKI信任域下载证书撤销列表（CRL），在全局配置模式下，使用以下命令：

```
pki crl request trust-domain-name
```

- *trust-domain-name* – 指定PKI信任域的名称。系统将根据PKI信任域中的CRL配置地址下载当前的证书撤销列表。

导出和导入PKI信任域信息

为简化配置，用户可以将PKI信任域的证书（CA证书和本地证书）以及本地证书对应的私钥信息以PKSC12格式一并从一台设备上导出，然后再一并导入到另外一台设备。

导出PKI信任域信息

导出PKI信任域信息，在全局配置模式下，使用以下命令：

```
pki export trust-domain trust-domain-name pkcs12 pass-phrase
```

- *trust-domain-name* – 指定PKI信任域的名称。
- *pass-phrase* – 指定用于解密PKCS12数据的密码。

用户还可以通过命令行导出文件类型的PKI信任域信息到FTP服务器、TFTP服务器。

导出PKI信任域信息到FTP服务器，在执行模式下使用以下命令：

```
export pki trust-domain trust-domain-name pkcs12 password to ftp server ip-address [user user-name password password word [file-name] | file-name]
```

- *trust-domain-name* – 指定PKI信任域的名称。
- **pkcs12** *password* – 指定私钥保护口令，用于解密私钥。
- *ip-address* – 指定FTP服务器的IP地址。
- **user** *user-name* **password** *password* – 指定FTP服务器的用户名和密码。
- *file-name* – 指定导出的PKI信任域信息的文件名称。

导出PKI信任域信息到TFTP服务器，在执行模式下使用以下命令：

```
export pkitrust-domain trust-domain-name pkcs12 password to tftp server ip-address [file-name]
```

导入PKI信任域信息

导入PKI信任域信息，在全局配置模式下，使用以下命令：

```
pki import trust-domain trust-domain-name pkcs12 pass-phrase
```

- *trust-domain-name* – 指定PKI信任域的名称。
- *pass-phrase* – 指定用于解密PKCS12数据的密码。

执行该命令后，系统提示用户将PKI信任域信息内容拷贝到指定的位置，回车后输入句点（.），之后再次敲回车。系统将开始导入PKI信任域信息。

用户还可以通过命令行，导入文件类型的PKI信任域信息。导入的方式包括通过FTP和TFTP服务器导入。

从FTP服务器导入PKI信任域信息，在执行模式下使用以下命令：

```
import pki trust-domain trust-domain-name pkcs12 password from ftp server ip-address {user user-name password password file-name | file-name}
```

- *trust-domain-name* – 指定PKI信任域的名称。
- *pkcs12 password* – 指定私钥保护口令，用于解密私钥。
- *ip-address* – 指定FTP服务器的IP地址。
- *user user-name password password file-name* – 指定FTP服务器的用户名和密码，以及导出的PKI信任域信息的文件名称。
- *file-name* – 指定导入的PKI信任域信息的文件名称。

从TFTP服务器导入PKI信任域信息，在执行模式下使用以下命令：

```
import pki trust-domain trust-domain-name pkcs12 password from tftp server ip-address file-name
```

证书链

对于包含多级证书的PKCS#7、PKCS#12文件、CERT-BUNDLE文件，用户可将其导入系统，然后将其与密钥对文件组合使用，创建成一条证书链。创建完成的证书链可直接被其他功能引用，如SSL模板。用户也可将证书链导出，便于在另一台设备上导入并使用。

创建证书链

创建证书链，在全局配置模式下，使用以下命令：

```
pki cert-chain chain-name
```

- *chain-name* - 指定证书链的名称。执行该命令后，系统生成指定名称的证书链并且进入证书链配置模式；如果指定的名称已存在，则直接进入证书链配置模式。

在全局配置模式下，使用`no pki cert-chain chain-name`命令删除指定的证书链。

导出证书链

导出证书链，在全局配置模式下，使用以下命令：

```
pki export cert-chain chain-name
```

- *chain-name* - 指定证书链的名称。

用户还可以通过命令行，导出文件类型的证书链到FTP服务器、TFTP服务器。

导出证书链到FTP服务器，在执行模式下，使用以下命令：

```
export pki cert-chain chain-name { pkcs7 | pkcs12-der password | cert-bundle } to ftp server ip-address [vrouter VR-name] [user user-name password password [file-name] | file-name]
```

- *chain-name* - 指定证书链的名称。
- **pkcs7** - 指定导出的证书链文件为PKCS#7格式。
- **pkcs12-der** *password* - 指定导出的证书链文件为PKCS#12格式，并指定私钥保护口令，用于解密私钥。
- **cert-bundle** - 指定导出的证书链文件为CERT-BUNDLE格式，即PEM编码的多个证书串联证书链。系统允许导入的证书链不完整但需连续，例如完整的证书链为TerCert<-MidCACert<-RootCACert，导入的文件允许仅包含TerCert<-MidCACert两种即可，但不支持仅包含TerCert和RootCACert的情况。此外，系统支持证书链乱序，即只要链式关系完整，证书链可被正确解析。
- *ip-address* - 指定FTP服务器的IP地址。
- **vrouter** *VR-name* - 指定所属VRouter的名称。
- **user** *user-name* **password** *password* *file-name* - 指定FTP服务器的用户名和密码，以及导出的证书链的文件名称。
- *file-name* - 指定导出的证书链的文件名称。

导出证书链到TFTP服务器，在执行模式下使用以下命令：

```
export pki cert-chain chain-name { pkcs7 | pkcs12-der password | cert-bundle } password to tftp server ip-address [vrouter VR-name [file-name] | file-name]
```

导入证书链

导入证书链，在全局配置模式下，使用以下命令：

```
pki import cert-chain chain-name
```

- *chain-name* - 指定证书链的名称。

执行该命令后，系统提示用户将证书链信息内容拷贝到指定的位置，回车后输入句点（.），之后再次敲回车。系统将开始导入证书链信息。

用户还可以通过命令行，导入文件类型的证书链。导入的方式包括通过FTP和TFTP服务器。

从FTP服务器导入证书链，在执行模式下使用以下命令：

```
import pki cert-chain chain-name { pkcs7 | pkcs12-der password | cert-bundle } from ftp server ip-address [vrrouter VR-name] {user user-name password password [file-name] | file-name}
```

- *chain-name* – 指定证书链的名称。
- **pkcs7** – 指定导入的证书链文件为PKCS#7格式。
- **pkcs12-der password** – 指定导入的证书链文件为PKCS#12格式，并指定私钥保护口令，用于解密私钥。
- **cert-bundle** - 指定导入的证书链文件为CERT-BUNDLE格式，即PEM编码的多个证书串联证书链。系统允许导入的证书链不完整但需连续，例如完整的证书链为TerCert<-MidCACert<-RootCACert，导入的文件允许仅包含TerCert<-MidCACert两种即可，但不支持仅包含TerCert和RootCACert的情况。此外，系统支持证书链乱序，即只要链式关系完整，证书链可被正确解析。
- *ip-address* – 指定FTP服务器的IP地址。
- **vrrouter VR-name** - 指定所属VRouter的名称。
- **user user-name password password file-name** – 指定FTP服务器的用户名和密码，以及导入的证书链的文件名称。
- *file-name* – 指定导入的证书链的文件名称。

从TFTP服务器导入证书链，在执行模式下使用以下命令：

```
import pki cert-chain chain-name { pkcs7 | pkcs12-der password | cert-bundle } from tftp server ip-address {vrrouter VR-name file-name | file-name}
```

显示证书链配置信息

显示证书链的配置信息，在任何模式下，使用以下命令：

```
show pki cert-chain [chain-name]
```

- *chain-name* – 显示指定名称的证书链的配置信息。如果不指定该参数，则显示系统中所有证书链的配置信息。

重新自签名

对于自签名证书，系统将提供一个刷新方法，使用户可以重新自签名。

系统规定自签名证书的有效期为10年，用户可以在全局配置模式下使用以下命令刷新自签名证书，重新自签名：

```
pki refresh trust-domain-name
```

- *trust-domain-name* – 指定PKI信任域的名称。

显示PKI配置信息

用户可以随时使用show命令显示PKI的配置信息。显示密钥对的配置信息，在任何模式下，使用以下命令：

```
show pki key [label key-name]
```

- *label key-name* – 显示指定名称的密钥对配置信息。如果不指定该参数值，则显示系统中所有密钥对的配置信息。

显示PKI信任域的配置信息，在任何模式下，使用以下命令：

```
show pki trust-domain [trust-domain-name]
```

- *trust-domain-name* – 显示指定名称的PKI信任域的配置信息。如果不指定该参数，则显示系统中所有PKI信任域的配置信息。

第8章 对象

对象相关配置包括如下：

- [命名规则](#)
- [地址簿](#)
- [服务簿](#)
- [域名簿](#)
- [时间表](#)
- [用户与角色](#)
- [监测对象](#)

命名规则

为不同的对象命名时，请遵循以下规则：

- 系统不建议使用以下特殊符号：逗号（,）、单引号（'）、双引号（"）、制表符、空格、分号（;）、反斜杠（\）、斜杠（/）、尖括号（<>）、特殊字符（&、#）。为避免产生错误，建议用户尽量使用数字（0-9）和字母（a-z，A-Z）组成对象名称。
- 使用CLI创建对象时，如果对象名称中包含空格，请用双引号引住对象名称。在WebUI上创建带空格名称的对象时则无此限制，可直接输入对象名称。

地址簿

IP地址是多个功能模块配置的重要组成元素，例如策略规则、网络地址转换规则以及会话数限制等。因此，为方便引用IP地址，实现灵活配置，设备支持地址簿功能。用户可以给一个IP地址范围指定一个名称，在配置时，只需引用该名称。而地址簿就是系统中用来储存IP地址范围与其名称的对应关系的数据库。地址簿中的IP地址与名称的对应关系条目被称作地址条目。

地址条目

设备拥有一个全局地址簿。用户需要为全局地址簿定义地址条目。在定义地址条目时，DNS名称可以直接用来代替IP地址范围。已经配置好IP地址的接口也会作为地址条目自动添加到地址簿中，方便用户做NAT时使用。地址条目还具有以下特点：

- 地址簿中有一条默认条目“Any”和“private_network”。“Any”对应的IP地址是0.0.0.0/0，也就是代表所有IP地址。“private_network”对应的IP地址成员有10.0.0.0/8、172.16.0.0/12、192.168.0.0/16，代表所有私网地址。
“Any”不可以编辑也不可以被删除。“private_network”可以编辑或删除。
- 一条地址条目中可以包含地址簿中另外的地址条目。
- 如果地址条目的IP地址范围发生了变化，系统会自动更新其它引用了该地址条目的模块。

配置地址簿

用户可以通过CLI对地址簿进行以下配置：

- 添加或者删除地址条目
- 指定地址条目的IP地址范围
- 查看地址簿信息

添加或者删除地址条目

在全局配置模式，使用**address**命令向地址簿中添加一个地址条目，同时进入地址配置模式：

```
address address-entry
```

- *address-entry* - 指定要添加的地址条目的名称。

使用该命令**no**的形式将地址条目从地址簿中删除：

```
no address address-entry
```



注意：已经被其它模块或者其它地址条目引用的地址条目不能被删除。

指定地址条目的IP地址范围

在系统中，地址条目的IP地址范围是其成员IP地址范围的总和。地址条目成员有以下几种：

- IP地址：包括两种类型，一种为“IP地址/子网掩码”，如10.100.2.0/24；另一种为“IP地址 通配符掩码”，如192.168.0.1 255.255.0.255
- 精确域名，如host1.hillstonenet.com，或含有通配符的域名，如*.baidu.com
- IP地址段，如10.100.2.3 – 10.100.2.100
- 国家/地区：某一国家或地区的IP地址的集合。
- 其它地址条目

在地址配置模式下，使用**ip**命令来为地址条目添加指定IP地址范围成员。用该命令**no**的形式删除指定成员。

```
ip {ip-address {netmask | wildcardmask} | ip/netmask}
```

- *ip-address* – 指定IP成员的IP地址。
- *netmask* | *wildcardmask* – 指定子网掩码（*netmask*）或者通配符掩码（*wildcardmask*）。系统不支持掩码转换为二进制后，其位数里从右往左第一个“1”左边的“0”的个数超过8个的通配符掩码（“0”可以连续也可以不连续），比如255.0.0.255是无效的通配符掩码；255.0.255.0和255.32.255.0等都为有效的通配符掩码。
- *ip/netmask* – 指定IP成员的IP地址和网络掩码。

```
no ip {ip-address {netmask | wildcardmask} | ip/netmask}
```

在地址配置模式下，用**host**命令来为地址条目添加域名成员。用该命令**no**的形式删除指定成员。

```
host host-name [vrouter vrouter-name]
```

- *host-name* – 指定精确域名或通配符域名名称，名称范围是1到255个字符。用户最多可配置1024个精确域名。在不同AX设备上，用户可配置的通配符域名数限制不同，具体如下。

设备型号	可配置的通配符域名数
SG-6000-AX02	256
SG-6000-AX04、SG-6000-AX08、SG-6000-AX500	512
SG-6000-AX1000/1000S	1024
SG-6000-AX2000/2000S、SG-6000-AX4060/4060S	2048

- *vrouter-name* -指定域名所属的VRouter。

no host *host-name* [**vrouter** *vrouter-name*]

在地址配置模式下，用**range**命令来为地址条目添加IP地址段成员。用该命令**no**的形式删除指定成员。

- **range** *min-ip* [*max-ip*]
- **no range** *min-ip* [*max-ip*]

在地址配置模式下，用**country**命令为地址条目添加某一国家或地区的IP地址的集合。用该命令**no**的形式删除指定成员。

- **country** *country-name*
- **no country** *country-name*

*country-name*的可选值，可通过在**country**关键字后使用TAB键进行查看。

在地址配置模式下，用**member**命令为地址条目添加另一地址条目。用该命令**no**的形式删除指定条目。

- **member** *address-entry*
- **no member** *address-entry*

在配置地址簿时，请注意如下事项：

- “国家/地区”成员仅在IPv4地址簿中支持。
- 添加了“国家/地区”成员的地址簿，仅可以被策略规则和策略路由规则引用。
- 添加了“国家/地区”成员的地址簿，不支持排除地址成员配置。

指定排除地址条目成员

系统的地址簿中同时支持IPv4和IPv6的地址条目，用户可以通过配置排除地址功能，将个别IPv4地址条目成员从地址簿中排除。可以排除的IPv4地址条目成员有以下2种：

- IP地址：IPv4地址包括两种类型，一种为“IP地址/子网掩码”，如10.100.2.0/24；另一种为“IP地址 通配符掩码”，如192.168.0.1 255.255.0.255；
- IP地址段，如10.100.2.3 - 10.100.2.100



注意：每个地址簿能够配置的排除地址条目成员有限，最多占地址条目成员最大值的10%。

指定排除IPv4地址条目成员

为IPv4地址条目排除IP地址范围成员，在地址配置模式下，使用以下命令：

```
exclude ip ip-address {netmask | wildcardmask}
```

- *ip-address* - 指定排除IPv4地址条目成员的IP地址。
- *netmask* | *wildcardmask* - 指定子网掩码（*netmask*）或者通配符掩码（*wildcardmask*）。系统不支持掩码转换为二进制后，其位数里从右往左第一个“1”左边的“0”的个数超过8个的通配符掩码（“0”可以连续也可以不连续），比如255.0.0.255是无效的通配符掩码；255.0.255.0和255.32.255.0等都为有效的通配符掩码。

使用**no exclude ip** *ip-address* {*netmask* | *wildcardmask*} 恢复排除的IP地址范围成员。

为IPv4地址条目排除IP地址段成员，在地址配置模式下，使用以下命令：

```
exclude range min-ip max-ip
```

- *min-ip max-ip* - 指定IP地址范围的两个IP地址。

使用**no exclude range** *min-ip max-ip*恢复排除的IP地址段成员。

重新命名地址条目

在地址配置模式下，使用**rename**命令来重新命名已创建的地址条目：

```
rename name
```

- *name* - 指定新的地址条目名称。如果出现重名，该命令会失效。

查看地址条目关联项

在系统中，地址条目可以被其他功能模块引用，比如策略规则、网络地址转换规则以及会话数限制等。用户可以在任何模式下查看地址条目被系统其它功能模块引用的情况，即地址条目的关联项。命令如下：

```
show reference address address-entry
```

- *address-entry* - 显示指定地址条目的关联项。

查看地址簿信息

用户可以在任何模式下使用以下命令查看全局地址簿的具体信息，包括地址簿内地址条目的名称、地址条目的成员数以及成员的具体内容。命令如下：

```
show address [filter-ip A.B.C.D [filter-unreferenced]] | [address-entry] | [filter-unreferenced]
```

- **show address** - 显示地址簿内所有地址条目的具体信息。
- **filter-ip A.B.C.D** - 显示包含有指定IP地址的地址条目信息。
- *address-entry* - 显示指定地址条目的具体信息。
- **filter-unreferenced** - 显示未被系统其它功能模块引用的地址条目信息。

用户可以在任何模式下使用以下命令查看指定IP地址所在的国家或地区。命令如下：

```
show country ip A.B.C.D
```

- *A.B.C.D* - 输入待查询IP地址。

服务簿

服务（Service）是具有协议标准的信息流。服务具有一定的特征，例如相应的协议、端口号等，举例来讲，FTP服务使用TCP传输协议，其目的端口号是21。服务是多个功能模块配置的重要组成元素，例如网络地址转换规则等。

设备提供多种预定义服务、预定义服务组，同时用户也可以根据自己的需要自定义服务、自定义服务组。设备用服务簿来储存和管理这些服务和组。

通过CLI查看服务信息

用户可以在任何模式下通过使用**show service**命令查看到所有服务的信息，包括预定义服务/用户自定义服务的名称、协议、目的端口、源端口、超时时间信息以及未被系统其它功能模块引用的服务信息。该命令的使用方法为：

```
show service {predefined | userdefined | name service-name | unreferenced}
```

- **predefined** – 指定显示预定义服务信息。
- **userdefined** – 指定显示用户自定义服务信息。
- **name service-name** - 指定显示某个服务信息。
- **unreferenced** - 显示未被系统其它功能模块引用的服务信息。

查看TCP或者UDP协议类型对应的服务信息，在任何模式下，使用以下命令：

```
show service protocol {tcp | udp} [dst-port {port-number | range min-port max-port}] [src-port {port-number | range min-port max-port}]
```

- **tcp | udp** – 指定显示TCP或者UDP协议类型的服务信息。
- **dst-port {port-number | range min-port max-port}** – 显示指定目的端口号的服务信息。*port-number*为单一目的端口号，如果目的端口号为一个范围，*min-port*为最小目的端口号，*max-port*为最大目的端口号，范围是0到65535。
- **src-port {port-number | range min-port max-port}** - 显示指定源端口号的服务信息。*port-number*为单一源端口号，如果源端口号为一个范围，*min-port*为最小源端口号，*max-port*为最大源端口号，范围是0到65535。

查看ICMP或者ICMPv6协议类型对应的服务信息，在任何模式下，使用以下命令：

```
show service protocol {icmp | icmpv6} [type type-number [code {code-number | range min-code max-code}]]
```

- **icmp | icmpv6** – 指定显示ICMP或者ICMPv6协议类型的服务信息。
- **type type-number** – 显示指定ICMP type值或者ICMPv6 type值的的服务信息。

- **code** {*code-number* | **range** *min-code max-code*} - 显示指定ICMP code值或者ICMPv6 code值的服务信息。
*code-number*为单一code值，如果code值为一个范围，*min-code*为最小code值，*max-code*为最大code值，Code值取值范围为0到255。

查看其他指定协议类型对应的服务信息，在任何模式下，使用以下命令：

show service protocol *protocol-number*

- *protocol-number* - 显示指定协议号的服务信息。取值范围为1到255。

用户可以在任何模式下通过使用以下命令查看所有服务组的信息，包括预定义服务组、用户自定义服务组以及未被系统其它功能模块引用的服务组信息等。该命令的使用方法为：

show servgroup [**predefined** | **userdefined** | **name** *servicegroup-name* | **unreferenced**]

- **predefined** - 指定显示预定义服务组信息。
- **userdefined** - 指定显示用户自定义服务组信息。
- **name** *servicegroup-name* - 指定显示某个服务组信息。
- **unreferenced** - 显示未被系统其它功能模块引用的服务组信息。

查看服务关联项

在系统中，服务可以被其他功能模块引用，比如网络地址转换规则等。用户可以在任何模式下查看服务或者服务组被系统其它功能模块引用的情况，即服务或者服务组的关联项。命令如下：

show reference service *service-name*

- *service-name* - 显示指定服务或者服务组的关联项。

预定义服务（Predefined Services）

系统提供百余种预定义服务。使用以上**show**命令或者通过WebUI页面可以查看当前版本支持的所有预定义服务。

以下介绍几个常见的预定义服务。

远程Shell (RSH)

RSH ALG (Remote Shell) 允许被认证的用户在远程主机上运行shell命令。设备支持透明模式、路由模式和NAT模式的RSH服务。

Sun远程程序调用 (Sun RPC)

Sun RPC (Sun Remote Procedure Call) 提供了一种方法能够使一台主机上运行的程序调用另一台主机正在运行的程序的过程。因为RPC服务数量众多，并且有广播的需要，RPC服务的传输地址是基于服务程序的数量和版本而动态协商的。人们会定义一些绑定的协议将RPC程序数量和版本映射到传输地址。

设备支持Sun RPC预定义服务，使用户能够根据所配置的策略允许或者拒绝流量。用户可以定义一条设备策略来允许或者拒绝所有RPC请求。例如，需要使用网络文件系统 (NFS)，请通过策略规则允许SunRPC服务。

微软远程过程调用 (MS RPC)

微软远程过程调用应用层网关是微软对分布式计算环境RPC的实现。MS RPC提供一种方法，使一台主机上运行的程序能够调用另一台主机上正在运行的程序过程。因为RPC服务数量众多，并且有广播的需求，RPC的传输地址将基于服务程序的UUID (Universal Unique Identifier) 进行动态协商。

设备支持MS RPC预定义服务，使用户能够根据所配置的策略允许或者拒绝流量。用户可以定义一条策略来允许或者拒绝所有的RPC请求。例如，需要使用Outlook/Exchange交互或者MSQueue服务，请通过策略规则允许MSRPC服务。

修改预定义服务超时时间

在全局配置模式下，使用**service service - name**命令，可以进入指定的服务配置模式。用户可以在该模式下对预定义服务的超时时间进行修改。

- 修改预定义服务ICMP的超时时间，在服务配置模式下输入以下命令：

```
icmp type any code any timeout timeout-value
```

- 修改预定义服务PING的的超时时间，在PING服务配置模式下输入以下命令：

```
icmp type 8 code 0 timeout timeout-value
```

- 修改其它预定义服务（TCP或者UDP类型）的超时时间，在相应服务的配置模式输入以下命令：

{tcp | udp} dst-port min-port [max-port] [src-port min-port [max-port]] timeout timeout-value

使用以上命令时，输入的协议类型（TCP或者UDP）、目标端口号（dst-port）和源端口号（src-port）必须与被修改的服务相一致；如果源端口号为any，则src-port一项可以省略。例如，修改预定义服务FTP的超时值的命令为：**tcp dst-port 21 timeout 30**

预定义服务组

预定义服务组中包含相关的预定义服务，可方便用户配置。系统提供10余种预定义服务组。其中，包含动态识别预定义服务的预定义服务组为动态识别预定义服务组，需要与其它服务组区分开单独配置。通过特征库更新动态识别预定义服务时，也将同时更新动态识别预定义服务组。用户可以查看和使用预定义服务组，但是不能编辑和删除预定义服务组。

查看预定义服务组，在任何模式下，使用以下命令：

show predefined-servgroup

用户自定义服务

除了使用系统提供的预定义服务以外，用户还可以很容易地创建自己的自定义服务。用户自定义服务可包含最多8条服务条目。用户需指定的自定义服务条目的参数包括：

- 名称
- 传输协议
- TCP或UDP类型服务的源和目标端口号或者ICMP类型服务的type和code值
- 超时时间
- 应用类型

创建和删除自定义服务

在CLI中创建一个服务并将其添加到服务簿，请在全局配置模式下使用以下命令，并且用该命令no的形式删除一个服务：

service service-name

no service service-name

- *service-name* – 指定自定义服务的名称。长度范围是1至31个字符。该名称在整个系统中必须是唯一的。运行命令后，CLI进入所创建服务的配置模式。

为自定义服务添加和删除自定义服务条目

每一个自定义服务可最多包含八个服务条目。根据服务条目的协议类型的不同，添加服务条目所使用的命令也不同。

添加TCP或者UDP类型服务条目，在服务配置模式下输入以下命令：

```
{tcp | udp} dst-port min-port [max-port] [src-port min-port [max-port]] [timeout time-out-value | timeout-day time-out-value]
```

- **dst-port min-port [max-port]** – 指定自定义服务的目的端口号。如果目的端口号为一个范围，*min-port*为最小目的端口号，*max-port*为最大目的端口号。目的端口号的范围是0到65535，并且目的端口号不能为单一的0，例如，目的端口号可以是0到20，但是不能仅为0。
- **src-port min-port [max-port]** – 指定自定义服务的源端口号。如果源端口号为一个范围，*min-port*为最小源端口号，*max-port*为最大源端口号。源端口号的范围是0到65535。
- **timeout time-out-value** – 指定超时时间。取值范围1-65535。单位为秒。
- **timeout-day time-out-value** – 指定长连接的超时时间。取值范围1-1000。单位为天。如需配置长连接超时时间，需要在全局配置模式下开启longlife-sess-percent。

添加ICMP类型服务条目，在服务配置模式下输入以下命令：

```
icmp type type-value [code min-code [max-code]] [timeout time-out-value | timeout-day time-out-value]
```

- *type-value* – 指定自定义服务的ICMP type值。范围是3（Destination-Unreachable）、4（Source Quench）、5（Redirect）、8（Echo）、11（Time Exceeded）、12（Parameter Problem）、13（Timestamp）和15（Information）以及any（表示以上所有type值）。
- **code min-code [max-code]** – 指定自定义服务的ICMP code值。范围是0到5。默认值是“0-5”。
- **timeout time-out-value** – 指定超时时间。取值范围1-65535。单位为秒。
- **timeout-day time-out-value** – 指定长连接的超时时间。取值范围1-1000。单位为天。如需配置长连接超时时间，需要在全局配置模式下开启longlife-sess-percent。

添加其它类型服务条目，在服务配置模式下输入以下命令：

protocol *protocol-number* [**timeout** *time-out-value* | **timeout-day** *time-out-value*]

- *protocol-number* – 指定自定义服务的协议号。范围是1到255。
- **timeout** *time-out-value* – 指定超时时间。取值范围1-65535。单位为秒。
- **timeout-day** *time-out-value* – 指定长连接的超时时间。取值范围1-1000。单位为天。如需配置长连接超时时间，需要在全局配置模式下开启 *longlife-sess-percent*。

使用以上三条命令 **no** 的形式可以删除服务条目。并且已经创建的服务条目不能修改只能删除。

- **no** {**tcp** | **udp**} **dst-port** *min-port* [*max-port*] [**src-port** *min-port* [*max-port*]]
- **no icmp type** *type-value* [**code** *min-code* [*max-code*]]
- **no protocol** *protocol-number*

重命名自定义服务

为已创建的自定义服务重命名，在服务配置模式下，使用以下命令：

rename *new-name*

- *new-name* – 指定自定义服务的新名称。

用户还可以在全局配置模式下，使用以下命令为指定的自定义服务重命名。

rename service *old-name* *new-name*

- *old-name* – 指定自定义服务的旧名称。
- *new-name* – 指定自定义服务的新名称。

服务组 (Service Group)

用户将一些服务组织到一起便组成了服务组。用户可以直接将服务组应用到设备策略中，这样便简化了管理。系统服务组有以下特征：

- 服务簿中的每一条服务都可以被一个或多个服务组引用。
- 每个服务组中既可以包含预定义服务，也可以包含用户自定义服务。
- 服务组可以包含服务组。系统的服务组支持8层嵌套。

服务组还有以下限制：

- 服务组名称与服务名称不能相同。
- 被策略引用的服务组不能被删除。如果要删除一个服务组，必须首先从其它模块中删除对该服务组的引用。
- 如果用户从服务簿中删除了一条用户自定义服务，该条服务也将会从所有引用它的服务组中被删除。

创建和删除服务组

在CLI中创建一个服务组并将该组添加到服务簿中，请在全局配置模式下，输入以下命令：

```
servgroup servicegroup-name
```



注意：服务组的名称必须是唯一的。

运行该命令后，系统进入服务组配置模式。

删除一个服务组，请在全局配置模式下，输入以下命令：

```
no servgroup servicegroup-name
```

为服务组添加和删除服务或者服务组

服务组的成员可以是一条服务，也可以是一个服务组。在CLI中为服务组添加或者删除服务，请在服务组配置模式输入以下命令：

```
service {service-name | servicegroup-name}
```

```
no service {service-name | servicegroup-name}
```

为服务组添加服务或者服务组时，请注意以下两点：

- 服务组中的服务必须是唯一的。
- 每个服务组最多可以包含64条服务；服务组与服务组之间最多可以嵌套8层。

为服务或者服务组添加/删除描述信息

在CLI的服务或服务组配置模式下，用户可以通过使用以下命令为服务或服务组添加描述信息。

description *description*

- *description* – 指定服务或服务组的描述信息。范围是1到255字节。

在CLI的服务或服务组配置模式下，使用以下命令删除服务或服务组的描述信息。

no description

域名簿

用户可以将一个域名或多个域名的集合指定一个名称，在配置时，只需引用该名称。域名簿(Host book)就是系统中用来存储域名集合与其名称的对应关系的数据库。域名簿中的域名与名称的对应关系条目被称作域名条目 (Host entry)。

需要注意的是：

- 域名条目个数的最大值为地址条目个数最大值的四分之一。
- 每条策略路由规则只可以配置一个域名条目。

用户可以通过CLI对域名簿进行以下配置：

- 添加或者删除域名条目
- 指定域名条目的域名范围
- 查看域名簿信息

添加或者删除域名条目

在全局配置模式，使用**host-book**命令向域名簿中添加一个域名条目，同时进入域名配置模式：

host-book *host-book-entry*

- *host-book-entry* – 指定要添加的域名条目的名称。

使用该命令no的形式将域名条目从域名簿中删除：

no host-book *host-book-entry*

指定域名条目的域名范围

在系统中，域名条目的域名范围是其成员域名范围的总和。域名条目成员有以下几种：

- 域名：系统支持一级域名，例如：baidu.com。可使用通配符，例如：*baid*。
- IP地址：指定IP地址，例如：61.155.169.229。

在域名配置模式下，使用**host**命令来为域名条目添加成员。

host *host-name*

- *host-name* – 指定域名或IP地址。系统支持同时添加多个成员，各成员之间用“;” 隔开。

用该命令**no**的形式删除指定成员。

no host *host-name*

查看域名簿信息

用户可以在任何模式下使用以下命令查看域名簿的具体信息，包括域名簿内域名条目的名称、域名条目的成员数以及成员的具体内容。命令如下：

show host-book [*host-book-entry*]

- **show host-book** – 显示域名簿内所有域名条目的具体信息。
- *host-book-entry* – 显示指定域名条目的具体信息。

时间表

设备支持时间表（Schedule）功能。时间表功能可以使策略规则在指定的时间生效，也可以控制PPPoE接口与因特网的连接时间。时间表包含绝对计划和周期计划。周期计划通过周期条目指定时间表的时间点或者时间段；而绝对计划决定周期计划的生效时间。每个周期计划最多可以拥有16条周期条目。

创建时间表

创建一个时间表，在全局配置模式下，使用以下命令：

schedule *schedule-name*

- *schedule-name* – 指定时间表的名称。范围是1到31个字符。

执行该命令后，系统创建指定名称的时间表并且进入时间表配置模式；如果指定的名称已存在，则直接进入时间表配置模式。在时间表配置模式下，用户可以配置时间表的周期和绝对时间。

使用**no schedule** *schedule-name*命令删除指定的时间表。删除时间表之前，请从其它模块中取消对该时间表的引用。

指定绝对计划

绝对计划是一个时间范围，指定的周期计划会在绝对计划的时间范围内生效。同时，用户也可以不启用绝对计划功能，此时周期计划会在被应用到系统中某项功能上时，立即生效。指定绝对计划，在时间表配置模式下，使用以下命令：

absolute {[**start** *start-date start-time*] [**end** *end-date end-time*]}

- **start** *start-date start-time* – 指定绝对计划的开始时间点，包括日期和具体时间。*start-date*为开始的日期，书写格式为“月/日/年”，例如10/23/2007；*start-time*为开始的具体时间，书写格式为“小时：分钟：秒钟”，例如15：30：20。如果不指定该参数的值，开始时间为当前时间。
- **end** *end-date end-time* – 指定绝对计划的结束时间点，包括日期和具体时间。*end-date*为结束的日期，书写格式为“月/日/年”，例如11/05/2007；*end-time*为结束的具体时间，书写格式为“小时：分钟：秒钟”，例如09：00：07。如果不指定该参数的值，则无结束时间，周期会从开始时间起，一直有效。

使用**no absolute**命令关闭绝对计划功能，使周期计划能够即时生效。

指定周期计划

周期计划的时间是该周期计划中周期条目的总和。一个周期计划中最多可以添加16个条周期条目。用户可以配置三种类型的周期条目：

- 每天：每天的指定时间。例如每天的9：00：30到18：00:20。
- 每周的某几天：一周中指定天的指定时间。例如每周一、周二和周六的9：00：00到13：30：45。
- 每周一段时间：一周中的一个连续时间段。例如从周一早上9：30：15到周三下午15：00：55。

指定“每天”或者“每周的某几天”类型周期条目，在时间表配置模式下，使用以下命令：

periodic {**daily** | **weekdays** | **weekend** | [**monday**] [...] [**sunday**] } *start-time to end-time*

- **daily** – 每一天（周一到周日）。
- **weekdays** – 工作日（周一到周五）。
- **weekend** – 周末（周六到周日）。
- **[monday] [...] [sunday]** – 选择需要的日期。例如选择周二、周三和周六，命令关键字为 `tuesday wednesday saturday`。
- *start-time* – 开始时间。书写格式为“小时：分钟”，例如09：00：15。
- *end-time* – 结束时间。书写格式为“小时：分钟”，例如16：30：30。

使用多条该命令添加多个“每天”或者“每周的某几天”类型周期条目。

使用 **no periodic {daily | weekdays | weekend | [monday] [...] [sunday]} start-time to end-time** 命令删除指定的周期条目。

指定“每周一段时间”类型周期条目，在时间表配置模式下，使用以下命令：

periodic {[monday] | [...] | [sunday]} start-time to {[monday] | [...] | [sunday]} end-time

- **[monday] | [...] | [sunday]** – 开始日期，可以是周一到周日的任意一天。
- *start-time* – 开始时间。书写格式为“小时：分钟：秒钟”，例如09：00：23。
- **[monday] | [...] | [sunday]** – 结束日期，与开始日期相同或者晚于开始日期。
- *end-time* – 结束时间。书写格式为“小时：分钟：秒钟”，例如16：30：37。

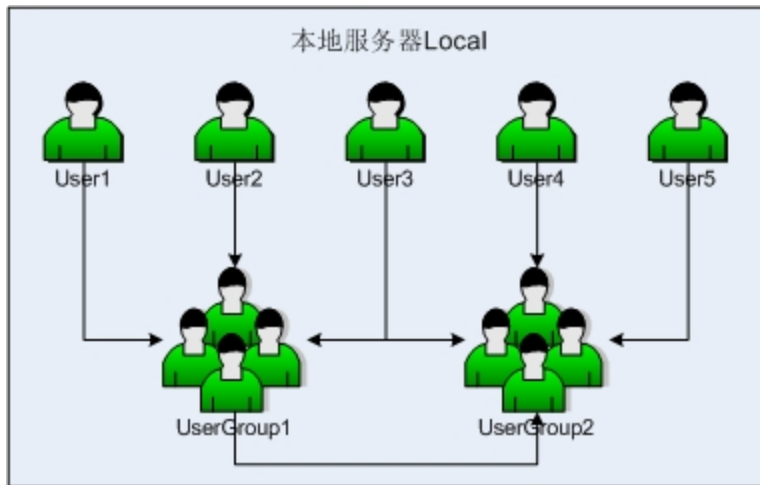
使用多条该命令添加多条“每周一段时间”类型周期条目。

使用 **no periodic {[monday] | [...] | [sunday]} start-time to {[monday] | [...] | [sunday]} end-time** 命令删除指定的周期条目。

用户与角色

系统中的用户（User）是指使用设备提供的功能、服务、被设备认证、管理的用户。被设备认证的用户有本地和外部两种。本地用户（Local User）由系统管理员创建，分属于不同的本地认证服务器，储存在系统的配置文件中；外部用户（External User）储存在外部服务器上，例如AD服务器、LDAP服务器。为方便管理用户，系统支持用户组功能，属于同一本地认证服务器的用户可以划分到不同的用户组中，并且同一个用户可以同时属于不同的用户组，属于同一个本地认证服务器的用户组可以划分

到不同的用户组中，并且同一个用户组可以同时属于不同的用户组。下图以缺省本地AAA认证服务器“Local”的用户配置说明用户以及用户组关系：



如上图所示，用户User1、User2和User3均属于用户组UserGroup1，而User3又同时属于用户组UserGroup2，UserGroup2中还包含User4、User5以及用户组UserGroup1。

角色拥有某些特定的权限，例如某角色可以访问某指定网络资源或者某角色可以独享一定带宽等。在系统中，用户与权限并不直接关联，而是需要通过角色把二者联系起来。

角色映射规则定义角色和用户的对应关系。功能配置中，为不同的角色指定不同的服务，由此，角色对应的用户即可拥有其角色的服务。

设备支持角色组合，即通过对角色进行“与”、“或”逻辑运算，将角色进行组合。被不同功能模块引用的角色对应的用户将是经过运算后的角色对应的用户。

设备支持以下基于角色的功能：

- 基于角色的策略规则：实现不同用户的访问控制。
- 基于角色的iQoS：实现不同用户的带宽控制。
- 基于角色的统计集：统计不同用户的带宽、会话以及新建会话数。
- 基于角色的会话限制：实现对特定用户的会话数限制。
- 基于角色的策略路由：实现根据不同源用户选择路由。

用户

用户配置包括静态绑定用户的配置和系统本地认证用户的配置。

配置静态绑定用户

在全局配置模式下，使用以下命令将IP地址绑定到用户：

```
user-binding aaa-server-name user-name {ip ipv4-address [auth-check-only | vrouter vr-name [auth-check-only]] }
```

- *aaa-server-name* – 指定用户所属的AAA服务器名称。
- *user-name* – 指定用户名称。
- **ip** *ipv4-address* - 指定IPv4地址。
- **auth-check-only** – 配置了该参数后，系统在对用户进行认证之前将会先检查该用户IP地址的合法性，即检查是否与该用户绑定的IP地址一致。如果一致，则允许对用户进行认证。
- **vrouter** *vr-name* – 指定IP地址或MAC地址所属的VRouter的名称。默认为缺省VR，即trust-vr。

在全局配置模式下，使用该命令no的形式取消将IP地址绑定到用户：

```
no user-binding aaa-server-name user-name ip ipv4-address [auth-check-only] [vrouter vr-name]
```

配置认证用户

用户可以为不同的本地AAA服务器配置用户或者用户组。进入本地AAA认证服务器配置模式，在全局配置模式下使用**aaa-server** *aaa-server-name* **type local**命令。

创建本地用户，在本地AAA服务器配置模式下，使用以下命令：

```
user user-name
```

- *user-name* – 指定用户名称。长度范围是1到63个字符。

或者，在全局配置模式下，使用以下命令：

```
user user-name aaa-server aaa-server-name
```

- *user-name* – 指定用户名称。长度范围是1到63个字符。
- *aaa-server-name* - 指定用户将属于的AAA服务器。

执行该命令后，系统创建指定名称的用户并且进入用户配置模式；如果指定的用户名称已存在，则直接进入用户配置模式。在本地AAA服务器配置模式下，使用该命令no的形式删除指定用户：

```
no user user-name
```

用户配置可分三类，分别是

- 用户基本配置：用户密码配置、用户过期时间配置、用户描述以及用户组配置。
- 拨号VPN相关配置：IKE ID配置
- PnPPVPN相关配置：DNS服务器配置、WINS服务器配置、DHCP地址池IP地址配置、DHCP地址池网络掩码配置、DHCP地址池网关配置以及隧道路由配置。具体配置命令，请参阅《防火墙》的“网络参数”。

指定用户密码

指定用户密码，在用户配置模式下，使用以下命令：

```
password password
```

- *password* – 指定用户的密码。长度范围是1到31个字符。

在用户配置模式下使用该命令no的形式取消密码的配置：

```
no password
```

指定用户有效期

超过有效期的用户不可以通过设备的认证，因此不可以在系统中继续使用。默认情况下，用户没有有效期限限制。指定用户的有效期限，在用户配置模式下，使用以下命令：

```
expire Month/day/year HH:MM
```

- *Month/day/year HH:MM* – 指定用户有效期时间，格式为“月/日/年 小时:分钟”。例如命令expire 02/12/2010 12:00表示用户将在2010年2月12日的12: 00过期。

在用户配置模式下使用该命令no的形式取消用户有效期配置：

```
no expire
```

配置用户描述信息

为用户提供描述信息，在用户配置模式下，使用以下命令：

```
desc string
```


- *string* – 指定描述信息，范围是1到31个字符。

在用户配置模式下，使用该命令`no`的形式取消用户描述信息的指定：

```
no desc
```

指定IKE ID

对于拨号VPN用户，需要为其指定IKE ID。指定IKE ID，在用户配置模式下，使用以下命令：

```
ike-id {fqdn string | asn1dn string | key-id string }
```

- **fqdn string** – 指定使用FQDN（Fully Qualified Domain Name）类型的IKE ID。*string*为ID的具体内容。
- **asn1dn string** – 指定使用Asn1dn类型的ID，该类型只可应用于使用证书的情况。*string*为ID的具体内容。
- **key-id string** – 指定使用Key ID类型的ID。该类型仅应用于XAUTH功能。

在用户配置模式下使用该命令`no`的形式取消IKE ID的配置：

```
no ike-id
```

指定用户组

用户可以根据不同类别组织到不同的用户组中。同一个用户可以同时属于多个用户组。为用户指定用户组，在用户配置模式下，使用以下命令：

```
group user-group-name
```

- *user-group-name* – 指定系统中已配置的用户组的名称。长度范围是1到127个字符。

配置多条该命令为同一用户指定多个用户组。

在用户配置模式下使用该命令`no`的形式取消用户组的指定：

```
no group user-group-name
```

用户组

用户可以为不同的本地AAA服务器配置用户或者用户组。进入本地AAA认证服务器配置模式，在全局配置模式下使用**aaa-server***aaa-server-name* **type local**命令。创建本地用户组，在本地AAA服

务器配置模式下，使用以下命令：

user-group *user-group-name*

- *user-group-name* – 指定用户组名称。

执行该命令后，系统创建指定名称的用户组并且进入用户组配置模式；如果指定的用户组名称已存在，则直接进入用户组配置模式。在本地AAA服务器配置模式下，使用该命令no的形式删除指定用户：

no user-group *user-group-name*

在用户组配置模式下，使用以下命令为用户组添加成员，用户组成员可以是用户或者其它的用户组：

member {**user** *user-name* | **group** *user-group-name*}

- *user-name* – 指定用户的名称。
- *user-group-name* – 指定用户组的名称。系统支持的用户组的嵌套层数最多为5层，并且不支持回环嵌套，用户组不可以再嵌套它所属的用户组。

配置多条该命令为用户组添加多个成员。

在用户组配置模式下，使用该命令no的形式将成员从用户组中删除：

no member {**user** *user-name* | **group** *user-group-name*}

显示用户/用户组信息

在任何模式下，使用以下命令查看用户或用户组的信息。

- 查看系统中的用户信息：

show user aaa-server *server-name* [*user-name*]

- 查看静态绑定用户的信息：

show user-binding aaa-server *server-name*

- 查看系统中的用户组信息：

show user-group aaa-server *server-name* [*user-group-name*]

角色

角色配置包括：

- 创建角色
- 配置角色映射规则
- 配置角色组合

创建角色

创建角色，在全局配置模式下使用以下命令：

```
role role-name [description]
```

- *role-name* – 指定角色名称。长度范围是1到31个字符。
- *description* - 添加该角色的描述信息。

在全局配置模式下使用该命令no的形式删除指定的角色：

```
no role role-name
```

配置角色映射规则

角色映射规则表达式指定角色与用户或者用户组的映射关系。系统最多支持64条角色映射规则，每个规则中最多可以包含256条映射条目。

配置角色映射规则，需要首先进入角色映射规则配置模式，在全局配置模式下，使用以下命令：

```
role-mapping-rule rule-name
```

- *rule-name* – 指定角色映射规则的名称。长度范围是1到31个字符。执行该命令后，系统创建指定名称的角色映射规则，并且进入角色映射规则配置模式。如果指定的名称已存在，则直接进入角色映射规则配置模式。

在全局配置模式下使用该命令no的形式删除指定的角色映射规则：

```
no role-mapping-rule rule-name
```

在角色映射规则配置模式下，使用以下命令配置角色映射条目：

```
match {any | user user-name | user-group user-group-name | cn cn-field | ou ou-field} role role-name
```

- **any** | **user** *user-name* | **user-group** *user-group-name* | **cn** *cn-field* | **ou** *ou-field* – 指定映射条目中的用户、用户组、证书名称或者组织机构。**any**表示系统中任何用户、用户组、证书名称或者组织机构。
- **role** *role-name* – 指定用户、用户组、证书名称或者组织机构相对应的角色名称。

配置多条该命令添加多个映射条目。

在角色映射规则配置模式下使用该命令no的形式删除指定的映射条目：

```
no match {any | user user-name | user-group user-group-name | cn cn-field | ou ou-field } role role-name
```

配置角色组合

设备支持角色组合，即通过逻辑运算重新组合已有角色。配置角色组合，在全局配置模式下使用以下命令：

```
role-expression [not] r1 [{and | or} [not] r2] role r3
```

- **[not]** *r1* – 指定表达式中的第一个角色。**not**表示“非”；*r1*为系统中已创建的角色名称。例如，**not testrole1**表示的结果为非testrole1以外的所有角色。
- **and** | **or** – 指定运算符符号。**and**表示“和”；**or**表示“或”。
- **[not]** *r2* – 指定表达式中的第二个角色。**not**表示“非”；*r2*为系统中已创建的角色名称。
- **role** *r3* – 指定角色运算的结果角色。**role**关键字为推导符，*r3*为结果角色名称。

在全局配置模式下使用该命令no的形式删除指定的角色表示式：

```
no role-expression [not] r1 [{and | or} [not] r2] role r3
```

显示角色信息

用户可以在任何模式下使用show命令查看角色信息。

- 显示角色信息：**show role**
- 显示角色映射信息：**show role-mapping-rule** *[rule-name]*
- 显示角色组合信息：**show role-expression**

监测对象

设备的监测功能能够监测指定的目标（IP地址或者主机）是否可达或者接口的链路是否连通，以及监测目标或接口链路是否出现拥塞。如果监测目标不可达或接口链路没有连通，系统会直接判断监测失败；如果监测目标可达或接口链路连通，系统可以继续根据报文延时和接口流量判断监测目标或链路是否出现拥塞。监测功能主要用在HA、策略路由等场景，用户可以通过配置监控功能确保系统始终选择相对健康的链路。



注意:

- 监测失败后，系统会断开到监测对象的所有会话。
- 出现拥塞后，系统仍会保留到监测对象的所有会话，但不允许新建会话。

配置监测功能，首先需配置监测对象，在全局配置模式下，使用以下命令：

track *track-object-name*

- *track-object-name* – 指定监测对象名称。范围是1到31个字符。

执行该命令后，系统创建指定名称的监测对象，并且进入监测对象配置模式；如果指定的名称已存在，则直接进入监测对象的配置模式。使用该命令no的形式删除指定的监测对象：

no track *track-object-name*

设备支持通过Ping报文、HTTP报文、ARP报文、DNS报文和TCP报文五种方式对目标进行监测。

ICMP报文监测

通过ICMP报文对目标进行监测，在监测对象配置模式下使用以下命令：

icmp {*A.B.C.D* | **host** *host-name*} **interface** *interface-name* [**interval** *value*] [**threshold** *value*] [**src-interface** *interface-name*] [**prior-used-srcip** *A.B.C.D*] [**weight** *value*] [**delay high-watermark** *value* **low-watermark** *value*] [**delay-weight** *value*]

- **A.B.C.D | host host-name** – 指定监测目标的IP地址或者主机名称。主机名称范围是1到63个字符。
- **interface interface-name** – 指定发送Ping检测报文的出接口。
- **interval value** – 指定发送Ping报文的时间间隔，单位为秒。范围是1到255秒。默认值是3秒。
- **threshold value** – 指定判断监测失败的警戒值。如果系统连续未收到该参数指定个数的响应报文，就判断为监测失败，即目标不可达。取值范围是1到255。默认值是3。
- **src-interface interface-name** – 指定Ping检测报文的源接口。
- **prior-used-srcip A.B.C.D** – 若源接口上已配置多个IP，将其中一个IP指定为prior-used-srcip后，系统将使用此IP发送track报文；若没有指定该参数，则使用默认的源接口主IP发送track报文。
- **weight value** – 指定该条监测失败对整个监测对象失败贡献的权重值。取值范围是1到255。默认值是255。
- **delay high-watermark value low-watermark value** – 指定监测目标响应Ping报文延时的高水位线和低水位线，单位为毫秒。取值范围是1到65535毫秒。延时小于指定的高水位线，系统会判断链路为正常状态；延时大于或等于指定的高水位下，系统会判断出现链路拥塞；出现链路拥塞后，只有在延时小于或等于指定的低水位线后系统才会判断链路恢复正常状态。这种高低水位线的设计可以有效的防范链路在正常与拥塞状态之间频繁切换。
- **delay-weight value** – 指定该条监测出现链路拥塞对整个监测对象出现链路拥塞所贡献的权重值。取值范围是1到255。默认值是255。

用户可以配置多条该命令为监测对象指定多个监测条目。使用该命令no的形式删除指定的监测条目：

no icmp {A.B.C.D | host host-name} interface interface-name [delay]

ICMPv6报文监测

通过ICMP报文对目标进行监测，在监测对象配置模式下使用以下命令：

icmp6 {X:X:X:X::X | host host-name} interface interface-name [interval value] [threshold value] [src-interface interface-name [prior-used-srcip X:X:X:X::X]] [weight value]

- **X:X:X:X::X | host host-name** – 指定监测目标的IPv6地址或者主机名称。主机名称范围是1到63个字符。
- **interface interface-name** – 指定发送Ping检测报文的出接口。
- **interval value** – 指定发送Ping报文的时间间隔，单位为秒。范围是1到255秒。默认值是3秒。

- **threshold value** – 指定判断监测失败的警戒值。如果系统连续未收到该参数指定个数的响应报文，就判断为监测失败，即目标不可达。取值范围是1到255。默认值是3。
- **src-interface interface-name** – 指定Ping检测报文的源接口。
- **prior-used-srcip X:X:X:X::X** – 若源接口上已配置多个IP，将其中一个IP指定为prior-used-srcip后，系统将使用此IP发送track报文；若没有指定该参数，则使用默认的源接口主IP发送track报文。
- **weight value** – 指定该条监测失败对整个监测对象失败贡献的权重值。取值范围是1到255。默认值是255。

用户可以配置多条该命令为监测对象指定多个监测条目。使用该命令no的形式删除指定的监测条目：

```
no icmp6 { X:X:X:X::X | host host-name } interface interface-name
```

HTTP报文监测

通过HTTP报文对目标进行监测，在监测对象配置模式下使用以下命令：

```
http { A.B.C.D | host host-name } interface interface-name [interval value] [threshold value] [src-interface interface-name] [weight value] [delay high-watermark value low-watermark value] [delay-weight value]
```

- **A.B.C.D | host host-name** – 指定监测目标的IP地址或者主机名称。主机名称范围是1到63个字符。
- **interface interface-name** – 指定发送HTTP检测报文的出接口。
- **interval value** – 指定发送HTTP报文的时间间隔，单位为秒。范围是1到255秒。默认值是3秒。
- **threshold value** – 指定判断监测失败的警戒值。如果系统连续未收到该参数指定个数的响应报文，就判断为监测失败，即目标不可达。取值范围是1到255。默认值是3。
- **src-interface interface-name** – 指定HTTP检测报文的源接口。
- **weight value** – 指定该条监测失败对整个监测对象失败贡献的权重值。取值范围是1到255。默认值是255。
- **delay high-watermark value low-watermark value** – 指定监测目标响应HTTP报文延时高水位线和低水位线，单位为毫秒。取值范围是1到65535毫秒。延时小于指定的高水位线，系统会判断链路为正常状态；延时大于或等于指定的高水位下，系统会判断出现链路拥塞；出现链路拥塞后，只有在延时小于或等于指定的低水位线后系统才会判断链路恢复正常状态。这种高低水位线的设计可以有效的防范链路在正常与拥塞状态之间频繁切换。

- **delay-weight value** – 指定该条监测出现链路拥塞对整个监测对象出现链路拥塞所贡献的权重值。取值范围是1到255。默认值是255。

用户可以配置多条该命令为监测对象指定多个监测条目。使用该命令**no**的形式删除指定的监测条目：

```
no http {A.B.C.D | host host-name} interface interface-name [delay]
```

IPv6 HTTP报文监测

通过HTTP报文对目标进行监测，在监测对象配置模式下使用以下命令：

```
http ipv6 {X:X:X:X::X | host host-name} interface interface-name [interval value] [threshold value]  
[src-interface interface-name] [weight value]
```

- *X:X:X:X::X* | **host** *host-name* – 指定监测目标的IPv6地址或者主机名称。主机名称范围是1到63个字符。
- **interface** *interface-name* – 指定发送HTTP检测报文的出接口。
- **interval value** – 指定发送HTTP报文的时间间隔，单位为秒。范围是1到255秒。默认值是3秒。
- **threshold value** – 指定判断监测失败的警戒值。如果系统连续未收到该参数指定个数的响应报文，就判断为监测失败，即目标不可达。取值范围是1到255。默认值是3。
- **src-interface** *interface-name* – 指定HTTP检测报文的源接口。
- **weight value** – 指定该条监测失败对整个监测对象失败贡献的权重值。取值范围是1到255。默认值是255。

用户可以配置多条该命令为监测对象指定多个监测条目。使用该命令**no**的形式删除指定的监测条目：

```
no http ipv6 {X:X:X:X::X | host host-name} interface interface-name
```

ARP报文监测

通过ARP报文对目标进行监测，在监测对象配置模式下使用以下命令：

```
arp A.B.C.D interface interface-name [interval value] [threshold value] [weight value]
```

- *A.B.C.D* – 指定监测目标的IP地址。
- **interface** *interface-name* – 指定发送ARP检测报文的出接口。
- **interval value** – 指定发送ARP报文的时间间隔，单位为秒。范围是1到255秒。默认值是3秒。

- **threshold value** – 指定判断监测失败的警戒值。如果系统连续未收到该参数指定个数的响应报文，就判断为监测失败，即目标不可达。取值范围是1到255。默认值是3。
- **weight value** – 指定该条监测失败对整个监测对象失败贡献的权重值。取值范围是1到255。默认值是255。

用户可以配置多条该命令为监测对象指定多个监测条目。使用该命令no的形式删除指定的监测条目：

```
no arp {A.B.C.D} interface interface-name
```

NDP报文监测

通过NDP报文对目标进行监测，在监测对象配置模式下使用以下命令：

```
arp X:X:X:X::X interface interface-name [interval value] [threshold value] [weight value]
```

- **X:X:X:X::X** – 指定监测目标的IPv6地址。
- **interface interface-name** – 指定发送NDP检测报文的出接口。
- **interval value** – 指定发送NDP报文的时间间隔，单位为秒。范围是1到255秒。默认值是3秒。
- **threshold value** – 指定判断监测失败的警戒值。如果系统连续未收到该参数指定个数的响应报文，就判断为监测失败，即目标不可达。取值范围是1到255。默认值是3。
- **weight value** – 指定该条监测失败对整个监测对象失败贡献的权重值。取值范围是1到255。默认值是255。

用户可以配置多条该命令为监测对象指定多个监测条目。使用该命令no的形式删除指定的监测条目：

```
no arp X:X:X:X::X interface interface-name
```

DNS报文监测

通过DNS报文对目标进行监测，在监测对象配置模式下使用以下命令：

```
dns A.B.C.D interface interface-name [interval value] [threshold value] [weight value] [src-interface interface-name] [delay high-watermark value low-watermark value] [delay-weight value]
```

- **A.B.C.D** – 指定监测目标的IP地址。
- **interface interface-name** – 指定发送DNS检测报文的出接口。
- **interval value** – 指定发送DNS报文的时间间隔，单位为秒。范围是1到255秒。默认值是3秒。

- **threshold value** – 指定判断监测失败的警戒值。如果系统连续未收到该参数指定个数的响应报文，就判断为监测失败，即目标不可达。取值范围是1到255。默认值是3。
- **weight value** – 指定该条监测失败对整个监测对象失败贡献的权重值。取值范围是1到255。默认值是255。
- **src-interface interface-name** – 指定DNS检测报文的源接口。
- **delay high-watermark value low-watermark value** – 指定监测目标响应DNS报文延时高水位线和低水位线，单位为毫秒。取值范围是1到65535毫秒。延时小于指定的高水位线，系统会判断链路为正常状态；延时大于或等于指定的高水位下，系统会判断出现链路拥塞；出现链路拥塞后，只有在延时小于或等于指定的低水位线后系统才会判断链路恢复正常状态。这种高低水位线的设计可以有效的防范链路在正常与拥塞状态之间频繁切换。
- **delay-weight value** – 指定该条监测出现链路拥塞对整个监测对象出现链路拥塞所贡献的权重值。取值范围是1到255。默认值是255。

用户可以配置多条该命令为监测对象指定多个监测条目。使用该命令**no**的形式删除指定的监测条目：

```
no dns A.B.C.D interface interface-name [delay]
```

TCP报文监测

通过TCP报文对目标端口进行监测，在监测对象配置模式下使用以下命令：

```
tcp {A.B.C.D | host host-name} port port-number interface interface-name [interval value] [threshold value] [src-interface interface-name] [weight value] [delay high-watermark value low-watermark value] [delay-weight value]
```

- **A.B.C.D | host host-name** – 指定监测目标的IP地址或者主机名称。主机名称范围是1到63个字符。
- **port port-number** – 指定监测目标的目的端口号。取值范围为0到65535。
- **interface interface-name** – 指定发送TCP检测报文的出接口。
- **interval value** – 指定发送TCP报文的时间间隔，单位为秒。范围是1到255秒。默认值是3秒。
- **threshold value** – 指定判断监测失败的警戒值。如果系统连续未收到该参数指定个数的响应报文，就判断为监测失败，即目标不可达。取值范围是1到255。默认值是3。
- **src-interface interface-name** – 指定TCP检测报文的源接口。

- **weight value** – 指定该条监测失败对整个监测对象失败贡献的权重值。取值范围是1到255。默认值是255。
- **delay high-watermark value low-watermark value** – 指定监测目标响应TCP报文延时的高水位线和低水位线，单位为毫秒。取值范围是1到65535毫秒。延时小于指定的高水位线，系统会判断链路为正常状态；延时大于或等于指定的高水位下，系统会判断出现链路拥塞；出现链路拥塞后，只有在延时小于或等于指定的低水位线后系统才会判断链路恢复正常状态。这种高低水位线的设计可以有效的防范链路在正常与拥塞状态之间频繁切换。
- **delay-weight value** – 指定该条监测出现链路拥塞对整个监测对象出现链路拥塞所贡献的权重值。取值范围是1到255。默认值是255。

用户可以配置多条该命令为监测对象指定多个监测条目。对于同一个监测对象，不能同时配置对同一目标主机的HTTP监测和对端口80（port 80）的TCP监测。使用该命令no的形式删除指定的监测条目：

```
no tcp {A.B.C.D | host host-name} port port-number interface interface-name [delay]
```

IPv6 TCP报文监测

通过TCP报文对目标端口进行监测，在监测对象配置模式下使用以下命令：

```
tcp {X:X:X:X::X | host host-name} port port-number interface interface-name [interval value]
[threshold value] [src-interface interface-name] [weight value]
```

- **X:X:X:X::X | host host-name** – 指定监测目标的IPv6地址或者主机名称。主机名称范围是1到63个字符。
- **port port-number** – 指定监测目标的目的端口号。取值范围为0到65535。
- **interface interface-name** – 指定发送TCP检测报文的出接口。
- **interval value** – 指定发送TCP报文的时间间隔，单位为秒。范围是1到255秒。默认值是3秒。
- **threshold value** – 指定判断监测失败的警戒值。如果系统连续未收到该参数指定个数的响应报文，就判断为监测失败，即目标不可达。取值范围是1到255。默认值是3。
- **src-interface interface-name** – 指定TCP检测报文的源接口。
- **weight value** – 指定该条监测失败对整个监测对象失败贡献的权重值。取值范围是1到255。默认值是255。

用户可以配置多条该命令为监测对象指定多个监测条目。对于同一个监测对象，不能同时配置对同一目标主机的HTTP监测和对端口80（port 80）的TCP监测。使用该命令no的形式删除指定的监测条目：

```
no tcp ipv6 {X:X:X:X::X | host host-name} port port-number interface interface-name
```

接口链路状态监测

配置监测接口的链路状态，在监测对象配置模式下使用以下命令：

```
interface interface-name [weight value]
```

- *interface-name* – 指定被监测接口的名称。
- **weight value** – 指定该条监测失败对整个监测对象失败贡献的权重值。取值范围是1到255。默认值是255。

用户可以配置多条该命令为监测对象指定多个监测条目。使用该命令no的形式删除指定的监测条目：

```
no interface interface-name
```

接口链路质量监测

通过统计指定接口的采样流量信息，系统可以监测该接口的链路状态。配置接口链路对象监测，在监测对象配置模式下使用以下命令：

```
traffic-condition [ ipv6 ] interface interface-name [interval value] [threshold value] [weight value]  
[condition-threshold low-watermark high-watermark]
```

- **ipv6** – 指定为IPv6类型的接口链路监测对象。如果不指定该参数，默认指定为IPv4类型的接口链路监测对象。
- *interface-name* – 指定被监测接口的名称。
- **interval value** – 指定每个监测周期的持续时间，单位为秒。取值范围是1到255秒。默认值是3秒。每个监测周期结束后，系统会重置探测到的新建会话相关数值。
- **threshold value** – 指定判断监测失败的警戒值。如果系统连续检测到该指定次数的监测失败情况，就判断该条监测失败。取值范围是1到255。默认值是3。
- **weight value** – 指定该条监测失败对整个监测对象失败贡献的权重值。取值范围是1到255。默认值是255。

- **condition-threshold** *low-watermark high-watermark* – 指定每个监测周期的新建会话成功率阈值。默认情况下，失败界定阈值为30，成功界定阈值为50。取值范围是0到100。在某个监测周期内，当新建会话成功率小于指定的失败界定阈值时，判断为监测失败；当新建会话成功率大于指定的成功界定阈值时，判断为监测成功；当新建会话成功率大于等于失败界定阈值且小于等于成功界定阈值时，系统保持原来的监测状态。

用户可以重复该命令为监测对象指定多个接口链路质量的监测条目。

在监测对象配置模式下，使用该命令no的形式删除指定的监测条目：

```
no traffic-condition [ ipv6 ] interface interface-name
```

接口流量监测

配置监测接口流量，在监测对象配置模式下使用以下命令：

```
bandwidth interface interface-name direction {in | out | both} high-watermark value low-watermark value [interval value] [threshold value] [weight value]
```

- **interface-name** – 指定被监测接口的名称。
- **direction** {*in* | *out* | *both*} – 指定监测的流量方向。*in*指流入方向，*out*指流出方向，*both*指双方向。默认为流出方向（*out*）。
- **high-watermark** *value* **low-watermark** *value* – 指定接口流量的高水位线和低水位线，单位为kbps。取值范围是1到100000000kbps。接口流量小于指定的高水位线，系统会判断链路为正常状态；接口流量大于或等于指定的高水位下，系统会判断出现链路拥塞；出现链路拥塞后，只有在接口流量小于或等于指定的低水位线后系统才会判断链路恢复正常状态。这种高低水位线的设计可以有效的防范链路在正常与拥塞状态之间频繁切换。
- **interval** *value* – 指定监控接口流量的间隔时间，单位为秒。取值范围是1到255秒。默认值是1秒。
- **threshold** *value* – 指定判断该条监测出现拥塞的警戒值。如果系统连续检测到参数指定次数的链路过载情况，就判断该条监测出现拥塞。取值范围是1到255。默认值是3。
- **weight** *value* – 指定该条监测出现拥塞对整个监测对象出现拥塞贡献的权重值。取值范围是1到255。默认值是255。

用户可以配置多条该命令为监测对象指定多个监测条目。使用该命令no的形式删除指定的监测条目：

```
no bandwidth interface interface-name
```

配置警戒值

警戒值用于判断整个监测对象失败或出现拥塞。当监测对象中同类型监测条目的权重值总和大于等于对应的警戒值时，系统会判断整个监测对象失败或出现拥塞。用户可以针对监测对象失败、报文超时导致的监测对象拥塞和接口流量过载导致的监测对象拥塞三种情况分别设置不同类型的警戒值：监测对象警戒值、报文超时警戒值和接口流量警戒值。

监测对象警戒值

当监测对象中失败的监测条目的权重值的总和大于等于一定值，系统就判断整个监测对象失败。该值即为监测对象的警戒值。指定监测对象的警戒值，在监测对象配置模式下使用以下命令：

threshold value

- *value* – 指定监测对象警戒值的大小。范围是1到255。默认值是255。

在监测对象配置模式使用该命令no的形式恢复警戒值的默认值：

no threshold

报文延时警戒值

当监测对象中报文延时所导致链路拥塞的权重值的总和大于等于一定值，系统就判断整个监测对象出现拥塞。该值即为报文延时的警戒值。指定报文延时的警戒值，在监测对象配置模式下使用以下命令：

delay-threshold value

- *value* – 指定报文延时警戒值的大小。范围是1到255。默认值是255。

在监测对象配置模式使用该命令no的形式恢复警戒值的默认值：

no delay-threshold

例如，配置监测对象如下：

```
hostname(config)# track delay-test  
  
hostname(config-trackip)# delay-threshold 250  
  
hostname(config-trackip)# dns 1.1.1.1 interface ethernet0/1 delay high-water-  
mark 100 low-watermark 50 delay-weight 50
```

```
hostname(config-trackip)# dns 1.1.1.2 interface ethernet0/1 delay high-watermark 100 low-watermark 50 delay-weight 220
```

完成该配置后，如果监测目标1.1.1.1和1.1.1.2均出现链路拥塞（即DNS报文延时均超过100毫秒），则 $\text{delay-weight}=50+220=270>250$ ，系统判定监测对象**delay-test**出现拥塞。

接口流量警戒值

当监测对象中接口流量过载所导致链路拥塞的权重值的总和大于等于一定值，系统就判断整个监测对象出现拥塞。该值即为接口流量的警戒值。指定接口流量的警戒值，在监测对象配置模式下使用以下命令：

bandwidth-threshold *value*

- *value* – 指定接口流量警戒值的大小。范围是1到255。默认值是255。

在监测对象配置模式使用该命令no的形式恢复警戒值的默认值：

no bandwidth-threshold

例如，配置监测对象如下：

```
hostname(config)# track bandwidth-test
hostname(config-trackip)# bandwidth-threshold 250
hostname(config-trackip)# bandwidth interface ethernet0/1 direction both
high-watermark 20 low-watermark 10 threshold 5 weight 220
hostname(config-trackip)# bandwidth interface ethernet0/2 direction both
high-watermark 20 low-watermark 10 threshold 5 weight 50
```

完成该配置后，如果监测目标接口eth0/1和eth0/2均出现链路过载（即上述接口上均出现过5次或5次以上流量超过20kbps的情况），则 $\text{bandwidth-threshold}=50+220=270>250$ ，系统判定监测对象**bandwidth-test**出现拥塞。

当被监控接口的监测对象失败或出现拥塞后，系统会自动禁止这些接口的相关路由（静态路由、动态路由、策略路由等）参与流量转发，即正常的流量转发不再匹配到这些接口的路由，但当系统只有一条出口默认路由时，此规则无效。

用户可以在任何模式下使用show命令查看监测对象的配置信息：

show track *tack-object-name*

系统监控报警

系统监控报警功能能够监控系统资源的使用状况，并根据配置发出报警信息。当前版本支持的报警方式为日志信息和SNMP Trap信息。

配置系统监控报警功能，首先要进入监控配置模式。进入监控配置模式，在全局配置模式下，使用以下命令：

monitor

进入监控配置模式后，用户可以根据需要监控的系统资源对象，设置相应的监控规则：

```
{cpu | memory utilization | interface-bandwidth interface-name utilization | log-buffer { config | event | network | traffic{pbr | nat}} utilization | session utilization | snat-resource utilization } interval interval-value absolute rising-threshold threshold-value sample-period period-value [count count-value] {log [snmp-trap] | snmp-trap }
```

- **cpu | memory utilization | interface-bandwidth *interface-name* utilization | log-buffer { config | event | network | security | traffic{pbr | nat} } utilization | session utilization | snat-resource utilization** - 指定监控对象，可以为系统CPU（cpu）、内存（memory）、接口带宽（interface-bandwidth）、日志容量（log-buffer）、会话（session）和SNAT转换后的IP地址端口资源（snat-resource）。
- ***interface-name*** - 指定监控的接口名称。
- **config | event | network | security | traffic{pbr | nat}** - 指定具体的日志类型。
- **utilization** - 指定监控值为各对象的利用率。CPU（cpu）的监控值默认为利用率，不需要指定。
- **interval *interval-value*** - 指定监控间隔，即系统在报警计算时间段（sample-period *period-value*）内，每次取值后等待的时间间隔。取值范围为3到10秒。
- **absolute** - 指定监控值为绝对值。
- **rising-threshold *threshold-value*** - 指定上升阈值，即实际监控值超过该阈值满足报警条件的百分比。取值范围为1到99。
- **sample-period *period-value*** - 指定报警计算时间段。取值范围为30到3600秒。
- **count *count-value*** - 指定在报警计算时间段（sample-period）内，监控对象的实际监控数值超过阈值（rising-threshold）的次数。取值范围为1到1000。如果配置该参数，在监控时间段内，若监控对象值超过阈值的次

数大于该count值，则发出警告；如果不配置该参数，在监控时间段内，若监控对象值的平均值大于阈值（rising-threshold），则发出警告。

- **log [snmp-trap] | snmp-trap** - 指定报警方式。可以使用日志（log）或者SNMP Trap报文（snmp-trap），也可以同时使用这两种报警方式。

例如：

配置CPU峰值监控：

```
hostname(config)# monitor
```

```
hostname(config-monitor)# cpu interval 5 absolute rising-threshold 65 sample-period 600 count 50 log
```

完成该配置后，在600秒内，如果CPU利用率超过了阈值65%，且发生过最少50次，则发出报警日志

配置会话均值监控：

```
hostname(config)# monitor
```

```
hostname(config-monitor)# session utilization interval 8 absolute rising-threshold 90 sample-period 600 log
```

完成该配置后，在600秒内，如果会话平均利用率超过了阈值90%，则发出报警日志

在监控配置模式下使用该命令no的形式删除指定的监控规则：

```
no {cpu | memory utilization | interface-bandwidth interface-name utilization | log-buffer { config | event | network | security | traffic{pbr | nat}} utilization | session utilization | snat-resource utilization}
```

注意：



注意：

- 不支持对SNAT转换后地址为出接口IP地址（cif-ip）的端口资源的监控报警；
- 对于每种监控对象，只有最后配置的一条监控规则生效。

查看系统监控报警配置，在任意模式下，使用以下命令：

```
show monitor
```

系统监控报警功能的日志信息类别为事件（Event），严重等级为严重（Critical）。用户可以查看系统事件日志信息，或者配置事件日志email提醒功能将日志信息发送到管理员邮件。

第9章 流量管理

本章包含以下内容：

- [iQoS](#)：介绍了iQoS的实现机制、智能流量管理的处理流程、管道的概念及如何配置iQoS等。
- [会话限制](#)：介绍了会话限制的相关概念及配置方法。

iQoS

系统提供iQoS（智能流量管理）功能，能够管理和优化网络带宽，提高用户的网络体验和带宽资源利用率。

iQoS为特定流量提供更高优先服务的同时控制抖动和延迟的能力，并且能够降低数据传输丢包率。当网络过载或拥塞时，系统能够确保重要业务流量的正常传输。iQoS功能受许可证控制，安装许可证后，iQoS功能才可使用。

管道与流控层级

系统支持两层流控，即第一层流控和第二层流控。在每层流控中，流量的具体控制通过管道来实现。

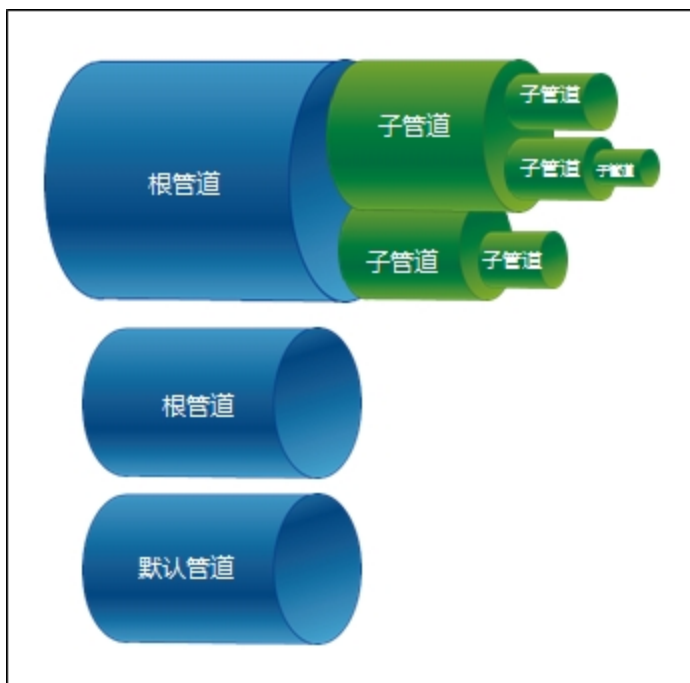
管道

设备通过配置管道来实现iQoS。管道，即带宽通道，是一个虚拟概念。系统以管道为单位对流量进行划分，并根据管道配置的流控动作对管道内的流量进行管控。所有流经设备的流量，都将按照设置的匹配条件进入虚拟管道。未匹配到的流量将进入系统预定义的默认管道。

管道（除默认管道）必须包含两部分，分别是流量匹配条件和流量管理动作。

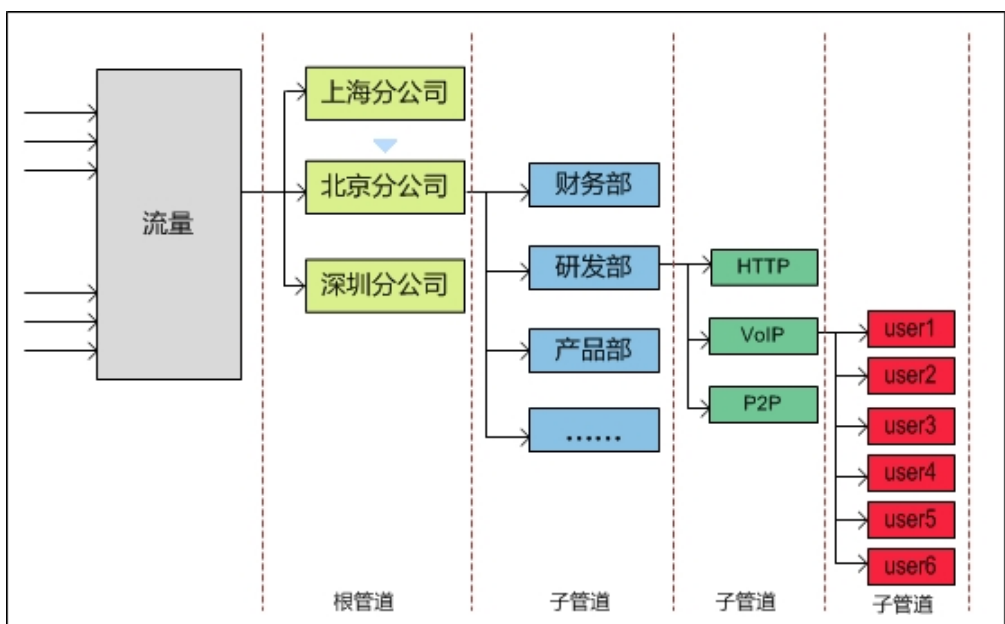
- 流量匹配条件：定义设备需要匹配的流量，从而设备可以将流量进行区分。流经设备的流量会根据用户设置的条件分类，划入对应的管道。系统为匹配到匹配条件的流量提供带宽控制。一个管道可以有多个流量匹配条件，各个匹配条件之间为“或”的关系。流量只要匹配到其中一个匹配条件，就会进入该管道。
- 流量管理动作：对已被划分到管道中的流量所做的动作。流控分为正向控制和反向控制。正向控制即对从源到目的方向的流量进行控制；反向控制即对从目的到源方向的流量进行控制。

为了给用户灵活和方便的配置，系统支持多级管道。配置多级管道，可将不同用户的不同应用分别限制在一定带宽之内，从而能优先保障重要用户或重要应用的带宽。管道最多支持四级嵌套，默认管道不可嵌套子管道。管道逻辑关系如下图所示：



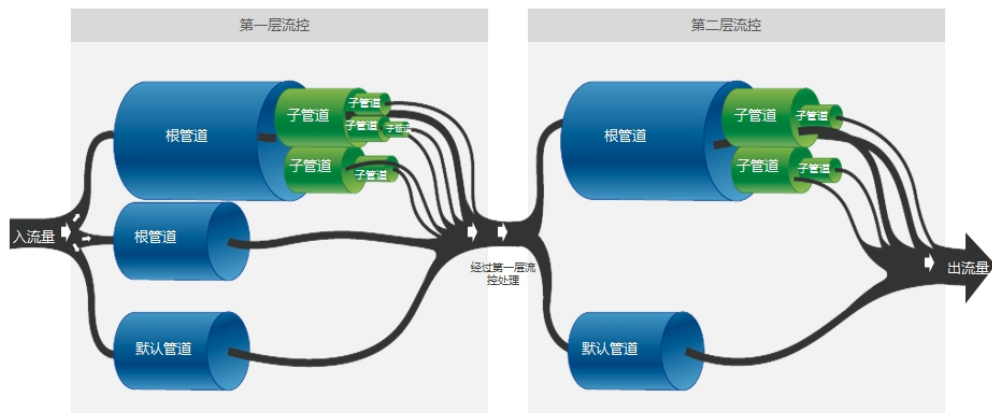
- 用户可创建多个根管道，各个根管道之间是彼此独立的。每个根管道下均可嵌套三级子管道。
- 子管道的最小带宽之和不能大于其上一级管道的最小带宽，最大带宽也不能大于其上一级管道的最大带宽
- 用户若在根管道上配置了正向或反向的流量管理动作后，该根管道下的所有子管道都必须继承根管道设定的流量方向。
- 仅配置了反向流量管理动作的管道不可用。

以某企业的应用场景为例说明如何嵌套多级管道。如下图所示，管理员可创建一个根管道，限制该企业北京分公司的流量。创建一个子管道，限制其研发部门的流量。再创建子管道对研发部应用进行划分，限制不同应用拥有不同的带宽。最后为某种应用的每用户设置子管道，限制该应用的每位用户的流量。



流控层级

系统支持两层流控，即第一层流控和第二层流控。在每层流控中，流量的具体控制通过管道来实现。经过第一层流控处理过的流量进入第二层流控，系统再根据第二层流控的管道设置对流量进行进一步管控。流量进入设备后，iQoS处理流程如下图所示：



根据上图所示，系统的流控处理流程描述如下：

1. 流量首先进入第一层流控，系统根据第一层流控中管道的匹配条件设置划分流量到不同的管道中。不匹配任何管道的流量进入默认管道。如果存在相同匹配条件的根管道，流量优先匹配位置靠前的根管道。流量进入根管道后，再根据子管道的匹配条件逐层匹配。

2. 系统根据管道配置的流控动作对匹配到的流量进行管控。
3. 经过第一层流控处理的流量进入第二层流控进行再次管控。系统在第二层流控中的管道匹配以及流量管控原理与第一层流控相同。
4. 流控处理结束。

配置iQoS

系统通过创建管道来实现流量管理，进而保障和优化管理网络带宽。创建管道，包括：

1. 创建流量匹配条件，系统对匹配到匹配条件的流量进行控制。若为管道配置多个匹配条件，各匹配条件之间为“或”的关系。
2. 根据需求创建流量白名单。目前仅根管道和默认管道支持配置白名单。配置后，系统将不对白名单中指定的流量做流量管理。
3. 指定流量管理动作，即对已被划分到管道中的流量指定动作。

指定流控层级

指定进入第一层流控或第二层流控，并进入流控模式，用户可创建管道实现流量管理。在全局配置模式下，使用以下命令：

```
qos-engine {first | second}
```

- **first** – 指定进入第一层流控。
- **second** – 指定进入第二层流控。

启用/禁用流控层级/根管道/子管道

启用/禁用流控层级，在指定层级的流控模式下，使用以下命令：

- 禁用：**disable**
- 启用：**no disable**

启用/禁用根管道，在指定根管道配置模式下，使用以下命令：

- 禁用: **disable**
- 启用: **no disable**

启用/禁用子管道, 在指定子管道配置模式下, 使用以下命令:

- 禁用: **disable**
- 启用: **no disable**



注意: 被禁用的流控层级或者管道不参与流控处理。不可用的管道也不参与流控处理。

启用/禁用NAT IP匹配

在指定层级的流控模式下, 用户可按需启用NAT IP匹配功能。启用后, 对于该流控层级, 系统将使用流量的源NAT后和目的NAT前的IP地址作为匹配项。如果匹配成功, 系统将会对这些IP地址进行流控管理。启用NAT IP匹配功能, 在指定层级的流控模式下, 使用以下命令:

match-nat-ip enable

在指定层级的流控模式下, 使用**no match-nat-ip enable**禁用NAT IP匹配。



注意: 在启用NAT IP匹配功能之前, 必须配置NAT规则。否则, 该配置不生效。

创建根管道

创建根管道, 并进入该根管道配置模式。如果指定的根管道名称已经存在, 则直接进入根管道配置模式。在流控模式下, 使用以下命令:

root-pipe {pipe-name | default}

- **pipe-name** – 指定将要创建的根管道名称。
- **default** – 进入默认管道。

在流控模式下, 使用该命令**no**的形式删除创建的根管道:

no root-pipe pipe-name



注意:

- 管道名字不能超过63个字符。
- 根管道下可嵌套3级子管道。
- 默认管道不能删除。

进入根管道配置模式后，可进行如下配置：

- 启用/禁用根管道
- 配置根管道流量匹配条件
- 配置根管道流量白名单
- 配置根管道流量管理动作
- 配置根管道流控模式
- 为根管道指定时间表
- 创建子管道

创建子管道

创建子管道，并进入子管道配置模式。如果指定的子管道名称已经存在，则直接进入子管道配置模式。在管道配置模式下，使用以下命令：

pipe *pipe-name*

- *pipe-name* – 指定将要创建的子管道名称。

在管道配置模式下，使用该命令no的形式删除创建的子管道：

no pipe *pipe-name*



注意:

- 管道名字不能超过63个字符。
- 删除子管道，需在其父管道配置模式下，使用**no pipe pipe-name**命令。

进入子管道配置模式后，可进行如下配置：

- 启用/禁用子管道
- 配置子管道流量匹配条件
- 创建子管道

配置流量匹配条件

配置匹配条件前，用户需先创建匹配条件并进入其匹配条件配置模式。如果指定的ID已存在，直接进入其匹配条件配置模式。若不指定ID，系统将直接创建一个匹配条件并进去其配置模式。创建匹配条件并且进入匹配条件配置模式。在管道配置模式下，使用以下命令：

pipe-map *[id]*

- *id* – 指定匹配条件的ID。

使用**no pipe-map** *[id]*命令删除指定的匹配条件。

进入匹配条件配置模式后，可使用的配置流量匹配条件的命令如下：

- 指定流量源安全域的名称：**src-zone** *src-zone*
- 删除流量源安全域的名称：**no src-zone**
- 指定流量目的安全域的名称：**dst-zone** *dst-zone*
- 删除流量目的安全域的名称：**no dst-zone**
- 指定流量的源主机名称：**src-host** *host-name*
- 删除流量的源主机名称：**no src-host** *host-name*
- 指定流量的目的主机名称：**dst-host** *host-name*

- 删除流量的目的主机名称: **no dst-host** *host-name*
- 指定流量的源地址 (IPv4或IPv6) : **src-ip** {*ip/netmask* | *ip-address netmask* | *ipv6-address/prefix* }
- 删除指定流量的源地址 (IPv4或IPv6) : **no src-ip** {*ip/netmask* | *ip-address netmask* | *ipv6-address/prefix* }
- 指定流量的目的地址 (IPv4或IPv6) : **dst-ip** {*ip/netmask* | *ip-address netmask* | *ipv6-address/prefix* }
- 删除流量的目的地址 (IPv4或IPv6) : **no dst-ip** {*ip/netmask* | *ip-address netmask* | *ipv6-address/prefix* }
- 指定流量的源地址范围 (IPv4或IPv6) : **src-range** *min-ip* [*max-ip*]
- 删除流量的源地址范围 (IPv4或IPv6) : **no src-range** *min-ip* [*max-ip*]
- 指定流量的目的地址范围 (IPv4或IPv6) : **dst-range** *min-ip* [*max-ip*]
- 删除流量的目的地址范围 (IPv4或IPv6) : **no dst-range** *min-ip* [*max-ip*]
- 指定流量的入接口名称: **ingress-if** *interface-name*
- 删除流量的入接口名称: **no ingress-if** *interface-name*
- 指定流量的出接口名称: **egress-if** *interface-name*
- 删除流量的出接口名称: **no egress-if** *interface-name*
- 指定流量的源地址条目 (IPv4或IPv6) : **src-addr** *address-book*
- 删除流量的源地址条目 (IPv4或IPv6) : **no src-addr** *address-book*
- 指定流量的目的地址条目 (IPv4或IPv6) : **dst-addr** *address-book*
- 删除流量的目的地址条目 (IPv4或IPv6) : **no dst-addr** *address-book*
- 指定用户及其所属的AAA服务器: **user** *AAA-server user-name*
- 删除用户及其所属的AAA服务器: **no user** *AAA-server user-name*
- 指定用户组及其所属的AAA服务器: **user-group** *AAA-server usergroup-name*
- 删除用户组及其所属的AAA服务器: **no user-group** *AAA-server usergroup-name*

- 指定应用或应用组，包括预定义应用和自定义应用：**application** *app-name*
- 删除应用或应用组，包括预定义应用和自定义应用：**no application** *app-name*
- 指定服务组或者服务的名称：**service** *service-name*
- 删除服务组或者服务的名称：**no service** *service-name*
- 指定ToS字段：**tos** *tos-value*
- 删除ToS字段：**no tos** *tos-value*
- 指定Vlan信息：**vlan** *vlan-id*
- 删除Vlan信息：**no vlan** *vlan-id*
- 指定URL类别：**url-category** *category-name*
- 删除URL类别：**no url-category** *category-name*
- 指定TrafficClass字段：**traffic-class** *traffic-class-value*
- 删除TrafficClass字段：**no traffic-class** *traffic-class-value*

配置流量白名单

配置流量白名单。配置后，系统将不对白名单中指定的流量做流量管理。用户可为根管道或默认管道指定流量白名单。

配置白名单前，用户需先创建白名单并进入其白名单配置模式。如果指定的ID已存在，直接进入其白名单配置模式。若不指定ID，系统将直接创建一个白名单并进去其配置模式。创建白名单并且进入白名单配置模式，在管道配置模式下，使用以下命令：

exception-map [*id*]

- *id* – 指定白名单的ID。

使用 **no exception-map** [*id*] 命令删除指定的白名单。

进入白名单配置模式后，可使用的配置白名单匹配条件的命令如下：

- 指定流量源安全域的名称: **src-zone** *src-zone*
- 删除流量源安全域的名称: **no src-zone**
- 指定流量目的安全域的名称: **dst-zone** *dst-zone*
- 删除流量目的安全域的名称: **no dst-zone**
- 指定流量的入接口名称: **ingress-if** *interface-name*
- 删除流量的入接口名称: **no ingress-if** *interface-name*
- 指定流量的出接口名称: **egress-if** *interface-name*
- 删除流量的出接口名称: **no egress-if** *interface-name*
- 指定流量的源地址: **src-ip** {*ip/netmask* | *ip-address netmask*}
- 删除指定流量的源地址: **no src-ip** {*ip/netmask* | *ip-address netmask*}
- 指定流量的目的地址: **dst-ip** {*ip/netmask* | *ip-address netmask*}
- 删除流量的目的地址: **no dst-ip** {*ip/netmask* | *ip-address netmask*}
- 指定用户及其所属的AAA服务器: **user** *AAA-server user-name*
- 删除用户及其所属的AAA服务器: **no user** *AAA-server user-name*
- 指定用户组及其所属的AAA服务器: **user-group** *AAA-server usergroup-name*
- 删除用户组及其所属的AAA服务器: **no user-group** *AAA-server usergroup-name*
- 指定应用或应用组, 包括预定义应用和自定义应用: **application** *app-name*
- 删除应用或应用组, 包括预定义应用和自定义应用: **no application** *app-name*
- 指定服务组或者服务的名称: **service** *service-name*
- 删除服务组或者服务的名称: **no service** *service-name*
- 指定ToS字段: **tos** *tos-value*

- 删除ToS字段: **no tos** *tos-value*
- 指定Vlan信息: **vlan** *vlan-id*
- 删除Vlan信息: **no vlan** *vlan-id*

配置根管道流量管理动作

配置根管道流量管理动作，在根管道配置模式下，使用以下命令：

```
pipe-rule {forward | backward} bandwidth {Kbps | Mbps | Gbps} bandwidth-value [per-ip-min min-value] [per-ip-max max-value] [delay delay-time] [per-ip-using {src-ip | dst-ip}] [tos-marking tos-value] [mode aggressive [strength-level level-value]] [priority value]
```

```
pipe-rule {forward | backward} bandwidth {Kbps | Mbps | Gbps} [per-user-min min-value] [per-user-max max-value] [delay delay-time] [tos-marking tos-value] [mode aggressive [strength-level level-value]] [priority value]
```

```
pipe-rule {forward | backward} bandwidth {Kbps | Mbps | Gbps} bandwidth-value average-using {src-ip | dst-ip | user} [tos-marking tos-value] [mode aggressive [strength-level level-value]] [priority value]
```

- **forward** - 对匹配到匹配条件中从源到目的方向的流量指定流控动作。
- **backward** - 对匹配到匹配条件中从目的到源方向的流量指定流控动作。
- **bandwidth {Kbps | Mbps | Gbps}** - 指定管道的最小带宽值。选择**Kbps**时，取值范围为32Kbps到100000000Kbps；选择**Mbps**时，取值范围为1Mbps到100000Mbps；选择**Gbps**时，取值范围为1Gbps到100Gbps。percent, **Mbps**, **Gbps**只在配置子管道的时候生效。
- **per-ip-min min-value** - 指定每个IP的最小带宽值。取值范围为32Kbps到1000000Kbps。
- **per-ip-max max-value** - 指定每个IP的最大带宽值。取值范围为32Kbps到1000000Kbps。
- **per-ip-using {src-ip | dst-ip}** - 选择为管道内每个源IP（src-ip）或者目的IP（dst-ip）限制带宽。该选项仅当用户配置了每IP最小/最大带宽值时生效。
- **per-user-min min-value** - 指定每个用户的最小带宽值。选择**Kbps**时，取值范围为32Kbps到10000000KBPS；选择**Mbps**时，取值范围为1Mbps到10000Mbps。
- **per-user-max max-value** - 指定每个用户的最大带宽值。选择**Kbps**时，取值范围为32Kbps到10000000Kbps；选择**Mbps**时，取值范围为1Mbps到10000Mbps。

- **delay** *delay-time* - 指定延时时间。取值范围为1秒到3600秒。在延时时间范围内，对每IP/用户的最大带宽限制不生效。
- **tos-marking** *tos-value* - 指定TOS字段。
- **mode aggressive** [**strength-level** *level-value*] - 开启对端抑制功能。默认情况下，该功能为关闭状态。对端抑制功能可根据用户分配的带宽，使到达设备的流量尽可能与分配带宽相符，以减少设备上的丢包。开启对端抑制功能后，默认抑制强度（**strength-level**）为1，抑制强度取值范围为1-8。数值越大，抑制强度越大，丢包越少。
- **priority** *value* - 指定管道优先级。取值范围为0到7，默认值为7。数值越小，表示该管道的优先级越高。优先级较高的管道，系统将优先调度，并优先借用其他管道的空闲带宽。
- **average-using** {**src-ip** | **dst-ip** | **user**} - 对管道内每个源IP（src-ip）或者目的IP（dst-ip）或者用户（user）平均分配带宽。

使用该命令no的形式删除指定方向的流量管理动作。



注意:

- 不可同时指定每用户和每IP的带宽限制。
- 对端抑制功能只能在正反流控的一个方向开启。只有最末端管道支持配置对端抑制功能。

配置子管道流量管理动作

配置子管道流量管理动作，在根管道配置模式下，使用以下命令：

```
pipe-rule {forward | backward} {min | reserve-bandwidth} {percent | Kbps | Mbps | Gbps} value max {percent | Kbps | Mbps | Gbps} max-value [per-ip-min min-value] [per-ip-max max-value [delay delay-time]] [per-ip-using {src-ip | dst-ip}] [tos-marking tos-value] [mode aggressive [strength-level level-value]] [priority value]
```

```
pipe-rule {forward | backward} {min | reserve-bandwidth} {percent | Kbps | Mbps | Gbps} min-value max {percent | Kbps | Mbps | Gbps} max-value [per-user-min min-value] [per-user-max max-value [delay delay-time]] [tos-marking tos-value] [mode aggressive [strength-level level-value]] [priority value]
```

- **forward** - 对匹配到匹配条件中从源到目的方向的流量指定流控动作。
- **backward** - 对匹配到匹配条件中从目的到源方向的流量指定流控动作。
- **{min | reserve-bandwidth} {percent | Kbps | Mbps | Gbps} value** - 指定管道的最小带宽值，或为管道设定保留带宽。**min**代表指定最小带宽。**reserve-bandwidth**代表指定保留带宽。设定最小带宽/保留带宽时，**percent**表示此管道的最小带宽/保留带宽占父管道带宽的百分比，取值范围为1到100；选择**Kbps**时，取值范围为32Kbps到100000000Kbps；选择**Mbps**时，取值范围为1Mbps到100000Mbps；选择**Gbps**时，取值范围为1Gbps到100Gbps。
- **max {percent | Kbps | Mbps | Gbps} max-value** - 指定管道的最大带宽值或最大带宽占比。**percent**表示此管道的最大带宽占父管道带宽的百分比，取值范围为1到100；选择**Kbps**时，取值范围为32Kbps到100000000Kbps；选择**Mbps**时，取值范围为1Mbps到100000Mbps；选择**Gbps**时，取值范围为1Gbps到100Gbps。
- **per-ip-min min-value** - 指定每个IP的最小带宽值。取值范围为32Kbps到1000000Kbps。
- **per-ip-max max-value** - 指定每个IP的最大带宽值。取值范围为32Kbps到1000000Kbps。
- **per-ip-using {src-ip | dst-ip}** - 选择为管道内每个源IP（src-ip）或者目的IP（dst-ip）限制带宽。该选项仅当用户配置了每IP最小/最大带宽值时生效。
- **per-user-min min-value** - 指定每个用户的最小带宽值。选择**Kbps**时，取值范围为32Kbps到10000000KBPS；选择**Mbps**时，取值范围为1Mbps到10000Mbps。
- **per-user-max max-value** - 指定每个用户的最大带宽值。选择**Kbps**时，取值范围为32Kbps到10000000Kbps；选择**Mbps**时，取值范围为1Mbps到10000Mbps。
- **delay delay-time** - 指定延时时间。取值范围为1秒到3600秒。在延时时间范围内，对每IP/用户的最大带宽限制不生效。
- **tos-marking tos-value** - 指定TOS字段。
- **mode aggressive [strength-level level-value]** - 开启对端抑制功能。默认情况下，该功能为关闭状态。对端抑制功能可根据用户分配的带宽，使到达设备的流量尽可能与分配带宽相符，以减少设备上的丢包。开启对端抑制功能后，默认抑制强度（**strength-level**）为1，抑制强度取值范围为1-8。数值越大，抑制强度越大，丢包越少。

- **priority value** - 指定管道优先级。取值范围为0到7，默认值为7。数值越小，表示该管道的优先级越高。优先级较高的管道，系统将优先调度，并优先借用其他管道的空闲带宽。



注意:

- 不可同时指定每用户和每IP的带宽限制。
- 对端抑制功能只能在正反流控的一个方向开启。只有最末端管道支持配置对端抑制功能。

配置根管道的流控模式

根管道的流控模式可以为以下三种模式：

- 整形模式：配置该模式后，系统能够限制数据传输速率，使流量平滑地转发。根管道范围内流量将支持带宽借用和优先级调度
- 管制模式：配置该模式后，系统将对超出带宽限制的流量进行丢弃。该模式不支持带宽借用和优先级调度，且不做最小带宽保障。
- 监控模式：配置该模式后，系统仅对匹配到的流量进行监控和统计，不对流量进行任何控制。

带宽借用：即同一根管道内的所有子管道，在确保自身管道流量正常转发的情况下，可将空闲流量分配给带宽不足的管道。

优先级调度：即在流量拥塞时，超出带宽限制的流量将进入等待队列，用户可设置优先级以确保某些应用优先调度。

默认情况下。流控模式为整形模式。指定根管道的流控模式，在根管道配置模式下，使用以下命令：

```
qos-mode {police | shape | stat}
```

- **police** - 指定流控模式为管制模式。
- **shape** - 指定流控模式为整形模式。
- **stat** - 指定流控模式为监控模式。

配置根管道时间表

设备支持时间表功能，用户可以为根管道指定一个时间表条目，令根管道在指定的时间内生效。配置根管道时间表功能，在根管道配置模式下，使用以下命令：

schedule *schedule-name*

- *schedule-name* – 指定时间表的名称。

使用 **no schedule** *schedule-name* 取消时间表配置。



提示：关于如何创建时间表，请参阅《系统管理》的“[配置时间表功能](#)”部分。

配置子管道时间表

用户可以为子管道指定一个时间表条目，令子管道在指定的时间内生效。配置子管道时间表功能，在子管道配置模式下，使用以下命令：

schedule *schedule-name*

- *schedule-name* – 指定时间表的名称。

使用 **no schedule** *schedule-name* 取消时间表配置。

查看流控层级及管道的配置信息

查看流控层级及管道的配置信息，在任何模式下，使用以下命令：

show qos-engine {**first** | **second**} [**root-pipe** *pipe-name*]

- **first** – 查看第一层流控及其管道的配置信息。
- **second** – 查看第二层流控及其管道的配置信息。
- **root-pipe** *pipe-name* – 查看指定根管道的配置信息。

配置阈值告警功能

系统支持管道使用率阈值告警功能。在开启该功能并指定告警阈值后，当管道使用率达到或超过指定的告警阈值时，系统会记录警告级别的事件日志。对于同一个管道，系统记录事件日志的时间间隔为10秒钟，即每10秒记录一次事件日志。

开启/关闭阈值告警功能

默认情况下，阈值告警功能为开启状态。开启/关闭阈值告警功能，在全局配置模式下，使用以下命令：

```
qos-threshold-switch {on | off}
```

- **on** – 开启阈值告警功能。
- **off** – 关闭阈值告警功能。

指定告警阈值

指定管道使用率的告警阈值，在全局配置模式下，使用以下命令：

```
qos-threshold threshold
```

- *threshold* – 指定管道使用率的告警阈值。单位为百分比。取值范围为50到100。默认值为80。

显示阈值告警功能的启用状态

显示管道使用率的阈值告警功能的启用状态，在任何模式下，使用以下命令：

```
show qos-threshold
```

会话限制

设备支持基于安全域的会话限制功能。用户可以对安全域内的源IP地址、目的IP地址、指定的IP地址、特定协议类型、应用、角色或用户进行会话数量或者建立会话速率控制，从而保护连接表不被DoS攻击填满，并且能够在一定程度上限制一些应用的带宽，如IM或者P2P等。

会话限制配置

配置会话限制功能，在安全域配置模式下，使用以下命令：

ad session-limit [**id** *id*] { {**src-ip** *address-entry* **dst-ip** *address-entry* | **ip** *address-entry* } [**protocol** *protocol-id*] [**application** *application-name*] [**role** *role-name* | **user** *aaa-server-name* *user-name* | **user-group** *aaa-server-name* *user-group-name*] } {**session** {**unlimit** | **max** *number* [**per-srcip** | **per-dstip** | **per-ip**] | **per-user**} | **ramp-rate** **max** *number*} [**schedule** *schedule-name*] [**log**]

- **id** *id* – 指定安全域的会话限制规则ID。
- **src-ip** *address-entry* – 限制安全域的源IP地址会话数。*address-entry*为**src-ip**的IP地址范围。该参数值为地址簿中定义的一条地址条目。
- **dst-ip** *address-entry* – 限制安全域的目的IP地址会话数。*address-entry*为**dst-ip**的IP地址范围。该参数值为地址簿中定义的一条地址条目。
- **ip** *address-entry* – 限制安全域中某个IP地址段的会话数。*address-entry*为**ip**的IP地址范围。该参数值为地址簿中定义的一条地址条目。
- **protocol** *protocol-id* – 限制安全域中特定IP协议类型的会话数。*protocol-id*为**ip**的协议号，取值范围为1到255。
- **application** *application-name* – 限制安全域中特定应用的会话数。
- **role** *role-name* – 限制特定角色的会话数。
- **user** *aaa-server-name* *user-name* – 限制特定用户的会话数。*aaa-server-name*为用户所属的AAA服务器名称，*user-name*为用户名称。
- **user-group** *aaa-server-name* *user-group-name* – 限制特定用户组的会话数。*aaa-server-name*为用户组所属的AAA服务器名称，*user-name*为用户组名称。
- **session** {**unlimit** | **max** *number* [**per-srcip** | **per-dstip** | **per-ip**] | **per-user**} – 指定IP地址或角色的最大会话数。**unlimit**为无会话数限制。**session max number**指定地址条目中所有IP地址的最大会话数或者角色对应的所有用户的最大会话数；如果使用**per-srcip**、**per-dstip**、**per-ip**或者**per-user**关键字，则**session max number**指定的为每个IP地址的最大会话数或者角色对应的每个用户的最大会话数。**per-srcip**、**per-dstip**、**per-ip**和**per-user**四个关键字需和前面的**src-ip**、**dst-ip**、**ip**和**role**关键字一一对应，如：只有在前面指定了**src-ip**才可以在后面选择**per-srcip**。
- **ramp-rate** **max** *number* – 指定IP地址或者角色每5秒钟可建立的最大会话数。

- **schedule** *schedule-name* – 指定会话限制规则的生效时间。
- **log** - 指定记录会话限制日志。



注意: 会话限制功能支持IPv4地址和IPv6地址。如开启接口的IPv6功能，用户可配置IPv6类型的地址条目。源地址条目与目的地址条目的地址类型需一致。

在安全域配置模式下，使用以下命令删除安全域的会话限制规则：

no ad session-limit id *id*

- **id** *id* – 安全域的会话限制规则ID。可通过show session-limit命令获取相应规则的ID。

配置会话限制功能后，超出最大会话数限制的会话将被丢弃，用户可以通过show session-limit命令查看被丢弃的会话数统计信息。删除特定会话限制规则中被丢弃会话数的统计信息，请在任何置模式下使用以下命令：

clear session-limit id *id* **statistics**

- **id** *id* – 指定规则ID以删除特定会话限制规则中被丢弃的会话数统计信息。

会话限制显示

配置会话限制功能后，在任何模式下使用以下命令查看会话限制配置信息：

show session-limit

第10章 安全策略

安全策略可控制安全域间/不同地址段间的流量转发。默认情况下，ADC设备会允许设备上所有安全域/地址段之间的信息传输。而安全策略则通过策略规则决定从一个安全域到另一个安全域，以及从一个地址段到另一个地址段的哪些流量该被允许，哪些流量该被拒绝。

策略规则的基本元素包括：

- 流量的源安全域/源地址
- 流量的目的安全域/目的地址
- 流量的服务类型
- 设备在遇到指定类型流量时所做的行为，包括允许（Permit）和拒绝（Deny）。

策略规则分为两部分：过滤条件和行为。安全域间流量的源安全域/源地址、目的安全域/目的地址以及服务类型构成策略规则的过滤条件。策略规则都有其独有的ID号。策略规则ID会在定义规则时自动生成，同时用户也可以按自己的需求为策略规则指定ID。整个系统的所有策略规则有特定的排列顺序。在流量进入系统时，系统会对流量按照找到的第一条与过滤条件相匹配的策略规则进行处理。

不同ADC设备平台支持的全局最大策略规则数不同。

安全策略支持指定IPv4和IPv6格式的地址条目。

本章节包含以下内容：

- 配置策略规则
 - [进入策略配置模式](#)
 - [创建策略规则](#)
 - [编辑策略规则](#)
 - [指定缺省行为](#)
 - [修改规则排列顺序](#)

- [规则冗余检测](#)
- [查看策略规则信息](#)
- [查看设备的当前策略配置信息](#)
- [查看策略规则匹配次数](#)
- [策略组](#)
- [策略助手](#)
- [聚合策略](#)

配置策略规则

进入策略配置模式

进入策略配置模式，在全局配置模式下使用以下命令：

```
policy-global
```

创建策略规则

在全局配置模式或者策略配置模式下，执行以下命令创建策略规则：

```
rule [id id] [name name] [top | before {name rule-name | id} | after {name rule-name | id}] [from
{host host-name | range min-ip max-ip | src-addr}] [to {host host-name | range min-ip max-ip |
dst-addr}] [from-zone zone-name to-zone zone-name] [service service-name] [application app-name]
[permit | deny]
```

- **id id** – 指定策略规则的ID。如果不指定，系统将会为策略规则自动分配一个ID。规则ID在整个系统中必须是唯一的。
- **name name** – 指定策略规则的名称。
- **top | before {name rule-name | id} | after {name rule-name | id}** – 指定策略规则的位置。默认情况下，系统会将新创建的策略规则放到所有规则的末尾。

- **top**: 指定策略规则的位置为所有规则的首位。
- **before {name rule-name | id}**: 指定策略规则的位置为某个规则ID或者名称之前。
- **after {name rule-name | id}**: 指定策略规则的位置为某个规则ID或者名称之后。
- **from {host host-name | range min-ip max-ip | src-addr}** - 指定策略规则的源地址。
 - **host host-name**: 为地址簿中定义的主机类型的源地址条目。
 - **min-ip max-ip**: 为地址簿中定义的IP地址段类型的源地址条目。
 - **src-addr**: 为地址簿中定义的地址条目。
- **to {host host-name | range min-ip max-ip | dst-addr}** - 指定策略规则的目的地址。
 - **host host-name**: 为地址簿中定义的主机类型的目的地址条目。
 - **range min-ip max-ip**: 为地址簿中定义的IP地址段类型的目的地址条目。
 - **dst-addr**: 为地址簿中定义的地址条目。
- **from-zone zone-name** - 指定策略规则的源安全域。
- **to-zone zone-name** - 指定策略规则的目的安全域。
- **service service-name** - 指定策略规则的服务名称。*service-name*为服务簿中定义的服务。
- **application app-name** - 指定策略规则的应用名称。*app-name*为应用簿中定义的应用名称。
- **permit | deny** - 指定策略规则的行为。具体描述如下:
 - **permit**: 允许流量通过。
 - **deny**: 拒绝流量通过。

例如，创建允许从任意地址到任意地址的ICMP服务的策略规则，请输入以下命令：

```
hostname(config)# policy-global
hostname(config-policy)# rule from any to any service icmp permit
Rule id 5 is created.
```

删除策略规则，在全局配置模式或者策略配置模式下，使用以下命令：

no rule [*id id*] [*name name*]

- **id id** – 删除指定ID的策略规则。
- **name name** – 删除指定名称的策略规则。

提示：关于如何配置其它策略相关参数，请参考[编辑策略规则](#)。

编辑策略规则

创建好的策略规则可以进行编辑来修改不合适的参数值，但是修改工作必须在规则配置模式下进行。在CLI中进入策略规则配置模式，请在全局配置模式或策略配置模式下输入以下命令：

rule [*id id*] [**top** | **before** {*name name* | *id*} | **after** {*name name* | *id*}]

进入策略规则配置模式后，可使用的编辑策略规则的命令如下：

- 命名/重新命名策略规则：**name** *policy-name*
- 指定/修改源安全域：**src-zone** *src-zone*
- 删除源安全域：**no src-zone**（执行该命令后，策略规则无源安全域限制）
- 指定/修改目的安全域：**dst-zone** *dst-zone*
- 删除目的安全域：**no dst-zone**（执行该命令后，策略规则无目的安全域限制）
- 添加地址簿条目类型源地址：**src-addr** *src-addr*
- 删除地址簿条目类型源地址：**no src-addr** *src-addr*
- 添加IP成员类型源地址：**src-ip** *ip/netmask*
- 删除IP成员类型源地址：**no src-ip** *ip/netmask*
- 添加主机成员类型源地址：**src-host** *host-name*
- 删除主机成员类型源地址：**no src-host** *host-name*
- 添加IP地址范围类型源地址：**src-range** *min-ip* [*max-ip*]
- 删除IP地址范围类型源地址：**no src-range** *min-ip* [*max-ip*]

- 添加地址簿条目类型目的地址: **dst-addr** *dst-addr*
 - 删除地址簿条目类型目的地址: **no dst-addr** *dst-addr*
 - 添加IP成员类型目的地址: **dst-ip** {*ip/netmask* | *ip-address netmask*}
 - 删除IP成员类型目的地址: **no dst-ip** {*ip/netmask* | *ip-address netmask*}
 - 添加主机成员类型目的地址: **dst-host** *host-name*
 - 删除主机成员类型目的地址: **no dst-host** *host-name*
 - 添加IP地址范围类型目的地址: **dst-range** *min-ip* [*max-ip*]
 - 删除IP地址范围类型目的地址: **no dst-range** *min-ip* [*max-ip*]
 - 添加服务类型: **service** *service-name*
 - 删除服务类型: **no service** *service-name*
- 说明:** 服务规则包括服务的协议类型和端口号, 可以根据需要的协议和端口号, 配置服务规则并在策略中添加该服务规则。关于如何添加/删除服务规则, 请参阅[配置服务规则](#)。
- 添加应用类型: **application** *application-name*
 - 删除应用类型: **no application** *application-name*
 - 修改处理行为: **action** {**permit** | **deny**}
 - 配置时间表: **schedule** *schedule-name*
 - 删除时间表: **no schedule** *schedule-name*



注意: 默认情况下, 配置的策略规则会即时生效, 而当为策略规则配置时间表功能后, 策略规则就只在时间表所指定的时间内生效。用户最多可以为一条策略规则配置8个时间表, 策略规则的生效时间为所有被配置到该策略规则的时间表的时间的总和。关于如何配置时间表, 请参阅[配置时间表功能](#)。

- 添加描述: **description** *description* (*description*的取值范围是1到255字节)

- 删除描述: **no description** *description*
- 修改规则的QoS标签: **policy-qos-tag** *tag* (*tag*的取值范围是1到1024)
- 删除规则的QoS标签: **no policy-qos-tag** *tag*
- 允许应用未被识别的流量通过: **unknown-application-action permit**
- 默认情况下, 拒绝应用未被识别的流量通过: **no unknown-application-action permit**

启用/禁用策略规则

默认情况下, 配置好的策略规则会在系统中立即起效。用户可以通过命令禁用某条策略规则, 使其不对流量进行控制。禁用或者启用某条策略规则, 在策略规则配置模式下, 使用以下命令:

- 禁用: **disable**
- 启用: **enable**

策略规则的日志管理

用户可以根据需要, 通过系统日志信息记录流量对策略规则的匹配情况:

- 对于permit类型的策略规则, 可以记录两种情况, 分别是符合策略规则的流量建立会话时生成日志信息和结束会话时生成日志信息。
- 对于deny类型的策略规则, 可以记录的情况为: 符合策略规则的流量被deny时生成日志信息。

使用该功能前, 必须保证系统的流量日志功能是开启的, 即在全局配置模式下, 执行**logging traffic on**命令。配置规则的日志管理, 在策略规则配置模式下, 使用以下命令:

log {policy-deny | session-start | session-end}

- **policy-deny** - 适用于deny类型的策略规则。使系统生成规则拒绝流量的日志信息。
- **session-start** - 适用于permit类型的策略规则。使系统生成会话建立的日志信息。
- **session-end** - 适用于permit类型的策略规则。使系统生成会话结束的日志信息

使用**no log {policy-deny | session-start | session-end}**命令取消策略规则日志管理功能的配置。

另外，对于从指定源安全域到目的安全域的未匹配到策略规则的流量，用户可以指定是否为其生成日志信息。默认情况下，系统不为此类流量生成日志信息。生成日志信息，在策略配置模式下，使用以下命令：

```
log policy-default
```

在策略配置模式下，使用该命令no的形式恢复默认值：

```
no log policy-default
```

配置服务规则

在配置策略规则的服务时，可以添加服务簿中已配置好的预定义服务或者自定义服务。当所需要的服务在服务簿中不存在时，管理员可以通过配置服务规则，直接指定服务的协议类型以及端口号等信息，从而简化策略的配置步骤。

配置TCP或者UDP类型服务规则，在策略规则配置模式下，使用以下命令：

```
service-rule {tcp | udp} dst-port min-port [max-port] [src-port min-port [max-port]]
```

- **tcp | udp** - 指定服务规则的协议类型：TCP或者UDP。
- **dst-port min-port [max-port]** - 指定服务规则的目的端口号。如果目的端口号为一个范围，*min-port*为最小目的端口号，*max-port*为最大目的端口号；如果不配置*max-port*，系统将使用*min-port*作为单一目的端口号。目的端口号的范围是0到65535。
- **src-port min-port [max-port]** - 指定服务规则的源端口号。如果源端口号为一个范围，*min-port*为最小源端口号，*max-port*为最大源端口号；如果不配置*max-port*，系统将使用*min-port*作为单一源端口号。源端口号的范围是0到65535。

配置ICMP类型服务规则，在策略规则配置模式下，使用以下命令：

```
service-rule icmp type type-value [code min-code [max-code]]
```

- **type-value** - 指定服务规则的ICMP type值。范围是0 (Echo-Reply)、3 (Destination-Unreachable)、4 (Source Quench)、5 (Redirect)、8 (Echo)、11 (Time Exceeded)、12 (Parameter Problem)、13 (Timestamp)、14 (Timestamp Reply)、15 (Information Request)、16 (Information Reply)、17 (Address Mask Request)、18 (Address Mask Reply)、30 (Traceroute)、31 (Datagram Conversion)

Error)、32 (Mobile Host Redirect)、33 (IPv6 Where-Are-You)、34 (IPv6 I-Am-Here)、35 (Mobile Registration Request)、36 (Mobile Registration Reply)。

- **code min-code [max-code]** – 指定服务规则的ICMP code值。如果ICMP code值为一个范围，*min-code*为最小code值，*max-code*为最大code值；如果不配置*max-code*，系统将使用*min-code*作为单一code值。范围是0到15。默认值是*min-code*为0、*max-code*为15。

配置ICMPv6类型服务规则，在策略规则配置模式下，使用以下命令：

service-rule icmpv6 type type-value [code min-code [max-code]]

- *type-value* – 指定服务规则的ICMPv6 type值。取值范围请参考[附表：ICMPv6 Type以及Code值对照表](#)。
- **code min-code [max-code]** – 指定服务规则的ICMPv6 code值。如果ICMPv6 code值为一个范围，*min-code*为最小code值，*max-code*为最大code值；如果不配置*max-code*，系统将使用*min-code*作为单一code值。范围是0到255。默认值是*min-code*为0、*max-code*为255。

配置其它类型服务规则，在策略规则配置模式下输入以下命令：

service-rule protocol protocol-number

- *protocol-number* – 指定服务规则的协议号。范围是1到255。

使用以上四条命令no的形式可以删除对应服务规则。

- **no service-rule {tcp | udp} dst-port min-port [max-port] [src-port min-port [max-port]]**
- **no service-rule icmp type type-value [code min-code [max-code]]**
- **no service-rule icmpv6 type type-value [code min-code [max-code]]**
- **no service-rule protocol protocol-number**

指定缺省行为

用户可以为未匹配到任何已配置策略规则的流量指定缺省行为，系统将按照指定的缺省行为对此类流量进行处理。默认情况下，系统会允许未匹配到任何已配置策略规则的流量通过。指定缺省行为为允许，在策略配置模式下，使用以下命令：

default-action permit

在策略配置模式下，使用该命令**no**的形式，指定缺省行为为“拒绝”：

no default-action permit

修改规则排列顺序

每一条策略规则都有唯一一个ID号和名称。流量进入山石网科设备时，山石网科设备对策略规则进行顺序查找，然后按照查找到的相匹配的第一条规则对流量进行处理。但是，策略规则ID的大小顺序并不是规则查找时的匹配顺序。使用**show policy**命令列出的规则顺序才是规则匹配顺序（系统将由上到下进行查找）。用户在创建策略规则时可以指定该规则的排列位置，也可以在策略配置模式下修改其位置。策略规则的排列位置可以是绝对位置，即处在首位（Top）或者处在末位（Bottom），也可以是相对位置，即位于某个ID或者名称的前后。修改规则排列顺序，在策略配置模式下使用以下命令：

```
move {name name | id} {top | bottom | before {name rule-name | id} | after {name rule-name | id}}
```

- **name name | id** – 指定需要修改排列顺序的策略规则ID或者名称。
- **top** – 指定策略规则修改后的位置为所有规则的首位。
- **before {name rule-name | id}** – 指定策略规则修改后的位置为某个规则ID或者名称之前。
- **after {name rule-name | id}** – 指定策略规则修改后的位置为某个规则ID或者名称之后。

规则冗余检测

为保证策略中规则的有效性，系统可对规则进行冗余检测，即检查规则的覆盖情况，帮助用户排除由于规则覆盖导致的匹配问题。

在任何模式下，使用以下命令开始规则的冗余检测：

exec policy redundancy-check start

检测开始后，将持续一段时间，请耐心等待。检测完成后，用户可使用**show policy redundancy-check**命令查看策略规则ID和被覆盖的规则ID。

用户也可使用**exec policy redundancy-check stop**命令停止冗余检测，或使用**exec policy redundancy-check clear**命令清除上一次的规则冗余检测结果缓存。

查看策略规则信息

用户可以在任何模式下，通过show命令查看策略规则的具体信息。具体命令以下：

```
show policy [id id] [from src-zone] [to dst-zone] [src-addr src-addr] [dst-addr dst-addr] [protocol protocol] [service service-name] [application application-name] [description description] [name name] [name-filter filter-name]
```

- **id id** – 显示指定ID规则的详细信息。
- **from src-zone** – 显示源安全域为指定域的规则的详细信息。
- **to dst-zone** – 显示目标安全域为指定域的规则的详细信息。
- **src-addr src-addr** – 显示指定地址簿条目类型源地址的规则的信息。
- **dst-addr dst-addr** – 显示指定地址簿条目类型目的地址的规则的信息。
- **protocol protocol** - 显示指定协议的规则的信息。
- **service service-name** – 显示指定服务类型的规则详细信息。
- **application application-name** – 显示指定应用类型的规则详细信息。
- **description description** – 显示指定描述信息的规则详细信息。
- **name name** – 显示指定名称的规则详细信息。
- **name-filter filter-name** – 显示名称包含指定关键字的所有规则详细信息。

查看设备的当前策略配置信息

查看设备的当前策略配置信息，在任何命令模式下输入以下命令：

```
show configuration policy [name name | id id | by-line | last number]
```

- **name name** – 单行显示指定名称的策略规则配置信息。
- **id id** – 单行显示指定ID的策略规则配置信息。

- **by-line** – 单行显示所有策略规则配置信息。
- **last number**- 显示从倒数指定数值的条目开始到最后条目的策略规则配置信息。

查看策略规则匹配次数

为方便用户对策略规则的管理和维护，山石网科设备支持策略规则匹配次数统计功能。该功能能够对系统流量与策略规则的匹配次数进行统计，即每当进入系统的流量与某条策略规则相匹配时，该策略规则的匹配次数会自动加1。用户可以在任何模式下通过以下命令查看策略规则匹配次数统计信息：

show policy hit-count [**id** *id* | **name** *name* | [**from** *src-zone*] [**to** *dst-zone*] **top** {**10** | **20** | **50** | **all** }]

- **id** *id* – 显示指定ID规则的匹配次数统计信息。
- **name** *name* – 显示指定名称规则的匹配次数统计信息。
- **from** *src-zone* – 显示源安全域为指定域的规则的匹配次数统计信息。
- **to** *dst-zone* – 显示目标安全域为指定域的规则的匹配次数统计信息。
- **top** {**10** | **20** | **50** | **all**} – 显示匹配次数位于前10、20、50位的规则的匹配次数统计信息或者按降序方式显示所有规则的匹配次数统计信息。

例如：

查看所有规则的匹配次数统计信息

```
hostname(config)# show policy hit-count
```

Most hit policy rules:

```
=====
=====
```

No.	Id	Name	Src-zone	Dst-zone	Src-addr	Dst-addr	Service	Applica~	Action	Hit-count
1	1	test	Any	Any	Any	Any	Any	PERMIT	0	
2	2	test1	Any	Any	private_ne~	Any	Any	PERMIT	0	
3	4	test2	Any	Any	Any	Any	Any	PERMIT	0	

```
4 5 test3 Any Any Any Any Any PERMIT 0
```

```
5 6 Any Any 0
```

```
6 dft Any Any 0
```

```
=====
```

查看指定ID规则的匹配次数统计信息

```
hostname(config)# show policy hit-count id 1
```

```
Policy id 1 is hit 342424 times
```

查看指定名称规则的匹配次数统计信息

```
SG-6000(config)# show policy hit-count name a
```

```
Policy "a" is hit 0 times
```

查看匹配次数位于前10位的规则的匹配次数统计信息

```
hostname(config)# show policy hit-count top 10
```

```
Most hit policy rules:
```

```
=====
```

No.	Id	Name	Src-zone	Dst-zone	Src-addr	Dst-addr	Service	Applica~	Action	Hit-count

```
-----
```

1	1	test	Any	Any	Any	Any	Any	PERMIT	0

2	2	test1	Any	Any	private_ne~	Any	Any	PERMIT	0

3	4	test2	Any	Any	Any	Any	Any	PERMIT	0

4	5	test3	Any	Any	Any	Any	Any	PERMIT	0

5	6	Any	Any						0

6	dft	Any	Any						0

```
=====
```


按降序方式查看所有规则的匹配次数统计信息

```
hostname(config)# show policy hit-count top all
```

Most hit policy rules:

```
=====
=====

No. Id Name Src-zone Dst-zone Src-addr Dst-addr Service Applica~ Action Hit-
count
-----

1 1 test Any Any Any Any Any PERMIT 0
2 2 test1 Any Any private_ne~ Any Any PERMIT 0
3 4 test2 Any Any Any Any Any PERMIT 0
4 5 test3 Any Any Any Any Any PERMIT 0
5 6 Any Any 0
6 dft Any Any 0

=====
=====
```

清除策略规则匹配次数统计信息，请在任意模式下使用以下命令：

```
clearpolicy hit-count {all | id id | name name}
```

- **all** – 清除所有规则的匹配次数统计信息。
- **id id** – 清除指定ID规则的匹配次数统计信息。
- **name name** – 清除指定名称规则的匹配次数统计信息。

清除策略规则的缺省行为匹配次数统计信息，请在任意模式下使用以下命令：

```
clear policy hit-count default-action
```

策略组

用户可以将一些策略规则组织到一起便组成了策略组。用户可以直接将对策略组进行配置，这样便简化了管理。

配置策略组

用户可以通过CLI对策略组进行以下配置：

- [新建/删除策略组](#)
- [启用/禁用策略组](#)
- [添加/删除策略组描述信息](#)
- [添加/删除策略规则成员](#)
- [策略组重命名](#)

新建/删除策略组

新建策略组，请在全局配置模式下，输入以下命令：

```
policy-group group-name
```

- *group-name* - 指定策略组名称。范围是1到95个字符。

运行该命令后，系统进入策略组配置模式。

删除策略组，请在全局配置模式下，输入以下命令：

```
no policy-group group-name
```

启用/禁用策略组

默认情况下，策略组为启用状态。启用/禁用策略组，在策略组配置模式下，使用以下命令：

- 启用：**enable**
- 禁用：**disable**



注意：

- 启用/禁用策略组后，策略组中的策略规则成员启用状态同时被修改。



- 策略规则在被引用时，不允许启用或者禁用。

添加/删除策略组描述信息

在策略组配置模式下，用户可以通过使用以下命令为策略组添加描述信息。

description *description*

- *description* – 指定策略组的描述信息。范围是1到255字节。

在策略组配置模式下，使用以下命令删除策略组的描述信息。

no description

添加/删除策略规则成员

在策略组配置模式下，用户可以通过使用以下命令为策略组添加策略规则成员。

rule *id*

- *id* – 指定策略规则ID。

在策略组配置模式下，使用以下命令删除策略组的策略规则成员。

no rule *id*



注意: 一条策略规则只能添加到一个策略组中。

策略组重命名

在全局配置模式下，用户可以通过使用以下命令为策略组重命名。

rename policy-group *old-name new-name*

- *old-name* – 指定策略组的旧名称。
- *new-name* – 指定策略组的新名称。

查看策略组配置信息

查看策略组配置信息，在任何模式下，使用以下命令：

```
show policy-group [name]
```

- *name* – 查看指定策略组名称的配置信息。

策略助手

为了提高用户配置安全策略的完整性、准确性和快速性，系统提供策略助手功能。策略助手能够提取命中指定策略ID的流量作为流量数据分析源，并根据用户设置的聚合规则聚合数据流量列表，最后自动生成符合用户期望的安全策略规则。

开启/关闭策略助手

启用策略助手功能，在策略规则配置模式下，使用以下命令：

```
assistant enable
```



注意: 根VSYS最多支持开启4个策略规则ID的策略助手功能；非根VSYS最多支持开启1个策略规则ID的策略助手功能。

关闭策略助手功能，在策略规则配置模式下，使用以下命令：

```
assistant disable
```

示例：

```
hostname(config)# policy-global  
  
hostname(config-policy)# rule id 2  
  
hostname(config-policy-rule)# assistant enable
```

查看开启策略助手的策略

查看已开启策略助手功能的策略的详细信息，在任意模式下，使用以下命令：

```
show policy assistant-enable
```

聚合策略

用户可以根据场景需要，创建聚合策略并且将一些具有相同作用或者相同属性的策略规则加入聚合策略，管理员调整聚合策略的优先级后，所有聚合策略成员的优先级将会一起调整，实现对策略规则的批量管理。

聚合策略的配置包括：

- 创建聚合策略
- 添加聚合策略成员
- 移出聚合策略成员
- 删除聚合策略
- 调整优先级
- 启用/禁用聚合策略
- 添加/删除聚合策略描述信息

创建聚合策略

创建聚合策略，需进行如下两步操作：

1. 创建一条包含名称的策略规则。
2. 进入该策略规则配置模式后，将新创建的策略规则指定为聚合策略。



注意：如需要将之前已存在的策略规则指定为聚合策略，策略规则的配置需满足以下要求，否则无法指定为聚合策略：

- 必须包含名称的配置。
- 可包含启用状态或描述配置，并且除名称、启用状态或描述配置外，不包含其他配置。

创建策略规则并进入该策略规则的配置模式，在全局配置模式下，使用以下命令：

```
rule [id id] { name name }
```

- **id** *id* - 指定策略的ID。如果不指定，系统将会为策略规则自动分配一个ID。规则ID在整个系统中必须是唯一的。
- **name** *name* - 指定聚合策略的名称。范围是1到95个字符，该名称为必配项。

指定为聚合策略，在策略规则配置模式下，使用以下命令：

aggregate-type

添加聚合策略成员

当聚合策略创建完成后，管理员可以将策略规则添加到聚合策略中成为聚合策略成员。首先，使用 **rule id** *id* 进入要被添加的策略规则的配置模式，然后，使用以下命令：

aggregate-rule { **name** *name* | **id** *id* } [**top** | **before** { **name** *rule-name* | *id* } | **after** { **name** *rule-name* | *id* }]

- **name** *name* | **id** *id* - 指定需要加入到的聚合策略名称或规则ID。
- **top** | **before** { **name** *rule-name* | *id* } | **after** { **name** *rule-name* | *id* } - 指定聚合策略成员在聚合策略中的位置。默认情况下，将会排列在聚合策略中所有成员的末尾。
 - **top** - 指定聚合策略成员的位置为聚合策略中的所有成员的首位。
 - **before** { **name** *rule-name* | *id* } - 指定聚合策略成员的位置为聚合策略中某个成员的ID或者名称之前。
 - **after** { **name** *rule-name* | *id* } - 指定聚合策略成员的位置为聚合策略中某个成员的ID或者名称之后。



注意:

- 一条策略规则只能添加到一个聚合策略中。
- 如果一条策略规则已经被添加到聚合策略中，执行该命令后，将会加入到新指定的聚合策略中。
- 聚合策略不能作为聚合策略成员加入到另一个聚合策略中。



- 策略组中的策略成员不能被添加到聚合策略中。

移出聚合策略成员

从聚合策略中移出某个聚合策略成员，使用**rule id id**进入要被移出的聚合策略成员的配置模式，然后使用以下命令：

```
no aggregate-rule
```



注意：

- 当**top**位置的聚合策略成员被移出聚合策略后，将会被排列到该聚合策略之前。
- 当非**top**位置的聚合策略成员被移出聚合策略后，将会被排列到该聚合策略之后。

删除聚合策略

删除聚合策略并移出其中的聚合策略成员，在全局配置模式或者策略配置模式下，使用以下命令：

```
no rule {id id | name name}
```

- **id id** – 删除指定ID的聚合策略。
- **name name** – 删除指定名称的聚合策略。

删除聚合策略及其聚合策略成员，即删除聚合策略的同时，将其中的聚合策略成员一并删除，在全局配置模式或者策略配置模式下，使用以下命令：

```
no rule {id id | name name} include-member
```

调整优先级

调整聚合策略或其中聚合策略成员的优先级，修改其排列顺序，在策略配置模式下使用以下命令：

```
move {name name | id} {top | bottom | before {name rule-name | id} | after {name rule-name | id}}
}
```

- **name name | id** – 指定需要调整优先级的聚合策略或其中成员ID或者名称。
- **top** – 如果移动的是**聚合策略**，指定该聚合策略移动到所有策略规则的首位；如果移动的是**聚合策略成员**，指定该聚合策略成员移动到其所属聚合策略中所有成员的首位。
- **bottom** – 如果移动的是**聚合策略**，指定该聚合策略移动到所有策略规则的末尾；如果移动的是**聚合策略成员**，指定该聚合策略成员移动到其所属聚合策略中所有成员的末尾。
- **before {name rule-name | id}** – 指定聚合策略移动到某个规则ID或者名称之前。如果移动的是**聚合策略成员**，*rule-name*或 *id*仅可指定为所属聚合策略中的其他成员的ID或名称。
- **after {name rule-name | id}** – 指定聚合策略移动到某个规则ID或者名称之后。如果移动的是**聚合策略成员**，*rule-name*或 *id*仅可指定为所属聚合策略中的其他成员的ID或名称。



注意:

- 用户调整聚合策略的优先级后，所有聚合策略成员的优先级将会一起调整。
- 不支持通过调整策略规则的优先级实现添加到聚合策略或者从聚合策略中移出。

启用/禁用聚合策略

默认情况下，配置好的聚合策略会在系统中立即起效。管理员可以通过命令禁用某条聚合策略，使其不对流量进行控制。禁用或者启用某条聚合策略，在聚合策略的配置模式下，使用以下命令：

- 禁用: **disable**
- 启用: **enable**



注意:

- 禁用聚合策略后，聚合策略中的聚合策略成员同时被禁用。



- 启用聚合策略后，聚合策略中的聚合策略成员状态将会保持原有启用/禁用状态。例如，某个聚合策略成员原有状态为禁用，那么当启用其所属的聚合策略后，该聚合策略成员状态依旧保持禁用状态。

添加/删除聚合策略描述信息

在聚合策略的配置模式下，管理员可以通过使用以下命令为聚合策略添加描述信息。

description *description*

- *description* – 指定聚合策略描述信息。范围是1到95个字符。

在聚合策略的配置模式下，使用以下命令删除聚合策略的描述信息。

no description

附表：ICMPv6 Type以及Code值对照表

ICMPv6 Type	ICMPv6 Code	Reference
1 Destination Unreachable	0 - no route to destination	[RFC4443]
	1 - communication with destination administratively prohibited	[RFC4443]
	2 - beyond scope of source address	[RFC4443]
	3 - address unreachable	[RFC4443]
	4 - port unreachable	[RFC4443]
	5 - source address failed ingress/egress policy	[RFC4443]
	6 - reject route to destination	[RFC4443]
2 Packet Too Big	0	[RFC4443]
3 Time Exceeded	0 - hop limit exceeded in transit	[RFC4443]
	1 - fragment reassembly time exceeded	[RFC4443]
4 Parameter Problem	0 - erroneous header field encountered	[RFC4443]
	1 - unrecognized Next Header type encountered	[RFC4443]
	2 - unrecognized IPv6 option encountered	[RFC4443]

ICMPv6 Type	ICMPv6 Code	Reference
100 Private experimentation	-	[RFC4443]
101 Private experimentation	-	[RFC4443]
102-126 Unassigned	-	[RFC4443]
127 Reserved for expansion of ICMPv6 error messages	-	[RFC4443]
128 Echo Request	0	[RFC4443]
129 Echo Reply	0	[RFC4443]
130 Multicast Listener Query	0	[RFC2710]
131 Multicast Listener Report	0	[RFC2710]
132 Multicast Listener Done	0	[RFC2710]
133 Router Solicitation	0	[RFC4861]
134 Router Advertisement	0	[RFC4861]
135 Neighbor Solicitation	0	[RFC4861]
136 Neighbor Advertisement	0	[RFC4861]
137 Redirect Message	0	[RFC4861]
138 Router Renumbering	0 - Router Renumbering Command	[Crawford] [RFC2894]
	1 - Router Renumbering Result	[Crawford] [RFC2894]
	255 - Sequence Number Reset	[Crawford] [RFC2894]
139 ICMP Node Information	0 - The Data field contains an IPv6 address which is the Subject of this	[RFC4620]

ICMPv6 Type	ICMPv6 Code	Reference
Query	Query	
	1 - The Data field contains a name which is the Subject of this Query, or is empty, as in the case of a NOOP.	[RFC4620]
	2 - The Data field contains an IPv4 address which is the Subject of this Query.	[RFC4620]
140 ICMP Node Information Response	0 - A successful reply. The Reply Data field may or may not be empty.	[RFC4620]
	1 - The Responder refuses to supply the answer. The Reply Data field will be empty.	[RFC4620]
	2 - The Qtype of the Query is unknown to the Responder. The Reply Data field will be empty.	[RFC4620]
141 Inverse Neighbor Discovery Solicitation Message	0	[RFC3122]
142 Inverse Neighbor Discovery Advertisement Message	0	[RFC3122]
143 Version 2 Multicast Listener Report	-	[RFC3810]
144 Home Agent Address Discovery Request Message	0	[RFC3775]
145 Home Agent Address Discovery Reply Message	0	[RFC3775]
146 Mobile Prefix Solicitation	0	[RFC3775]
147 Mobile Prefix Advertisement	0	[RFC3775]
148 Certification Path Solicitation Message	-	[RFC3971]
149 Certification Path Advertisement Message	-	[RFC3971]
150 ICMP messages utilized by experimental mobility protocols such as Seamoby	-	[RFC4065]

ICMPv6 Type	ICMPv6 Code	Reference
151 Multicast Router Advertisement	-	[RFC4286]
152 Multicast Router Solicitation	-	[RFC4286]
153 Multicast Router Termination	-	[RFC4286]
154 FMIPv6 Messages	-	[RFC5268]
200 Private experimentation	-	[RFC4443]
201 Private experimentation	-	[RFC4443]
255 Reserved for expansion of ICMPv6 informational messages	-	[RFC4443]

第11章 威胁防护

攻击防护

网络中存在多种防不胜防的攻击，如侵入或破坏网络上的服务器、盗取服务器的敏感数据、破坏服务器对外提供的服务，或者直接破坏网络设备导致网络服务异常甚至中断。作为网络安全设备，必须具备攻击防护功能来检测各种类型的网络攻击，从而采取相应的措施保护内部网络免受恶意攻击，以保证内部网络及系统正常运行。

系统提供基于安全域的攻击防护功能，能够对网络攻击进行合理处理从而保证用户网络系统的安全。

常见网络攻击概述

本节介绍一些常见的网络攻击。设备能够对这些网络攻击进行合理处理从而保证用户网络系统的安全。

ICMP Flood和UDP Flood攻击

这种攻击在短时间内向被攻击目标发送大量的ICMP消息（如ping）和UDP报文，请求回应，致使被攻击目标负担过重而不能完成正常的传输任务。

ARP欺骗攻击

局域网的网络流通根据MAC地址进行传输。ARP欺骗攻击是通过填写错误的发送端MAC地址和IP地址，使目标主机的ARP缓存表中IP地址和MAC地址对应关系错误。导致目标主机后续将IP数据报文时发给错误主机，目标网络不通且报文资源被窃取。

SYN Flood攻击

由于资源的限制，服务器只能允许有限个TCP连接。而SYN Flood攻击正是利用这一点，它伪造一个SYN报文，将其源地址设置成伪造的或者不存在的地址，然后向服务器发起连接。服务器在收到报文后用SYN-ACK应答，而此应答发出去后，不会收到ACK报文，从而造成半连接。如果攻击者发送大量这样的报文，会在被攻击主机上出现大量的半连接，直到半连接超时，从而消耗尽其资源，使正常的用户无法访问。在连接不受限制的环境里，SYN Flood会消耗掉系统的内存等资源。

WinNuke攻击

WinNuke攻击通常向装有Windows系统的特定目标的NetBIOS端口（139）发送OOB（out-of-band）数据包，引起一个NetBIOS片断重叠，致使被攻击主机崩溃。还有一种是IGMP分片报文。一般情况下，IGMP报文是不会分片的，所以，不少系统对IGMP分片报文的处理有问题。如果收到IGMP分片报文，则基本可判定受到了攻击。

IP地址欺骗（IP Spoofing）攻击

IP地址欺骗攻击是一种获取对计算机未经许可的访问的技术，即攻击者通过伪IP地址向计算机发送报文，并显示该报文来自于真实主机。对于基于IP地址进行验证的应用，此攻击方法能够使未被授权的用户访问被攻击系统。即使响应报文不能到达攻击者，被攻击系统也会遭到破坏。

地址扫描与端口扫描攻击

这种攻击运用扫描工具探测目标地址和端口，对此作出响应的表示其存在，从而确定哪些目标系统确实活着并且连接在目标网络上，这些主机使用哪些端口提供服务。

Ping of Death攻击

Ping of Death就是利用一些尺寸超大的ICMP报文对系统进行的一种攻击。IP报文的字段长度为16位，这表明一个IP报文的最大长度为65535字节。对于ICMP回应请求报文，如果数据长度大于65507字节，就会使ICMP数据、IP头长度（20字节）和ICMP头长度（8字节）的总合大于65535字节。一些路由器或系统在接收到这样一个报文后会由于处理不当，造成系统崩溃、死机或重启。

Teardrop攻击防护

Teardrop攻击是一种拒绝服务攻击。是基于UDP的病态分片数据包的攻击方法，其工作原理是向被攻击者发送多个分片的IP包（IP分片数据包中包括该分片数据包属于哪个数据包以及在数据包中的位置等信息），某些操作系统收到含有重叠偏移的伪造分片数据包时将会出现系统崩溃、重启等现象。

Smurf攻击

Smurf攻击分简单和高级两种。简单Smurf攻击用来攻击一个网络。方法是将ICMP应答请求包的目标地址设置为被攻击网络的广播地址，这样该网络的所有主机都会对此ICMP应答请求作出答复，从而导致网络阻塞。高级Smurf攻击主要用来攻击目标主机。方法是将ICMP应答请求包的源地址更改为被攻击主机的地址，最终导致被攻击主机崩溃。理论上讲，网络的主机越多，攻击的效果越明显。

Fraggle攻击

Fraggle攻击与Smurf攻击为同种类型攻击。不同之处在于Fraggle攻击使用UDP包形成攻击。

Land攻击

在Land攻击中，攻击者将一个特别打造的数据包的源地址和目标地址都设置成被攻击服务器地址。这样被攻击服务器向它自己的地址发送消息，结果这个地址又发回消息并创建一个空连接，每一个这样的连接都将保留直到超时。在这种Land攻击下，许多服务器将崩溃。

IP Fragment攻击

攻击者通过向目标主机发送分片偏移小于5的分片报文，导致主机对分片报文进行重组时发生错误而造成系统崩溃。

IP Option攻击

攻击者利用IP报文中的异常选项的设置，达到探测网络结构的目的，也可由于系统缺乏对错误报文的处理而造成系统崩溃。

Huge ICMP包攻击

某些主机或设备收到超大的报文，会引起内存分配错误而导致协议栈崩溃。攻击者通过发送超大ICMP报文，让目标主机崩溃，达到攻击目的。

TCP Flag异常攻击

不同操作系统对于非常规的TCP标志位有不同的处理。攻击者通过发送带有非常规TCP标志的报文探测目标主机的操作系统类型，若操作系统对这类报文处理不当，攻击者便可达到使目标主机系统崩溃的目的。

DNS Query Flood攻击

DNS服务器收到任何DNS Query报文时都会试图进行域名解析并且回复该DNS报文。攻击者通过构造并向DNS服务器发送大量虚假DNS Query报文，占用DNS服务器的带宽或计算资源，使得正常的DNS Query得不到处理。

TCP Split Handshake攻击

客户端与恶意TCP服务器建立TCP连接时，恶意服务器伪造SYN包及其内容，向客户端发起TCP连接。建立TCP连接后，恶意TCP服务器反转角色变成了发起TCP连接的“客户端”，使得恶意流量进入内网。

配置攻击防护功能

设备的攻击防护功能在默认情况下，只有部分功能在Untrust安全域是开启的，包括IP地址欺骗攻击防护、IP扫描攻击防护、端口扫描攻击防护、ICMP Flood攻击防护、SYN Flood攻击防护、UDP Flood攻击防护、WinNuke攻击防护、Ping of Death攻击防护、Teardrop攻击防护、IP Option攻击防护、IP Fragment攻击防护、IP Directed Broadcast攻击防护和Land攻击防护。

开启安全域的所有攻击防护功能，在安全域配置模式下，使用以下命令：

ad all

在安全域配置模式下使用**no ad all**命令关闭安全域的所有攻击防护功能。

用户可以对各种攻击防护功能的具体参数根据需求进行配置。Hillstone设备的攻击防护配置包括：

- 配置IP地址扫描攻击防护功能
- 配置端口扫描攻击防护功能
- 配置IP地址欺骗攻击防护功能

- 配置SYN Flood攻击防护功能
- 配置SYN-Proxy功能
- 配置ICMP Flood攻击防护功能
- 配置UDP Flood攻击防护功能
- 配置Huge ICMP包攻击防护功能
- 配置WinNuke攻击防护功能
- 配置Ping of Death攻击防护功能
- 配置Teardrop攻击防护功能
- 配置IP Option攻击防护功能
- 配置TCP异常攻击防护功能
- 配置Land攻击防护功能
- 配置IP 碎片攻击防护功能
- 配置Smurf和Fraggle攻击防护功能
- 配置ARP欺骗防护功能
- 配置DNS Query Flood攻击防护功能
- 配置DNS Reply Flood攻击防护功能
- 限制IP地址连接数
- 显示安全域的攻击防护配置和统计信息

配置IP地址扫描攻击防护功能

用户可以单独开启或者关闭安全域的IP地址扫描攻击防护功能，也可以配置地址扫描的警戒时间值和设备采取的行为。配置指定域的IP地址扫描攻击防护功能，在安全域配置模式使用以下命令：

```
ad ip-sweep [threshold value | action {alarm | drop}]
```

- **ad ip-sweep** - 开启安全域的IP地址扫描攻击防护功能。使用**no ad ip-sweep**关闭该功能。
- **threshold value** - 指定地址扫描的时间警戒值。如果设备探测到在该指定时间内有10个以上来自同一个源IP地址的ICMP包发往不同的主机，设备就认为是受到IP地址扫描攻击。默认值是1，单位是毫秒，取值范围是1到5000毫秒。使用**no ad ip-sweep threshold**命令恢复警戒默认值。
- **action {alarm | drop}** - 指定设备对于IP地址扫描攻击的所采取的行为。**alarm** - 发出警报但是允许包通过；**drop** - 在指定时间内（**threshold value**），设备仅允许10个来自同一个源IP地址的发往不同主机的ICMP包通过，并且发出警报，指定时间内的其它同类包将会被丢弃。默认行为是drop。使用**no ad ip-sweep action**恢复默认操作。

配置端口扫描攻击防护功能

用户可以单独开启或者关闭安全域的端口扫描攻击防护功能，也可以配置端口扫描的警戒时间值和设备采取的行为。配置安全域的端口扫描攻击防护功能，在安全域配置模式使用以下命令：

```
ad port-scan [threshold value | action {alarm | drop}]
```

- **ad port-scan** - 开启安全域的端口扫描攻击防护功能。使用**no ad port-scan**关闭该功能。
- **threshold value** - 指定端口扫描的时间警戒值。如果设备探测到同一个源IP地址在该指定时间内有10个以上TCP SYN包发往同一目标的不同端口，Hillstone设备就认为是受到了端口扫描攻击。默认值是1，单位是毫秒，取值范围是1到5000毫秒。使用**no ad port-scan threshold**命令恢复警戒默认值。
- **action {alarm | drop}** - 指定设备对于端口扫描攻击所采取的行为。**alarm** - 发出警报但是允许包通过；**drop** - 在指定时间内（**threshold value**），设备仅允许10个发往同一目标的不同端口的TCP SYN包通过，并且发出警报，指定时间内的其它同类包将会被丢弃。默认行为是drop。使用**no ad port-scan action**恢复默认操作。

配置IP地址欺骗攻击防护功能

系统可防护三层IP地址欺骗攻击。

开启设备的三层IP地址欺骗攻击防护功能后，数据包进入设备后，系统会对其源IP地址进行反向路由查询，并根据反向路由查询结果采取不同的行为，包括：

- 如果以该IP为源地址的数据包进入设备的安全域和以该IP为目的地址的数据包离设备的安全域是一致的（根据反向路由查询结果可以知道以该IP为目的地址的数据包离设备的安全域），则该数据包正常通过。
- 反之，系统判断该数据包为非正常数据包，将发出警报并丢弃该数据包。

开启安全域的三层IP地址欺骗攻击防护功能，在三层安全域配置模式下使用以下命令：

ad ip-spoofing

在安全域配置模式下使用**no ad ip-spoofing**关闭安全域的IP地址欺骗攻击防护功能。

配置SYN Flood攻击防护功能

用户可以单独开启或者关闭域的SYN Flood攻击防护功能，也可以配置SYN Flood攻击的源IP、目的IP和目的端口的警戒值以及设备的采取的行为。配置设备的SYN Flood攻击防护功能，在域配置模式下使用以下命令：

ad syn-flood [source-threshold *number* | destination-threshold [ip-based | port-based] *number* | destination [ip-based | port-based] [address-book *address-entry* | A.B.C.D/M] | action {alarm | drop}]

- **ad syn-flood** – 开启安全域的SYN Flood攻击防护功能。使用**no ad syn-flood**关闭该功能。
- **source-threshold *number*** – 指定一秒钟内从一个源IP地址发出的SYN包的个数，无论目标IP地址和端口号是什么。如果设备探测到一秒钟内从同一个源IP地址发出的SYN包多于该指定数，就判断为受到了SYN Flood攻击。默认值是1500个。取值范围是0到50000个。0表示不对源警戒值进行检测。使用**no ad syn-flood source-threshold**命令恢复默认值。
- **destination-threshold [ip-based | port-based] *number*** – 指定一秒钟内同一个目的IP地址（**ip-based**）或者同一目的IP的同一个目的端口（**port-based**）收到的SYN包个数，若不指定，则默认为**ip-based**。如果设备探测到一秒钟同一个目的IP地址或者同一目的IP的同一个目的端口收到的SYN包多于该指定数，就认为是受到了SYN Flood攻击。默认值是1500个。取值范围是0到50000个。0表示不对目的警戒值进行检测。使用**no ad syn-flood destination-threshold [ip-base | port-base]**命令恢复默认值。
- **destination [ip-based | port-based] [address-book *address-entry* | A.B.C.D/M]** – 开启基于目的IP地址（**ip-based**）或者目的端口（**port-based**）的SYN Flood攻击防护功能，若不指定，则默认为**ip-based**。使用**address-book *address-entry* | A.B.C.D/M**参数，指定开启特定网段的基于目的端口的SYN Flood攻击防护功

能，其它网段做基于目的IP地址的SYN Flood攻击防护。目的IP地址掩码取值范围是24到32。使用**no ad syn-flood destination**命令取消相应配置。

- **action {alarm | drop}** – 指定设备对于SYN Flood攻击采取的行为。**alarm** – 发出警报但是允许包通过；**drop** – 设备仅允许指定个数（**source-threshold number** | **destination-threshold number**）的SYN包通过，并且发出警报；如果同时配置了源和目的警戒值，系统会先检查其是否为目的SYN Flood攻击，如果是，则丢弃并报警，如果不是，再检查其是否为源SYN Flood攻击，是则丢弃并报警。默认行为是drop。使用**no ad syn-flood action**恢复默认操作。

配置SYN-Proxy功能

设备还提供SYN-Proxy功能配合**ad syn-flood**命令来共同防护SYN Flood攻击。当**ad syn-flood**和SYN-Proxy功能都开启时，SYN-Proxy功能对已经通过**ad syn-flood**检测的数据包起效。

设备支持SYN-Cookie功能。SYN-Cookie是一种无状态的SYN-Proxy机制。

配置安全域的SYN-Proxy以及SYN-Cookie功能，在安全域配置模式下使用以下命令：

ad syn-proxy [min-proxy-rate number | max-proxy-rate number | proxy-timeout number | cookie]

- **ad syn-proxy** – 开启安全域的SYN-Proxy功能用以防护SYN Flood攻击。使用**no ad syn-proxy**关闭该功能。
- **min-proxy-rate number** – 指定激活SYN-Proxy机制或者SYN-Cookie机制（通过**cookie**参数开启SYN-Cookie功能后）的最小SYN包个数值。如果一个目的IP地址的同一个端口在一秒钟内收到的SYN包个数多于该参数的指定值，就会激活SYN-Proxy或者SYN-Cookie机制。**number**默认值是1000个每秒，取值范围是0到50000。使用**no ad syn-proxy min-proxy-rate**恢复默认值。
- **max-proxy-rate number** – 指定SYN-Proxy机制或者SYN-Cookie机制（通过**cookie**参数开启SYN-Cookie功能后）在指定时间内允许通过的最大SYN包个数。如果一个目的IP地址的同一个端口在一秒钟内收到的SYN包个数多于该参数的指定值，设备会在当前秒和下一秒内仅允许该指定数值的SYN包通过，其它同类包将会被丢弃。**number**默认值是3000个每秒，取值范围是1到1500000。使用**no ad syn-proxy max-proxy-rate**命令恢复默认值。
- **proxy-timeout number** – 指定半连接的超时时间值。半连接达到该超时值后会被丢弃。默认值是30，单位为秒，取值范围是1到180秒。使用**no ad syn-proxy proxy-timeout**命令恢复默认值。

- **cookie** – 开启SYN-Cookie功能（如果需要开启该功能，请先开启SYN-Proxy功能）。该功能开启后，能够在功能上扩大设备处理多个SYN包的能力，因此用户可以适当的增大**min-proxy-rate**和**max-proxy-rate**两个参数之间的范围。使用**no ad syn-proxy cookie**命令关闭SYN-Cookie功能。

配置ICMP Flood攻击防护功能

用户可以单独开启或者关闭安全域的ICMP Flood攻击防护功能，也可以配置ICMP包个数的警戒值以及设备采取的操作。配置设备的ICMP Flood攻击防护功能，在安全域配置模式下使用以下命令：

ad icmp-flood [threshold number | action {alarm | drop}]

- **ad icmp-flood** – 开启安全域的ICMP Flood攻击防护功能。使用**no ad icmp-flood**关闭该功能。
- **threshold number** – 指定设备收到的ICMP包的个数的警戒值。如果同一个目的IP地址在一秒钟内收到的ICMP包的个数超过该警戒值，Hillstone设备就判断为受到ICMP Flood攻击，从而采取相应的处理。**number**的默认值是1500个，取值范围是1到50000。使用**no ad icmp-flood threshold**恢复默认值。
- **action {alarm | drop}** – 指定设备对于ICMP Flood攻击采取的行为。**alarm** – 发出警报但是允许包通过；**drop** – 在发生攻击的当前秒和下一秒这段时间内，设备仅允许指定个数（**threshold number**）的ICMP包通过，并且发出警报，在这段时间内的其它同类包将会被丢弃。默认行为是**drop**。使用**no ad icmp-flood action**恢复默认操作。

配置UDP Flood攻击防护功能

用户可以单独开启或者关闭安全域的UDP Flood攻击防护功能，也可以配置UDP包个数的警戒值以及设备采取的操作。配置设备的UDP Flood攻击防护功能，在安全域配置模式下使用以下命令：

ad udp-flood [source-threshold number | destination-threshold number | action {alarm | drop}]

- **ad udp-flood** – 开启安全域的UDP Flood攻击防护功能。使用**no ad udp-flood**关闭该功能。
- **source-threshold number** – 指定设备发送的UDP包的个数的警戒值。如果同一个源IP地址在一秒钟内发送的UDP包的个数超过该警戒值，设备就判断为受到UDP Flood攻击，从而采取相应的处理。**number**的默认值是1500个，取值范围是0到300000。使用**no ad udp-flood source-threshold**恢复默认值。
- **destination-threshold number** – 指定设备收到的UDP包的个数的警戒值。如果同一个目的IP地址的同一个端口号在一秒钟内收到的UDP包的个数超过该警戒值，设备就判断为受到UDP Flood攻击，从而采取相应的

处理。number的默认值是1500个，取值范围是0到300000。使用**no ad udp-flood destination-threshold**恢复默认值。

- **action {alarm | drop}** – 指定设备对于UDP Flood攻击采取的行为。**alarm** – 发出警报但是允许包通过；**drop** – 在发生攻击的当前秒和下一秒这段时间内，设备仅允许指定个数（**source-threshold number | destination-threshold number**）的UDP包通过，并且发出警报，在这段时间内的其它同类包将会被丢弃。默认行为是drop。使用**no ad udp-flood action**恢复默认操作。

配置Huge ICMP包攻击防护功能

用户可以单独开启或者关闭安全域的Huge ICMP攻击防护功能，也可以配置ICMP包的大小的警戒值以及设备采取的行为。配置设备的Huge ICMP攻击防护功能，在安全域配置模式下使用一下命令：

ad huge-icmp-pak [threshold number | action {alarm | drop}]

- **ad huge-icmp-pak** – 开启安全域的Huge ICMP包攻击防护功能。使用**no ad huge-icmp-pak**关闭该功能。
- **threshold number** – 指定ICMP包的大小的警戒值。如果收到的ICMP包的大小大于该指定值，设备就判断为受到Huge ICMP包攻击，从而采取相应的处理措施。number默认值是1024字节，取值范围是1到50000字节。使用**no ad huge-icmp-pak threshold**恢复默认值。
- **action {alarm | drop}** – 指定Hillstone设备对于Huge ICMP包攻击采取的行为。**alarm** – 发出警报但是允许包通过；**drop** – 发出警报并且丢弃攻击包。默认行为是drop。使用**no ad udp-flood action**恢复默认操作。

配置WinNuke攻击防护功能

WinNuke攻击防护功能开启后，当设备发现受到WinNuke攻击后，会丢弃攻击包并且发出警报通知。开启安全域的WinNuke攻击防护功能，在安全域配置模式使用以下命令：

ad winnuke

在安全域配置模式下，使用**no ad winnuke**关闭安全域的WinNuke攻击防护功能。

配置Ping of Death攻击防护功能

Ping of Death攻击防护功能开启后，当设备发现受到Ping of Death攻击后，会丢弃攻击包并且发出警报通知。开启安全域的Ping of Death攻击防护功能，在安全域配置模式使用以下命令：

ad ping-of-death

在安全域配置模式下，使用**no ad ping-of-death**关闭安全域的Ping of Death攻击防护功能。

配置Teardrop攻击防护功能

Teardrop攻击防护功能开启后，当设备发现受到Teardrop攻击后，会丢弃攻击包并且发出警报通知。开启安全域的Teardrop攻击防护功能，在安全域配置模式使用以下命令：

ad tear-drop

在安全域配置模式下，使用**no ad tear-drop**关闭安全域的Teardrop攻击防护功能。

配置IP Option攻击防护功能

IP Option攻击防护功能开启后，默认情况下当Hillstone设备发现受到IP Option攻击后，会丢弃攻击包并且发出警报通知。用户可以根据需要改变Hillstone设备的行为。Hillstone设备会对以下IP Option类型进行防护：Security、Loose Source Route、Record Route、Stream ID、Strict Source Route和Timestamp。配置IP Option攻击防护功能，在安全域配置模式使用以下命令：

ad ip-option [action {alarm | drop}]

- **ad ip-option** – 开启安全域的IP Option攻击防护功能。使用**no ad ip-option**命令关闭该功能。
- **action {alarm | drop}** – 指定设备对于IP Option攻击采取的行为。**alarm** – 发出警报但是允许包通过；**drop** – 发出警报并且丢弃攻击包。默认行为是drop。使用**no ad ip-option action**恢复默认行为。

配置TCP异常攻击防护功能

TCP异常攻击防护功能开启后，默认情况下当Hillstone设备发现受到TCP异常攻击后，会丢弃攻击包并且发出警报通知。用户可以根据需要改变Hillstone设备的行为。当Hillstone设备检测到以下各种情况，就会判断为受到TCP异常攻击：

- SYN包被分片；
- TCP包仅设置了FIN flag；
- TCP包仅没有设置flag；
- TCP包的FIN和RST flag同时被设置；
- TCP包的SYN和URG flag同时被设置；

- TCP包的SYN和RST flag同时被设置；
- TCP包的SYN和FIN flag同时被设置。

配置TCP异常攻击防护功能，在安全域配置模式使用以下命令：

```
ad tcp-anomaly [action {alarm | drop}]
```

- **ad tcp-anomaly** - 开启安全域的TCP异常攻击防护功能。使用**no ad tcp-anomaly**命令关闭该功能。
- **action {alarm | drop}** - 指定Hillstone设备对于TCP异常攻击采取的行为。**alarm** - 发出警报但是允许包通过；**drop** - 发出警报并且丢弃攻击包。默认行为是drop。使用**no ad tcp-anomaly action**恢复默认操作。

配置Land攻击防护功能

Land攻击防护功能开启后，默认情况下当设备发现受到Land攻击后，会丢弃数据包并且发出警报通知。用户可以根据需要改变设备的行为。配置Land攻击防护功能，在安全域配置模式使用以下命令：

```
ad land-attack [action {alarm | drop}]
```

- **ad land-attack** - 开启安全域的Land攻击防护功能。使用**no ad land-attack**命令关闭该功能。
- **action {alarm | drop}** - 指定设备对于Land攻击采取的行为。**alarm** - 发出警报但是允许包通过；**drop** - 发出警报并且丢弃攻击包。默认行为是drop。使用**no ad land-attack action**恢复默认操作。

配置IP 碎片攻击防护功能

数据包在不同网络间进行传输时，有时需要根据网络的MTU值将数据包分片。攻击者可以通过修改IP碎片在重组过程中发现漏洞进行攻击。当被攻击方收到被修改过的IP碎片后，轻则不能正确重组碎片，重则导致整个系统崩溃。

默认情况下当设备发现受到IP碎片攻击后，会丢弃攻击包并且发出警报通知。用户可以根据需要改变设备的行为。配置IP 碎片攻击防护功能，在安全域配置模式使用以下命令：

```
ad ip-fragment [action {alarm | drop}]
```

- **ad ip-fragment** - 开启安全域的IP碎片攻击防护功能。使用**no ad ip-fragment**命令关闭该功能。
- **action {alarm | drop}** - 指定设备对于IP碎片攻击采取的行为。**alarm** - 发出警报但是允许包通过；**drop** - 发出警报并且丢弃攻击包。默认行为是drop。使用**no ad ip-fragment action**恢复默认操作。

配置Smurf和Fraggle攻击防护功能

Smurf和Fraggle攻击防护功能开启后，默认情况下当设备发现受到Smurf或者Fraggle攻击后，会丢弃数据包并且发出警报通知。用户可以根据需要改变设备的行为。配置Smurf和Fraggle攻击防护功能，在安全域配置模式下使用以下命令：

ad ip-directed-broadcast [action {alarm | drop}]

- **ad ip-directed-broadcast** – 开启安全域的Smurf和Fraggle攻击防护功能。使用**no ad ip-directed-broadcast**命令关闭该功能。
- **action {alarm | drop}** – 指定设备对于Smurf和Fraggle攻击采取的行为。**alarm** – 发出警报但是允许包通过；**drop** – 发出警报并且丢弃所有包。默认行为是drop。使用**no ad ip-directed-broadcast action**恢复默认操作。

配置ARP欺骗防护功能

设备的ARP欺骗防护功能能够保护内网不受ARP欺骗攻击。配置ARP欺骗防护功能，在安全域配置模式使用以下命令：

ad arp-spoofing {reverse-query | ip-number-per-mac *number* [action [drop | alarm]] | gratuitous-arp-send-rate *number*}

- **reverse-query** – 开启ARP反向查询功能。当设备收到ARP请求后，会纪录IP地址并且发送ARP请求，检查是否会收到不同MAC地址的返回包或者返回包的MAC地址与ARP请求包的MAC地址是否相同。使用**no ad arp-spoofing reverse-query**命令关闭ARP反向查询功能。
- **ip-number-per-mac *number*** – 指定是否检查ARP表中一个MAC地址对应的IP地址数。如果该参数值为0（参数的默认值），则不检查；如果非0，则进行检查，并且如果每个MAC地址对应的IP地址数多于该参数的值，系统将按照**action [drop | alarm]**参数的配置进行处理，处理行为可以是发出警报并且丢弃该ARP包（drop）或者发出警报但是允许包通过（alarm）。该参数值的范围是0到1024。使用**no ad arp-spoofing ip-number-per-mac**命令恢复参数默认值。
- **gratuitous-arp-send-rate *number*** – 指定设备是否发出Gratuitous ARP包。如果该参数值是0，则不发Gratuitous ARP包（参数的默认值）；如果非0，则发出，并且每秒钟发出包的个数为该参数的值。该参数的取值范围是0到10。使用**no ad arp-spoofing gratuitous-arp-send-rate**命令恢复参数的默认值。

配置DNS Query Flood攻击防护功能

DNS是域名系统（Domain Name System）的简称，用来实现域名转换为IP地址和IP地址解析为域名。DNS是应用层协议，既可以基于TCP连接也可以基于UDP连接，DNS Query Flood攻击主要是指基于UDP的DNS查询报文洪水攻击。

DNS Query Flood攻击采用的方法是向被攻击的DNS服务器发送大量的域名解析请求，通常请求解析的域名是随机生成或者是网络上根本不存在的域名。被攻击的DNS服务器在接收到域名解析请求时，首先会在服务器上查找是否有对应的缓存，如果查找不到并且该域名无法直接由服务器解析时，DNS服务器会向其上层DNS服务器递归查询域名信息。域名解析的过程给服务器带来了很大的负载，每秒钟域名解析请求超过一定的数量就会造成DNS服务器解析域名超时。

设备支持DNS Query Flood攻击防护功能，用户可以单独开启或者关闭安全域的DNS Query Flood攻击防护功能，也可以配置DNS查询报文个数的警戒值以及设备采取的操作。配置设备的DNS Query Flood攻击防护功能，在安全域配置模式下使用以下命令：

```
ad dns-query-flood [recursion] [source-threshold number] [destination-threshold number | action {alarm | drop}]
```

- **ad dns-query-flood** – 开启安全域的DNS Query Flood攻击防护功能。使用**no ad dns-query-flood**关闭该功能。
- **recursion** – 指定仅限制DNS递归查询报文。当不设置此选项时，表示限制所有DNS查询报文。
- **source-threshold** *number* – 指定设备发送的DNS查询报文或DNS递归查询报文的个数的警戒值。如果一秒钟内同一个源IP地址发送的DNS查询报文个数超过该警戒值，设备就判断为受到DNS Query Flood攻击，从而采取相应的处理措施。*number*的默认值是1500个，取值范围是0到300000。使用**no ad dns-query-flood source-threshold**恢复默认值。
- **destination-threshold** *number* – 指定设备收到的DNS查询报文或DNS递归查询报文的个数的警戒值。如果一秒钟内设备收到的到达同一个目的IP地址的DNS查询报文个数超过该警戒值，设备就判断为受到DNS Query Flood攻击，从而采取相应的处理措施。*number*的默认值是1500个，取值范围是0到300000。使用**no ad dns-query-flood destination-threshold**恢复默认值。
- **action** {**alarm** | **drop**} – 指定设备对DNS Query Flood攻击采取的行为。**alarm** – 发出警报但是允许DNS查询报文通过；**drop** – 在发生攻击的当前秒和下一秒这段时间内，设备仅允许指定个数（*threshold number*）的DNS查询报文或DNS递归查询报文通过，并且发出警报，在这段时间内的其它同类包将会被丢弃。默认行为是drop。使用**no ad dns-flood action**恢复默认操作。



注意: DNS Query Flood攻击防护功能仅对UDP DNS查询报文有效。

配置DNS Reply Flood攻击防护功能

设备支持DNS响应洪水攻击防护功能，用户可以单独开启或者关闭安全域的DNS Reply Flood攻击防护功能，也可以配置DNS响应报文个数的警戒值以及设备采取的操作。

配置设备的DNS Reply Flood攻击防护功能，在安全域配置模式下使用以下命令：

```
ad dns-reply-flood [ source-threshold number ] [ destination-threshold number | action { alarm | drop } ]
```

- **ad dns-reply-flood** – 开启安全域的DNS Reply Flood攻击防护功能。使用**no ad dns-reply-flood**关闭该功能。
- **source-threshold *number*** – 指定设备发送的DNS响应报文的个数的警戒值。如果一秒钟内同一个源IP地址发送的DNS响应报文个数超过该警戒值，设备就判断为受到DNS Reply Flood攻击，从而采取相应的处理措施。*number*的默认值是1500个，取值范围是0到300000。使用**no ad dns-reply-flood source-threshold**恢复默认值。
- **destination-threshold *number*** – 指定设备收到的DNS响应报文的个数的警戒值。如果一秒钟内设备收到的到达同一个目的IP地址的DNS响应报文个数超过该警戒值，设备就判断为受到DNS Reply Flood攻击，从而采取相应的处理措施。*number*的默认值是1500个，取值范围是0到300000。使用**no ad dns-reply-flood destination-threshold**恢复默认值。
- **action {alarm | drop}** – 指定设备对DNS Reply Flood攻击采取的行为。**alarm** – 发出警报但是允许DNS响应报文通过；**drop** – 在发生攻击的当前秒和下一秒这段时间内，设备仅允许指定个数（**threshold *number***）的DNS响应报文通过，并且发出警报，在这段时间内的其它同类包将会被丢弃。默认行为是**drop**。使用**no ad dns-flood action**恢复默认操作。



注意: DNS Reply Flood攻击防护功能仅对UDP DNS响应报文有效。

配置TCP Split Handshake攻击防护功能

TCP Split Handshake攻击防护功能开启后，默认情况下当设备发现受到此类型攻击后，会丢弃数据包并且发出警报通知。用户可以根据需要改变设备的行为。配置TCP Split Handshake攻击防护功能，在安全域配置模式使用以下命令：

ad tcp-split-handshake [action {alarm | drop}]

- **ad tcp-split-handshake** – 开启安全域的TCP Split Handshake攻击防护功能。使用**no ad tcp-split-handshake**命令关闭该功能。
- **action {alarm | drop}** – 指定设备对于TCP Split Handshake攻击采取的行为。**alarm**发出警报但是允许包通过；**drop**发出警报并且丢弃攻击包。默认行为是drop。使用**no ad land-attack action**恢复默认操作。

配置攻击防护白名单

开启攻击防护功能后，安全域中的所有流量都会受到攻击防护功能的检查。在实际应用中，用户可能出于测试等目的不希望某些主机所发送的、发送到某些主机的流量进行检查。针对这种情况，用户可以将特定的地址或地址范围添加到攻击防护白名单。白名单中的地址或地址范围不受攻击防护功能的检查。

配置攻击防护白名单，在安全域配置模式下，使用以下命令：

ad whitelist [id id] {source-ip | destination-ip} {A.B.C.D/M | address-entry}

- **id** – 指定白名单规则的ID。各设备型号ID取值范围不同。如果不指定，系统将自动为该条规则分配一个ID。
- **source-ip | destination-ip** - 指定白名单的地址类型：源地址 **source-ip** 和目的地址 **destination-ip**。
- **A.B.C.D/M** – 指定添加到白名单规则中的IP地址和网络掩码。
- **address-entry** – 指定添加到白名单规则中的地址条目。

使用该命令**no**的形式删除指定的白名单规则：

no ad whitelist {id id | {source-ip | destination-ip} {A.B.C.D/M | addr-book}}

显示安全域的攻击防护配置和统计信息

系统能够显示安全域的攻击防护配置和统计信息。显示安全域的攻击防护配置和统计信息，在任何模式下使用以下命令：

```
show ad zone zone-name {statistics | configuration | whitelist}
```

- *zone-name* - 指定安全域的名称。
- **statistics** - 显示指定安全域的统计信息。
- **configuration** - 显示指定安全域的攻击防护配置信息。
- **whitelist** - 显示指定安全域的攻击防护白名单配置信息。

第12章 VPN

系统支持如下VPN功能：

- [IPSec VPN](#)：IPSec是IETF制定的三层隧道加密协议，它为互联网上传输的数据提供了高质量的、基于密码学的安全保证，是一种传统的实现三层VPN的安全技术。IPSec通过在特定通信方之间（例如两个安全设备之间）建立“通道”，来保护通信方之间传输的用户数据，该通道通常称为IPSec隧道。
- [IKEv2 VPN](#)：IKEv2 VPN相关配置。
- [GRE VPN](#)
- [VXLAN](#)
- [IPv6 6to4隧道](#)
- [IPv6 4to6隧道](#)
- [ISATAP隧道](#)

IPSec协议

IPSec协议介绍

IPSec是为实现VPN功能而最普遍使用的协议。IPSec不是一个单独的协议，它给出了应用于IP层上网络数据安全的一整套体系结构。该体系结构包括认证头协议（Authentication Header，简称为AH）、封装安全负载协议（Encapsulating Security Payload，简称为ESP）、密钥管理协议（Internet Key Exchange，简称为IKE）和用于网络认证及加密的一些算法等。IPSec规定了如何在对等体之间选择安全协议、确定安全算法和密钥交换，向上提供了访问控制、数据源认证、数据加密等网络安全服务。

- 认证头协议（AH）：IPsec体系结构中的一种主要协议，它为IP数据包提供无连接完整性的保护与数据源认证，并提供保护以避免重播情况。AH尽可能为IP头和上层协议数据提供足够多的认证。

- IPsec封装安全负载（ESP）：IPsec 体系结构中的一种主要协议。ESP加密需要保护的数据并且在IPsec ESP的数据部分进行数据的完整性校验，以此来保证机密性和完整性。ESP 提供了与AH相同的安全服务并提供了一种保密性（加密）服务，ESP与AH各自提供的认证根本区别在于它们的覆盖范围。
- 密钥管理协议（IKE）：用于协商AH和ESP所使用的密码算法，并将算法所需的必备密钥放到恰当位置。



注意: IPsec VPN支持使用国家商用密码算法配置。详细的国密算法标准，请参阅国家密码管理局颁发的《IPsec VPN技术规范》。

安全联盟（Security Association）

IPsec在两个端点之间提供安全通信，两个端点被称为IPsec ISAKMP网关。安全联盟（简称为SA）是IPsec的基础，也是IPsec的本质。SA是通信对等体间对某些要素的约定，例如使用哪种协议、协议的操作模式、加密算法（DES、3DES、AES-128、AES-192和AES-256）、特定流中保护数据的共享密钥以及SA的生存周期等。

安全联盟是单向的，在两个对等体之间的双向通信，最少需要两个安全联盟来分别对两个方向的数据流进行安全保护。

SA建立方式

建立安全联盟的方式有两种，一种是手工方式（Manual），一种是IKE自动协商（ISAKMP）方式。

手工方式配置比较复杂，创建安全联盟所需的全部信息都必须手工配置，而且IPsec的一些高级特性（例如定时更新密钥）不能被支持，但优点是可以不依赖IKE而单独实现IPsec功能。该方式适用于当与之进行通信的对等体设备数量较少的情况，或是IP地址相对固定的环境中。

IKE自动协商方式相对比较简单，只需要配置好IKE协商安全策略的信息，由IKE自动协商来创建和维护安全联盟。该方式适用于中、大型的动态网络环境中。该方式建立SA的过程分两个阶段。第一阶段，协商创建一个通信信道（ISAKMP SA），并对该信道进行认证，为双方进一步的IKE通信提供机密性、数据完整性以及数据源认证服务；第二阶段，使用已建立的ISAKMP SA建立IPsec SA。分两个阶段来完成这些服务有助于提高密钥交换的速度。

第一阶段SA

第一阶段SA为建立信道而进行的安全联盟。第一阶段协商的步骤是：

1. 参数配置。包括：
 - 认证方法：选择预共享密钥或数字证书认证
 - Diffie-Hellman组的选择
2. 策略协商。包括：
 - 加密算法：选择DES、3DES、AES-128、AES-192或AES-256
 - hash算法：选择MD5、SHA-1或SHA-2
3. DH交换。虽然名为“密钥交换”，但事实上在任何时候，两台通信主机之间都不会交换真正的密钥，它们之间交换的只是一些DH算法生成共享密钥所需要的基本材料信息。DH交换，可以是公开的，也可以受保护。在彼此交换过密钥生成“材料”后，两端主机可以各自生成出完全一样的共享“主密钥”，保护紧接其后的认证过程。
4. 认证。DH交换需要得到进一步认证，如果认证不成功，通信将无法继续下去。“主密钥”结合在第一步中确定的协商算法，对通信实体和通信信道进行认证。在这一步中，整个待认证的实体载荷，包括实体类型、端口号和协议，均由前一步生成的“主密钥”提供机密性和完整性保证。

第二阶段SA

第二阶段SA为快速SA，为数据传输而建立的安全联盟。这一阶段协商建立IPsec SA，为数据交换提供IPSec服务。第二阶段协商消息受第一阶段SA保护，任何没有第一阶段SA保护的消息将被拒收。第二阶段协商（快速模式协商）步骤是：

1. 策略协商，双方交换保护需求：
 - 使用哪种IPSec协议：AH或ESP
 - 是否使用hash算法：MD5、SHA-1、SHA-2或NULL
 - 是否要求加密，若是，选择加密算法：DES或3DES、AES-128、NULL、AES-192或AES-256
 - 是否使用压缩算法：DEFLATE
 - 在上述四方面达成一致后，将建立起两个SA，分别用于入站和出站通信。
2. 会话密钥“材料”刷新或交换。

在这一步中，将通过DH交换生成加密IP数据包的“会话密钥”。
3. 将SA递交给IPSec驱动程序。

在第二阶段协商过程中，如果响应超时，则自动尝试重新进行第二阶段SA协商。

验证算法

AH和ESP都能够对IP报文的完整性进行验证，以判别报文在传输过程中是否被篡改。验证算法的实现主要是通过杂凑函数。杂凑函数是一种能够接受任意长的消息输入，并产生固定长度输出的算法，该输出称为消息摘要。IPSec对等体计算摘要，如果两个摘要是相同的，则表示报文是完整未经篡改的。一般来说IPSec使用下列验证算法：

- MD5：MD5输入任意长度的消息，产生128bit的消息摘要。
- SHA-1：SHA-1输入长度小于2的64次方比特的消息，产生160bit的消息摘要。SHA-1的摘要长于MD5，因而更安全。
- SHA-2：SHA-2一般包含SHA-256、SHA-384和SHA-512三种杂凑函数，能将输入消息对应到更长的消息摘要。SHA-256输入长度小于2的64次方比特的消息，产生256bit的消息摘要；SHA-384输入长度小于2的128次方比特的消息，产生384bit的消息摘要；SHA-512输入长度小于2的128次方比特的消息，产生512bit的消息摘要。
- SM3：SM3输入长度小于2的64次方比特的消息，产生256bit的消息摘要。

加密算法

ESP能够对IP报文内容进行加密保护，防止报文内容在传输过程中被窥探。加密算法实现主要通过对称密钥系统，它使用相同的密钥对数据进行加密和解密。StoneOS实现了五种加密算法：

- DES（Data Encryption Standard）：使用56bit的密钥对每个64bit的明文块进行加密。
- 3DES（Triple DES）：使用三个56bit的DES密钥（共168bit密钥）对明文进行加密。
- AES（Advanced Encryption Standard）：StoneOS实现了128bit、192bit和256bit密钥长度的AES算法。
- SM1：国家密码管理局编制的一种商用密码分组标准对称算法。分组长度和密钥长度都为128bit。仅国密设备支持该算法。
- SM4：国家密码管理局编制的一种商用密码分组标准对称算法。分组长度和密钥长度都为128bit。

压缩算法

IPComp（IP Payload Compression，IP有效载荷压缩）是一个减少IP数据报长度的协议，该协议通过支持不同的压缩算法对IP数据报的有效负载进行压缩处理，从而实现通信数据在低带宽条件下的高负载传输。

应用IPComp的关键在于通信的两个端点之间必须首先建立一个IPComp关联（IPCA），此关联中包含了IPComp操作要求的所有信息，例如所使用的压缩算法以及所选择的压缩算法要求的参数等。使用IPComp对IPSec处理的网络数据流进行压缩时，用户可以手工配置创建IPCA，也可以通过动态协商创建IPCA。当使用动态协商方式时，ISAKMP网关提供建立IPCA必须的机制。Hillstone设备的IPSec功能提供以下IPComp压缩算法：

- DEFLATE：使用LZ77算法和Huffman译码，是一种可以在IPComp中实现的自由可用的无损耗压缩算法。

相关资料

StoneOS的IPSec功能遵循RFC中IPSec协议的规定。关于IPSec协议的更多详细信息，请参阅以下RFC文档的相关章节：

- Security Architecture for the Internet Protocol: RFC2401/RFC4301
- ESP：RFC2406/RFC4303
- AH：RFC2402/RFC4302
- 加密算法参考：RFC2410（Null Encryption），RFC2405（DES-CBC），RFC2451（3DES-CBC）以及RFC3602（AES-CBC）
- 验证算法参考：：FIPS180-2（SHA），RFC2404（SHA-1），RFC4868（SHA-2）以及RFC2403（MD5）
- 压缩算法参考：RFC2393（IPComp）以及RFC2394（DEFLATE）

IPSec VPN的应用

StoneOS通过“基于策略的VPN”和“基于路由的VPN”两种方式把配置好的VPN隧道应用到Hillstone设备上，实现流量的加密解密安全传输。

- 基于策略的VPN：将配置成功的VPN隧道名称引用到策略规则中，使符合条件的流量通过指定的VPN隧道进行传输。
- 基于路由的VPN：将配置成功的VPN隧道与隧道接口绑定；配置静态路由时，将隧道接口指定为下一跳路由。

IPSec VPN

IPSec是为实现VPN功能而使用的协议。IPSec给出了应用于IP层上网络数据安全的一整套体系结构。该体系结构包括认证头协议（Authentication Header，简称为AH）、封装安全负载协议（Encapsulating Security Payload，简称为ESP）、密钥管理协议（Internet Key Exchange，简称为IKE）和用于网络认证及加密的一些算法等。IPSec规定了如何在对等体之间选择安全协议、确定安全算法和密钥交换，向上提供了访问控制、数据源认证、数据加密等网络安全服务。

IPSec VPN基础概念

- 安全联盟
- 封装方式
- 协商方式
- 引用IPSec VPN

安全联盟

IPSec在两个端点之间提供安全通信，两个端点被称为IPSec ISAKMP网关。安全联盟（Security Association, 简称为SA）是IPSec的基础，也是IPSec的本质。SA是通信对等体间对某些要素的约定，例如使用哪种协议、协议的操作模式、加密算法（DES、3DES、AES-128、AES-192和AES-256）、特定流中保护数据的共享密钥以及SA的生存周期等。

安全联盟是单向的，在两个对等体之间的双向通信，最少需要两个安全联盟来分别对两个方向的数据流进行安全保护。

建立安全联盟的方式有两种，一种是手工方式（Manual），一种是IKE自动协商（ISAKMP）方式。

封装方式

IPSec有如下两种工作模式：

- 隧道（tunnel）模式：用户的整个IP数据包被用来计算AH或ESP头，AH或ESP头以及ESP加密的用户数据被封装在一个新的IP数据包中。通常，隧道模式应用在两台设备之间的通讯。
- 传输（transport）模式：只是传输层数据被用来计算AH或ESP头，AH或ESP头以及ESP加密的用户数据被放在原IP包头后面。通常，传输模式应用在两台主机之间的通讯，或一台主机和一台设备之间的通讯。

协商方式

手工方式配置比较复杂，创建安全联盟所需的全部信息都必须手工配置，而且IPSec的一些高级特性（例如定时更新密钥）不能被支持，但优点是可以不依赖IKE而单独实现IPSec功能。该方式适用于当与之进行通信的对等体设备数量较少的情况，或是IP地址相对固定的环境中。

IKE自动协商方式相对比较简单，只需要配置好IKE协商安全策略的信息，由IKE自动协商来创建和维护安全联盟。该方式适用于中、大型的动态网络环境中。该方式建立SA的过程分两个阶段。第一阶段，协商创建一个通信信道（ISAKMP SA），并对该信道进行认证，为双方进一步的IKE通信提供机密性、数据完整性以及数据源认证服务；第二阶段，使用已建立的ISAKMP SA建立IPSec SA。分两个阶段来完成这些服务有助于提高密钥交换的速度。

引用IPSec VPN

设备通过“基于策略的VPN”和“基于路由的VPN”两种方式把配置好的VPN隧道调用到设备上，实现流量的加密解密安全传输。

- 基于策略的VPN：将配置成功的VPN隧道名称引用到策略规则中，使符合条件的流量通过指定的VPN隧道进行传输。
- 基于路由的VPN：将配置成功的VPN隧道与隧道接口绑定；配置静态路由时，将隧道接口指定为下一跳路由。



相关链接：

- ["配置IKE VPN" 在第676页](#)
- ["配置手工密钥VPN" 在第694页](#)
- ["配置IPSec-XAUTH地址池" 在第698页](#)
- ["配置IPSec VPN监控" 在第703页](#)

配置IKE VPN

IKE自动协商方式相对比较简单，只需要配置好IKE协商安全策略的信息，由IKE自动协商来创建和维护安全联盟。该方式适用于中、大型的动态网络环境中。该方式建立SA的过程分两个阶段。第一阶段，协商创建一

个通信信道（ISAKMP SA），并对该信道进行认证，为双方进一步的IKE通信提供机密性、数据完整性以及数据源认证服务；第二阶段，使用已建立的ISAKMP SA建立IPSec SA。分两个阶段来完成这些服务有助于提高密钥交换的速度。

配置IKE VPN，需要确认第一阶段提议，第二阶段提议，以及VPN对端信息。确认这三部分内容后，可继续完成IKE VPN的配置。

- [配置P1提议](#)
- [配置P2提议](#)
- [配置ISAKMP网关](#)
- [配置隧道](#)

配置P1提议

P1提议是IKE安全提议，用来协商IKE SA，可应用到ISAKMP网关上，在SA第一阶段使用。对IKE安全提议的配置包括指定认证方式、加密算法、验证算法、DH组和安全联盟的生命周期。

创建P1提议

创建一个P1提议，即IKE安全提议，在全局配置模式下使用以下命令：

```
isakmp proposal p1-name
```

- *p1-name* – 指定所创建的P1提议的名称。执行该命令后，进入到P1提议配置模式。用户可以在该模式下对P1提议进行参数配置。

使用**no isakmp proposal** *p1-name*命令删除指定的P1提议。

指定认证方式

此处指定的是IKE身份认证的方式。身份认证用来确认通信双方的身份。方式有预共享密钥认证、数字证书认证和国密数据信封认证。对于预共享密钥认证方式，认证字用来作为一个输入产生密钥，认证字不同是不可能在双方产生相同的密钥的。

指定IKE安全提议的身份认证方式，在P1提议配置模式下使用以下命令：

```
authentication {pre-share | rsa-sig | dsa-sig | gm-de}
```

- **pre-share** – 指定使用预共享密钥认证方式。该方式为默认认证方式。
- **rsa-sig** – 指定使用RSA数字证书认证方式。
- **dsa-sig** – 指定使用DSA数字证书认证方式。此方式对应的验证算法只能为SHA-1。
- **gm-de** – 指定使用国密数据信封认证方式。当认证方式为此选项时，加密算法仅支持使用SM1和SM4，验证算法仅支持使用SHA或SM3。

使用**no authentication**命令恢复默认的认证方式**pre-share**。

指定加密算法

指定IKE安全提议的加密算法，在P1提议配置模式下使用以下命令：

```
encryption {3des | aes | des | aes-192 | aes-256 | sm4}
```

- **3des** – 指定使用3DES加密方法。密钥长度为192比特。该方法为默认方法。
- **aes** – 指定使用AES加密方法。密钥长度为128比特。
- **des** – 指定使用DES加密方法。密钥长度为64比特。
- **aes-192** – 指定使用192bit AES加密方法。密钥长度为192比特。
- **aes-256** – 指定使用256bit AES加密方法。密钥长度为256比特。
- **sm4** – 指定使用国家商用密码SM4分组密码算法。密钥长度为128比特。

使用**no encryption**命令恢复默认加密算法。

指定验证算法

指定IKE安全提议的验证算法，在P1提议模式下使用以下命令：

```
hash {md5 | sha | sha256 | sha384 | sha512 | sm3}
```

- **md5** – 指定使用MD5验证算法。摘要为128比特。
- **sha** – 指定使用SHA-1验证算法。摘要为160比特。该算法为默认算法。
- **sha256** – 指定使用SHA-256验证算法。摘要为256比特。

- **sha384** – 指定使用SHA-384验证算法。摘要为384比特。
- **sha512** – 指定使用SHA-512验证算法。摘要为512比特。
- **sm3** – 指定使用国密SM3验证算法。摘要为256比特。该算法用于密码应用中的数字签名和验证、消息认证的生成与验证，可满足多种密码应用的安全需求。

使用**no hash**命令恢复默认认证方式。

选择DH组

Diffie-Hellman (DH) 是一种建立密钥的方法。DH组决定DH交换中密钥生成“材料”的长度。密钥的牢固性部分决定于DH组的强度。密钥“材料”长度越长，所生成的密钥安全度也就越高，越难被破译。DH组的选择很重要，因为DH组只在第一阶段的SA协商中确定，第二阶段的协商不再重新选择DH组，两个阶段使用的是同一个DH组，因此该DH组的选择将影响所有会话密钥的生成。在协商过程中，两个ISAKMP网关间应选择同一个DH组，即密钥“材料”长度应该相等。若DH组不匹配，将协商失败。

在P1提议选择DH组，在P1提议配置模式下使用以下命令：

group {1 | 2 | 5 | 14 | 15 | 16 | 19 | 20 | 21 | 24}

- **1** – 选择DH组1。密钥的长度为768比特 (MODP Group)。
- **2** – 选择DH组2。密钥的长度为1024比特 (MODP Group)。2为系统默认值。
- **5** – 选择DH组5。密钥的长度为1536比特 (MODP Group)。
- **14** – 选择DH组14。密钥的长度为2048比特 (MODP Group)。
- **15** – 选择DH组15。密钥的长度为3072比特 (MODP Group)。
- **16** – 选择DH组16。密钥的长度为4096比特 (MODP Group)。
- **19** - 选择DH组19。密钥的长度为256比特 (ECP Group)。
- **20** - 选择DH组20。密钥的长度为384比特 (ECP Group)。
- **21** - 选择DH组21。密钥的长度为521比特 (ECP Group)。
- **24** - 选择DH组24。密钥的长度为2048比特 (MODP Group with 256-bit Prime Order Subgroup)。

使用**no group**命令恢复默认DH组。

在P2提议中配置PFS时，也可选用如上DH组。

指定安全联盟的生命周期

第一阶段SA有一个默认的生命周期，如果ISAKMP SA生命期时间到，要向对方发送第一阶段SA删除消息，通知对方第一阶段SA已经过期。之后需要重新进行SA协商。指定安全联盟的生命周期，在P1提议配置模式下使用以下命令：

lifetime *time-value*

- *time-value* – 指定SA第一阶段的生命周期长度。单位为秒，取值范围是300到86400秒。默认为86400秒。

使用**no lifetime**命令恢复默认生命周期长度。

配置P2提议

P2提议使用在SA第二阶段。对P2提议的配置包括指定协议类型、加密算法、验证算法、压缩算法和生命周期。

创建P2提议

创建P2提议，即IPSec安全提议，在全局配置模式下使用以下命令：

ipsec proposal *p2-name*

- *p2-name* – 指定所创建的P2提议的名称。执行该命令后，进入到P2提议配置模式。对P2提议各项参数的配置都要在该模式下进行。

使用**no ipsec proposal** *p2-name*命令删除指定的P2提议。

指定协议类型

P2提议可使用的协议类型有AH以及ESP。为P2提议指定协议类型，在P2提议配置模式下使用以下命令：

protocol {**esp** | **ah**}

- **esp** – 指定使用ESP协议。该协议为系统默认协议。
- **ah** – 指定使用AH协议。

使用**no protocol**命令恢复默认协议配置。

指定验证算法

用户可以为P2提议指定至少一种最多三种验证算法。为P2提议指定验证算法，在P2提议配置模式下使用以下命令：

```
hash {md5 | sha | sha256 | sha384 | sha512 | sm3 | null} [md5 | sha | sha256 | sha384 | sha512 | sm3 | null] [md5 | sha | sha256 | sha384 | sha512 | sm3 | null]
```

- **md5** – 指定使用MD5验证算法。摘要为128比特。
- **sha** – 指定使用SHA-1验证算法。摘要为160比特。该算法为默认算法。
- **sha256** – 指定使用SHA-256验证算法。摘要为256比特。
- **sha384** – 指定使用SHA-384验证算法。摘要为384比特。
- **sha512** – 指定使用SHA-512验证算法。摘要为512比特。
- **sm3** – 指定使用国密SM3验证算法。摘要为256比特。
- **null** – 不使用验证功能。

使用**no hash**命令恢复默认验证算法。

指定加密算法

用户可以为P2提议指定至少一种最多四种加密算法。为P2提议指定加密算法，在P2提议配置模式下使用以下命令：

```
encryption {3des | des | aes | aes-192 | aes-256 | sm4 | null} [3des | des | aes | aes-192 | aes-256 | sm4 | null] [3des | des | aes | aes-192 | aes-256 | sm4 | null]……
```

- **3des** – 指定使用3DES加密方法。密钥长度为192比特。该方法为系统默认方法。
- **des** – 指定使用DES加密方法。密钥长度为64比特。
- **aes** – 指定使用AES加密方法。密钥长度为128比特。
- **aes-192** – 指定使用192bit AES加密方法。密钥长度为192比特。
- **aes-256** – 指定使用256bit AES加密方法。密钥长度为256比特。

- **sm4** – 指定使用国家商用密码SM4分组密码算法。密钥长度为128比特。
- **null** – 不使用加密功能。

使用**no encryption**命令恢复默认加密算法。

指定压缩算法

默认情况下，P2提议不使用任何压缩算法。为P2提议指定压缩算法（DEFLATE算法），在P2提议配置模式下使用以下命令：

compression deflate

使用**no compression**命令取消对压缩算法的指定。

配置PFS功能

PFS（Perfect Forward Security）功能决定新密钥的生成方式，而不是新密钥的生成时间。PFS保证无论在哪个阶段，一个密钥只能使用一次，而且，生成密钥的“材料”也只能使用一次。某个“材料”在生成了一个密钥后就被弃，绝不用来再生成任何其它密钥。这样可以确保一旦单个密钥泄密，最多只可能影响用该密钥加密的数据，而不会危及整个通信。PFS功能是由DH算法做保障的。配置P2提议的PFS功能，在P2提议配置模式下使用以下命令：

group {nopfs | 1 | 2 | 5 | 14 | 15 | 16 | 19 | 20 | 21 | 24}

- **1** – 选择DH组1。密钥的长度为768比特（MODP Group）。
- **2** – 选择DH组2。密钥的长度为1024比特（MODP Group）。
- **5** – 选择DH组5。密钥的长度为1536比特（MODP Group）。
- **14** – 选择DH组14。密钥的长度为2048比特（MODP Group）。
- **15** – 选择DH组15。密钥的长度为3072比特（MODP Group）。
- **16** – 选择DH组16。密钥的长度为4096比特（MODP Group）。
- **19** - 选择DH组19。密钥的长度为256比特（ECP Group）。
- **20** - 选择DH组20。密钥的长度为384比特（ECP Group）。

- **21** - 选择DH组21。密钥的长度为521比特（ECP Group）。
- **24** - 选择DH组24。密钥的长度为2048比特（MODP Group with 256-bit Prime Order Subgroup）。

使用**no group**命令恢复默认配置。

指定生命周期

Hillstone设备有两种衡量生命周期的方法，分别是按时间和按流量。当SA的流量或者时间达到特定值时，SA就会过期，需要重新进行协商。指定P2提议的生命周期，在P2提议配置模式，使用以下命令：

lifetime *seconds*

- *seconds* – 指定时间类型生命周期的时间长度，单位为秒。默认值是28800秒。

lifesize *kilobytes*

- *kilobytes* – 指定流量类型周期的流量值，单位为字节。默认值是0，意义为没有周期流量限制。

使用以上两个命令**no**的形式恢复默认配置。即

no lifetime

no lifesize

配置ISAKMP网关

创建一个ISAKMP网关，即创建一个VPN对端后，用户可以配置ISAKMP网关的IKE协商模式、ISAKMP网关IP地址及类型、IKE安全提议、预共享密钥、PKI信任域、本地ID、ISAKMP网关ID、ISAKMP网关连接方式以及是否开启ISAKMP网关的NAT穿越功能等。

创建ISAKMP网关

创建ISAKMP网关，在全局配置模式下，使用以下命令：

isakmp peer *peer-name*

- *peer-name* – 指定ISAKMP网关的名称。

执行该命令后，CLI进入到ISAKMP网关配置模式。用户可以在该模式下对ISAKMP网关进行参数配置。

在全局配置模式下使用**no isakmp peer** *peer-name*命令删除指定的ISAKMP网关。

绑定接口到ISAKMP网关

用户可以绑定某个接口到ISAKMP网关。将接口绑定到ISAKMP网关，在ISAKMP网关配置模式下使用以下命令：

```
interface interface-name
```

- *interface-name* – 指定被绑定接口的名称。

使用**no interface** 命令取消接口的绑定。

配置IKE协商模式

IKE的协商模式有两种：主模式（main mode）和野蛮模式（aggressive mode）。IKE野蛮模式不提供身份保护，以下情况只能用野蛮模式：中心设备的IP地址为固定分配的地址，而客户端设备的IP地址为动态获取的地址。配置IKE协商模式，在ISAKMP网关配置模式下使用以下命令：

```
mode {main | aggressive}
```

- **main** – 指定使用主模式，可提供ID保护功能。该模式为系统的默认模式。
- **aggressive** – 指定使用野蛮模式。

使用**no mode**命令恢复默认协商模式。

配置自定义IKE协商端口

用户可以自定义UDP端口进行IKE协商，并且建立IPSec连接。配置自定义IKE协商端口，在ISAKMP网关配置模式下使用以下命令：

```
ipsec-over-udp port port-number
```

- *port-number* – 指定UDP端口号。取值范围是1到65535。

使用**no ipsec-over-udp**命令取消自定义的UDP端口配置。

指定对端的IP地址及类型

用户可以为所创建的ISAKMP网关指定对端的IP地址和IP地址的类型（静态或者动态）。指定对端的IP地址，在ISAKMP网关配置模式下使用以下命令：

```
type {dynamic | static}
```

- **dynamic** – 指定对端的IP地址为动态IP地址。
- **static** – 指定对端的IP地址为静态IP地址。该选项为系统的默认选项。

使用**no type**命令恢复对端IP地址的默认类型。

peer ip-address

- *ip-address* - 指定对端的IP地址或主机名称。该IP地址只有当对端的IP地址类型是静态的时候才有效。

使用**no peer**命令取消对端IP地址或主机名称的指定。

指定P1提议

为ISAKMP网关指定P1提议，在ISAKMP网关配置模式下使用以下命令：

isakmp-proposal *p1-proposal1* [*p1-proposal2*] [*p1-proposal3*] [*p1-proposal4*]

- *p1-proposal1* – 指定P1提议的名称。用户最多可以为ISAKMP网关指定4个P1提议供对端选择使用。

使用**no isakmp-proposal**取消对P1提议的指定。

配置预共享密钥

如果使用预共享密钥认证方式，用户就需要指定预共享密钥。为ISAKMP网关指定预共享密钥，在ISAKMP网关配置模式下使用以下命令：

pre-share *string*

- *string* – 指定预共享密钥的内容。

使用**no pre-share**取消对预共享密钥的指定。

配置PKI信任域

如果使用数字证书认证方式，用户就需要指定数字证书的PKI信任域。为ISAKMP网关指定PKI信任域，在ISAKMP网关配置模式下使用以下命令：

trust-domain *string*

- *string* – 指定PKI信任域。

使用**no trust-domain**取消对PKI信任域的指定。



提示: 关于如何配置PKI信任域, 请参阅《用户认证》的“[PKI配置](#)”部分。

配置对端证书的信任域

对端证书一般用于协商中数据加密以及认证, 需由发起VPN连接的一端先导入对端证书。该命令仅适用于国密1.0版本。配置对端证书所在的信任域, 在ISAKMP网关配置模式下使用以下命令:

remote-trust-domain *string*

- *string* – 指定对端证书所在的信任域。

使用**no remote-trust-domain**命令删除对端证书的信任域配置。

配置加密证书的信任域

加密证书一般用于协商中数据加密。该命令仅适用于国密1.1版本, 需为系统指定双证书。配置加密证书所在的信任域, 在ISAKMP网关配置模式下使用以下命令:

trust-domain-enc *string*

- *string* – 指定加密证书所在的信任域。

使用**no trust-domain-enc**命令删除加密证书的信任域配置。

配置协商协议标准

协商协议标准分为国际标准IKEv1和国密标准。默认情况下, 系统使用国际标准IKEv1为协商协议标准。指定协商协议的标准, 在ISAKMP网关配置模式下使用以下命令:

protocol-standard {*ikev1* | *guomi* [*v1.0* | *v1.1*]}

- **ikev1** – 指定使用国际标准IKEv1为协商协议标准。
- **guomi** [*v1.0* | *v1.1*] – 指定使用国密标准为协商协议标准。*v1.0*为国密1.0版本; *v1.1*为国密1.1版本。如指定版本号*v1.0*或*v1.1*, 进行协商的两端设备必须是相同的版本号才能协商成功, 否则协商失败。如不指定版本号, 那么发起端国密协议版本号为国密*v1.0*或*v1.1*都可协商。

使用**no protocol-standard**命令取消协商协议标准的配置。

配置本端ID

配置本端的ID，在ISAKMP网关配置模式下使用以下命令：

```
local-id {fqdn string | asn1dn [string] | u-fqdn string | key-id string | ip ip-address | ipv6 ipv6-address}
```

- **fqdn string** - 指定使用FQDN类型的ID。string为ID的具体内容。
- **asn1dn [string]** - 指定使用Asn1dn类型的ID，该类型只可应用于使用证书的情况。string为ID的具体内容。用户可以不指定ID的具体内容，在此种情况下，系统将从证书中获取ID。
- **u-fqdn string** - 指定使用U-FQDN类型的ID，即电子邮件地址类型，例如user1@hillstonenet.com。
- **key-id string** - 指定使用Key ID类型的ID。该类型仅应用于XAUTH功能。
- **ip ip-address** - 指定使用IPv4地址类型的ID。ip-address为ID的具体内容。
- **ipv6 ipv6-address** - 指定使用IPv6地址类型的ID。ipv6-address为ID的具体内容。

使用**no local-id**命令取消对本端ID的配置。

配置对端ID

配置对端的ID，请在ISAKMP网关配置模式下使用以下命令：

```
peer-id {fqdn | asn1dn | u-fqdn | key-id | ip | ipv6} string
```

- **fqdn** - 指定使用FQDN类型的ID。string为ID的具体内容。
- **asn1dn** - 指定使用Asn1dn类型的ID，该类型只可应用于使用证书的情况。string为ID的具体内容。
- **u-fqdn** - 指定使用U-FQDN类型的ID，即电子邮件地址类型，例如user1@hillstonenet.com。
- **key-id** - 指定使用Key ID类型的ID。该类型仅应用于XAUTH功能。
- **ip** - 指定使用IPv4地址类型的ID。
- **ipv6** - 指定使用IPv6地址类型的ID。

使用**no peer-id**命令取消对对端ID的配置。

指定连接类型

创建的ISAKMP网关可以是发起端、响应端或者既是发起端也是响应端。指定ISAKMP网关的连接类型，在ISAKMP网关配置模式下使用以下命令：

connection-type {bidirectional | initiator-only | responder-only}

- **bidirectional** – 指定该ISAKMP网关既是发起端也是响应端。该选项为系统的默认选项。
- **initiator-only** – 指定该ISAKMP网关仅是发起端。
- **responder-only** – 指定该ISAKMP网关仅是响应端。

使用**no connection-type**命令恢复默认连接方式。

开启NAT穿越功能

在IPSec或者IKE组建的VPN隧道中，若存在NAT网关设备，且NAT网关设备对VPN数据进行了NAT转换，则必须开启IPSec或者IKE的NAT穿越功能。默认情况下，NAT穿越功能是关闭的。开启NAT穿越功能，在ISAKMP网关配置模式下，使用以下命令：

nat-traversal

使用**no nat-traversal**命令关闭NAT穿越功能。

接受对端ID

使所创建的ISAKMP网关接受任意的对端ID，不对对端进行ID检查，在ISAKMP网关配置模式下使用以下命令：

accept-all-peer-id

使用**no accept-all-peer-id**关闭该功能。

配置自动生成路由功能

对于IKEv1 VPN，当指定对端的IP地址类型为static或dynamic时，配置自动生成路由功能后，每创建一个IPSec SA，设备会将目的地址为对端的local ID、下一跳为隧道接口的路由条目添加到自己的路由表。删除一个IPSec SA后，相应的路由条目也会被删除。

默认情况下，设备的自动生成路由功能是关闭的。开启此功能，在ISAKMP配置模式下，使用以下命令：

generate-route

使用**no generate-route**命令关闭自动生成路由功能。

配置DPD功能

DPD（Dead Peer Detection）为安全隧道对端状态探测功能。该功能开启后，系统将按照指定的时间间隔，周期性的向对端发送请求报文，对ISAKMP网关是否存在进行检测。默认情况下，DPD功能是关闭的。

配置DPD功能，在ISAKMP网关配置模式下使用以下命令：

dpd [*interval seconds*]

- **interval seconds** – 指定向对端发送查询请求的时间间隔。间隔范围是0到10秒。默认值是0，表示不开启DPD功能。

使用**no dpd**命令恢复默认的DPD配置。

指定描述信息

为所配置的ISAKMP网关指定描述信息，在ISAKMP网关配置模式下使用以下命令：

description *string*

- *string* – ISAKMP网关的描述信息。

使用**no description**命令删除ISAKMP网关的描述信息。

配置隧道

通过IKE配置IPSec隧道，即配置IKE VPN完成自动协商IPSec SA，用户需要配置的选项有指定协议类型、ISAKMP网关、IKE安全提议、ID号、是否分片以及防重放等。

创建IKE隧道

创建IKE隧道，在全局配置模式下，使用以下命令：

tunnel ipsec *tunnel-name* **auto**

- *tunnel-name* - 指定所创建的IKE隧道的名称。

执行该命令后，CLI进入到IKE隧道配置模式。对IKE隧道的所有参数配置都需要在该模式下进行。

在全局配置模式下使用**no tunnel ipsec** *tunnel-name* **auto**删除指定的IKE隧道。

启用/禁用IPSec VPN隧道

启用/禁用IPSec VPN隧道，在IKE隧道配置模式下，使用以下命令：

- **enable** - 启用该IPSec VPN隧道。
- **disable** - 禁用该IPSec VPN隧道。

指定IPSec协议的操作模式

为IKE隧道指定操作模式，在IKE隧道配置模式下使用以下命令：

mode {transport | tunnel}

- **transport** - 指定IPSec协议的操作模式为传输模式。
- **tunnel** - 指定IPSec协议的操作模式为隧道模式。该模式为系统默认模式。

使用**no mode**命令恢复默认模式。

指定ISAKMP网关

为IKE隧道指定ISAKMP网关，在IKE隧道配置模式下使用以下命令：

isakmp-peer peer-name

- *peer-name* - 指定ISAKMP网关的名称。

使用**no isakmp-peer**取消对ISAKMP网关的指定。

指定P2提议

为IKE隧道指定P2提议，在IKE隧道配置模式下使用以下命令：

ipsec-proposal p2-name

- *p2-name* - 指定P2提议的名称。

使用**no ipsec-proposal**取消对P2提议的指定。

指定第二阶段ID

为IKE IPSec隧道指定第二阶段ID，在IKE隧道配置模式下使用以下命令：

id {**auto** | **local** {*ip-address/mask* | *ipv6-address/prefix*} **remote** {*ip-address/mask* | *ipv6-address/prefix*} **service** *service-name*}

- **auto** – 自动指定第二阶段ID。此参数为系统默认配置。
- **local** {*ip-address/mask* | *ipv6-address/prefix*} – 指定本端第二阶段local ID。
- **remote** {*ip-address/mask* | *ipv6-address/prefix*} – 指定本端第二阶段remote ID。
- **service** *service-name* – 指定服务名称。

用户可配置最多64个第二阶段ID用于协商建立多个IKE隧道。

使用**no id** {**auto** | **local**{*ip-address/mask* | *ipv6-address/prefix*} **remote**{*ip-address/mask* | *ipv6-address/prefix*} **service** *service-name*}命令恢复系统默认配置。

配置IPsec VPN流量分流与限流

流量分流功能根据第二阶段ID的配置，在IKE隧道入口对进入IKE隧道的流量进行分流。如果流量的源IP地址、目的IP地址、以及流量的类型(service)匹配某一个第二阶段ID的配置，则该流量进入相应的IKE隧道进行封装发送。如果没有匹配的第二阶段ID，则该流量被丢弃。

流量限流功能根据第二阶段ID的配置，在IKE隧道出口对解封装后的流量进行限流。如果解封装后流量的源IP地址、目的IP地址、以及流量的类型(service)匹配某一个第二阶段ID的配置，则该流量被接收设备继续处理；如果流量无法匹配任何一个第二阶段ID的配置，则该流量被丢弃。

开启流量分流与限流功能，在IKE隧道配置模式，使用如下命令：

check-id

在IKE隧道配置模式下，使用该命令**no**的形式关闭流量分流与限流功能。

启用接受对端ID功能

默认情况下，该功能为禁用状态。开启该功能后，设备将接受对端的ID并将此ID作为IKE协商的第二阶段ID返回给对端，由此来保证在未知对端ID或者两端ID不一致的情况下，IKE隧道能够协商成功。当配置了多个第二阶段ID，期望协商出多个IKE隧道时，由于隧道两端ID均需保持一致，因此该功能不再适用，需要关闭该功能。

在IKE隧道配置模式下，使用以下命令开启接受对端ID的功能：

accept-all-proxy-id

在IKE隧道配置模式下，使用**no accept-all-proxy-id**命令关闭接受对端ID功能。

配置自动连接功能

设备提供了两种触发建立SA的方式：自动方式和流量触发方式。

- 自动方式是指设备每60秒检查一次SA的状态，如果SA未建立则自动发起协商请求；
- 流量触发方式是指当有数据流量需要通过隧道进行传输时，该隧道才发起协商请求。

默认情况下，使用流量触发方式。欲使用自动方式，在IKE隧道配置模式下使用以下命令：

auto-connect

使用**no auto-connect**命令恢复系统的默认设置。



注意：自动连接功能仅在对端IP地址为静态类型且本端可以作为发起端时有效。

配置分片功能

用户可以指定是否允许转发设备将包进行分片处理。为IKE隧道配置分片功能，在IKE隧道配置模式下使用以下命令：

df-bit {copy | clear | set}

- **copy** – 直接从发包端拷贝IP包的DF选项。该选项为系统默认选项。
- **clear** – 允许转发设备对包做分片处理。
- **set** – 不允许转发设备对包做分片处理。

使用**no df-bit**命令恢复系统的默认设置。

配置防重放功能

防重放（anti-replay）指防止恶意用户通过重复发送捕获到的数据包所进行的攻击，即接收方会拒绝旧的或重复的数据包。默认情况下，防重放功能是关闭的。为IKE IPSec隧道配置防重放功能，在IKE IPSec隧道配置模式下使用以下命令：

anti-replay {32 | 64 | 128 | 256 | 512}

- 32 – 指定防重放的窗口为32。
- 64 – 指定防重放的窗口为64。
- 128 – 指定防重放的窗口为128。
- 256 – 指定防重放的窗口为256。
- 512 – 指定防重放的窗口为512。

在网络状况较差时，例如存在严重乱序现象等，请选择较大的窗口。

使用**no anti-replay**命令关闭防重放功能。

开启/关闭VPN隧道状态通知功能

默认情况下，VPN隧道状态通知功能为关闭状态。在开启VPN隧道状态通知功能后，如果是基于路由的VPN，系统一旦监测到中断的VPN隧道，会立即通知路由模块中断的VPN隧道信息并进行隧道路由的更新处理；如果是基于策略的VPN，系统一旦监测到中断的VPN隧道，会立即通知策略模块中断的VPN隧道信息并进行隧道策略的更新处理。用户可以通过命令开启/关闭VPN隧道状态通知功能，对中断状态下的VPN隧道信息进行通知。

开启/关闭VPN隧道状态通知功能，在IKE IPSec隧道配置模式下，使用以下命令：

- 开启：**tunnel-state-notify**
- 关闭：**no tunnel-state-notify**

设置Commit位

用户可以配置使响应方设置Commit位，从而防止出现丢包和时间差现象。但是，设置Commit位可能导致响应速度变慢。设置Commit位，在IKE IPSec隧道配置模式下使用以下命令：

响应方设置Commit位：**responder-set-commit**

响应方不设置Commit位：**no responder-set-commit**

指定描述信息

为所配置的IKE隧道指定描述信息，在IKE IPSec隧道配置模式下使用以下命令：

description *string*

- *string* – IKE隧道的描述信息。

使用**no description**命令删除IKE隧道的描述信息。



相关链接：

- "配置手工密钥VPN" 在第694页
- "配置PnPVPN" 在第736页
- "配置IPSec-XAUTH地址池" 在第698页
- "配置IPSec VPN监控" 在第703页

配置手工密钥VPN

手工密钥VPN的配置包括指定IPSec协议的操作模式、安全参数索引、协议类型、加密算法/验证算法和压缩算法等。

创建手工密钥VPN

创建手工密钥VPN，在全局配置模式下，使用以下命令：

```
tunnel ipsec name manual
```

- *name* – 指定所创建的手工密钥VPN隧道的名称。执行该命令后，CLI进入到手工密钥VPN配置模式。对手工密钥VPN的所有参数配置都需要在该模式下进行。

在全局配置模式下使用以下命令删除指定的手工密钥VPN隧道：

```
no tunnel ipsec name manual
```

指定IPSec协议的操作模式

指定IPSec协议的操作模式，可以是隧道模式或者传输模式，在手工密钥VPN配置模式下使用以下命令：

mode {**transport** | **tunnel**}

- **transport** – 指定IPSec协议的操作模式为传输模式。
- **tunnel** – 指定IPSec协议的操作模式为隧道模式。该模式为系统默认模式。

使用**no mode**命令恢复默认模式。

指定对端IP地址

配置对端的IP地址，在手工密钥VPN配置模式下使用以下命令：

peer *ip-address*

- *ip-address* – 指定对端的IP地址。

使用**no peer**命令取消对端IP地址的配置。

指定安全参数索引

安全参数索引（Security Parameter Index，简称为SPI）是为唯一标识SA而生成的一个32比特的数值，它在AH和ESP头中传输。SPI的作用是查找对应的VPN隧道进行解密。指定手工密钥VPN隧道的SPI，在手工密钥VPN配置模式下使用以下命令：

spi *spi-number out-spi-number*

- *spi-number* – 指定本端的SPI参数。
- *out-spi-number* – 指定对端的SPI参数。

使用**no spi**命令取消对SPI参数的配置。

在为系统配置安全联盟时，必须分别设置进方向（inbound）和出方向（outbound）两个方向的安全联盟的参数。并且在隧道的两端设置的安全联盟参数必须是完全匹配的。本端的入方向安全联盟的SPI必须和对端的出方向安全联盟的SPI一样；本端的出方向安全联盟的SPI必须和对端的入方向安全联盟的SPI一样。

指定出接口

为手工密钥VPN隧道指定出接口，在手工密钥VPN配置模式下使用以下命令：

- **interface** *interface-name*
- *interface-name* – 指定出接口名称。

使用**no interface**命令取消对出接口的指定。



注意: 非根VSYN中的出接口不可以为VSYN共享接口。

指定协议类型

IPSec协议的类型为ESP和AH两种。为手工密钥VPN隧道指定协议类型，在手工密钥VPN配置模式下使用以下命令：

```
protocol {esp | ah}
```

- **esp** – 指定使用ESP协议。该协议为系统默认协议。
- **ah** – 指定使用AH协议。

使用**no protocol**恢复默认协议配置。

指定加密算法

为手工密钥VPN隧道指定加密算法，在手工密钥VPN配置模式下使用以下命令：

```
encryption {3des | des | aes | aes-192 | aes-256 | null}
```

- **3des** – 指定使用3DES加密方法。密钥长度为192比特。该方法为系统默认方法。
- **des** – 指定使用DES加密方法。密钥长度为64比特。
- **aes** – 指定使用AES加密方法。密钥长度为128比特。
- **aes-192** – 指定使用192bit AES加密方法。密钥长度为192比特。
- **aes-256** – 指定使用256bit AES加密方法。密钥长度为256比特。
- **null** – 不使用加密功能。

使用**no encryption**命令恢复默认加密算法。

配置协议的加密密钥

用户需要为安全隧道两端均配置协议的加密密钥，且本端入方向加密密钥必须与对端出方向的加密密钥相同，而本端出方向的加密密钥必须与对端入方向的加密密钥相同。配置协议加密密钥，在手工密钥VPN配置模式下使用以下命令：

encryption-key *inbound hex-number-string* **outbound** *hex-number-string*

- **inbound** *hex-number-string* – 配置本端进方向的加密密钥。
- **outbound** *hex-number-string* – 配置本端出方向的加密密钥。

使用**no encryption-key**命令取消对加密密钥的配置。

指定验证算法

为手工密钥VPN隧道指定验证算法，在手工密钥VPN配置模式下使用以下命令：

hash {*md5* | *sha* | *sha256* | *sha384* | *sha512* | *null*}

- **md5** – 指定使用MD5验证算法。摘要为128比特。
- **sha** – 指定使用SHA-1验证算法。摘要为160比特。该算法为默认算法。
- **sha256** – 指定使用SHA-256验证算法。摘要为256比特。
- **sha384** – 指定使用SHA-384验证算法。摘要为384比特。
- **sha512** – 指定使用SHA-512验证算法。摘要为512比特。
- **null** – 不使用验证功能。

使用**no hash**命令恢复默认验证算法。

配置协议的验证密钥

用户需要为安全隧道两端均配置协议的验证密钥，且本端入方向验证密钥必须与对端出方向的验证密钥相同，而本端出方向的验证密钥必须与对端入方向的验证密钥相同。配置协议验证密钥，在手工密钥VPN配置模式下使用以下命令：

hash-key *inbound hex-number-string* **outbound** *hex-number-string*

- **inbound** *hex-number-string* – 配置本端进方向的验证密钥。
- **outbound** *hex-number-string* – 配置本端出方向的验证密钥。

使用**no hash-key**命令取消对验证密钥的配置。

指定压缩算法

默认情况下，手工密钥VPN不使用任何压缩算法。为手工密钥VPN隧道指定压缩算法（DEFLATE算法），请在手工密钥VPN配置模式下使用以下命令：

compression deflate

使用**no compression**命令取消对压缩算法的指定。



相关链接：

- "配置手工密钥VPN" 在第694页
- "配置PnPPVPN" 在第736页
- "配置IPSec-XAUTH地址池" 在第698页
- "配置IPSec VPN监控" 在第703页

配置IPSec-XAUTH地址池

XAUTH是对IKE协议的扩展和增强，允许设备结合已配置的认证服务器（RADIUS和本地AAA服务器）对试图访问IPSec VPN网络的用户进行身份认证，目前大量应用在移动终端上。远程用户发起VPN连接请求后，设备上的XAUTH服务器会中断VPN协商过程并要求用户输入有效的用户名和密码进行认证，认证成功后会继续VPN协商过程并为合法的客户端分配IP地址，否则会中断VPN连接。

XAUTH通过地址池给用户分配IP地址。当客户端连接XAUTH服务端成功后，设备会从地址池里取出一个IP地址与其它相关参数（如DNS服务器地址与WINS服务器地址等）一起分配给用户。

XAUTH服务器通过创建和执行IP地址绑定规则来满足客户端的固定IP地址需求。IP地址绑定规则包括IP用户绑定规则和IP角色绑定规则。IP用户绑定规则将客户端用户与已配置地址池中的某个固定IP地址绑定，当客户端连接成功后，设备端会将绑定的IP地址分配给客户端；IP角色绑定规则是将角色与已配置地址池中的某一IP地址范围绑定，当此客户端连接成功后，设备端会从绑定的地址范围中取出一个IP地址分配给客户端。

当XAUTH通过地址池给客户端分配IP地址时，系统会按照一定的顺序对客户端的IP地址绑定规则进行检查，决定如何为客户端分配IP地址：

1. 检查是否已为客户端用户配置IP用户绑定规则，如果是，则将绑定的IP地址分配给客户端；否则，需要进一步检查。注意，如果此IP用户绑定规则中的IP地址已被占用，则该用户无法登录。
2. 检查是否已为客户端用户配置IP角色绑定规则，如果是，则从绑定的地址范围中取出一个IP地址分配给客户端；否则，该用户无法登录。



注意: IP用户绑定规则中的IP地址和IP角色绑定规则中的IP地址不能重叠。

启用XAUTH服务器

XAUTH服务器在设备上默认是禁用的。启用XAUTH服务器，在ISAKMP网关配置模式下，使用以下命令：

```
xauth server
```

在ISAKMP网关配置模式下，使用**no xauth server**命令禁用XAUTH服务器。

配置XAUTH地址池

XAUTH通过地址池为客户端分配IP地址。当客户端连接XAUTH服务端成功后，设备端会从地址池里取出一个IP地址与其它相关参数（如DNS服务器地址、WINS服务器地址等）一起分配给客户端。

创建XAUTH地址池

创建XAUTH地址池，在全局配置模式下，使用以下命令：

```
xauth pool pool-name
```

- *pool-name* - 指定XAUTH地址池名称并进入XAUTH地址池配置模式。如果指定的名称已存在，系统会直接进入XAUTH地址池配置模式。

在全局配置模式下，使用**no xauth pool** *pool-name*命令删除指定的XAUTH地址池。

配置XAUTH地址池的IP地址范围

指定XAUTH地址池中允许分配的IP地址范围，在XAUTH地址池配置模式下，使用以下命令：

```
address start-ip end-ip netmask mask
```

- *start-ip* - 指定XAUTH地址池的起始IP地址。
- *end-ip* - 指定XAUTH地址池的结束IP地址。
- *mask* - 指定网络掩码。

在XAUTH地址池配置模式下，使用**no address**命令删除指定的IP地址范围。

配置XAUTH地址池的保留地址

保留地址池中的IP地址为XAUTH地址池中的部分IP地址，当XAUTH服务器从地址池里取出IP地址分配给客户端时，可以保留已经被占用的部分IP地址，不进行分配。

指定保留地址范围，在XAUTH地址池配置模式下，使用以下命令：

exclude-address *start-ip end-ip*

- *start-ip* - 指定XAUTH保留地址池的起始IP地址。
- *end-ip* - 指定XAUTH保留地址池的结束IP地址。

在XAUTH地址池配置模式下，使用**no exclude-address**命令删除指定的保留地址池IP范围。

绑定地址池到XAUTH服务器

XAUTH地址池只有在绑定到XAUTH服务器后才会生效。将指定的XAUTH地址池绑定到XAUTH服务器，在ISAKMP网关配置模式下，使用以下命令：

xauth pool-name *pool-name*

- *pool-name* - 指定绑定的地址池名称。

在ISAKMP网关配置模式下，使用**no xauth pool-name**命令取消地址池的绑定。

配置IP用户绑定和IP角色绑定规则

XAUTH服务器通过创建和执行IP地址绑定规则来满足客户端的固定IP地址需求。IP地址绑定规则包括IP用户绑定规则和IP角色绑定规则。IP用户绑定规则将客户端用户与已配置地址池中的某个固定IP地址绑定，当客户端连接成功后，设备端会将绑定的IP地址分配给客户端；IP角色绑定规则是将角色与已配置地址池中的某一IP地址范围绑定，当此客户端连接成功后，设备端会从绑定的地址范围中取出一个IP地址分配给客户端。

当XAUTH通过地址池给客户端分配IP地址时，系统会按照一定的顺序对客户端的IP地址绑定规则进行检查，决定如何为客户端分配IP地址：

1. 检查是否已为客户端用户配置 IP 用户绑定规则，如果是，则将绑定的 IP 地址分配给客户端；否则，需要进一步检查。注意，如果此 IP 用户绑定规则中的 IP 地址已被占用，则该用户无法登录。
2. 检查是否已为客户端用户配置 IP 角色绑定规则，如果是，则从绑定的地址范围中取出一个 IP 地址分配给客户端；否则，在未绑定的 IP 地址范围中取出一个 IP 地址分配给客户端。注意，如果绑定的地址范围中的地址都已经被分配，则该用户无法登录。



注意: IP 用户绑定规则中的 IP 地址和 IP 角色绑定规则中的 IP 地址不能重叠。

配置 IP 用户绑定规则

配置 IP 用户绑定规则，在 XAUTH 地址池配置模式下使用以下命令：

```
ip-binding user user-name ip ip-address
```

- **user** *user-name* - 指定客户端用户名。
- **ip** *ip-address* - 指定绑定的 IP 地址。此地址必须为地址池中可以分配的地址。

在 XAUTH 地址池配置模式下，使用 **no ip-binding user** *user-name* 命令取消对特定用户 IP 用户绑定规则的配置。

配置 IP 角色绑定规则

配置 IP 角色绑定规则，在 XAUTH 地址池配置模式下使用以下命令：

```
ip-binding role role-name ip-range start-ip end-ip
```

- **role** *role-name* - 指定角色名称。
- **ip-range** *start-ip end-ip* - 指定绑定的 IP 范围的起始 IP 地址 *start-ip* 和结束 IP 地址 *end-ip*。此地址范围必须为地址池中可以分配的地址范围。

在 XAUTH 地址池配置模式下，使用 **no ip-binding role** *role-name* 命令取消对特定角色的 IP 角色绑定规则的配置。

修改 IP 角色绑定规则排列顺序

一个用户可以绑定到一个或者多个角色，不同角色可以配置不同的 IP 角色绑定规则。对于绑定到多个角色且多个角色有相应的 IP 角色绑定规则的用户，设备会对 IP 角色绑定规则进行顺序查找，然后按照查找到的相匹

配的第一条规则为用户分配地址。默认情况下，系统会将新创建的规则放到所有规则的末尾，管理员可以移动已有的IP角色绑定规则从而改变规则的排列顺序。

改变规则的排列顺序，在XAUTH地址池配置模式下使用以下命令：

```
move role-name1 {before role-name2 | after role-name2 | top | bottom}
```

- *role - name1* - 指定被移动的IP角色绑定规则的角色名称。
- **before** *role-name2* - 将IP角色绑定规则移动到某个IP角色绑定规则(角色名称为 *role-name2* 的规则)之前。
- **after** *role-name2* - 将IP角色绑定规则移动到某个IP角色绑定规则(角色名称为 *role-name2* 的规则)之后。
- **top** - 将IP角色绑定规则移动到所有IP角色绑定规则之首。
- **bottom** - 将IP角色绑定规则移动到所有IP角色绑定规则的末尾。

配置推送到客户端的WINS/DNS服务器

配置DNS服务器，在XAUTH地址池配置模式下使用以下命令：

```
dns address1 [address2]
```

- *address1* - 指定DNS服务器IP地址。用户最多可配置2个DNS服务器。

在XAUTH地址池配置模式下，使用**no dns**命令取消对DNS服务器的指定。

配置WINS服务器，在XAUTH地址池配置模式下使用以下命令：

```
wins address1 [address2]
```

- *address1* - 指定WINS服务器IP地址。用户最多可配置2个WINS服务器。

在XAUTH地址池配置模式下，使用**no wins**命令取消对WINS服务器的指定。

强制断开客户端XAUTH连接

XAUTH服务端可以通过命令强制断开某个客户端与设备端的连接。强制断开客户端XAUTH连接，在任意配置模式使用以下命令：

```
exec xauth isakmp-peer-name kickout user-name
```

- *isakmp-peer-name* - 指定ISAKMP对端的名称。
- *user-name* - 指定被强制断开连接的用户名称。

配置IPSec VPN监控

Hillstone设备能够监测指定的VPN隧道是否连通，并且能够实现两条或者多条VPN隧道的备份或者分流。该功能仅对基于路由的VPN以及基于策略的VPN均有效。具体实现包括以下两种环境：

- 为同一个远程对端配置备份VPN隧道，并且在任意时刻只有一个隧道处于活动状态。最初，主VPN隧道处于活动状态，如果监测到该主隧道中断，Hillstone设备会通过备份隧道重新传输信息流；
- 为同一个远程对端配置了两个或者多个VPN隧道，所有隧道都同时处于活动状态，并且通过等价多径路由（ECMP）实现负载均衡。如果监测到隧道中断，Hillstone设备会通过其它隧道重新传输信息流。

配置VPN监控

VPN监控功能支持通过Ping报文对目标隧道进行监测。默认情况下，该功能是关闭的。

配置VPN监控功能，在IKE IPSec隧道配置模式下使用以下命令：

```
vpn-track [A.B.C.D | X:X:X:X::X] [src-ip {A.B.C.D | X:X:X:X::X}] [intervaltime-value] [thresholdvalue]
```

- **A.B.C.D | X:X:X:X::X** – 指定监测目标的IP地址。当对端设备为Hillstone设备时，如果不指定该参数，系统默认为对端IP地址。以IPv4类型的地址为例，此IP地址不能为“0.0.0.0”和“255.255.255.255”。
- **src-ip {A.B.C.D | X:X:X:X::X}** – 指定发送Ping监测报文的源IP地址。当对端设备为Hillstone设备时，如果不指定该参数，系统默认为出接口IP地址。以IPv4类型的地址为例，此IP地址不能为“0.0.0.0”和“255.255.255.255”。
- **interval time-value** – 指定发送Ping监测报文的时间间隔，单位为秒。范围是1到255秒。默认值是10秒。
- **threshold value** – 指定判断监测失败的警戒值。如果系统连续未收到该参数指定个数的响应报文，就判断为监测失败，即目标隧道中断。取值范围是1到255。默认值是10。

在IKE IPSec隧道配置模式下，使用**no vpn-track**命令取消VPN监控功能的配置。

禁用或者启用VPN监控失败通知

默认情况下，如果是基于路由的VPN，VPN监控功能一旦监测到中断的VPN隧道，会立即通知路由模块中断的VPN隧道信息并进行隧道路由的更新处理；如果是基于策略的VPN，VPN监控功能一旦监测到中断的VPN

隧道，会立即通知策略模块中断的VPN隧道信息并进行隧道策略的更新处理。用户可以通过命令禁用VPN监控失败通知功能，使其不对监测失败的隧道信息进行通知。

禁用或者启用VPN监控失败通知功能，在IKE IPSec隧道配置模式下，使用以下命令：

```
track-event-notify {disable | enable}
```

- **disable** – 禁用。
- **enable** – 启用。默认状态下，系统启用该功能。

查看VPN监控

VPN监控功能包括active和inactive两种状态。用户可以使用相应的**show**命令在CLI的任何模式下查看VPN监控功能的状态以及配置信息：

- 查看VPN监控功能的状态：**show ipsec sa {id}**
- 查看VPN监控功能的配置情况：**show tunnel ipsec {manual | auto | ikev2} {tunnel-name}**

例如：

查看VPN监控功能状态

```
hostname(config)# show ipsec sa 5
```

VPN Name: vpn1

Outbound

Gateway: 1.1.1.2

.....

VPN track status: alive

Inbound

Gateway: 1.1.1.2

.....

VPN track status: alive

查看VPN监控功能配置

```
hostname(config)# show tunnel ipsec auto vpn1
```

Name: vpn1


```
mode: tunnel

.....

vpn-track: enable

tracknotify: enable

vpnttrack destination 1.1.1.1

vpnttrack source ip: 2.2.2.2

vpnttrack interval: 3

vpnttrack threshold: 3
```

配置举例

本节介绍通过手工密钥VPN和IKE VPN两种方式建立安全联盟的具体实例、VPN监控及冗余备份的具体实例以及XAUTH的配置实例。

- [手工密钥VPN](#)
- [IKE VPN](#)
- [基于路由的VPN监控及冗余备份功能](#)
- [基于策略的VPN监控及冗余备份功能](#)
- [XAUTH](#)

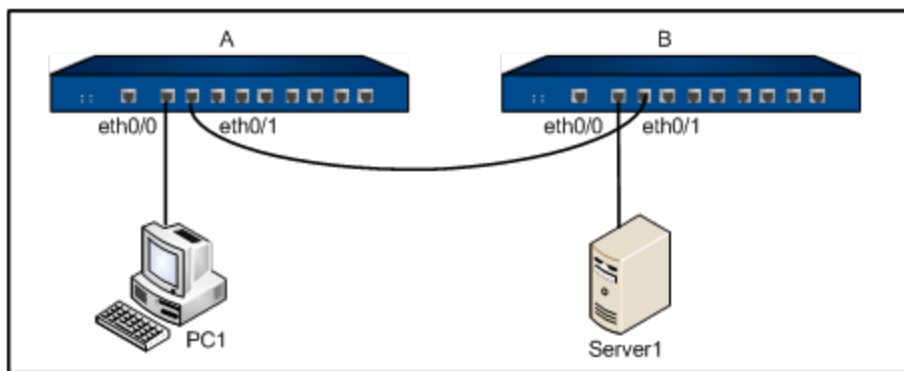
手工密钥VPN

手工密钥VPN隧道要求安全联盟的所有相关配置都由用户手动一一指定。请看以下实例。

组网需求

在Hillstone设备A和Hillstone设备B之间建立一个安全隧道，PC1作Hillstone设备A端的主机，IP地址为188.1.1.2，网关为188.1.1.1；server1作为Hillstone设备B端的服务器，IP地址为10.110.88.210，网关是10.110.88.220。要求对PC1代表的子网（188.1.1.0/24）与Server1代表的子网（10.110.88.0/24）之间的数据流进行安全保护（通过

基于策略的VPN方式实现VPN的应用)。安全协议采用ESP协议,加密算法采用3DES,验证算法采用SHA1,压缩算法采用DEFLATE。下图为该需求的组网图。



配置步骤

第一步: 配置Hillstone设备接口。

Hillstone设备A

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 188.1.1.1/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 192.168.1.2/24
hostname(config-if-eth0/1)# exitip address 10.1.1.1/24
```

Hillstone设备B

```
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 10.110.88.220/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/0
hostname(config)# interface ethernet0/1
```

```
hostname(config-if-eth0/1)# zone untrust

hostname(config-if-eth0/1)# ip address 192.168.1.3/24

hostname(config-if-eth0/1)# exitip route 172.16.10.0/24 tunnel1 10
```

第二步：配置路由。

Hillstone设备A

```
hostname(config)# ip vrouter trust-vr

hostname(config-vrouter)# ip route 10.110.88.0/24 192.168.1.3

hostname(config-vrouter)# exit
```

Hillstone设备B

```
hostname(config)# ip vrouter trust-vr

hostname(config-vrouter)# ip route 188.1.1.0/24 192.168.1.2

hostname(config-vrouter)# exit
```

第三步：手动配置名为VPN1的隧道。

Hillstone设备A

```
hostname(config)# tunnel ipsec vpn1 manual

hostname(config-tunnel-ipsec-manual)# interface ethernet0/1

hostname(config-tunnel-ipsec-manual)# protocol esp

hostname(config-tunnel-ipsec-manual)# peer 192.168.1.3

hostname(config-tunnel-ipsec-manual)# hash sha

hostname(config-tunnel-ipsec-manual)# hash-key inbound 1234 outbound 5678

hostname(config-tunnel-ipsec-manual)# encryption 3des

hostname(config-tunnel-ipsec-manual)# encryption-key inbound 00ff outbound 123a

hostname(config-tunnel-ipsec-manual)# compression deflate

hostname(config-tunnel-ipsec-manual)# spi 6001 6002

hostname(config-tunnel-ipsec-manual)# exit
```

Hillstone设备B

```
hostname(config)# tunnel ipsec vpn1 manual

hostname(config-tunnel-ipsec-manual)# interface ethernet0/1

hostname(config-tunnel-ipsec-manual)# protocol esp

hostname(config-tunnel-ipsec-manual)# peer 192.168.1.2

hostname(config-tunnel-ipsec-manual)# hash sha

hostname(config-tunnel-ipsec-manual)# hash-key inbound 5678 outbound 1234

hostname(config-tunnel-ipsec-manual)# encryption 3des

hostname(config-tunnel-ipsec-manual)# encryption-key inbound 123a outbound 00ff

hostname(config-tunnel-ipsec-manual)# compression deflate

hostname(config-tunnel-ipsec-manual)# spi 6002 6001

hostname(config-tunnel-ipsec-manual)# exit
```

第四步：配置Hillstone设备策略规则。

Hillstone设备A

```
hostname(config)# policy-global

hostname(config-policy)# rule

hostname(config-policy-rule)# src-zone trust

hostname(config-policy-rule)# dst-zone untrust

hostname(config-policy-rule)# src-addr any

hostname(config-policy-rule)# dst-addr any

hostname(config-policy-rule)# service any

hostname(config-policy-rule)# action fromtunnel vpn1

hostname(config-policy-rule)# exit

hostname(config-policy)# exit

hostname(config)#
```

Hillstone设备B

```
hostname(config)# policy-global

hostname(config-policy)# rule

hostname(config-policy-rule)# src-zone trust

hostname(config-policy-rule)# dst-zone untrust

hostname(config-policy-rule)# src-addr any

hostname(config-policy-rule)# dst-addr any

hostname(config-policy-rule)# service any

hostname(config-policy-rule)# action tunnel vpn1

hostname(config-policy-rule)# exit

hostname(config-policy)# rule

hostname(config-policy-rule)# src-zone untrust

hostname(config-policy-rule)# dst-zone trust

hostname(config-policy-rule)# src-addr any

hostname(config-policy-rule)# dst-addr any

hostname(config-policy-rule)# service any

hostname(config-policy-rule)# action fromtunnel vpn1

hostname(config-policy-rule)# exit

hostname(config-policy)# exit

hostname(config)#
```

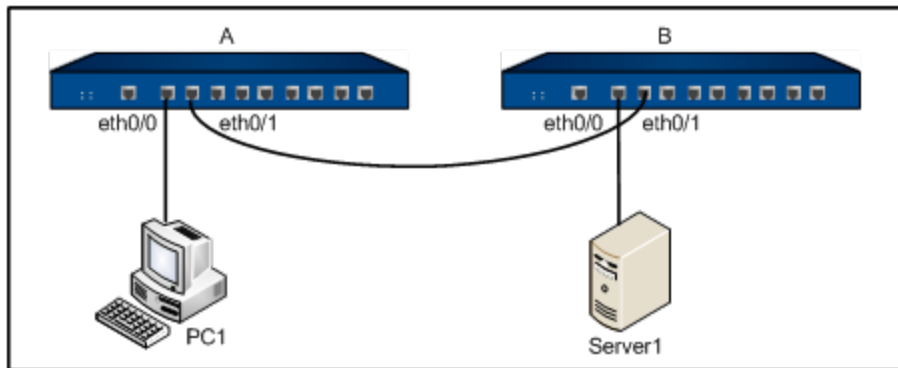
完成以上配置后，Hillstone设备A和Hillstone设备B之间的安全隧道便建立成功了。子网（188.1.1.0/24）与server1代表的子网（10.110.88.0/24）之间的数据流将会被加密传输。

IKE VPN

本节介绍通过IKE方式创建安全联盟的实例。

组网需求

在Hillstone设备A和Hillstone设备B之间建立一个安全隧道，PC1作为Hillstone设备A端的主机，IP地址为10.1.1.1，网关为10.1.1.2；Server1作为Hillstone设备B端的服务器，IP地址为192.168.1.1，网关是192.168.1.2。要求对PC1代表的子网（10.1.1.0/24）与server1代表的子网（192.168.1.0/24）之间的数据流进行安全保护（通过基于路由的VPN方式实现VPN的应用）。安全协议采用ESP协议，加密算法采用3DES，验证算法采用SHA1，压缩算法采用DEFLATE。组网图请参考下图：



配置步骤

第一步：配置Hillstone设备接口。

Hillstone设备A

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 10.1.1.2/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if)# zone untrust
hostname(config-if-eth0/1)# ip address 1.1.1.1/24
hostname(config-if-eth0/1)# exit
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone trust
```

```
hostname(config-if-tun1)# exit
```

Hillstone设备B

```
hostname(config)# interface ethernet0/0
```

```
hostname(config-if-eth0/0)# zone trust
```

```
hostname(config-if-eth0/0)# ip address 192.168.1.2/24
```

```
hostname(config-if-eth0/0)# exit
```

```
hostname(config)# interface ethernet0/1
```

```
hostname(config-if-eth0/1)# zone untrust
```

```
hostname(config-if-eth0/1)# ip address 1.1.1.2/24
```

```
hostname(config-if-eth0/1)# exit
```

```
hostname(config)# interface tunnel1
```

```
hostname(config-if-tun1)# zone trust
```

```
hostname(config-if-tun1)# exit
```

第二步：配置Hillstone设备策略规则。

Hillstone设备A

```
hostname(config)# policy-global
```

```
hostname(config-policy)# rule
```

```
hostname(config-policy-rule)# src-zone trust
```

```
hostname(config-policy-rule)# dst-zone untrust
```

```
hostname(config-policy-rule)# src-addr any
```

```
hostname(config-policy-rule)# dst-addr any
```

```
hostname(config-policy-rule)# service any
```

```
hostname(config-policy-rule)# action permit
```

```
hostname(config-policy-rule)# exit
```

```
hostname(config-policy)# rule
```

```
hostname(config-policy-rule)# src-zone untrust

hostname(config-policy-rule)# dst-zone trust

hostname(config-policy-rule)# src-addr any

hostname(config-policy-rule)# dst-addr any

hostname(config-policy-rule)# service any

hostname(config-policy-rule)# action permit

hostname(config-policy-rule)# exit

hostname(config-policy)# rule

hostname(config-policy-rule)# src-zone trust

hostname(config-policy-rule)# dst-zone trust

hostname(config-policy-rule)# src-addr any

hostname(config-policy-rule)# dst-addr any

hostname(config-policy-rule)# service any

hostname(config-policy-rule)# action permit

hostname(config-policy-rule)# exit

hostname(config-policy)# exit

hostname(config)#
```

Hillstone设备B

```
hostname(config)# policy-global

hostname(config-policy)# rule

hostname(config-policy-rule)# src-zone trust

hostname(config-policy-rule)# dst-zone untrust

hostname(config-policy-rule)# src-addr any

hostname(config-policy-rule)# dst-addr any

hostname(config-policy-rule)# service any

hostname(config-policy-rule)# action permit
```



```

hostname(config-policy-rule)# exit

hostname(config-policy)# rule

hostname(config-policy-rule)# src-zone untrust

hostname(config-policy-rule)# dst-zone trust

hostname(config-policy-rule)# src-addr any

hostname(config-policy-rule)# dst-addr any

hostname(config-policy-rule)# service any

hostname(config-policy-rule)# action permit

hostname(config-policy-rule)# exit

hostname(config-policy)# rule

hostname(config-policy-rule)# src-zone trust

hostname(config-policy-rule)# dst-zone trust

hostname(config-policy-rule)# src-addr any

hostname(config-policy-rule)# dst-addr any

hostname(config-policy-rule)# service any

hostname(config-policy-rule)# action permit

hostname(config-policy-rule)# exit

hostname(config-policy)# exit

hostname(config)#

```

第三步：配置路由。

Hillstone设备A

```

hostname(config)# ip vrouter trust-vr

hostname(config-vrouter)# ip route 192.168.1.0/24 tunnel1

hostname(config-vrouter)# exit

```

Hillstone设备B

```
hostname(config)# ip vrouter trust-vr  
hostname(config-vrouter)# ip route 10.1.1.0/24 tunnel1  
hostname(config-vrouter)# exit
```

第四步：配置P1提议。

Hillstone设备A

```
hostname(config)# isakmp proposal p1  
hostname(config-isakmp-proposal)# authentication pre-share  
hostname(config-isakmp-proposal)# group 2  
hostname(config-isakmp-proposal)# hash sha  
hostname(config-isakmp-proposal)# encryption 3des  
hostname(config-isakmp-proposal)# exit
```

Hillstone设备B

```
hostname(config)# isakmp proposal p1  
hostname(config-isakmp-proposal)# authentication pre-share  
hostname(config-isakmp-proposal)# group 2  
hostname(config-isakmp-proposal)# hash sha  
hostname(config-isakmp-proposal)# encryption 3des  
hostname(config-isakmp-proposal)# exit
```

第五步：配置ISAKMP网关。

Hillstone设备A

```
hostname(config)# isakmp peer east  
hostname(config-isakmp-peer)# interface ethernet0/1  
hostname(config-isakmp-peer)# isakmp-proposal p1  
hostname(config-isakmp-peer)# peer 1.1.1.2  
hostname(config-isakmp-peer)# pre-share hello1
```

```
hostname(config-isakmp-peer)# exit
```

Hillstone设备B

```
hostname(config)# isakmp peer west
```

```
hostname(config-isakmp-peer)# interface ethernet0/1
```

```
hostname(config-isakmp-peer)# isakmp-proposal p1
```

```
hostname(config-isakmp-peer)# peer 1.1.1.1
```

```
hostname(config-isakmp-peer)# pre-share hello1
```

```
hostname(config-isakmp-peer)# exit
```

第六步：配置P2提议。

Hillstone设备A

```
hostname(config)# ipsec proposal p2
```

```
hostname(config-ipsec-proposal)# protocol esp
```

```
hostname(config-ipsec-proposal)# hash sha
```

```
hostname(config-ipsec-proposal)# encryption 3des
```

```
hostname(config-ipsec-proposal)# compression deflate
```

```
hostname(config-ipsec-proposal)# exit
```

Hillstone设备B

```
hostname(config)# ipsec proposal p2
```

```
hostname(config-ipsec-proposal)# protocol esp
```

```
hostname(config-ipsec-proposal)# hash sha
```

```
hostname(config-ipsec-proposal)# encryption 3des
```

```
hostname(config-ipsec-proposal)# compression deflate
```

```
hostname(config-ipsec-proposal)# exit
```

第七步：配置名为VPN的隧道。

Hillstone设备A

```
hostname(config)# tunnel ipsec vpn auto

hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2

hostname(config-tunnel-ipsec-auto)# isakmp-peer east

hostname(config-tunnel-ipsec-auto)# id local 10.1.1.0/24 remote 192.168.1.0/24 service any

hostname(config-tunnel-ipsec-auto)# exit

hostname(config)# interface tunnel1

hostname(config-if-tun1)# tunnel ipsec vpn

hostname(config-if-tun1)# exit
```

Hillstone设备B

```
hostname(config)# tunnel ipsec vpn auto

hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2

hostname(config-tunnel-ipsec-auto)# isakmp-peer east

hostname(config-tunnel-ipsec-auto)# id local 192.168.1.0/24 remote 10.1.1.0/24 service any

hostname(config-tunnel-ipsec-auto)# exit

hostname(config)# interface tunnel1

hostname(config-if-tun1)# tunnel ipsec vpn

hostname(config-if-tun1)# exit
```

完成以上配置后，Hillstone设备A和Hillstone设备B之间的安全隧道便建立成功了。子网（10.1.1.0/24）与Server1代表的子网（192.168.1.0/24）之间的数据流将会被加密传输。

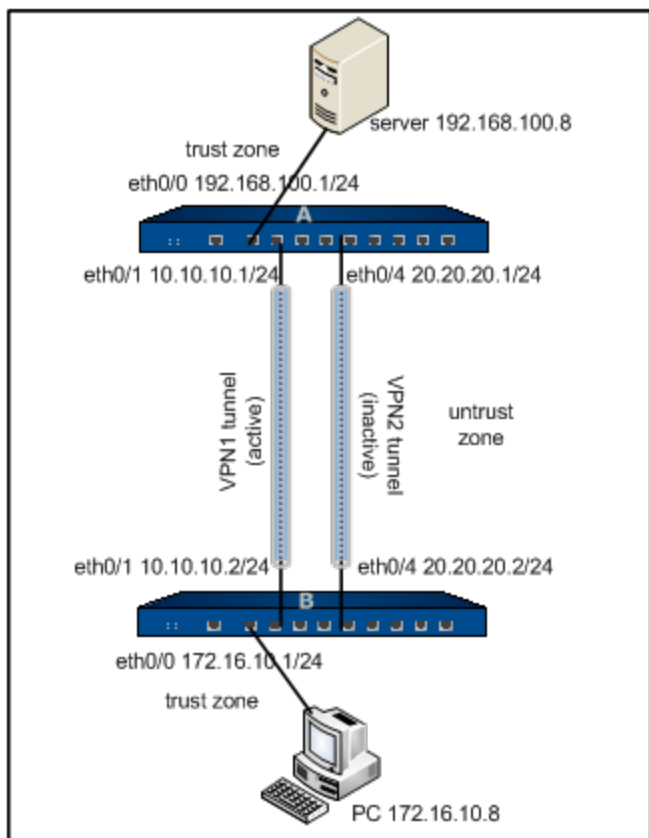
基于路由的VPN监控及冗余备份功能配置举例

该节介绍基于路由的VPN监控及冗余备份功能配置实例。

组网需求

在Hillstone设备A和Hillstone设备B之间配置IKE VPN隧道VPN1 tunnel和VPN2 tunnel，server作为Hillstone设备A端的服务器，IP地址为192.168.100.8，网关是192.168.100.1；PC作为Hillstone设备B端的主机，IP地址为172.16.10.8，网关为172.16.10.1。要求实现VPN1 tunnel和VPN2 tunnel的VPN监控，并当主隧道（VPN1 tunnel）

链路发生故障时，流量转向备份隧道（VPN2 tunnel）；主隧道恢复正常时，流量切换回主隧道。组网图参见下图：



配置步骤

第一步：配置Hillstone设备A：

配置接口：

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 192.168.100.1/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 10.10.10.1/24
```

```
hostname(config-if-eth0/1)# exit  
  
hostname(config)# interface ethernet0/4  
  
hostname(config-if-eth0/4)# zone untrust  
  
hostname(config-if-eth0/4)# ip address 20.20.20.1/24  
  
hostname(config-if-eth0/4)# exit
```

配置P1提议

```
hostname(config)# isakmp proposal p1  
  
hostname(config-isakmp-proposal)# authentication pre-share  
  
hostname(config-isakmp-proposal)# group 2  
  
hostname(config-isakmp-proposal)# hash md5  
  
hostname(config-isakmp-proposal)# encryption des  
  
hostname(config-isakmp-proposal)# exit
```

配置ISAKMP网关：

```
hostname(config)# isakmp peer gwa-peer-1  
  
hostname(config-isakmp-peer)# interface ethernet0/1  
  
hostname(config-isakmp-peer)# isakmp-proposal p1  
  
hostname(config-isakmp-peer)# peer 10.10.10.2  
  
hostname(config-isakmp-peer)# pre-share U8FdHNEEBz6sNn5Mvqx3yWuLRWce  
  
hostname(config-isakmp-peer)# exit  
  
hostname(config)# isakmp peer gwa-peer-2  
  
hostname(config-isakmp-peer)# interface ethernet0/4  
  
hostname(config-isakmp-peer)# isakmp-proposal p1  
  
hostname(config-isakmp-peer)# peer 20.20.20.2  
  
hostname(config-isakmp-peer)# pre-share i39jnnNiCSh9rXb77oGA7Fg7BNQy  
  
hostname(config-isakmp-peer)# exit
```

配置P2提议：

```
hostname(config)# ipsec proposal p2  
hostname(config-ipsec-proposal)# protocol esp  
hostname(config-ipsec-proposal)# hash md5  
hostname(config-ipsec-proposal)# encryption des  
hostname(config-ipsec-proposal)# exit
```

配置VPN隧道：

```
hostname(config)# tunnel ipsec vpn1-tunnel auto  
hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2  
hostname(config-tunnel-ipsec-auto)# isakmp-peer gwa-peer-1  
hostname(config-tunnel-ipsec-auto)# vpn-track interval 3 threshold 9  
hostname(config-tunnel-ipsec-auto)# track-event-notify enable  
hostname(config-tunnel-ipsec-auto)# exit  
hostname(config)# tunnel ipsec vpn2-tunnel auto  
hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2  
hostname(config-tunnel-ipsec-auto)# isakmp-peer gwa-peer-2  
hostname(config-tunnel-ipsec-auto)# vpn-track interval 3 threshold 9  
hostname(config-tunnel-ipsec-auto)# track-event-notify enable  
hostname(config-tunnel-ipsec-auto)# auto-connect  
hostname(config-tunnel-ipsec-auto)# exit
```

创建隧道接口并绑定VPN隧道：

```
hostname(config)# interface tunnel1  
hostname(config-if-tun1)# zone untrust  
hostname(config-if-tun1)#  
hostname(config-if-tun1)# tunnel ipsec vpn1-tunnel  
hostname(config-if-tun1)# exit  
hostname(config)# interface tunnel2
```

```
hostname(config-if-tun2)# zone untrust  
hostname(config-if-tun2)# ip address 10.2.2.1/24  
hostname(config-if-tun2)# tunnel ipsec vpn2-tunnel  
hostname(config-if-tun2)# exit
```

配置路由：

```
hostname(config)# ip vrouter trust-vr  
hostname(config-vrouter)#  
hostname(config-vrouter)# ip route 172.16.10.0/24 tunnel2 20  
hostname(config-vrouter)# exit
```

配置策略：

```
hostname(config)# policy-global  
hostname(config-policy)# rule  
hostname(config-policy-rule)# src-zone trust  
hostname(config-policy-rule)# dst-zone untrust  
hostname(config-policy-rule)# src-addr any  
hostname(config-policy-rule)# dst-addr any  
hostname(config-policy-rule)# service any  
hostname(config-policy-rule)# action permit  
hostname(config-policy-rule)# exit  
hostname(config-policy)# rule  
hostname(config-policy-rule)# src-zone untrust  
hostname(config-policy-rule)# dst-zone trust  
hostname(config-policy-rule)# src-addr any  
hostname(config-policy-rule)# dst-addr any  
hostname(config-policy-rule)# service any  
hostname(config-policy-rule)# action permit
```



```
hostname(config-policy-rule)# exit
```

```
hostname(config-policy)# exit
```

```
hostname(config)#
```

第二步：配置Hillstone设备B：

配置接口：

```
hostname(config)# interface ethernet0/0
```

```
hostname(config-if-eth0/0)# zone trust
```

```
hostname(config-if-eth0/0)# ip address 172.16.10.1/24
```

```
hostname(config-if-eth0/0)# exit
```

```
hostname(config)# interface ethernet0/1
```

```
hostname(config-if-eth0/1)# zone untrust
```

```
hostname(config-if-eth0/1)# ip address 10.10.10.2/24
```

```
hostname(config-if-eth0/1)# exit
```

```
hostname(config)# interface ethernet0/4
```

```
hostname(config-if-eth0/4)# zone untrust
```

```
hostname(config-if-eth0/4)# ip address 20.20.20.2/24
```

```
hostname(config-if-eth0/4)# exit
```

配置P1提议

```
hostname(config)# isakmp proposal p1
```

```
hostname(config-isakmp-proposal)# authentication pre-share
```

```
hostname(config-isakmp-proposal)# group 2
```

```
hostname(config-isakmp-proposal)# hash md5
```

```
hostname(config-isakmp-proposal)# encryption des
```

```
hostname(config-isakmp-proposal)# exit
```

配置ISAKMP网关：

```
hostname(config)# isakmp peer gwb-peer-1

hostname(config-isakmp-peer)# interface ethernet0/1

hostname(config-isakmp-peer)# isakmp-proposal p1

hostname(config-isakmp-peer)# peer 10.10.10.1

hostname(config-isakmp-peer)# pre-share U8FdHNEEBz6sNn5Mvqx3yWuLRWce

hostname(config-isakmp-peer)# exit

hostname(config)# isakmp peer gwb-peer-2

hostname(config-isakmp-peer)# interface ethernet0/4

hostname(config-isakmp-peer)# isakmp-proposal p1

hostname(config-isakmp-peer)# peer 20.20.20.1

hostname(config-isakmp-peer)# pre-share i39jnnNiCSh9rXb77oGA7Fg7BNQy

hostname(config-isakmp-peer)# exit
```

配置P2提议:

```
hostname(config)# ipsec proposal p2

hostname(config-ipsec-proposal)# protocol esp

hostname(config-ipsec-proposal)# hash md5

hostname(config-ipsec-proposal)# encryption des

hostname(config-ipsec-proposal)# exit
```

配置VPN隧道:

```
hostname(config)# tunnel ipsec vpn1-tunnel auto

hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2

hostname(config-tunnel-ipsec-auto)# isakmp-peer gwb-peer-1

hostname(config-tunnel-ipsec-auto)# vpn-track interval 3 threshold 9

hostname(config-tunnel-ipsec-auto)# track-event-notify enable

hostname(config-tunnel-ipsec-auto)# auto-connect

hostname(config-tunnel-ipsec-auto)# exit
```

```
hostname(config)# tunnel ipsec vpn2-tunnel auto

hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2

hostname(config-tunnel-ipsec-auto)# isakmp-peer gwb-peer-2

hostname(config-tunnel-ipsec-auto)# vpn-track interval 3 threshold 9

hostname(config-tunnel-ipsec-auto)# track-event-notify enable

hostname(config-tunnel-ipsec-auto)# auto-connect

hostname(config-tunnel-ipsec-auto)# exit
```

创建隧道接口并绑定VPN隧道：

```
hostname(config)# interface tunnel1

hostname(config-if-tun1)# zone untrust

hostname(config-if-tun1)# ip address 10.1.1.2/24

hostname(config-if-tun1)# tunnel ipsec vpn1-tunnel

hostname(config-if-tun1)# exit

hostname(config)# interface tunnel2

hostname(config-if-tun2)# zone untrust

hostname(config-if-tun2)# ip address 10.2.2.2/24

hostname(config-if-tun2)# tunnel ipsec vpn2-tunnel

hostname(config-if-tun2)# exit
```

配置路由：

```
hostname(config)# ip vrouter trust-vr

hostname(config-vrouter)# ip route 192.168.100.0/24 tunnel1 1

hostname(config-vrouter)# ip route 192.168.100.0/24 tunnel2 2

hostname(config-vrouter)# exit
```

配置策略：

```
hostname(config)# policy-global

hostname(config-policy)# rule
```

```

hostname(config-policy-rule)# src-zone trust

hostname(config-policy-rule)# dst-zone untrust

hostname(config-policy-rule)# src-addr any

hostname(config-policy-rule)# dst-addr any

hostname(config-policy-rule)# service any

hostname(config-policy-rule)# action permit

hostname(config-policy-rule)# exit

hostname(config-policy)# rule

hostname(config-policy-rule)# src-zone untrust

hostname(config-policy-rule)# dst-zone trust

hostname(config-policy-rule)# src-addr any

hostname(config-policy-rule)# dst-addr any

hostname(config-policy-rule)# service any

hostname(config-policy-rule)# action permit

hostname(config-policy-rule)# exit

hostname(config-policy)# exit

hostname(config)#

```

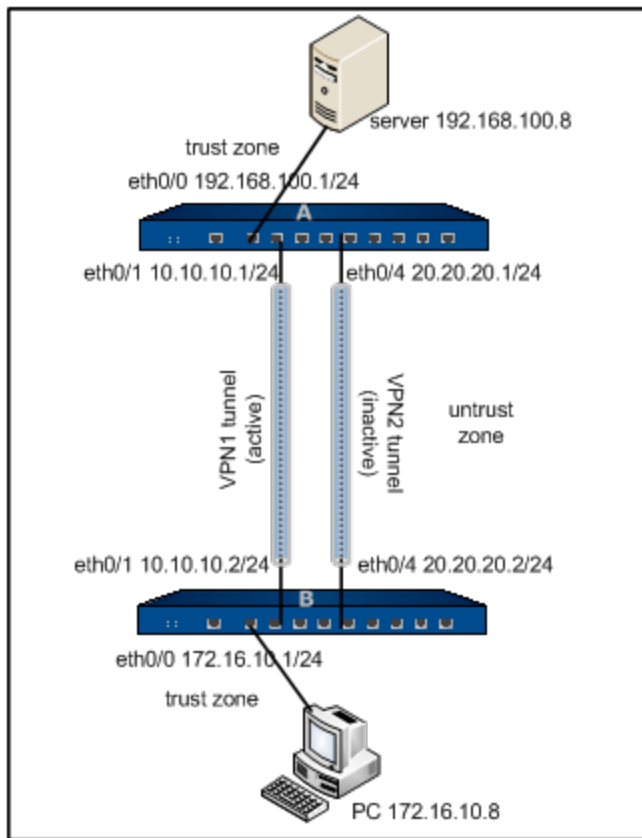
由于本例中VPN终端设备都是Hillstone设备，因此可使用缺省源和目标地址进行VPN监控。

基于策略的VPN监控及冗余备份功能配置举例

该节介绍基于策略的VPN监控及冗余备份功能配置实例。

组网需求

在Hillstone设备A和Hillstone设备B之间配置IKE VPN隧道VPN1 tunnel和VPN2 tunnel，server作为Hillstone设备A端的服务器，IP地址为192.168.100.8，网关是192.168.100.1；PC作为Hillstone设备B端的主机，IP地址为172.16.10.8，网关为172.16.10.1。要求实现VPN1 tunnel和VPN2 tunnel的VPN监控，并当主隧道（VPN1 tunnel）链路发生故障时，流量转向备份隧道（VPN2 tunnel）；主隧道恢复正常时，流量切换回主隧道。组网图参见下图：



配置步骤

第一步:配置Hillstone设备A:

配置接口:

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 192.168.100.1/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 10.10.10.1/24
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/4
```

```
hostname(config-if-eth0/4)# zone untrust
```

```
hostname(config-if-eth0/4)# ip address 20.20.20.1/24
```

```
hostname(config-if-eth0/4)# exit
```

配置路由：

```
hostname(config)# ip vrouter trust-vr
```

```
hostname(config-vrouter)# ip route 172.16.10.0/24 20.20.20.2
```

```
hostname(config-vrouter)# exit
```

配置P1提议

```
hostname(config)# isakmp proposal p1
```

```
hostname(config-isakmp-proposal)# authentication pre-share
```

```
hostname(config-isakmp-proposal)# group 2
```

```
hostname(config-isakmp-proposal)# hash md5
```

```
hostname(config-isakmp-proposal)# encryption des
```

```
hostname(config-isakmp-proposal)# exit
```

配置ISAKMP网关：

```
hostname(config)# isakmp peer gwa-peer-1
```

```
hostname(config-isakmp-peer)# interface ethernet0/1
```

```
hostname(config-isakmp-peer)# isakmp-proposal p1
```

```
hostname(config-isakmp-peer)# peer 10.10.10.2
```

```
hostname(config-isakmp-peer)# pre-share U8FdHNEEBz6sNn5Mvqx3yWuLRWce
```

```
hostname(config-isakmp-peer)# exit
```

```
hostname(config)# isakmp peer gwa-peer-2
```

```
hostname(config-isakmp-peer)# interface ethernet0/4
```

```
hostname(config-isakmp-peer)# isakmp-proposal p1
```

```
hostname(config-isakmp-peer)# peer 20.20.20.2
```

```
hostname(config-isakmp-peer)# pre-share i39jnnNiCSh9rXb77oGA7Fg7BNQy
```

```
hostname(config-isakmp-peer)# exit
```

配置P2提议：

```
hostname(config)# ipsec proposal p2
```

```
hostname(config-ipsec-proposal)# protocol esp
```

```
hostname(config-ipsec-proposal)# hash md5
```

```
hostname(config-ipsec-proposal)# encryption des
```

```
hostname(config-ipsec-proposal)# exit
```

配置VPN隧道：

```
hostname(config)# tunnel ipsec vpn1-tunnel auto
```

```
hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2
```

```
hostname(config-tunnel-ipsec-auto)# isakmp-peer gwa-peer-1
```

```
hostname(config-tunnel-ipsec-auto)# vpn-track interval 1 threshold 5
```

```
hostname(config-tunnel-ipsec-auto)# track-event-notify enable
```

```
hostname(config-tunnel-ipsec-auto)# exit
```

```
hostname(config)# tunnel ipsec vpn2-tunnel auto
```

```
hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2
```

```
hostname(config-tunnel-ipsec-auto)# isakmp-peer gwa-peer-2
```

```
hostname(config-tunnel-ipsec-auto)# vpn-track interval 1 threshold 5
```

```
hostname(config-tunnel-ipsec-auto)# track-event-notify enable
```

```
hostname(config-tunnel-ipsec-auto)# auto-connect
```

```
hostname(config-tunnel-ipsec-auto)# exit
```

配置策略：

```
hostname(config)# policy-global
```

```
hostname(config-policy)# rule id 1
```

```
hostname(config-policy-rule)# src-ip 192.168.100.8/24
```

```
hostname(config-policy-rule)# dst-ip 172.16.10.8/24
```

```
hostname(config-policy-rule)# service any

hostname(config-policy-rule)# action tunnel vpn1-tunnel

hostname(config-policy-rule)# exit

hostname(config-policy)# rule id 2

hostname(config-policy-rule)# src-ip 172.16.10.8/24

hostname(config-policy-rule)# dst-ip 192.168.100.8/24

hostname(config-policy-rule)# service any

hostname(config-policy-rule)# action fromtunnel vpn1-tunnel

hostname(config-policy-rule)# exit

hostname(config-policy)# rule id 3

hostname(config-policy-rule)# src-ip 192.168.100.8/24

hostname(config-policy-rule)# dst-ip 172.16.10.8/24

hostname(config-policy-rule)# service any

hostname(config-policy-rule)# action tunnel vpn2-tunnel

hostname(config-policy-rule)# exit

hostname(config-policy)# rule id 4

hostname(config-policy-rule)# src-ip 172.16.10.8/24

hostname(config-policy-rule)# dst-ip 192.168.100.8/24

hostname(config-policy-rule)# service any

hostname(config-policy-rule)# action fromtunnel vpn2-tunnel

hostname(config-policy-rule)# exit

hostname(config-policy)# rule id 5

hostname(config-policy-rule)# src-addr any

hostname(config-policy-rule)# dst-addr any

hostname(config-policy-rule)# service any

hostname(config-policy-rule)# action permit
```



```
hostname(config-policy-rule)# exit
```

```
hostname(config-policy)# exit
```

```
hostname(config)#
```

第二步：配置Hillstone设备B：

配置接口：

```
hostname(config)# interface ethernet0/0
```

```
hostname(config-if-eth0/0)# zone trust
```

```
hostname(config-if-eth0/0)# ip address 172.16.10.1/24
```

```
hostname(config-if-eth0/0)# exit
```

```
hostname(config)# interface ethernet0/1
```

```
hostname(config-if-eth0/1)# zone untrust
```

```
hostname(config-if-eth0/1)# ip address 10.10.10.2/24
```

```
hostname(config-if-eth0/1)# exit
```

```
hostname(config)# interface ethernet0/4
```

```
hostname(config-if-eth0/4)# zone untrust
```

```
hostname(config-if-eth0/4)# ip address 20.20.20.2/24
```

```
hostname(config-if-eth0/4)# exit
```

配置路由：

```
hostname(config)# ip vrouter trust-vr
```

```
hostname(config-vrouter)# ip route 192.168.100.0/24 20.20.20.1
```

```
hostname(config-vrouter)# exit
```

配置P1提议

```
hostname(config)# isakmp proposal p1
```

```
hostname(config-isakmp-proposal)# authentication pre-share
```

```
hostname(config-isakmp-proposal)# group 2
```

```
hostname(config-isakmp-proposal)# hash md5  
hostname(config-isakmp-proposal)# encryption des  
hostname(config-isakmp-proposal)# exit
```

配置ISAKMP网关：

```
hostname(config)# isakmp peer gwb-peer-1  
hostname(config-isakmp-peer)# interface ethernet0/1  
hostname(config-isakmp-peer)# isakmp-proposal p1  
hostname(config-isakmp-peer)# peer 10.10.10.1  
hostname(config-isakmp-peer)# pre-shareU8FdHNEEBz6sNn5Mvqx3yWuLRWce  
hostname(config-isakmp-peer)# exit  
hostname(config)# isakmp peer gwb-peer-2  
hostname(config-isakmp-peer)# interface ethernet0/4  
hostname(config-isakmp-peer)# isakmp-proposal p1  
hostname(config-isakmp-peer)# peer 20.20.20.1  
hostname(config-isakmp-peer)# pre-sharei39jnnNiCSh9rXb77oGA7Fg7BNQy  
hostname(config-isakmp-peer)# exit
```

配置P2提议：

```
hostname(config)# ipsec proposal p2  
hostname(config-ipsec-proposal)# protocol esp  
hostname(config-ipsec-proposal)# hash md5  
hostname(config-ipsec-proposal)# encryption des  
hostname(config-ipsec-proposal)# exit
```

配置VPN隧道：

```
hostname(config)# tunnel ipsec vpn1-tunnel auto  
hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2  
hostname(config-tunnel-ipsec-auto)# isakmp-peer gwb-peer-1
```

```

hostname(config-tunnel-ipsec-auto)# vpn-track interval 1 threshold 5

hostname(config-tunnel-ipsec-auto)# auto-connect

hostname(config-tunnel-ipsec-auto)# exit

hostname(config)# tunnel ipsec vpn2-tunnel auto

hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2

hostname(config-tunnel-ipsec-auto)# isakmp-peer gwa-peer-2

hostname(config-tunnel-ipsec-auto)# vpn-track interval 1 threshold 5

hostname(config-tunnel-ipsec-auto)# track-event-notify enable

hostname(config-tunnel-ipsec-auto)#auto-connect

hostname(config-tunnel-ipsec-auto)# exit

```

配置策略：

```

hostname(config)# policy-global

hostname(config-policy)# rule id 1

hostname(config-policy-rule)# src-ip 172.16.10.8/24

hostname(config-policy-rule)# dst-ip 192.168.100.8/24

hostname(config-policy-rule)# service any

hostname(config-policy-rule)# action fromtunnel vpn1-tunnel

hostname(config-policy-rule)# exit

hostname(config-policy)# rule id 2

hostname(config-policy-rule)# src-ip 192.168.100.8/24

hostname(config-policy-rule)# dst-ip 172.16.10.8/24

hostname(config-policy-rule)# service any

hostname(config-policy-rule)# action tunnel vpn1-tunnel

hostname(config-policy-rule)# exit

hostname(config-policy)# rule id 3

hostname(config-policy-rule)# src-ip 172.16.10.8/24

```

```

hostname(config-policy-rule)# dst-ip 192.168.100.8/24

hostname(config-policy-rule)# service any

hostname(config-policy-rule)# action fromtunnel vpn2-tunnel

hostname(config-policy-rule)# exit

hostname(config-policy)# rule id 4

hostname(config-policy-rule)# src-ip 192.168.100.8/24

hostname(config-policy-rule)# dst-ip 172.16.10.8/24

hostname(config-policy-rule)# service any

hostname(config-policy-rule)# action tunnel vpn2-tunnel

hostname(config-policy-rule)# exit

hostname(config-policy)# rule id 5

hostname(config-policy-rule)# src-addr any

hostname(config-policy-rule)# dst-addr any

hostname(config-policy-rule)# service any

hostname(config-policy-rule)# action permit

hostname(config-policy-rule)# exit

hostname(config-policy)# exit

hostname(config)#

```

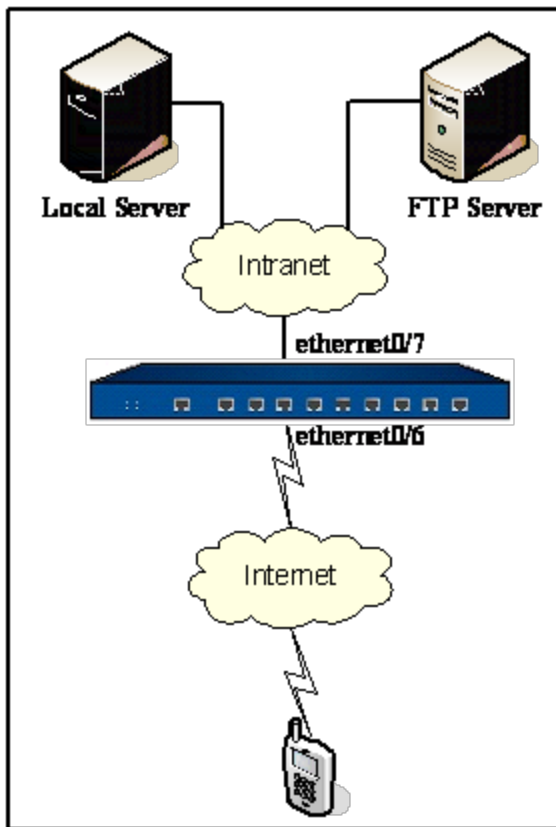
由于本例中VPN终端设备都是Hillstone设备，因此可使用缺省源和目标地址进行VPN监控。

XAUTH

本节介绍典型的XAUTH配置实例。

组网需求

Hillstone设备上启用了XAUTH服务器，使用本地AAA服务器认证用户。要求当用户试图通过手机终端创建VPN连接并访问内网的FTP服务器时，XAUTH服务器通过预共享秘钥方式对用户身份进行验证，并允许通过验证的用户访问内网资源。组网图请参考下图。



配置步骤

第一步：配置接口、安全域和策略：

接口配置：

```
hostname(config)# interface ethernet0/6
hostname(config-if-eth0/7)# zone trust
hostname(config-if-eth0/7)# ip address 6.6.6.6 255.255.255.0
hostname(config-if-eth0/7)# manage ping
hostname(config-if-eth0/7)# manage ssh
hostname(config-if-eth0/7)# manage http
hostname(config-if-eth0/7)# exit
hostname(config)# interface ethernet0/7
hostname(config-if-eth0/6)# zone untrust
```

```
hostname(config-if-eth0/6)# ip address 7.7.7.7 255.255.255.0
```

```
hostname(config-if-eth0/6)# exit
```

```
hostname(config)# rule top
```

```
hostname(config-policy-rule)# src-zone untrust
```

```
hostname(config-policy-rule)# dst-zone trust
```

```
hostname(config-policy-rule)# service any
```

```
hostname(config-policy-rule)# action permit
```

```
hostname(config-policy-rule)# exit
```

```
hostname(config)#
```

第二步：配置AAA服务器：

```
hostname(config)# aaa-server local type local
```

```
hostname(config-aaa-server)# user xauth
```

```
hostname(config-user)# password test
```

```
hostname(config-user)# ike-id key-id xauth
```

```
hostname(config-user)# end
```

```
hostname(config)#
```

第三步：配置XAUTH地址池

```
hostname(config)# xauth pool pool
```

```
hostname(config-xauth-pool)# address 9.9.9.9 9.9.9.99 netmask 255.255.255.0
```

```
hostname(config-xauth-pool)# exit
```

```
hostname(config)#
```

第四步：配置ISAKMP网关：

```
hostname(config)# isakmp peer xauth
```

```
hostname(config-isakmp-peer)# mode aggressive
```

```
hostname(config-isakmp-peer)# type usergroup
hostname(config-isakmp-peer)# psk-sha-aes128-g2
hostname(config-isakmp-peer)# pre-share XhF44BilJO3b/2HF15IVqXniqeMByq
hostname(config-isakmp-peer)# aaa-server local
hostname(config-isakmp-peer)# local-id key-id xauth
hostname(config-isakmp-peer)# xauth pool-name pool
hostname(config-isakmp-peer)# xauth server
hostname(config-isakmp-peer)# interfaceethernet0/7
hostname(config-isakmp-peer)# exit
hostname(config)#
```

第五步：创建IKE隧道和隧道接口：

```
hostname(config)# tunnel ipsec xauth auto
hostname(config-tunnel-ipsec-auto)# isakmp-peer xauth
hostname(config-tunnel-ipsec-auto)# esp-sha-aes128-g0
hostname(config-tunnel-ipsec-auto)# accept-all-proxy-id
hostname(config-tunnel-ipsec-auto)# exit
hostname(config)# interface tunnel22
hostname(config-if-tun22)# zone trust
hostname(config-if-tun22)# ip address 9.9.9.1 255.255.255.0
hostname(config-if-tun22)# manage telnet
hostname(config-if-tun22)# manage ssh
hostname(config-if-tun22)# manage ping
hostname(config-if-tun22)# manage http
hostname(config-if-tun22)# manage https
hostname(config-if-tun22)# manage snmp
```

```
hostname(config-if-tun22)# tunnel ipsec xauth
```

```
hostname(config-if-tun22)# exit
```

```
hostname(config)#
```

完成上述配置后，手机用户可以利用安卓或iOS系统中自带的VPN客户端完成认证（用户名xauth，密码test，IPSec标示符/群组名称xauth）并访问内网资源。

配置PnPVPN

IPSec VPN配置复杂，维护成本高，对网管人员技术要求高，针对该问题，为企业用户提供了一种简单易用的VPN技术——PnPVPN，即即插即用VPN。PnPVPN由两部分组成，分别是PnPVPN Server和PnPVPN Client，各自功能描述如下：

- **PnPVPN Server**：通常放置于企业总部，由总部IT工程师负责维护，客户端的大多数配置由服务器下发。PnPVPN Server通常由设备充当，一台设备可充当多个PnPVPN Server。
- **PnPVPN Client**：通常放置于企业分支机构（如办事处），可由总部工程师远程维护，只需要做简单配置（如客户端ID、密码和服务器端IP地址），和Server端协商成功后即可从Server端获取配置信息（如DNS、WINS、DHCP地址池等）。

设备既可以充当PnPVPN Server，又可以充当PnPVPN Client。当充当Server时，不同平台支持的VPN实例数和每个实例所支持的客户端数有所不同。

PnPVPN工作流程

PnPVPN的工作流程如下：

1. 客户端发起连接请求，并传送自己的ID以及密码到服务器端。
2. 服务器端收到请求后，验证客户端传送的ID和密码，验证通过即下发预配置的DHCP地址池、DHCP掩码、DHCP网关、WINS、DNS和隧道路由等信息到客户端。
3. 客户端把收到的信息下发到相应的功能模块。
4. 客户端PC自动获取IP地址、IP地址掩码和网关地址等网络参数，并正常接入VPN网络。

PnPVPN链路冗余

PnPVPN服务器端支持一个PnPVPN客户端拨入两条VPN链路并自动生成到客户端的路由、为客户端配置VPN监控。服务器端需要配置两个ISAKMP网关和两个隧道接口，两个VPN隧道分别引用不同的ISAKMP网关，并绑定到两个不同的隧道接口。

客户端支持通过VPN双链路拨入服务器端、VPN监控和冗余选路。PnP客户端的两个VPN隧道在和服务端协商时，会根据服务器端的隧道路由配置分别生成不同优先级的路由，优先级高的隧道作为主链路，优先级低的隧道作为备份链路，从而实现冗余选路。主VPN隧道会首先处于active状态，如果客户端监测到该主隧道中断，客户端设备会通过备份隧道重新传输数据；当监测到主隧道恢复正常后，客户端设备会重新启用主隧道传输数据。

PnPVPN服务器端配置

PnPVPN配置包括服务器端配置和客户端配置。服务器端可通过CLI和WebUI两种方式进行配置。

通过CLI配置PnPVPN服务器端

PnPVPN服务器端配置基于IPSec VPN命令行，此外，还有特有的命令行，本节仅介绍PnPVPN特有命令行。使用以下特有命令并不能完成服务器端的配置，完整配置请参见[PnPVPN配置举例部分](#)。

配置用户网络参数

客户端与服务器端VPN协商成功后，服务器端需要下发给用户端网络参数信息，包括DNS服务器地址、WINS服务器地址、隧道路由、DHCP地址池及其掩码和网关地址。这些网络参数需要在相应的用户配置模式下进行配置。DNS、WINS和隧道路由也可以在IKE隧道配置模式下配置，但用户配置模式下的配置优先级高于IKE隧道配置模式，即当用户配置模式和IKE隧道配置模式同时配置了DNS、WINS或隧道路由，服务器使用用户配置模式下的配置下发给客户端。

进入本地用户配置模式，在全局配置模式下，使用以下命令：

```
aaa-server aaa-server-name type local （进入本地AAA认证服务器配置模式）
```

在本地AAA认证服务器配置模式下，使用以下命令指定需下发给用户：

```
user user-name
```

- *user-name* – 指定用户名称进入相应用户的配置模式。

在上述用户的配置模式下，通过以下命令完成用户网络参数的配置，其中DHCP地址池、DHCP网络掩码和网关为必配网络参数。

dns *A.B.C.D* [*A.B.C.D*] [*A.B.C.D*] [*A.B.C.D*]

- *A.B.C.D* – 配置DNS服务器的IP地址，可同时指定1个主DNS服务器和最多3个备份服务器。使用**no dns**命令取消配置。

wins *A.B.C.D* [*A.B.C.D*]

- *A.B.C.D* – 配置WINS服务器的IP地址，可同时指定一个主WINS服务器和一个备份WINS服务器。使用**no wins**命令取消配置。

split-tunnel-route *A.B.C.D/Mask*

- *A.B.C.D/Mask* – 配置隧道路由。A.B.C.D为IP地址前缀，Mask为子网掩码的位数。最多可设置128条隧道路由。使用**no split-tunnel-route** *A.B.C.D/Mask*命令取消配置。

dhcp-pool-address *start-ipaddr end-ipaddr*

- *start-ipaddr end-ipaddr* – 配置DHCP地址池的起始IP地址和终止IP地址。使用**no dhcp-pool-address**命令取消配置。

dhcp-pool-netmask *A.B.C.D*

- *A.B.C.D* – 配置DHCP地址池的网络掩码。使用**no dhcp-pool-netmask**命令取消配置。

dhcp-pool-gateway *A.B.C.D*

- *A.B.C.D* – 配置DHCP地址池的网关地址。该地址用来作为PnPVPN客户端内网接口的IP地址，并被设置为PC的网关地址，PC的IP地址由以上设置的DHCP地址池的网段以及网络掩码确定，所以网关地址应该和DHCP地址池在同一个网段。

使用**no dhcp-pool-gateway**命令取消配置。

配置隧道网络参数

当所有或大部分客户端使用统一的DNS、WINS或隧道路由时，可以在IKE隧道配置模式下配置DNS、WINS或隧道路由以减少用户配置模式下的工作量。使用以下命令进入IKE隧道配置模式：

tunnel ipsec *tunnel-name* **auto**

- *tunnel-name* – 指定IKE隧道名称。

在IKE隧道配置模式下，通过以下命令完成DNS、WINS或隧道路由的配置：

dns *A.B.C.D* [*A.B.C.D*] [*A.B.C.D*] [*A.B.C.D*]

- *A.B.C.D* – 配置DNS服务器的IP地址，可同时指定1个主DNS服务器和最多3个备份服务器。使用**no dns**命令取消配置。

wins *A.B.C.D* [*A.B.C.D*]

- *A.B.C.D* – 配置WINS服务器的IP地址，可同时指定一个主WINS服务器和一个备份WINS服务器。使用**no wins**命令取消配置。

split-tunnel-route *A.B.C.D/Mask*

- *A.B.C.D/Mask* – 配置隧道路由。A.B.C.D为IP地址前缀，Mask为子网掩码的位数。最多可设置128条隧道路由。使用**no split-tunnel-route** *A.B.C.D/Mask*命令取消配置。

配置ISAKMP网关对端通配符

当PnVPN Server通过Radius服务器进行认证时，需要配置ISAKMP网关对端的通配符。Hillstone设备在收到客户端的VPN连接建立请求时，根据客户端的用户名与ISAKMP网关对端通配符的匹配结果，确定与客户端接入的PnVPN Server（一台Hillstone设备可同时充当多个PnVPN的Server），进而确定对用户进行认证的Radius服务器。

在ISAKMP网关配置模式下，使用以下命令配置ISAKMP网关对端通配符：

peer-id fqdn wildcard *string*

- **fqdn** – 指定使用FQDN类型的通配符。
- **wildcard** *string* – 指定通配符ID，通常为客户端的域名。如abc.com。

使用**no peer-id**命令取消通配符配置。

配置PnVPN客户端的隧道接口

为了使分支机构的多个子网网段可以访问服务器端，ADC支持在PnVPN服务器端为客户端的隧道接口指定IP地址，并启用SNAT规则。如果PnVPN客户端是由Hillstone SR系列安全路由器充当，那么需要SR系列产品的版本支持该功能。



注意: 该功能工作时，PnPVPN服务器端将无法访问客户端。

进入本地用户配置模式，使用以下命令：

aaa-server *aaa-server-name* **type local** （进入本地AAA认证服务器配置模式）

user *user-name*

- *user-name* – 指定用户名称。

在本地用户配置模式下，使用以下命令配置PnPVPN客户端的隧道接口：

tunnel-ip-address *A.B.C.D* [**snat**]

- *A.B.C.D* – 指定客户端隧道接口的IP地址，该地址不能与客户端已存在的IP地址冲突。
- **snat** – 启用SNAT规则。默认情况下，系统不开启隧道接口的SNAT规则。

在本地用户配置模式下，使用**no tunnel-ip-address**命令取消配置PnPVPN客户端的隧道接口。

通过WebUI配置服务器端

通过WebUI配置服务器端，用户需要在以下模块进行配置：

- 用户配置
- IKE VPN配置
- 隧道接口配置
- 路由配置
- 策略配置



注意: PnPVPN支持两种认证服务器：Local和Radius。以下配置列出使用本地服务器进行认证的情况，关于Radius服务器认证配置请参阅相应的Radius服务器使用手册。

用户配置

请按照以下步骤进行用户配置：

1. 选择“对象 > 用户 > 本地用户”。
2. 在<本地服务器>下拉菜单中选择需要的本地服务器名称，然后点击“新建 > 用户”，弹出<用户配置>对话框。
3. 在<基本配置>标签页输入用户名称、用户密码以及密码确认。
4. 在<高级配置>标签页指定用户IKE ID为“FQDN”，并在文本框中输入ID。PnVPN Client将使用该ID进行登录认证。
5. 在<高级配置>标签页，配置PnVPN具体选项，包括DHCP相关选项、DNS、WINS以及隧道路由。当该用户不使用隧道下已经配置的DNS、WINS和隧道路由选项或者新建隧道页面未配置这些选项时，这些选项必须在本页面完成配置。
6. 根据需要对该页面的其它选项进行配置。
7. 配置完成，点击“确定”。

IKE VPN配置

IKE VPN配置包括P1提议配置、P2提议配置、对端配置以及隧道配置。

按照以下步骤配置P1提议：

1. 选择“网络 > VPN > IKEv1和手动 > P1提议”，进入P1提议标签页。
2. 点击“新建”按钮，弹出<阶段1提议配置>对话框。
3. 指定P1提议名称。在“提议名称”文本框输入P1提议名称。
4. 指定认证方式。选中“pre-share”单选按钮。
5. 指定DH组。选中“Group2”单选按钮。
6. 根据需要对该页面的其它选项进行配置或保持其默认值。
7. 配置完成，点击“确定”。

按照以下步骤配置P2提议：

1. 选择“网络 > VPN > IKEv1和手动 > P2提议”，进入P2提议标签页。
2. 点击“新建”按钮，弹出“阶段2提议配置”对话框。
3. 指定P2提议名称。在“提议名称”文本框输入P2提议名称。
4. 选择使用的协议、验证算法、加密算法和PFS组。
5. 根据需要对该页面的其它选项进行配置或保持其默认值。
6. 配置完成，点击“确定”。

按照以下步骤配置对端：

1. 选择“网络 > VPN > IKEv1和手动 > VPN对端列表”，进入VPN对端标签页。
2. 点击“新建”，弹出<VPN对端配置>对话框。
3. 指定对端名称。在“对端名称”文本框输入对端名称。
4. 指定外网接口。从“接口”下拉菜单中选择需要的接口。
5. 指定模式和类型。选中“野蛮模式”和“用户组”单选按钮。
6. 指定认证服务器。从“AAA服务器”下拉菜单选择使用的认证服务器。
7. 指定P1提议。从“提议1”下拉菜单中选择需要的P1提议。
8. 指定预共享密钥。在“预共享密钥”文本框输入相应的预共享密钥。
9. 根据需要对该页面的其它选项进行配置或保持其默认值。
10. 点击“生成”，弹出<生成用户密钥>对话框。输入用户ID和预共享密钥，点击“生成”，生成的密钥将显示在<创建结果>文本框中。PnPVPN Client将使用该密钥作为密码进行登录认证。点击“关闭”按钮返回对端配置页面。
11. 点击“确定”按钮保存所做配置。



注意：当选用Radius服务器进行认证时，必须配置对端通配符。

按照以下步骤配置隧道：

1. 选择“网络 > VPN > IKEv1和手动 > IKE VPN列表”。
2. 点击IKE VPN列表左上方的“新建”按钮，弹出<IKE VPN配置>对话框。
3. 在<基本配置>标签页：
 - 在“对端选项”的下拉菜单中选择需要的对端。用户也可以直接在该页面新建对端（ISAKMP网关）。
 - 输入隧道名称。
 - 隧道模式选择“tunnel”。
 - 在“P2提议”的下拉菜单中选择需要的提议。
4. 在<高级配置>标签页：
 - 配置DNS和WINS服务器。通过该隧道接入的用户将使用此处指定的DNS和WINS。
 - 设置隧道路由。
 - 根据需要对该页面的其它选项进行配置或保持其默认值。
5. 点击“确定”按钮保存所做配置。

隧道接口配置

请按照以下步骤进行隧道接口配置：

1. 点击“网络 > 接口”，进入接口配置页面。
2. 点击“新建 > 隧道接口”，弹出<隧道接口>配置对话框。
3. 指定隧道接口名称。在“接口名称”后的文本框输入编号。
4. 指定隧道接口所属安全域类型。在“绑定安全域”部分选择“三层安全域”单选按钮，并在“安全域”下拉菜单中选择需要的安全域。
5. 绑定隧道。在<隧道绑定配置>部分选中“IPSec VPN”单选按钮，然后从“VPN名称”拉菜单选择VPN隧道名称。无需配置网关地址。
6. 点击“确定”保存所做配置。

路由配置

为实现服务器端网络的主机能够访问客户端网络，用户需要添加静态路由条目。按照以下步骤配置路由：

1. 访问“网络 > 路由 > 目的路由”，进入目的路由页面。
2. 点击“新建”，弹出<目的路由配置>对话框。
3. 配置目的IP。在“目的地”和“子网掩码”文本框中分别输入客户端网络内网IP前缀和子网掩码。
4. 配置下一跳。在“下一跳”部分选择“接口”单选按钮，然后从“接口”下拉菜单中选择VPN隧道绑定的隧道接口，并在“网关”文本框中填写设备端外网接口的IP地址。
5. 根据需要对页面的其它选项进行配置或保持其默认值。
6. 点击“确定”保存所做配置。

策略配置

根据网络拓扑情况，配置相应的访问策略（点击“配置 > 安全 > 策略”，进入策略页面）。

配置PnPVPN客户端

PnPVPN客户端仅支持WebUI方式配置。按照以下步骤通过WebUI配置PnPVPN客户端：

1. 选择“网络 > VPN > IKEv1和手动”，进入IPSec VPN页面。
2. 页面右上角的“PnPVPN客户端”按钮，弹出<PnPVPN配置>对话框。
3. 依次填写或者选择各项。配置选项具体描述如下：
 - 服务器地址1：指定服务器端IP地址。该选项为必选项。
 - 服务器地址2：指定服务器端IP地址。服务器地址1和服务器地址2可以相同，也可以不同。该选项为可选项。
 - ID：指定服务器端分配给用户端的IKE ID。
 - 密码：指定服务器端分配给用户端的密码。
 - 重新输入密码：再次输入密码以确认。

- 自动保存：勾选“启用”复选框，系统自动保存连接建立后PnPVPN服务器端下发给客户端的DHCP和WINS信息。
- VPN出接口1：VPN出接口1是接入Internet的接口，从下拉菜单中选择需要的接口名称。该选项为必选项。
- VPN出接口2：VPN出接口2是接入Internet的接口，从下拉菜单中选择需要的接口名称。出接口1和出接口2可以相同，也可以不同。该选项为可选项。
- VPN入接口：VPN入接口是内部PC或者各种应用服务器在PnPVPN客户端上的接入口，从下拉菜单中选择需要的接口名称。

4. 配置完成，点击“确定”保存所做配置并返回IPSec VPN页面。



注意:

- 服务器地址1和VPN出接口1是必须配置的，如果要配置备份链路，需要同时配置服务器地址2和VPN出接口2。
- 只要服务器地址和VPN出接口有一项不同，就会生成两条独立的VPN链路。如果服务器地址和VPN出接口的配置都相同，只会生成一条链路。
- 两个服务端的配置可以配置在一台设备上，也可以配置在主备两台不同的设备上。如果配置在两台设备上，在两台设备上都需要配置AAA用户，AAA用户中的DHCP配置必须相同，否则可能会导致客户端和服务器端协商成功但是流量不通。

PnPVPN配置举例

该节介绍PnPVPN配置实例。

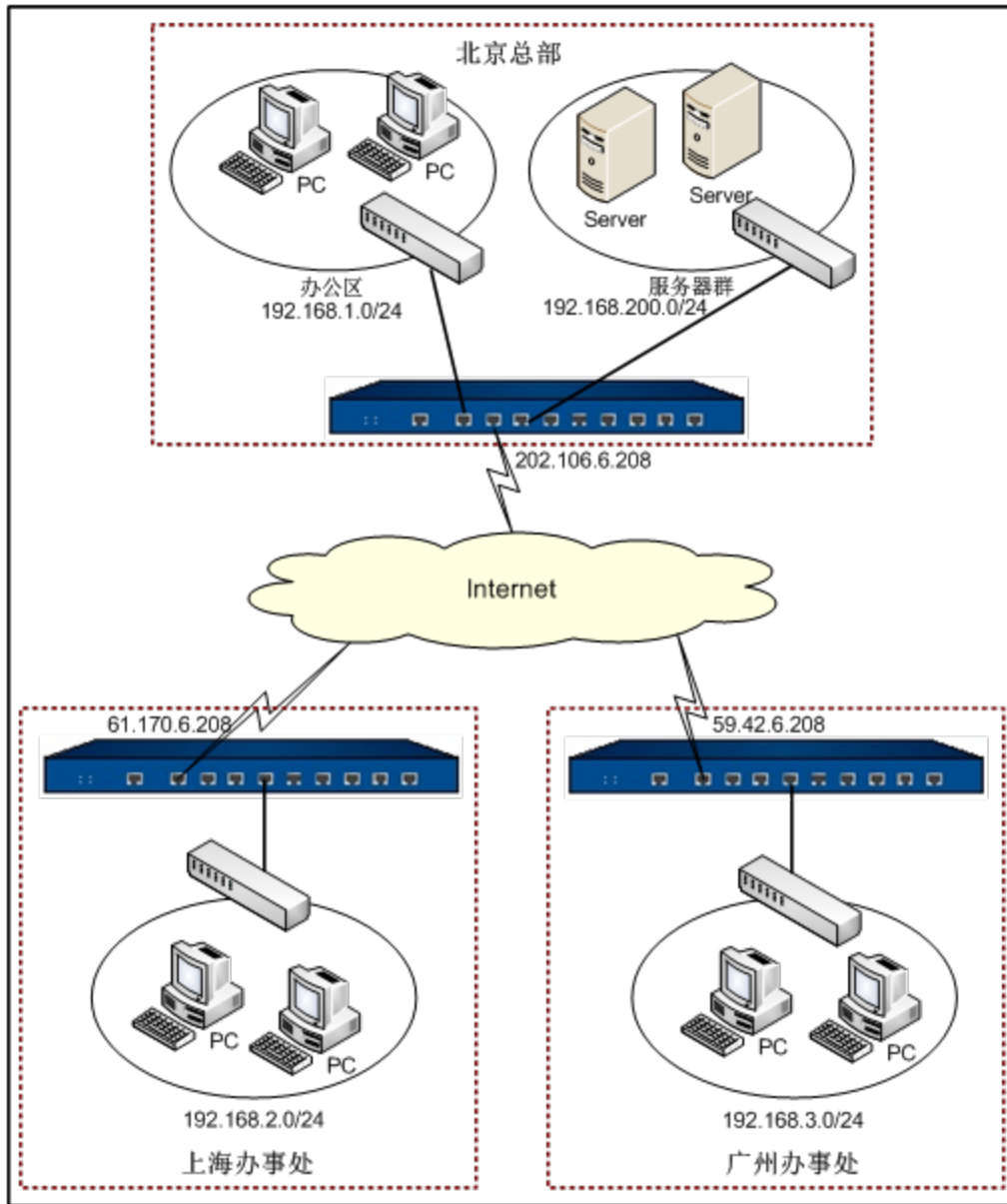
组网需求

某公司总部位于北京，在上海和广州设有办事处，三地均可成功接入Internet。由于业务需求，需要组建VPN网络，达到以下目的：

- 广州和上海办事处的员工通过VPN访问总部数据库；
- 公司员工（包括总部和两办事处三地）之间可以通过VPN共享资源。

通过配置PnPPVPN可实现以上需求，并且简单实用。组网图如图所示。配置方式如下：

- 公司总部选用一台Hillstone设备作为PnPPVPN Server，采用本地认证方式；
- 上海和广州办事处各部署一台Hillstone设备，作为PnPPVPN Client，接入总部VPN网络。
- 通过策略和路由配置实现允许公司员工之间的资源共享。



根据上图，具体网络环境描述如下：

- 总部局域网网段为192.168.1.0/24，通过接口ethernet0/0接入网络，属于trust安全域；
- 总部服务器群网段为192.168.200.0/24，通过接口ethernet0/2接入网络，属于trust安全域；
- 总部Hillstone设备通过接口ethernet0/1（IP地址为202.106.6.208）接入Internet，属于untrust安全域。
- 上海办事处设备接入Internet的接口IP地址为61.170.6.208，广州办事处设备接入Internet的IP地址为59.42.6.208。
- PnVPN Server将分配192.168.2.0/24网段到上海办事处，192.168.3.0/24网段到广州办事处。

配置步骤

配置步骤分服务器端配置和客户端配置。

服务器端配置

第一步：配置本地AAA认证服务器：

```
hostname(config)# aaa-server test type local
hostname(config-aaa-server)# exit
hostname(config)#
```

第二步：为上海办事处配置网络参数：

```
hostname(config)# aaa-server test type local
hostname(config-aaa-server)# user shanghai
hostname(config-user)# ike-id fqdn shanghai
hostname(config-user)# dhcp-pool-address 192.168.2.1 192.168.2.100
hostname(config-user)# dhcp-pool-netmask 255.255.255.0
hostname(config-user)# dhcp-pool-gateway 192.168.2.101
hostname(config-user)# split-tunnel-route 192.168.200.0/24
hostname(config-user)# split-tunnel-route 192.168.1.0/24
hostname(config-user)# split-tunnel-route 192.168.3.0/24
hostname(config-user)# exit
```

```
hostname(config-aaa-server)# exit
```

```
hostname(config)#
```

第三步：为广州办事处配置网络参数：

```
hostname(config)# aaa-server test type local
```

```
hostname(config-aaa-server)# user guangzhou
```

```
hostname(config-user)# ike-id fqdn guangzhou
```

```
hostname(config-user)# dhcp-pool-address 192.168.3.1 192.168.3.100
```

```
hostname(config-user)# dhcp-pool-netmask 255.255.255.0
```

```
hostname(config-user)# dhcp-pool-gateway 192.168.3.101
```

```
hostname(config-user)# split-tunnel-route 192.168.200.0/24
```

```
hostname(config-user)# split-tunnel-route 192.168.1.0/24
```

```
hostname(config-user)# split-tunnel-route 192.168.2.0/24
```

```
hostname(config-user)# exit
```

```
hostname(config-aaa-server)# exit
```

```
hostname(config)#
```

第四步：配置PnVPN Server：

```
hostname(config)# isakmp proposal test1
```

```
hostname(config-isakmp-proposal)# group 2
```

```
hostname(config-isakmp-proposal)# exit
```

```
hostname(config)# ipsec proposal test2
```

```
hostname(config-ipsec-proposal)# exit
```

```
hostname(config)# isakmp peer test1
```

```
hostname(config-isakmp-peer)# type usergroup
```

```
hostname(config-isakmp-peer)# mode aggressive
```

```
hostname(config-isakmp-peer)# interface ethernet0/1
```

```
hostname(config-isakmp-peer)# aaa-server test
hostname(config-isakmp-peer)# isakmp-proposal test1
hostname(config-isakmp-peer)# pre-share 123456
hostname(config-isakmp-peer)# generate-route
hostname(config-isakmp-peer)# exit
hostname(config)# tunnel ipsec test auto
hostname(config-tunnel-ipsec-auto)# ipsec-proposal test2
hostname(config-tunnel-ipsec-auto)# isakmp-peer test1
hostname(config-tunnel-ipsec-auto)# mode tunnel
hostname(config-tunnel-ipsec-auto)# id auto
hostname(config-tunnel-ipsec-auto)# dns 192.168.200.1 192.168.200.11
hostname(config-tunnel-ipsec-auto)# wins 192.168.200.2 192.168.200.12
hostname(config-tunnel-ipsec-auto)# exit
hostname(config)#
```

第五步：生成客户端密钥：

```
hostname(config)# exec generate-user-key rootkey 123456 userid shanghai
userkey: kyZAKmLWCc5Nz75fseDiM2r+4Vg=
hostname(config)# exec generate-user-key rootkey 123456 userid guangzhou
userkey: SdqhY4+dPThTtpipW2hs2OMB5Ps=
```

第六步：配置隧道接口和策略规则：

```
hostname(config)# zone VPN
hostname(config-zone-VPN)# exit
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone VPN
hostname(config-if-tun1)# tunnel ipsec test
```

```
hostname(config-if-tun1)# exit

hostname(config)# policy-global

hostname(config-policy)# rule

hostname(config-policy-rule)# src-zone VPN

hostname(config-policy-rule)# dst-zone trust

hostname(config-policy-rule)# src-addr any

hostname(config-policy-rule)# dst-addr any

hostname(config-policy-rule)# service any

hostname(config-policy-rule)# action permit

hostname(config-policy-rule)# exit

hostname(config-policy)# rule

hostname(config-policy-rule)# src-zone trust

hostname(config-policy-rule)# dst-zone VPN

hostname(config-policy-rule)# src-addr any

hostname(config-policy-rule)# dst-addr any

hostname(config-policy-rule)# service any

hostname(config-policy-rule)# action permit

hostname(config-policy-rule)# exit

hostname(config-policy)# rule

hostname(config-policy-rule)# src-zone VPN

hostname(config-policy-rule)# dst-zone VPN

hostname(config-policy-rule)# src-addr any

hostname(config-policy-rule)# dst-addr any

hostname(config-policy-rule)# service any

hostname(config-policy-rule)# action permit

hostname(config-policy-rule)# exit
```

```
hostname(config-policy)# exit
```

```
hostname(config)#
```

客户端配置

上海办事处设备配置如下：

1. 登录设备WebUI，点击“网络 > VPN > IPSec VPN”，进入IPSec VPN页面。
2. 在<IKE VPN配置>部分，点击右上方的“PnPVPN客户端”按钮，弹出<PnPVPN配置>对话框。在该对话框做以下配置：
 - 服务器地址：202.106.6.208
 - ID：shanghai
 - 密码：kyZAKmLWCc5Nz75fscDiM2r+4Vg=
 - 重新输入密码：kyZAKmLWCc5Nz75fscDiM2r+4Vg=
 - 自动保存：选中复选框
 - VPN出接口：ethernet0/0
 - VPN入接口：ethernet0/3
3. 点击“确定”按钮保存所做配置并发起链接。

广州办事处设备配置如下：

1. 登录设备WebUI，点击“网络 > VPN > IPSec VPN”，进入IPSec VPN页面。
2. 在<IKE VPN配置>部分，点击右上方的“PnPVPN客户端”按钮，弹出<PnPVPN配置>对话框。在该对话框做以下配置：
 - 服务器地址：202.106.6.208
 - ID：guangzhou
 - 密码：SdqhY4+dPThTtpipW2hs2OMB5Ps=
 - 重新输入密码：SdqhY4+dPThTtpipW2hs2OMB5Ps=

- 自动保存：选中复选框
- VPN出接口： ethernet0/0
- VPN入接口： ethernet0/3

3. 点击“确定”按钮保存所做配置并发起链接。

IKEv2 VPN

IKEv2 VPN的配置包括：

- [配置P1提议](#)
- [配置IKEv2对等体](#)
- [配置P2提议](#)
- [配置隧道](#)

配置P1提议

P1提议是IKEv2安全提议，用于保存IKE_SA_INIT交换中所使用的安全参数，包括加密算法、完整性验证算法、PRF（pseudo-random function）算法和DH组。一个完整的IKEv2安全提议中至少应该包含一组安全参数，即一个加密算法、一个完整性验证算法、一个PRF算法和一个DH组。

创建P1提议

创建一个P1提议，即IKEv2安全提议，在全局配置模式下使用以下命令：

ikev2 proposal *p1-name*

- *p1-name* – 指定所创建的P1提议的名称。执行该命令后，进入到P1提议配置模式。用户可以在该模式下对P1提议进行参数配置。

使用**no ikev2 proposal *p1-name***命令删除指定的P1提议。

指定验证算法

系统支持以下验证算法：MD5、SHA-1以及SHA-2（包括SHA-256、SHA-384和SHA-512）。用户可指定至少一种最多四种验证算法。指定IKEv2安全提议的验证算法，在P1提议模式下使用以下命令：

hash {md5 | sha | sha256 | sha384 | sha512}

- **md5** – 指定使用MD5验证算法。摘要为128比特。
- **sha** – 指定使用SHA-1验证算法。摘要为160比特。该算法为默认算法。
- **sha256** – 指定使用SHA-256验证算法。摘要为256比特。
- **sha384** – 指定使用SHA-384验证算法。摘要为384比特。
- **sha512** – 指定使用SHA-512验证算法。摘要为512比特。

使用**no hash**命令恢复默认认证方式。

指定PRF算法

系统支持以下PRF算法：MD5、SHA-1以及SHA-2（包括SHA-256、SHA-384和SHA-512）。用户可指定至少一种最多四种PRF算法。指定IKEv2安全提议的PRF算法，在P1提议模式下使用以下命令：

prf {md5 | sha | sha256 | sha384 | sha512}

- **md5** – 指定使用MD5算法。摘要为128比特。
- **sha** – 指定使用SHA-1算法。摘要为160比特。该算法为默认算法。
- **sha256** – 指定使用SHA-256算法。摘要为256比特。
- **sha384** – 指定使用SHA-384算法。摘要为384比特。
- **sha512** – 指定使用SHA-512算法。摘要为512比特。

使用**no prf**命令恢复默认认证方式。

指定加密算法

系统提供以下四种加密算法：3DES、128bit AES、192bit AES以及256bit AES。用户可指定至少一种最多四种加密算法。指定IKEv2安全提议的加密算法，在P1提议配置模式下使用以下命令：

encryption {3des | aes | aes-192 | aes-256}

- **3des** – 指定使用3DES加密方法。密钥长度为192比特。该方法为默认方法。
- **aes** – 指定使用AES加密方法。密钥长度为128比特。

- **aes-192** – 指定使用192bit AES加密方法。密钥长度为192比特。
- **aes-256** – 指定使用256bit AES加密方法。密钥长度为256比特。

使用**no encryption**命令恢复默认加密算法。

选择DH组

Diffie-Hellman (DH) 是一种建立密钥的方法。DH组决定DH交换中密钥生成“材料”的长度。密钥的牢固性部分决定于DH组的强度。指定IKEv2安全提议的DH组，在P1提议配置模式下使用以下命令：

group {1 | 2 | 5 | 14 | 15 | 16 | 19 | 20 | 21 | 24}

- **1** – 选择DH组1。密钥的长度为768比特（MODP Group）。
- **2** – 选择DH组2。密钥的长度为1024比特（MODP Group）。DH组2为系统默认选择。
- **5** – 选择DH组5。密钥的长度为1536比特（MODP Group）。
- **14** – 选择DH组14。密钥的长度为2048比特（MODP Group）。
- **15** – 选择DH组15。密钥的长度为3072比特（MODP Group）。
- **16** – 选择DH组16。密钥的长度为4096比特（MODP Group）。
- **19** – 选择DH组19。密钥的长度为256比特（ECP Group）。
- **20** – 选择DH组20。密钥的长度为384比特（ECP Group）。
- **21** – 选择DH组21。密钥的长度为521比特（ECP Group）。
- **24** – 选择DH组24。密钥的长度为2048比特（MODP Group with 256-bit Prime Order Subgroup）。

使用**no group**命令取消恢复默认DH组。

指定的生命周期

IKEv2 SA的生命周期不需要协商，由各自的配置决定，重协商总是由生命周期较小的一方发起，可尽量避免两端同时发起重协商造成冗余SA的生成，导致两端SA状态不一致。指定本端IKEv2 SA的生命周期，在P1提议配置模式下使用以下命令：

lifetime *time-value*

- *time-value* – 指定IKEv2 SA的生命周期长度，单位为秒。默认28800秒。范围是180到86400秒。

使用**no lifetime**命令恢复默认生命周期长度。

配置IKEv2对等体

创建一个IKEv2对等体后，用户可以配置对等体的IKE协商模式、对等体的IP地址、IKE安全提议、本地ID等。

创建IKEv2对等体

创建IKEv2对等体，在全局配置模式下，使用以下命令：

```
ikev2 peer peer-name
```

- *peer-name* – 指定对等体的名称。

执行该命令后，CLI进入到IKEv2对等体配置模式。用户可以在该模式下对IKEv2对等体进行参数配置。

在全局配置模式下使用**no ikev2 peer *peer-name***命令删除指定的IKEv2对等体。

绑定接口到对等体

用户可以绑定某个接口到IKEv2对等体。将接口绑定到IKEv2对等体，在IKEv2对等体配置模式下使用以下命令：

```
interface interface-name
```

- *interface-name* – 指定被绑定接口的名称。

使用**no interface**命令取消接口绑定。

指定对端的IP地址

用户可以为所创建的IKEv2指定对端的IP地址。指定对端的IP地址，在IKEv2对等体配置模式下使用以下命令：

```
match-peer ip-address
```

- *ip-address* - 指定对端的IP地址。

使用**no match-peer**命令取消对端IP地址。

配置认证方式

系统支持预共享密钥认证方式，且该认证方式为默认认证方式。为IKEv2对等体指定预共享密钥认证方式，在IKEv2对等体配置模式下使用以下命令：

```
auth psk
```

指定P1提议

为IKEv2对等体指定P1提议，在IKEv2对等体配置模式下使用以下命令：

```
ikev2-proposal p1-name
```

- *p1-name* – 指定P1提议的名称。

使用**no** `ikev2-proposal p1-name`取消对P1提议的指定。

配置本端ID

配置本端的ID，请在IKEv2对等体配置模式下使用以下命令：

```
local-id {fqdn string | key-id string | ip ip-address}
```

- *fqdn string* – 指定使用FQDN类型的ID。*string*为ID的具体内容。
- *key-id string* – 指定使用Key ID类型的ID。*string*为ID的具体内容。
- *ip ip-address* – 指定使用IP地址类型的ID。*ip-address*为ID的具体内容。

使用**no** `local-id`命令取消对本端ID的配置。

指定连接类型

创建的IKEv2对等体可以是发起端、响应端或者既是发起端也是响应端。指定IKEv2对等体的连接类型，在IKEv2对等体配置模式下使用以下命令：

```
connection-type {bidirectional | initiator-only | responder-only}
```

- **bidirectional** – 指定该ISAKMP网关既是发起端也是响应端。该选项为默认选项。
- **initiator-only** – 指定该ISAKMP网关仅是发起端。
- **responder-only** – 指定该ISAKMP网关仅是响应端。

使用**no** `connection-type`命令恢复默认连接方式。

创建IKEv2 Profile

IKEv2 profile用来保存非协商的IKEv2 SA的参数，例如对端的身份信息、预共享密钥、被保护数据流量的信息。IKEv2 profile在发起端和响应端都需要配置。创建IKEv2 Profile，在IKEv2对等体配置模式下使用以下命令：

```
ikev2-profile profile-name
```

- *profile-name* – 指定该IKEv2 profile的名称。

执行该命令后，CLI进入到IKEv2 profile配置模式。用户可以在该模式下对非协商的IKEv2 SA的参数进行配置。

在全局配置模式下使用**no ikev2-profile** *profile-name*命令删除指定的IKEv2 profile。

配置对端ID

配置对端的ID，请在IKEv2 profile配置模式下使用以下命令：

```
remote id {fqdn string | key-id string | ip ip-address}
```

- *fqdn string* – 指定使用FQDN类型的ID。*string*为ID的具体内容。
- **key-id** *string* - 指定使用Key ID类型的ID。*string*为ID的具体内容。
- **ip** *ip-address* - 指定使用IP地址类型的ID。*ip-address*为ID的具体内容。

使用**no remote id**命令取消对对端ID的配置。

配置预共享密钥

两端的预共享密钥的值相同时，IKEv2隧道才能建立。配置预共享密钥，在IKEv2 profile配置模式下使用以下命令：

```
remote key key-value
```

- *key-value* – 指定预共享密钥的值。

使用**no remote key**命令删除所指定的预共享密钥。

配置被保护的数据流量信息

IKEv2 VPN能够对一个或者多个数据流进行安全保护，也就是对需要进入IPSec隧道的流量进行保护。在某些情况下，通过IPSec隧道加密的数据流量，其源地址和目的地址可能为多个不同网段，因此，用户可以通过以下命令，在IKEv2 Profile下配置一个或者多个被保护的数据流量的信息。目前，同一个IKEv2 Profile下最多可以允许配置16个被保护的数据流。

创建被保护的数据流，在IKEv2 profile配置模式下使用以下命令：

traffic-selector *traffic-selector-name*

- *traffic-selector-name* – 指定被保护的数据流名称。

执行该命令后，CLI进入到被保护的数据流配置模式。用户可以在该模式下对被保护的数据流的参数（本端地址、对端地址）进行配置。

使用**no traffic-selector** *traffic-selector-name*命令删除所配置的被保护的数据流信息。

配置本端地址

配置被保护的数据流的本端地址，在被保护的数据流配置模式下，使用以下命令：

local *A.B.C.D/Mask*

- *A.B.C.D/Mask* – 被保护的数据流的本端地址和掩码。

使用**no local** *A.B.C.D/Mask*命令取消对被保护的数据流的本端地址的配置。

配置对端地址

配置被保护的数据流的对端地址，在被保护的数据流配置模式下，使用以下命令：

remote *A.B.C.D/Mask*

- *A.B.C.D/Mask* – 被保护的数据流的对端地址和掩码。

使用**no remote** *A.B.C.D/Mask*命令取消对被保护的数据流的对端地址的配置。

配置自动生成路由功能

对于IKEv2 VPN，配置自动生成路由功能后，每创建一个IPSec SA，设备会将目的地址为被保护的数据流的目的网段、下一跳为隧道接口的路由条目添加到自己的路由表。删除一个IPSec SA后，相应的路由条目也会被删除。

默认情况下，设备的自动生成路由功能是关闭的。开启此功能，在IKEv2对等体配置模式下，使用以下命令：

```
generate-route
```

使用**no generate-route**命令关闭自动生成路由功能。

配置P2提议

P2提议是IPSec安全提议，用于保存IPSec需要使用的安全协议、加密/认证算法等，为协商IPSec SA提供各种安全参数。对P2提议的配置包括指定协议类型、加密算法、验证算法、压缩算法和生命周期。

创建P2提议，即IPSec安全提议，在全局配置模式下使用以下命令：

```
ikev2 ipsec-proposal p2-name
```

- *p2-name* – 指定所创建的P2提议的名称。执行该命令后，进入到P2提议配置模式。对P2提议各项参数的配置都要在该模式下进行。

使用**no ikev2 ipsec-proposal *p2-name***命令删除指定的IPSec安全提议。

指定协议类型

P2提议可使用的协议类型有ESP。为P2提议指定协议类型，在P2提议配置模式下使用以下命令：

```
protocol esp
```

- **esp** – 指定使用ESP协议。该协议为系统默认协议。

指定验证算法

用户可以为P2提议指定至少一种最多四种验证算法。为P2提议指定验证算法，在P2提议配置模式下使用以下命令：

```
hash {md5 | sha | sha256 | sha384 | sha512 }
```

- **md5** – 指定使用MD5验证算法。摘要为128比特。
- **sha** – 指定使用SHA-1验证算法。摘要为160比特。该算法为默认算法。
- **sha256** – 指定使用SHA-256验证算法。摘要为256比特。
- **sha384** – 指定使用SHA-384验证算法。摘要为384比特。
- **sha512** – 指定使用SHA-512验证算法。摘要为512比特。

使用**no hash**命令恢复默认验证算法。

指定加密算法

用户可以为P2提议指定至少一种最多四种加密算法。为P2提议指定加密算法，在P2提议配置模式下使用以下命令：

```
encryption {3des| des | aes-192 | aes-256 }
```

- **3des** – 指定使用3DES加密方法。密钥长度为192比特。该方法为默认方法。
- **des** – 指定使用DES加密方法。密钥长度为64比特。
- **aes-192** – 指定使用192bit AES加密方法。密钥长度为192比特。
- **aes-256** – 指定使用256bit AES加密方法。密钥长度为256比特。

使用**no encryption**命令恢复默认加密算法。

配置PFS功能

PFS（Perfect Forward Security）功能决定新密钥的生成方式，而不是新密钥的生成时间。PFS保证无论在哪个阶段，一个密钥只能使用一次，而且，生成密钥的“材料”也只能使用一次。某个“材料”在生成了一个密钥后就被弃，绝不用来再生成任何其它密钥。这样可以确保一旦单个密钥泄密，最多只可能影响用该密钥加密的数据，而不会危及整个通信。PFS功能是由DH算法做保障的。

配置P2提议的PFS功能，在P2提议配置模式下使用以下命令：

```
group {nopfs | 1 | 2 | 5 | 14 | 15 | 16 | 19 | 20 | 21 | 24}
```

- **nopfs** – 不使用PFS功能。该选项为系统的默认选项。
- **1** – 选择DH组1。密钥的长度为768比特（MODP Group）。
- **2** – 选择DH组2。密钥的长度为1024比特（MODP Group）。
- **5** – 选择DH组5。密钥的长度为1536比特（MODP Group）。
- **14** – 选择DH组14。密钥的长度为2048比特（MODP Group）。
- **15** – 选择DH组15。密钥的长度为3072比特（MODP Group）。
- **16** – 选择DH组16。密钥的长度为4096比特（MODP Group）。

- 19 – 选择DH组19。密钥的长度为256比特（ECP Group）。
- 20 – 选择DH组20。密钥的长度为384比特（ECP Group）。
- 21 – 选择DH组21。密钥的长度为521比特（ECP Group）。
- 24 – 选择DH组24。密钥的长度为2048比特（MODP Group with 256-bit Prime Order Subgroup）。

使用**no group**命令恢复默认配置。

指定生命周期

Hillstone设备按时间衡量生命周期。当IPSec SA的时间达到特定值时，SA就会过期，需要重新进行协商。指定P2提议的生命周期，在P配置模式，使用以下命令：

lifetime seconds

- *seconds* – 指定时间类型生命周期的时间长度，单位为秒。默认值是28800秒。范围是180到86400秒。

使用**no lifetime**命令恢复默认配置。

配置隧道

通过IKEv2配置IPSec隧道，用户需要配置的选项有指定操作模式、IKEv2对等体、IKEv2安全提议、以及自动连接。

创建IKEv2隧道

创建IKEv2隧道，在全局配置模式下，使用以下命令：

tunnel ipsec tunnel-name ikev2

- **tunnel-name** - 指定所创建的IKEv2隧道的名称。

执行该命令后，CLI进入到IKEv2隧道配置模式。对IKEv2隧道的所有参数配置都需要在该模式下进行。

在全局配置模式下使用**no tunnel ipsec tunnel-name ikev2**删除指定的IKEv2隧道。

指定 IKEv2隧道的操作模式

系统支持IKEv2隧道的操作模式为隧道模式。该模式为系统默认模式。

指定IKEv2对等体

为IKEv2隧道指定IKEv2对等体，在IKEv2隧道配置模式下使用以下命令：

```
ikev2-peer peer-name
```

- *peer-name* – 指定IKEv2对等体的名称。

使用**no ikev2-peer**取消对IKEv2对等体的指定。

指定P2提议

为IKEv2隧道指定P2提议，在IKEv2隧道配置模式下使用以下命令：

```
ipsec-proposal p2-name1 [p2-name2] [p2-name3]
```

- *p2-name* – 指定P2提议的名称。用户最多可以为IKEv2隧道指定3个P2提议供对端选择使用。

使用**no ipsec-proposal**取消对P2提议的指定。

配置自动连接功能

设备支持自动方式触发建立SA。自动方式是指设备每60秒检查一次SA的状态，如果SA未建立则自动发起协商请求。自动连接功能默认不开启。使用自动方式，请在IKE隧道配置模式下使用以下命令：

```
auto-connect
```



注意：自动连接功能仅在本端可以作为发起端时有效。

GRE协议

GRE协议介绍

GRE（Generic Routing Encapsulation）是通用封装路由，是定义了在任何一种网络层协议上封装任意一个其它网络层协议的协议。系统支持GRE over IPSec功能，实现路由协议信息的安全传输。

GRE配置

设备的GRE配置包括：

- 配置GRE隧道
- 绑定GRE隧道到隧道接口

配置GRE隧道

GRE隧道配置需要在GRE隧道配置模式下进行。进入GRE隧道配置模式，在全局配置模式下，使用以下命令：

tunnel gre gre-tunnel-name

- *gre-tunnel-name* – 指定将要创建的GRE隧道的名称。执行该命令后，系统创建指定名称的GRE隧道，并且进入GRE隧道配置模式；如果指定的名称已存在，则直接进入GRE隧道配置模式。

使用以上命令no的形式删除指定的GRE隧道：

no tunnel gre gre-tunnel-name

进入GRE隧道配置模式后，用户需要为GRE隧道配置以下参数：

- 指定源接口/地址
- 指定目的地址
- 指定出接口
- 指定IPSec VPN隧道（可选）
- 指定验证密钥（可选）

指定源地址

为GRE隧道指定源地址，在GRE隧道配置模式下，使用以下命令：

source {interface interface-name [ipv6] | {ipv4-address | ipv6-address}}

- **interface interface-name [ipv6]** – 指定接口的IP地址为GRE隧道的源地址，也可指定IPv6地址为GRE隧道的源地址。通过*interface-name*参数指定接口名称。
- *ipv4-address | ipv6-address* – 为GRE隧道指定源地址（IPv4或IPv6地址）。

在GRE隧道配置模式下使用该命令no的形式取消源地址的配置：

no source

指定目的地址

为GRE隧道指定目的地址，在GRE隧道配置模式下，使用以下命令：

```
destination {ipv4-address | ipv6-address}
```

- *ipv4-address* | *ipv6-address* – 为GRE隧道指定目的地址（IPv4或IPv6地址）。

在GRE隧道配置模式下，使用下命令no的形式取消目的地址的配置：

```
no destination
```

指定出接口

为GRE隧道指定出接口，在GRE隧道配置模式下，使用以下命令：

```
interface interface-name
```

- *interface-name* – 指定出接口的名称。

在GRE隧道配置模式下使用该命令no的形式取消出接口配置：

```
no interface
```

指定IPSec VPN隧道

使用GRE over IPSec功能时，用户需要通过该命令指定IPSec VPN隧道对数据进行IPSec封装。指定IPSec VPN隧道，在GRE隧道配置模式下，使用以下命令：

```
next-tunnel ipsec tunnel-name
```

- *tunnel-name* – 指定IPSec VPN隧道的名称。

在GRE隧道配置模式下使用该命令no的形式取消IPSec VPN隧道的指定：

```
no next-tunnel
```

指定验证密钥

通过指定验证密钥，对进入GRE隧道的数据包进行封装与验证。当数据包携带的密钥与接收端配置的验证密钥相同时，数据包将会被解密。如果不相同，数据包将会被丢弃。指定验证密钥，在GRE隧道配置模式下，使用以下命令：

```
key key-value
```

- *key-value* – 指定验证密钥。取值范围为0到4294967295。

在GRE隧道配置模式下使用该命令no的形式取消验证密钥的指定：

```
no key
```

绑定GRE隧道到隧道接口

配置完成的GRE隧道需要绑定到隧道接口上才能够生效。绑定GRE隧道到隧道接口，在隧道接口配置模式下，使用以下命令：

```
tunnel gre gre-tunnel-name [gw ip-address]
```

- *gre-tunnel-name* – 指定将要绑定的GRE隧道的名称。该隧道为系统中已创建的GRE隧道。
- *gw ip-address* – 当配置多个隧道到隧道接口时，需要配置该参数。该参数指定GRE隧道的下一跳IP地址，为对端隧道接口的IP地址。系统默认值为0.0.0.0。

在隧道接口配置模式下，使用该命令no的形式取消GRE隧道的绑定：

```
no tunnel gre gre-tunnel-name
```

关于隧道接口的静态路由配置，请参阅“[路由](#)”章节。

显示GRE隧道配置信息

用户可以在任何模式下使用以下命令查看GRE隧道配置信息：

```
show tunnel gre [gre-tunnel-name]
```

- *gre-tunnel-name* – 显示指定名称的GRE隧道配置信息。

VXLAN

介绍

VXLAN是采用MAC in UDP（User Datagram Protocol）封装方式，是NOV3（Network Virtualization over Layer3）中的一种大二层虚拟网络扩展的隧道封装技术。VXLAN引入了类似VLAN ID的用户标识，称为VXLAN网络标识VNI（VXLAN Network ID），由24比特组成，可划分多达16M的VXLAN段，从而满足了大量

的用户标识。通过VXLAN构建大二层网络，保证了在虚拟迁移时虚拟机的IP地址、MAC地址等参数保持不变。

VXLAN使用VTEP（VXLAN Tunnel Endpoint）设备对VXLAN 报文进行封装与解封装，包括ARP请求报文和正常的VXLAN数据报文。VETP将原始以太网帧通过VXLAN封装后发送至对端VTEP设备，对端VETP设备接收到VXLAN报文后解封装，然后根据原始MAC进行转发，VTEP可以是物理交换机、物理服务器或者其他支持VXLAN的硬件设备或软件来实现。

配置VXLAN静态隧道

配置VXLAN静态隧道并进入VXLAN隧道配置模式，在全局配置模式下，使用以下命令：

tunnel vxlan *name*

- *name* - 指定VXLAN静态隧道的名称。

在全局配置模式下，使用命令**no tunnel vxlan** *name*取消配置VXLAN静态隧道。

配置VXLAN静态隧道的目的VETP的IP地址，在VXLAN隧道配置模式下，使用以下命令：

destination *ipv4-address*

- *ipv4-address* - 指定VXLAN静态隧道的目的VETP的IP地址。

在VXLAN隧道配置模式下，使用命令**no destination** 取消配置VXLAN静态隧道的目的VETP的IP地址。

配置VXLAN静态隧道的ID，即全局网络标识，在VXLAN隧道配置模式下，使用以下命令：

vni *id*

- *id* - 指定VXLAN静态隧道的ID，取值范围是1-16777215。

在VXLAN隧道配置模式下，使用命令**no vni** 取消配置VXLAN静态隧道的目的VETP的IP地址。

配置VXLAN静态隧道出接口，在VXLAN隧道配置模式下，使用以下命令：

interface *interface-name*

- *interface-name* - 指定VXLAN静态隧道的出接口。

在VXLAN隧道配置模式下，使用命令**no interface**取消配置VXLAN静态隧道的出接口。

为VXLAN隧道接口绑定二层安全域，在隧道接口配置模式下，使用以下命令：

zone *l2-zone*

l2-zone - 为VXLAN隧道指定绑定的二层安全域名称。

在隧道接口配置模式下，使用命令 `no zone l2-zone` 取消绑定二层安全域。

显示VXLAN隧道配置信息

- 显示VXLAN隧道配置信息：

```
show tunnel vxlan name
```

IPv6 6to4隧道配置

当前网络中，IPv4网络仍是主流网络，IPv6网络往往作为网络孤岛存在。而隧道技术则实现了IPv6孤岛之间通过IPv4网络的通信。系统支持对IPv6数据包的处理，并通过隧道技术实现IPv4与IPv6的互通。当前版本支持6to4手工隧道和6to4自动隧道。

- 6to4手工隧道：提供点到点的连接，其通道的终止点是手工静态配置的。
- 6to4自动隧道：点到多点的自动隧道，主要用于将多个IPv6孤岛通过IPv4网络连接到IPv6网络。根据不同网络环境，设备既可做6to4路由器，也可做6to4中继路由器。

6to4隧道配置如下：

- 创建隧道
- 指定隧道的出接口
- 指定手工隧道的目的地址
- 绑定隧道到隧道接口

创建隧道

创建IPv6 6to4隧道，在全局配置模式下使用以下命令。执行以下命令后，系统创建指定名称的IPv6 6to4隧道，并进入隧道配置模式；如果指定的名称已存在，则直接进入隧道配置模式。

```
tunnel ip6in4 tunnel-name {manual | 6to4}
```

- *tunnel-name* – 指定IPv6 6to4隧道的名称。
- **manual | 6to4** – 指定隧道类型，可以是6to4手工隧道（**manual**）或者6to4自动隧道（**6to4**）。

在全局配置模式下，使用以上命令 `no` 的形式删除指定的IPv6 6to4隧道：

```
no tunnel ip6in4 tunnel-name {manual | 6to4}
```

指定6to4子隧道最大数

不同型号的设备支持的最多可创建的6to4手工隧道、6to4自动隧道数量不同，但设备的每个接口最多可配置一个6to4隧道。每个隧道下最多可配置1200个子隧道。指定6to4子隧道数，在隧道配置模式下，使用以下命令：

```
subtunnel-limit maximum
```

- *maximum* – 指定6to4子隧道数，取值范围为1至1200，默认值为200。

在隧道配置模式下，使用该命令no的形式恢复子隧道数的默认值。

```
no subtunnel-limit
```

指定隧道的出接口

指定隧道的出接口，在隧道配置模式下，使用以下命令：

```
interface interface-name
```

- *interface-name* – 指定隧道出接口的名称。可以是物理接口或者逻辑接口（隧道接口除外）。

在隧道配置模式下，使用以上命令no的形式取消隧道出接口的指定。

```
no interface
```

绑定IPv6 6to4隧道到隧道接口

绑定IPv6 6to4隧道到隧道接口，在隧道接口配置模式下（全局配置模式下使用**interface tunnelX**命令进入隧道接口配置模式），使用以下命令：

```
tunnel ip6in4 ipv6-tunnel-name
```

- *ipv6-tunnel-name* – 指定IPv6 6to4隧道的名称。

隧道接口配置模式下，使用以上命令no的形式取消IPv6 6to4隧道与隧道接口的绑定：

```
no tunnel ip6in4 ipv6-tunnel-name
```

显示IPv6 6to4隧道配置信息

显示IPv6 6to4隧道配置信息，在任何模式下使用以下命令：

```
show ip6in4 {manual-tunnel | 6to4-tunnel}
```


IPv6 4to6隧道配置

当前网络中，IPv4网络仍是主流网络，但IPv6网络的应用越来越广泛。随着IPv6网络的大规模部署，为了让IPv4孤岛之间进行通信，StoneOS支持IPv6 4to6隧道技术，即通过IPv6网络实现IPv4孤岛之间的通信。

当前版本仅支持手工方式配置。手工隧道提供点到点的连接，其通道的终止点是手工静态配置的。

手工隧道配置方式如下：

- 创建隧道
- 指定隧道的源地址/出接口
- 指定隧道的目的地址
- 绑定隧道到隧道接口

创建隧道

创建IPv6 4to6手工隧道，在全局配置模式下使用以下命令。执行以下命令后，系统创建指定名称的IPv6 4to6隧道，并进入隧道配置模式；如果指定的名称已存在，则直接进入隧道配置模式。

```
tunnel ip4in6 tunnel-name manual
```

- *tunnel-name* – 指定IPv6 4to6隧道的名称。

在全局配置模式下，使用以上命令no的形式删除指定的IPv6手工隧道：

```
no tunnel ip4in6 tunnel-name manual
```

指定隧道的源地址/出接口

指定IPv6 4to6手工隧道的出接口和源地址，在隧道配置模式下，使用以下命令：

```
interface interface-name source ipv6-address
```

- *interface-name* – 指定隧道的出接口。
- *ipv6-address* – 指定IPv6 4to6隧道的源地址。该地址是一个IPv6地址。

在隧道配置模式下，使用该命令no的形式删除隧道出接口和源地址：

```
no interface
```

指定隧道的目的地址

指定IPv6 4to6手工隧道的目的地址，在隧道配置模式下，使用以下命令：

destination *ipv6-address*

- *ipv6-address* – 指定IPv6 4to6隧道的目的地址。该地址是一个IPv6地址。

在隧道配置模式下，使用以上命令no的形式取消隧道目的地址的指定：

no destination

绑定IPv6 4to6隧道到隧道接口

绑定IPv6 4to6手工隧道到隧道接口，在隧道接口配置模式下（全局配置模式下使用**interface tunnelX**命令进入隧道接口配置模式），使用以下命令：

tunnel ip4in6 *tunnel-name*

- *tunnel-name* – 指定IPv6 4to6手工隧道的名称。

在隧道接口配置模式下，使用以上命令no的形式取消IPv6 4to6隧道与隧道接口的绑定：

no tunnel ip4in6 *tunnel-name*

显示IPv6 4to6隧道配置信息

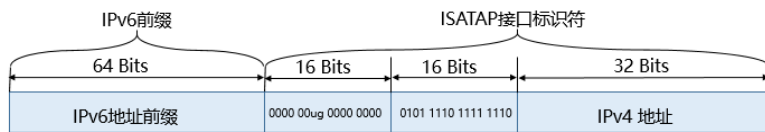
显示IPv6 4to6隧道配置信息，在任何模式下使用以下命令：

show ip4in6 manual-tunnel

ISATAP隧道配置

ISATAP（Intra-Site Automatic Tunnel Addressing Protocol）是一种IPv6点到多点的自动隧道技术，主要用于IPv4网络中的双栈主机通过ISATAP隧道访问IPv6网络，通过在IPv6报文的目的地址中嵌入的IPv4地址，可以自动获取隧道的终点。

使用ISATAP隧道时，IPv6报文的目的地址和隧道接口的IPv6地址都要采用特殊的ISATAP地址。ISATAP地址包含一个IPv6前缀和ISATAP接口标识符。ISATAP地址格式如下：



- 如果IPv4地址是全局唯一的，则u位为1，否则u位为0。
- g位是IEEE群体/个体标志，固定为0。

例如，IPv6地址前缀为：2001:DB8:1234:5678::/64；需要嵌入的IPv4地址为：10.173.129.8，该IPv4地址在ISATAP格式中表示为16进制：0AAD:8108；最终的ISATAP地址即为：2001:DB8:1234:5678:0000:5EFE:0AAD:8108。

ISATAP隧道配置如下：

- 创建ISATAP隧道
- 指定ISATAP子隧道最大数
- 指定ISATAP隧道的出接口
- 绑定ISATAP隧道到隧道接口

创建ISATAP隧道

创建ISATAP隧道，在全局配置模式下使用以下命令。执行以下命令后，系统创建指定名称的ISATAP隧道，并进入ISATAP隧道配置模式；如果指定的名称已存在，则直接进入ISATAP隧道配置模式。

tunnel ip6in4 *tunnel-name* **isatap**

- *tunnel-name* – 指定ISATAP隧道的名称。
- **isatap** – 指定隧道类型为ISATAP隧道。

在全局配置模式下，使用以上命令**no**的形式删除指定的ISATAP隧道：

no tunnel ip6in4 *tunnel-name* **isatap**

指定ISATAP子隧道最大数

系统内最多可创建10个ISATAP隧道，且每个接口最多可配置一个ISATAP隧道。每个隧道下最多可配置1200个子隧道。指定ISATAP子隧道数，在ISATAP隧道配置模式下，使用以下命令：

subtunnel-limit *maximum*

- *maximum* – 指定ISATAP子隧道数，取值范围为1至1200，默认值为200。

在ISATAP隧道配置模式下，使用该命令**no**的形式恢复子隧道数的默认值。

no subunnel-limit

指定ISATAP隧道的出接口

指定ISATAP隧道的出接口，在ISATAP隧道配置模式下，使用以下命令：

interface *interface-name*

- *interface-name* – 指定ISATAP隧道出接口的名称。可以是物理接口或者逻辑接口（隧道接口除外）。

在ISATAP隧道配置模式下，使用以上命令**no**的形式取消隧道出接口的指定。

no interface

绑定ISATAP隧道到隧道接口

绑定ISATAP隧道到隧道接口，在隧道接口配置模式下（全局配置模式下使用**interface tunnelX**命令进入隧道接口配置模式），使用以下命令：

tunnel ip6in4 *ipv6-tunnel-name*

- *ipv6-tunnel-name* – 指定ISATAP隧道的名称。

隧道接口配置模式下，使用以上命令**no**的形式取消ISATAP隧道与隧道接口的绑定：

no tunnel ip6in4 *ipv6-tunnel-name*

显示ISATAP隧道配置信息

显示ISATAP隧道配置信息，在任何模式下使用以下命令：

show ip6in4 isatap-tunnel

第13章 监控

监控相关配置包括如下：

- [监控](#)
- [日志](#)

监控介绍

系统的监控统计功能包括以下功能：

- 设备监控：基于设备的监控统计功能，统计会话、CPU/内存状态以及硬件状态统计信息。
- 链路监控：统计链路中特定接口的采样流量信息。
- 全局负载均衡监控：基于设备全局负载均衡功能的统计信息。
- 服务器负载均衡监控：基于设备服务器负载均衡功能的统计信息。
- 链路负载均衡监控：基于设备链路负载均衡规则的流量统计信息。
- SSL透视镜监控：基于SSL透视镜的统计功能，统计接收/发送字节总数、新建连接数、带宽大小、SSL会话数、缓存中证书数等



注意：Web界面可以更加直观的显示所有监控的数据信息，因此建议用户通过WebUI配置监控功能和查看监控结果，不建议使用CLI。

查看接口的统计信息

在任何模式下，使用以下命令查看指定接口的流量统计信息：

```
show statistics interface-counter interface interface-name {second | minute | hour}
```

- *interface-name* – 指定接口名称。
- **second** – 指定显示接口前60秒钟每5秒的流量统计信息。

- **minute** – 指定显示接口前60分钟每分钟的流量统计信息。
- **hour** – 指定显示接口前24小时每小时的流量统计信息。

链路状态监控

系统支持通过统计链路中特定接口的采样流量信息，包括延迟、丢包率、抖动，从而实现链路整体状态的监控和展示。也支持对特定目的IP进行链路探测，统计指定链路的流量信息，包括延迟和抖动。

开启/关闭接口的链路用户体验功能

开启接口的链路用户体验功能，需要首先配置绑定接口并进入链路监控配置模式，在全局配置模式下，使用以下命令：

link-perf-monitor interface *interface-name*

- *interface-name* – 指定接口名称。

使用**no link-perf-monitor interface** *interface-name*命令删除绑定接口。

开启接口的链路用户体验功能，在链路监控配置模式下，使用以下命令：

monitor on

使用**no monitor on**命令关闭接口的链路用户体验功能。

开启/关闭接口的应用维度

开启接口的应用维度后，系统可以统计链路中特定接口下具体应用的信息，包括延迟、丢包率、抖动。接口的应用维度默认情况下是关闭的。开启应用维度，在链路监控配置模式下，使用以下命令：

application on

使用**no application on**命令关闭指定接口的应用维度。

指定描述信息

为开启链路用户体验功能的接口指定描述信息，在链路监控配置模式下，使用以下命令：

description string

- *string* - 接口的描述信息。

使用**no description**命令删除接口的描述信息。

查看链路状态监控配置信息

查看链路状态监控的所有配置信息，在任何模式下使用以下命令：

```
show link-perf-monitor information
```

查看链路用户体验统计信息

查看链路用户体验统计信息，在任何模式下使用以下命令：

```
show link-perf-monitor statistics [interface interface-name [application application-name]] history {minute | hour | day | month}]] [ipv4 | ipv6]
```

- **interface** *interface-name* - 按照指定接口显示链路用户体验统计信息。
- **application** *application-name* - 按照指定应用显示链路用户体验统计信息。如果不指定该参数，则显示指定接口的所有统计信息。
- **history** {*minute* | *hour* | *day* | *month*} - 显示历史链路用户体验统计信息。
- **ipv4** | **ipv6** - 按照指定IP地址类型显示链路用户体验统计信息。如果不指定该参数，将默认显示包含IPv4和IPv6的全部链路用户体验统计信息。

配置链路探测目的IP

系统支持对特定目的IP进行链路探测，统计指定链路的流量信息。

配置探测目的IP，需要首先进入链路状态探测模式，在全局模式下，使用以下命令：

```
link-detect-object
```

配置IPv4类型的链路探测目的，在链路状态探测模式下，使用以下命令：

```
ip A.B.C.D protocol {tcp [port port-number] | icmp} [interval value] [description description]
```

- *A.B.C.D* - 指定探测目的的IP地址。
- **tcp** [port *port-number*] - 指定协议类型为TCP，并指定协议端口号。

- **icmp** - 指定协议类型为ICMP。
- **interval value** - 指定探测报文的发送间隔，取值范围是1到5秒，默认值是1。
- **description description** - 指定对该链路的描述信息。

使用**no ip A.B.C.D**删除配置的探测目的IP。

配置IPv6类型的链路探测目的，在链路状态探测模式下，使用以下命令：

ipv6 X:X:X:X::X protocol {tcp [port port-number] | icmpv6} [interval value] [description description]

- **X:X:X:X::X** - 指定探测目的的IPv6地址。
- **tcp [port port-number]** - 指定协议类型为TCP，并指定协议端口号。
- **icmpv6** - 指定协议类型为ICMPv6。
- **interval value** - 指定探测报文的发送间隔，取值范围是1到5秒，默认为1秒。
- **description description** - 指定对该链路的描述信息。

使用**no ipv6 X:X:X:X::X**删除配置的探测目的IP。

查看链路探测监控配置信息

查看链路状态监控配置信息，在任何模式下使用以下命令：

show link-detect-object {all | A.B.C.D | X:X:X:X::X}

- **all** - 显示所有目的地址的链路探测监控配置信息。
- **A.B.C.D | X:X:X:X::X** - 显示指定IPv4目的地址或IPv6目的地址的链路探测监控配置信息。

配置采样率

改变链路负载均衡监控的采样率，在全局配置模式下，使用以下命令：

link-perf-monitor sample-rate {auto | rate_value}

- **auto** - 指定参数为auto，系统将对采样率进行动态调整。
- **rate_value** - 输入采样率的数值，取值范围为1至128。如：输入“32”，表示1/32的采样率。

全局负载均衡监控

在任何模式下，使用以下命令查看全局负载均衡统计。使用前，请先确保在GSLB全局模式下，使用 **statistics enable** 开启GSLB统计。

- 查看DNS服务器统计信息：**show statistics gslb smart-dns {server server-name | view view-name}**
- 查看SmartDNS统计信息：**show statistics gslb smart-dns {host host-name | pool pool-name [group group-name] | server server-name}**

服务器负载均衡监控

在任何模式下，使用以下命令查看服务器负载均衡监控：

- 查看真实服务和服务器负载均衡历史信息记录的开关信息：**show history-stats**
- 查看真实服务的统计信息：**show statistics slb real-server server-name**
- 查看服务池的统计信息：**show statistics slb server-pool pool-name**
- 查看虚拟服务器的统计信息：**show statistics slb virtual-server virtual-server-name**
- 查看HTTP缓存的统计信息：**show statistics slb cache virtual-server-name**
- 查看HTTP压缩的统计信息：**show statistics slb compression**

开启/关闭服务器负载均衡统计

默认情况下，服务器负载均衡统计功能为开启状态。开启/关闭服务器负载均衡统计，在全局配置模式下，使用以下命令：

- 开启：**statistics slb enable**
- 关闭：**statistics slb disable**

链路负载均衡

在任何模式下，使用以下命令查看链路负载均衡监控：

- 查看指定链路负载均衡规则的流量统计信息：**show statistics llb rule rule-name**

SSL透视镜监控

开启/关闭SSL透视镜统计

默认情况下，SSL透视镜统计功能为开启状态。开启/关闭SSL透视镜统计，在全局配置模式下，使用以下命令：

- 开启： `statistics sll-inspection enable`
- 关闭： `statistics sll-inspection disable`

日志

设备支持日志管理功能。记录并输出设备的各种日志信息，分别是设备系统、威胁、NAT、PBR、负载均衡以及健康检查。

- 设备系统日志 - 包含事件日志信息、网络日志信息以及配置日志信息。
 - 事件日志 - 包括错误、警告、通告、信息、调试、紧急、警报和严重8个级别的系统事件信息。
 - 网络日志 - 与网络服务操作相关的日志信息，例如PPPoE以及DDNS等。
 - 配置日志 - 与CLI配置相关的日志信息，例如接口配置等。
 - 操作日志 - 包括所有命令以及对应WebUI操作相关的日志信息。
- NAT日志 - 与NAT行为相关的日志信息，例如NAT类型、源/目的IP地址、源/目的端口等。
- 会话日志 - 与会话相关的日志信息，例如会话的协议、源/目的IP地址、源/目的端口等。
- PBR日志 - 策略路由日志信息，与策略路由相关日志信息。
- 威胁日志 - 与系统威胁相关的日志信息。
- 七层/四层/全局负载均衡日志 - SLB流量日志信息，与负载均衡相关的流量日志信息。包括七层负载均衡日志、四层负载均衡日志、全局负载均衡日志。
- Web防护日志 - 与Web防护相关的日志信息。
- SSL透视镜日志 - 与SSL透视镜相关的日志信息。
- 健康检查日志 - 健康检查日志信息，与负载均衡健康检查相关的日志信息。

系统的多种日志信息能够有效的记录设备的运行情况，从而为用户分析网络情况和防护网络攻击提供依据。

日志的严重等级

系统的事件日志信息根据日志信息的严重程度区分的。系统日志的严重等级可分为8级，关于各级的具体信息，请参阅下表：

级别	级别号	描述	日志定义
紧急（Emergencies）	0	系统不可用信息。	LOG_EMERG
警报（Alerts）	1	需要立即处理的信息，如设备受到攻击等。	LOG_ALERT
严重（Critical）	2	危急信息，如硬件出错。	LOG_CRIT
错误（Errors）	3	错误信息。	LOG_ERR
警告（Warnings）	4	报警信息。	LOG_WARNING
通告（Notifications）	5	非错误信息，但需要特殊处理。	LOG_NOTICE
信息（Informational）	6	通知信息。	LOG_INFO
调试（Debugging）	7	调试信息，包括正常的使用信息。	LOG_DEBUG

日志信息输出目的地

日志信息可以输出到不同的目的地，设备支持以下7种日志信息输出目的地，用户可以根据自己的需要指定：

- Console - 日志信息的默认输出目的地。用户可以通过命令关闭此输出。
- 终端（Remote） - 包括Telnet和SSH两种终端。
- 内存缓存（Buffer） - 内存缓存。
- 文件（File） - 默认情况下，系统会生成一个文件记录日志信息，用户可以指定将信息输出到USB口的文件中。
- 系统日志服务器（Syslog Server） - 系统可以将日志信息发往 UNIX 或 Windows Syslog Server。
- Email地址 - 将日志信息发送到某个邮件地址。

- 手机 - 将日志信息以短信的形式发送到某个手机上。
- 本地数据库 (Localdb) - 将日志信息发送到本地数据库，即设备自带的1T硬盘中。

日志信息格式

为方便用户查阅和分析系统日志信息，系统按照固定的格式输出日志信息。该格式为：**时间，级别@模块：日志描述**。请参阅以下示例：

2013-02-05 01:51:21, WARNING@LOGIN: Admin user "admin" logged in through console from localhost.

配置系统日志功能

通过CLI，用户可以对系统日志功能做以下配置：

- [开启和关闭日志功能](#)
- [输出日志信息](#)
- [配置SMTP实例](#)
- [显示日志信息](#)
- [导出日志信息](#)
- [清除日志信息](#)

开启和关闭日志功能

开启或者关闭系统的各种日志功能，请在全局配置模式下输入以下命令：

- 开启：**logging {event | configuration | operation | network | health-check | threat | traffic [slb | gslb | ssl-inspection | nat | pbr | session] | web-protect | debug} on**
- 关闭：**no logging {event | configuration | operation | network | slb | health-check | threat | traffic [nat | pbr | session] | web-protect | debug} on**

流量日志信息包括PBR日志、会话日志、NAT日志、四层/七层负载均衡日志、全局负载均衡日志，和透视镜日志。**logging traffic on** 表示开启所有的流量日志（打开流量日志功能会影响系统性能），**logging traffic slb on** 表示开启负载均衡日志。

使用该命令前，请确保

- 在SSL透视镜模板配置模式下，使用**log enable**开启SSL透视镜日志开关。
- 在DNS服务器配置模式下，使用**log enable**开启GSLB日志开关。

输出日志信息

设备支持日志输出功能，包括：

- [输出流量日志](#)：包含NAT日志、PBR日志、会话日志和负载均衡日志的输出。
- [输出及过滤事件日志信息](#)
- [输出威胁日志信息](#)
- [输出Web防护日志信息](#)
- [输出配置、调试和网络日志信息](#)
- [输出健康检查日志信息](#)
- [配置日志信息的输出格式](#)
- [配置Syslog Server](#)
- [指定场所](#)
- [配置Email地址](#)

输出流量日志信息

流量日志信息包括PBR日志、会话日志、NAT日志和负载均衡日志，可以输出到缓存、Console口、Syslog服务器和本地数据库（仅负载均衡日志）。用户可以根据需要指定不同类别日志信息的输出目的地。

将流量日志信息输出到缓存、Console口、Syslog服务器和本地数据库，在全局配置模式下使用以下命令：

```
logging traffic [slb | gslb | ssl-inspection | nat | pbr | session] to {console | localdb | syslog [custom-format [distributed [round-robin | src-ip-hash]]] | buffer [size buffer-size]}
```

- **logging traffic** - 输出流量日志，包括PBR日志、NAT日志、会话日志、四层/七层负载均衡日志、全局负载均衡日志，和透视镜日志。
- **nat** - 输出NAT日志。
- **pbr** - 输出PBR日志。开启策略路由日志功能后，当策略路由规则被流量匹配到后，系统会产生策略路由日志。
- **session** - 输出会话日志。
- **slb** - 输出四层/七层负载均衡日志。
- **gslb** - 输出全局负载均衡日志。
- **ssl-inspection** - 输出透视镜日志。
- **console** - 指定将日志信息输出到console口。
- **syslog [custom-format [distributed [round-robin | src-ip-hash]]]** - 指定将日志信息输出到Syslog Server。关于如何配置Syslog Server，请参阅“[配置Syslog Server](#)”。
 - **custom-format** - 发送明文日志信息。默认情况下，系统发送明文日志信息。
 - **distributed** - 分布发送日志信息到多台日志服务器。
 - **src-ip-hash | round-robin** - 指定服务器选择算法。**src-ip-hash**为源地址哈希算法。**round-robin**为轮询调度算法，该算法为系统默认算法。
- **buffer [size buffer-size]** - 指定将日志信息输出到缓存，并指定缓存的大小，范围是4096到2097152字节。默认值为2097152。
- **localdb** - 指定将日志信息输出到本地数据库。仅支持将负载均衡日志输出到本地数据库。数据库位于设备自带的1T硬盘上。

在全局配置模式下，使用**no logging traffic [slb | gslb | ssl-inspection | nat | pbr | session] to {console | localdb | syslog [custom-format [distributed [round-robin | src-ip-hash]]] | buffer [size buffer-size]}**命令关闭相关的输出功能。



注意: 当配置了目的路由优先查找后，即使流量匹配到了策略路由规则，系统也不会产生策略路由日志。设备不支持输出二进制格式的策略路由日志。

配置PBR日志主机名/用户名的显示状态

默认情况下，策略路由日志中不显示主机名和用户名信息。在策略路由日志中显示主机名或用户名信息，请在全局配置模式下，使用以下命令：

```
logging pbr content {hostname | username}
```

在全局配置模式下，用 `no logging pbr content {hostname | username}` 命令取消在策略路由日志中显示主机名或用户名信息。

自定义不保存的日志类型

当设备每秒产生的负载均衡日志数量过多，导致数据库无法保存时，用户可在虚拟服务器配置模式下，使用以下命令自定义不需要保存的负载均衡日志。只有HTTP和HTTPS类型的虚拟服务器支持配置该功能。

```
log exclude {method {get | put | head | post | delete} | file-type {css | js | image | media}}
```

- `{method {get | put | head | post | delete}}` - 不保存method为get/put/head/post/delete类型的HTTP/HTTPS日志。
- `file-type {css | js | image | media}` - 不保存文件类型为css/js/image/media的HTTP/HTTPS日志。其中，image包括PNG/BMP/JPEG/GIF/JPE/JPG类型的图片；media包括FLV/SWF/MP4/MP3/AVI类型。

在虚拟服务器配置模式下，使用命令 `no log exclude {method {get | put | head | post | delete} | file-type {css | js | image | media}}` 删除自定义配置，系统将保存所有产生的日志。

输出及过滤事件日志信息

用户可以根据需要指定事件日志信息的输出目的地，并且按照日志信息的严重级别对输出信息进行过滤。

将事件日志信息输出到console、远程终端、系统日志服务器、手机或者使用事件日志email提醒功能，并且对日志信息进行过滤，在全局配置模式下使用以下命令：

```
logging event to {console | remote | syslog | sms | email} [severity severity-level]
```

- **console** – 指定将事件日志信息输出到console口。
- **remote** – 指定将事件日志信息输出到远程终端。
- **syslog** – 指定将事件日志信息输出到Syslog Server。关于如何配置Syslog Server，请参阅“[配置Syslog Server](#)”。
- **sms** – 指定将严重等级在严重（Critical）以上的事件日志信息以短信的形式输出到某个手机。关于如何设置手机号码，请参阅[配置接收事件日志信息的手机号码](#)一节。
- **email** – 使用事件日志email提醒功能。关于如何配置email地址，请参阅“[配置Email地址](#)”。
- **severity severity-level** – 指定输出的事件日志信息的级别从而对事件日志信息进行过滤。日志信息的级别和对应的级别号请参阅表5。输出信息的级别将会是指定级别或者高于指定级别，即数字等于或者小于指定级别。例如指定级别是通告，系统将会输出通告、警告和错误级别的日志信息。

在全局配置模式下，用以上命令no的形式可以关闭相关的输出功能。命令如下：

```
no logging event to { console | remote | syslog | sms | email }
```

将事件日志信息输出到设备硬盘卡（该功能仅部分型号的设备支持），在全局配置模式下使用以下命令：

```
logging event to localdb
```

在全局配置模式下，使用**no logging event to localdb**命令关闭相关的输出功能。

将事件日志信息输出到内存缓存，并且对日志信息进行过滤，在全局配置模式下使用以下命令：

```
logging event to buffer [severity severity-level] [size buffer-size]
```

- **severity severity-level** – 指定输出的事件日志信息的级别从而对事件日志信息进行过滤。日志信息的级别和对应的级别号请参阅表5。输出信息的级别将会是指定级别或者高于指定级别，即数字等于或者小于指定级别。例如指定级别是通告，系统将会输出通告、警告和错误级别的日志信息。
- **size buffer-size** – 指定内存缓存的大小。范围是4096到1048576字节。默认值为1048576。

在全局配置模式下，使用**no logging event to buffer**命令关闭相关的输出功能。

将事件日志信息输出到文件，并且对日志信息进行过滤，在全局配置模式下使用以下命令：

```
logging event to file [severity severity-level] [name [usb0 | usb1] file-name] [size file-size]
```


- **severity** *severity-level* – 指定输出的事件日志信息的级别从而对事件日志信息进行过滤。输出信息的级别将会是指定级别或者高于指定级别，即数字等于或者小于指定级别。例如指定级别是通告，系统将会输出通告、警告和错误级别的日志信息。
- **name** [*usb0* | *usb1*] *file-name* – 该参数用来指定保存日志信息的U盘和日志信息文件的名称。
- **size** *file-size* – 将事件日志信息输出到文件（U盘或者Flash）时，该参数用来指定日志信息文件的大小。范围是4096到1048576字节。默认是1048576字节。

在全局配置模式下，用以上命令**no logging event to file**命令关闭相关的输出功能。

配置接收事件日志信息的手机号码

用户可将严重等级在严重（Critical）以上的事件日志信息以短信的形式输出到某个手机。指定接收事件日志的手机号码，在全局配置模式下，使用以下命令：

logging sms *phone-number*

- *phone-number* – 指定接收事件日志的手机号码。

在全局配置模式下使用**no logging sms** *phone-number*命令取消手机号码的指定。

输出威胁日志信息

用户可以根据需要指定威胁日志信息的输出目的地。将威胁日志信息输出到console、远程终端、系统日志服务器或者使用威胁日志email提醒功能，在全局配置模式下使用以下命令：

logging threat to {*console* | *remote* | *syslog* [*custom-format* [*distributed* [*round-robin* | *src-ip-hash*]]] | *email*} [*severity severity-level*]

- **console** – 指定将威胁日志信息输出到console口。
- **remote** – 指定将威胁日志信息输出到远程终端。
- **syslog** – 指定将威胁日志信息输出到Syslog Server。关于如何配置Syslog Server，请参阅“[配置Syslog Server](#)”。
- **custom-format** – 发送明文日志信息。默认情况下，系统发送明文日志信息。
- **distributed** – 分布发送日志信息到多台日志服务器。

- **src-ip-hash** | **round-robin** – 指定服务器选择算法。**src-ip-hash**为源地址哈希算法。**round-robin**为轮询调度算法，该算法为系统默认算法。
- **email** – 使用威胁日志email提醒功能。关于如何配置email地址，请参阅“[配置Email地址](#)”。
- **severity severity-level** – 指定输出的威胁日志信息的级别从而对威胁日志信息进行过滤。输出信息的级别将会是指定级别或者高于指定级别，即数字等于或者小于指定级别。例如指定级别是通告，系统将会输出通告、警告和错误级别的日志信息。

在全局配置模式下，用以上命令**no**的形式可以关闭相关的输出功能。命令如下：

```
no logging threat to {console | remote | syslog [ custom-format [distributed [round-robin | src-ip-hash]]] | email }
```

将威胁日志信息输出到内存缓存，在全局配置模式下使用以下命令：

```
logging threat to buffer [severity severity-level] [size buffer-size]
```

- **severity severity-level** – 指定输出的威胁日志信息的级别从而对威胁日志信息进行过滤。输出信息的级别将会是指定级别或者高于指定级别，即数字等于或者小于指定级别。例如指定级别是通告，系统将会输出通告、警告和错误级别的日志信息。
- **size buffer-size** – 指定内存缓存的大小。范围是4096到1048576字节。默认值为1048576。

在全局配置模式下，用该命令**no logging threat to buffer**命令关闭相关的输出功能。

将威胁日志信息输出到文件，在全局配置模式下使用以下命令：

```
logging threat to file [severity severity-level] [name [usb0 | usb1] file-name] [size file-size]
```

- **severity severity-level** – 指定输出的威胁日志信息的级别从而对威胁日志信息进行过滤。输出信息的级别将会是指定级别或者高于指定级别，即数字等于或者小于指定级别。例如指定级别是通告，系统将会输出通告、警告和错误级别的日志信息。
- **name [usb0 | usb1] file-name** – 该参数用来指定保存日志信息的U盘和日志信息文件的名称。
- **size file-size** – 将威胁日志信息输出到文件（U盘或者Flash）时，该参数用来指定日志信息文件的大小。范围是4096到1048576字节。默认是1048576字节。

在全局配置模式下，用以上命令**no logging threat to file**命令关闭相关的输出功能。

输出Web防护日志信息

用户可以根据需要指定Web防护日志信息的输出目的地。将Web防护日志信息的输出到console口，在全局配置模式下使用以下命令：

```
logging web-protect to console
```

- **console** - 指定将威胁日志信息输出到console口。

将Web防护日志信息输出到内存缓存，在全局配置模式下使用以下命令：

```
logging web-protect to buffer [ size file-size]
```

- **size buffer-size** - 指定内存缓存的大小。范围是4096到5242880字节，默认值为1048576字节。

在全局配置模式下，用以上命令**no logging web-protect to {buffer | console}**命令关闭相关的输出功能。

输出配置、操作、调试和网络日志信息

用户可以根据需要指定日志信息的输出目的地，可以是缓存、Console口、Syslog服务器、文件和设备硬盘卡。

将日志信息输出到Console口、Syslog服务器，在全局配置模式下使用以下命令：

```
logging {configuration | operation | debug | network} to {console | syslog}
```

- **configuration | operation | network** - 指定将要输出的日志信息的类型，可以是配置（**configuration**）、操作（**operation**）、调试（**debug**）或者网络（**network**）。
- **console** - 指定日志信息的输出目的地为Console口。
- **syslog** - 指定日志信息的输出目的地为Syslog Server。关于如何配置Syslog Server，请参阅“[配置Syslog Server](#)”。

在全局配置模式下，用**no logging {configuration | operation | debug | network} to {console | syslog}**命令关闭相关的输出功能。

将配置和网络日志信息输出到文件，在全局配置模式下使用以下命令：

```
logging {configuration | operation | network} to file [name [usb0 | usb1] file-name] [size file-size]
```

- **configuration | operation | network** - 指定将要输出的日志信息的类型，可以是配置（**configuration**）、操作（**operation**）或者网络（**network**）。
- **name [usb0 | usb1] file-name** - 该参数用来指定保存日志信息的U盘和日志信息文件的名称。

- **size file-size** – 将配置和网络日志信息输出到文件（U盘或者Flash）时，该参数用来指定日志信息文件的大小。范围是4096到1048576字节。默认是1048576字节。

在全局配置模式下，用以上命令**no logging {configuration | operation | network} to file**命令关闭相关的输出功能。

将配置、调试和网络日志信息输出到内存缓存，在全局配置模式下使用以下命令：

logging {configuration | operation | debug | network} to buffer [size buffer-size]

- **configuration | operation | debug | network** – 指定将要输出的日志信息的类型，可以是配置（**configuration**）、操作（**operation**）调试（**debug**）或者网络（**network**）。
- **size buffer-size** - 内存缓存的大小。范围是4096到524288字节。默认值为1048576。

在全局配置模式下，用**no logging {configuration | operation | debug | network} to buffer**命令关闭相关的输出功能。

输出健康检查日志信息

用户可以根据需要指定健康检查日志信息的输出目的地。将健康检查日志信息输出到console、系统日志服务器、手机、本地数据库或者使用健康检查日志email提醒功能，在全局配置模式下使用以下命令：

logging health-check to {console | buffer [size buffer-size] | syslog | email | sms | localdb}

- **console** - 指定将健康检查日志信息输出到console口。
- **buffer [size buffer-size]** – 指定将日志信息输出到缓存，并指定缓存的大小，范围是4096到524288字节。默认值为1048576字节。
- **syslog** - 指定日志信息的输出目的地为Syslog Server。关于如何配置Syslog Server，请参阅“[配置Syslog Server](#)”。
- **email** – 使用健康检查日志email提醒功能。关于如何配置email地址，请参阅“[配置Email地址](#)”。
- **sms** – 指定将健康检查日志信息以短信的形式输出到某个手机。
- **localdb** – 指定将日志信息输出到本地数据库。数据库位于设备自带的1T硬盘上。

在全局配置模式下，用**no logging health-check to {console | buffer | syslog | email | sms | localdb}**命令关闭相关的输出功能。

配置日志信息的输出 格式

系统按照固定的格式输出日志信息，默认情况下，输出到Syslog Server的日志信息不显示年份、主机名称和日志级别，用户可以根据需要配置日志信息的输出格式。在全局配置模式下，使用以下命令使用以下命令：

- 指定输出的日志信息显示四位数字年份：**logging syslog 4digit-year-timestamp**
- 指定输出的日志信息显示主机名称和日志级别：**logging syslog additional-information**

在全局配置模式下，使用以上命令no的形式取消输出的日志信息显示年份、主机名称和日志级别：

- 取消显示四位数字年份：**no logging syslog 4digit-year-timestamp**
- 取消显示主机名称和日志级别：**no logging syslog additional-information**

配置Syslog Server

将日志信息输出到Syslog Server， 用户需要配置Syslog Server的IP地址或主机名称，也可以根据需要配置Syslog Server的VRouter名称、UDP或者TCP的端口号。进行Syslog Server的配置，在全局配置模式下，使用以下命令：

```
logging syslog {ip-address | hostname} [format-type SGCC] {vrouter vr-name | source-interface interface-name} {tcp port-number | udp port-number | secure-tcp port-number [server-cert-check-disable]} [type log-type]
```

```
logging syslog {ip-address | hostname} [format-type CUCC [default] | source-interface interface-name {tcp port-number | udp port-number | secure-tcp port-number [server-cert-check-disable]}] [type log-type]
```

- *ip-address | hostname* - 指定Syslog Server的IP地址或者主机名称。
- **format-type** { **SGCC** | **CUCC** [default] } - 指定Syslog Server日志服务器的日志输出格式，包括CUCC和SGCC，请根据对应的日志服务器类型进行选择。
 - **SGCC** - 指定Syslog Server日志服务器仅可接收SGCC格式的日志，如国家电网日志服务器。
 - **CUCC** [default] - 指定按照特殊格式（中国联通日志格式）发送NAT444日志信息。若配置default参数，表示按照默认格式发送其它类型的日志信息。
- **vrouter** *vr-name* - 指定VRouter的名称。
- **source-interface** *interface-name* - 指定发送日志信息的源接口，设备会以指定接口的IP地址为源IP，向日志服务器发送日志信息。如果该接口配有管理IP地址，优先使用管理IP地址。

- **tcp** *port-number* | **udp** *port-number* | **secure-tcp** *port-number* [**server-cert-check-disable**] – 指定协议类型及协议端口号。

若选择“Secure-TCP”协议，用户可根据需要指定**server-cert-check-disable**，系统将与日志服务器不需验证证书即可正常传输日志。

- **type** *log-type* – 指定日志信息类型。如果配置该参数，只有指定类型的日志信息会输出到该系统日志服务器。

在全局配置模式下使用以上命令**no**的形式取消对Syslog Server的配置。

配置GBK编码

输出到Syslog Server的日志信息默认的编码格式为UTF-8，用户可根据需要开启GBK编码。开启GBK编码格式后，输出到Syslog Server的日志编码格式将变为GBK编码。在全局配置模式下，使用以下命令：

logging syslog GBK

在全局配置模式下使用**no logging syslog GBK**命令关闭GBK编码，日志编码格式将恢复为UTF-8编码。

指定场所

当把日志信息输出到UNIX Syslog服务器时，用户需要为Syslog服务器指定场所（Facility）。指定场所，在全局配置模式下，使用以下命令：

logging facility local x

- **local x** – 指定场所。x的范围是0到7的整数。默认值是7。

在全局配置模式下使用**no logging facility**命令恢复场所的默认值。

配置Email地址

使用事件日志信息邮件提醒功能，用户需要配置接收日志信息邮件的email地址。配置email地址，在全局配置模式下，使用以下命令：

logging email to email-address smtp smtp-instance

- **email-address** – 指定接收日志信息邮件的email地址。
- **smtp smtp-instance** – 指定email地址的SMTP实例（必须为系统中已经配置成功的SMTP实例）。

在全局配置模式下使用以上命令**no**的形式取消对email地址的配置。

`no logging email to email-address`



注意: 用户最多允许配置5个Email地址。

配置SMTP实例

配置SMTP实例，在全局配置模式下，使用以下命令：

```
smtp name smtp-name server {ip-address | hostname} {from email-addr | vrouter vr-name from email-addr } [user-  
name user-name password password] [mode { plain | starttls | ssl}] [port server-port]
```

- *smtp-name* - 指定SMTP实例的名称。
- *ip-address* | *hostname* - 指定SMTP服务器的IP地址或者主机名称。
- *email-addr* - 指定发件人地址。
- **vrouter** *vr-name* - 指定SMTP服务器的VRouter的名称。
- **username** *user-name* **password** *password* - 指定发件人帐号的用户名和密码。
- **mode** { **plain** | **starttls** | **ssl** } - 指定系统发送的日志信息邮件的传输方式。
 - **plain**- 指定为plain方式，日志信息邮件将使用明文且非加密的方式传输。该方式为默认传输方式。
 - **starttls**- STARTTLS是对纯文本通信协议的扩展，它将纯文本连接升级为加密连接。指定为starttls方式，日志信息邮件将使用加密方式传输。
 - **ssl**- SSL协议是为网络通信提供安全及数据完整性的一种安全协议。指定为ssl方式，日志信息邮件将使用加密方式传输。
- **port** *server-port* - 指定SMTP服务器的端口号。范围是1到65535。不同传输方式下的默认端口号不同，PLAIN： 25，STARTTLS： 25，SSL： 465 。

在全局配置模式下，使用**no smtp name** *smtp-name*命令删除指定的SMTP实例。

配置日志参数

系统支持配置事件日志、网络日志、配置日志的参数，包括日志的级别、描述信息，也可以关闭指定日志生成。

关闭日志生成

关闭指定ID日志的生成，请在全局配置模式下，使用以下命令：

```
logging logid log-id off [severity severity-level] description description
```

- **logid** *log-id*- 关闭指定ID的日志生成。
- **severity** *severity-level*- 修改指定ID的日志级别。
- **description** *description*- 修改指定ID日志的描述信息。

在全局模式下，使用命令**no logging logid** *log-id* **off**取消关闭指定ID日志的生成。

配置日志级别

配置日志级别，请在全局配置模式下，使用以下命令：

```
logging logid logid severity severity-level description description
```

- **logid** *logid*- 配置指定ID的日志级别。
- **severity** *severity-level*- 指定日志的级别，包括紧急（EMERG）、警报（ALERT）、严重（ALERT）、错误（ERR）、警告（WARNING）、通告（NOTICE）及信息（INFO）。
- **description** *description*- 修改指定ID的日志描述信息。

在全局模式下，使用命令**no logging logid** *logid* **severity**取消配置指定ID日志的级别。

显示配置日志参数的日志条目

显示配置了日志参数的日志条目，请在全局模式下，使用以下命令：

```
show logging logid config
```


显示日志信息

用户可以在任何模式下通过以下命令查看日志配置信息：

- 查看系统日志信息配置状态：**show logging**
- 查看系统日志服务器的配置信息：**show logging syslog**
- 查看email地址的配置信息：**show logging email**
- 查看系统日志信息的统计信息：**show logging statistics**
- 查看接收事件日志的手机配置信息：**show logging sms**

用户可以在任何模式下通过以下命令查看日志信息：

- 显示事件日志信息：
show logging event [*severity severity-level*]
- 显示调试、网络或者威胁日志信息：
show logging {*debug* | *network* | *threat*}
- 显示配置日志信息：
show logging configuration
- 显示流量日志信息：
show logging traffic[*gslb* | *slb* | *pbr* | *ssl-inspection* | *session*]
- 显示NAT日志信息：
show logging traffic nat *filter-nat* [*src-ip A.B.C.D* | *src-port port-num* | *dst-ip A.B.C.D* | *dst-port port-num* | *protocol* {*icmp* | *tcp* | *udp* | *others*} | *trans-src-ip A.B.C.D* | *trans-src-port port-num* | *trans-dst-ip A.B.C.D* | | *snat-rule-id rule-id*]
- 显示Web防护日志信息：
show logging web-protect [{ *dst-ip* {*A.B.C.D* | *X:X:X:X::X*} | *dst-port port-num* | *path url-path* | *src-ip* {*A.B.C.D* | *X:X:X:X::X*} | *time from HH:MM:SS Month Day Year to HH:MM:SS Month Day Year* | *virtual-server vs-name* }]

其中*HH*、*MM*和*SS*分别表示小时、分钟和秒，*Month*、*Day*和*Year*分别表示月、日和年。

- 显示健康检查日志信息：

```
show logging health-check [hc-name value | ip {A.B.C.D | X:X:X:X::X} | module {gslb | slb} | pool-name pool_name | port port | rs-name rs_name | severity {alerts | critical | debugging | emergencies | errors | informational | notifications | warnings} | status {failure | success} | time from HH:MM:SS Month Day Year to HH:MM:SS Month Day Year]
```

其中**severity**表示健康检查日志的级别；**status**表示真实服务的状态；*HH*、*MM*和*SS*分别表示小时、分钟和秒，*Month*、*Day*和*Year*分别表示月、日和年。

导出日志信息

用户可以导出事件和威胁日志信息，导出的目的地包括FTP服务器、TFTP服务器和U盘。

导出事件或安全日志信息到FTP服务器，在执行模式使用以下命令：

```
export log {event | threat} to ftp server ip-address user user-name password password [file-name]
```

- **event** | **threat** - 指定导出的系统日志的类型。
- *ip-address* - 指定FTP服务器的IP地址。
- **user** *user-name* **password** *password* - 指定访问FTP服务器的用户名和密码。
- *file-name* - 指定导出的事件日志信息文件的名称。

导出事件或威胁日志信息到TFTP服务器，在执行模式下使用以下命令：

```
export log {event | threat} to tftp server ip-address [file-name]
```

清除日志信息

用户可以通过命令将日志信息从系统中清除。清除系统日志信息，在执行模式下，使用以下命令：

```
clear logging { configuration | debug | event | network | threat | traffic nat | web-protect}
```

- **configuration** - 清除所有系统存储的配置日志信息。
- **debug** - 清除所有系统存储的调试日志信息。
- **event** - 清除所有系统存储的事件日志信息。
- **network** - 清除所有系统存储的网络日志信息。

- **threat** – 清除所有系统存储的威胁日志信息。
- **traffic nat** – 清除所有系统存储的NAT日志信息。
- **web-protect** - 清除所有系统存储的Web防护日志信息。

日志分布式外发

设备产生大量的日志信息时，单台日志服务器可能无法满足日志信息的接收需求。针对这一问题，设备提供日志分布式外发功能，即设备能够按照一定的算法把日志信息分布发送到多个日志服务器，进而缓解单台日志服务器的压力，保证日志信息的完整、快速发送和接收。

配置NAT日志信息的分布式发送功能，在全局配置模式下使用以下命令：

```
logging {traffic nat} to syslog [binary-format [distributed [src-ip-hash | round-robin]] | custom-format]
```

- **syslog** – 发送日志信息到日志服务器。
- **binary-format** – 发送二进制类型日志信息。
- **distributed** – 分布发送二进制日志信息到多台日志服务器。
- **src-ip-hash | round-robin** – 指定服务器选择算法。**src-ip-hash**为源地址哈希算法。**round-robin**为轮询调度算法，该算法为系统默认算法。
- **custom-format** – 发送明文日志信息。默认情况下，系统发送明文日志信息。

在全局配置模式下，使用以下命令取消日志信息到日志服务器的输出：

```
no logging {traffic nat} to syslog
```

配置威胁日志信息的明文日志分布式发送功能，在全局配置模式下使用以下命令：

```
logging threat to syslog [custom-format [distributed [src-ip-hash | round-robin]]]
```

- **custom-format** – 发送明文日志信息。默认情况下，系统发送明文日志信息。
- **syslog** – 发送日志信息到日志服务器。
- **distributed** – 分布发送日志信息到多台日志服务器。
- **src-ip-hash | round-robin** – 指定服务器选择算法。**src-ip-hash**为源地址哈希算法。**round-robin**为轮询调度算法，该算法为系统默认算法。

在全局配置模式下，使用以下命令取消日志信息到日志服务器的输出：

```
no logging threat to syslog
```

第14章 高可靠性HA

高可靠性（High Availability），简称为HA，能够在通信线路或设备产生故障时提供备用方案，从而保证数据通信的畅通，有效增强网络的可靠性。实现HA功能，用户需要配置两台采用完全相同的硬件平台、固件版本、VSYX特性及相同的VR特性的AX设备，组成HA簇。当一台设备不可用或者不能处理来自客户端的请求时，该请求会及时转到另外的可用设备来处理，这样就保证了网络通信的不间断进行，极大地提高了通信的可靠性。

系统支持HA Active-Passive（A/P）模式，即在HA簇中配置两台设备组成一个HA组，组内只有一台主设备。主设备处于活动状态，转发报文，同时将其所有网络和配置信息以及当前会话信息传递给备份设备。当主设备出现故障时，备份设备接替主设备工作，转发报文。这种A/P模式具有较强冗余性，而且其网络结构简单，便于维护管理。



提示: 相同的VSYX特性即指两台HA设备均需安装VSYX License并同时开启VSYX或者两台HA设备均不使用VSYX；相同的VR特性指两台HA设备均开启多VR或均关闭多VR。

HA基础概念

HA簇

HA簇是实现HA功能的设备的组合。对于外部网络设备而言，一个HA簇是一个单一的设备，处理网络流量和提供安全服务。HA簇通过簇ID进行标识。为设备指定HA簇ID后，设备进入HA状态，执行HA功能。

HA组

系统会对HA簇中相同HA组ID的设备，按照HCMP协议，根据设备的HA配置，进行主备选举。主设备处于活动状态处理网络流量，而当主设备出现故障时，其它设备代替主设备继续工作。当为设备设置簇ID时，组ID为0的HA组会自动创建。在Active-Passive（A/P）模式中，设备仅具有HA组0。

HA Node

为区分HA簇中的HA设备，用户可使用 HA Node（节点）值来标识设备。

HA组接口和虚拟MAC

在HA环境中，每个HA组都具有接口，流量通过接口进行传输。每个HA组的主设备维护对应接口的虚拟MAC（VMAC）地址，流量通过这些具有VMAC地址的接口进行转发。HA簇中不同HA组之间不互相转发数据。VMAC地址由HA虚拟基MAC、簇ID、HA组ID以及物理接口索引确定。

HA选举

HA簇中，拥有同样HA组ID的具有高优先级的设备会被选举为HA组的主设备。

HA同步

为保证备份设备能够在主设备失效时代替主设备工作，主设备需要与备用设备进行同步。同步的信息包括：配置信息、文件以及RDO（Runtime Dynamic Object）。RDO的具体内容主要包括：

- 健康状态
- 会话信息
- 会话保持表
- DNS缓存映射条目
- ARP表
- PKI信息
- DHCP信息
- MAC表

系统使用两种方法进行同步，分别是实时同步和批量同步。当主设备刚刚选举成功时，系统会使用批量同步方法，将主设备信息全部同步到备份设备；当配置发生变化时，系统将使用实时同步的方法将变化的信息同步到备份设备。除HA相关配置和本地配置（例如，主机名称配置），其它的配置都会被同步。

配置HA

使用高可靠性功能，用户需要按照以下步骤进行配置：

1. 配置HA组。HA组的配置包括指定设备优先级（选举使用）以及设备HA报文相关参数等。
2. 配置HA组的接口。
3. 配置HA连接。包括HA连接接口和连接接口IP的配置。用于设备同步以及传输HA报文。
4. 配置HA簇。为设备指定HA簇ID，并且开启设备的HA功能。

配置HA功能，必须配置HA数据连接接口；且HA组0接口不能配置为HA数据连接接口，只能配置为HA控制连接接口。

配置HA组

HA组配置包括需要在HA组配置模式下进行。进入HA组配置模式，在全局配置模式下，输入以下命令：

```
ha group group-id
```

- *group-id* – 指定HA组的ID。目前仅支持HA组为0。

执行该命令后，系统进入HA组配置模式。使用该命令no的形式删除指定的HA组。

```
no ha group group-id
```

指定优先级

该命令指定的优先级用于HA选举。优先级高（数字小）的会被选举为主设备。为设备指定优先级，在HA组配置模式下使用以下命令：

```
priority number
```

- *number* – 指定优先级。范围是1到254的整数。默认值是100。

在HA组配置模式下使用该命令no的形式恢复优先级的默认值：

```
no priority
```

说明：相同优先级下，设备序列号的第10至14位数值越小，优先级越高。

指定Hello报文间隔

Hello报文间隔指HA设备向HA组中的其它设备发送心跳（Hello报文）的时间间隔。同一个HA组的设备的Hello报文间隔时间必须相同。指定该时间间隔，在HA组配置模式下使用以下命令：

hello interval time-interval

- **time-interval** – 指定发送心跳的时间间隔，单位为毫秒。范围是50到10000毫秒。默认值是200毫秒。

在HA组配置模式下使用该命令**no**的形式恢复时间间隔的默认值：

no hello interval

指定Hello报文警戒值

该命令指定失去心跳的警戒值，即如果设备没有收到对方设备的该命令指定个数的Hello报文，就判断对方无心跳。指定失去心跳的警戒值，在HA组配置模式下使用以下命令：

hello threshold value

- **value** – 指定失去心跳的警戒值。范围是3到255。默认值是15。

在HA组配置模式下使用该命令**no**的形式恢复警戒值的默认值：

no hello threshold

配置抢占模式

如果将设备配置为抢占模式，一旦设备发现自己的优先级高于主设备，就会将自己升级为主设备，而原先的主设备将变为备份设备；如果将设备设置为非抢占模式，即使设备的优先级高于主设备，它也只能在主设备故障时代替主设备工作。在配置抢占模式时，用户还可以设置延迟时间，使备份设备在延迟时间过后升级为主设备。配置抢占模式，在HA组配置模式下使用以下命令：

preempt [delay-time]

- **delay-time** – 指定延迟时间，单位为秒。范围是1到600秒。默认值为30秒。

在HA组配置模式下使用该命令**no**的形式恢复为非抢占模式：

no preempt

指定发送ARP包个数

当备份设备升级为主设备时，新主设备需要向网络中发送ARP请求包，通知相关网络设备更新其ARP表。该命令用来指定升级为主设备的设备向外发送ARP包的个数。新主设备发送的免费ARP包的最大个数由该命令所指定的发送ARP包个数决定，当设备发生主备切换后，系统将会立即发送5个免费ARP包，后续每秒发送1个ARP包，直到发送的ARP包个数达到该命令所指定的个数。指定发送ARP包的个数，在HA组配置模式下使用以下命令：

arp *number*

- *number* – 指定发送ARP请求包的个数。范围是10到180。默认值是15。

在HA组配置模式下使用该命令no的形式恢复发送ARP包个数的默认值：

no arp

手动发送免费ARP包

当备份设备升级为主设备时，由于新主设备向网络中发送的ARP请求包数量有限，可能导致部分服务器收不到ARP包而无法更新自己的ARP表，这样该部分服务器就无法在短时间内恢复业务。为解决该问题，系统支持通过指定接口手动发送免费ARP包的功能。配置通过指定接口手动发送免费ARP包功能，在执行模式下使用以下命令：

send gratuitous-arp interface *interface-name* [**count** *num* | **interval** *num*]

- **interface** *interface-name* – 指定发送免费ARP包的接口。可以是已配置IP地址的物理接口、VSwitch接口、集聚接口、冗余接口或者BGroup接口。
- **count** *num* – 指定发送ARP包的次数。取值范围为0到60。默认为5次。0表示不间断循环发送，可按“Ctrl+C” 停止发送。
- **interval** *num* – 指定发送ARP包的时间间隔。取值范围为1到60秒。默认为1秒。

指定描述信息

为设备指定描述信息，在HA组配置模式下使用以下命令：

description *string*

- *string* – 指定描述信息内容。

在HA组配置模式下使用该命令`no`的形式取消描述信息的指定：

no description

指定监测对象

用户可以为设备指定监测对象，监控设备的工作状态。一旦发现设备不能正常工作，即采取相应措施。指定监测对象，在HA组配置模式下使用以下命令：

monitor track *track-object-name*

- *track-object-name* – 指定系统中已配置的监测对象的名称。

在HA组配置模式下使用该命令`no`的形式取消监控配置：

no monitor track

注意：建议将HA组所引用的监测对象配置成Local属性。关于如何配置监测对象，请参阅“[配置监测对象](#)”。

HA连接配置

主设备与备份设备之间的同步信息以及Hello报文等都通过HA连接进行传输。HA连接有两种类型，分别是控制连接（ControlLink）和数据连接（Data Link）。控制连接同步两台设备间的所有数据；数据连接仅同步数据报文信息，如会话信息。用户可根据需求选择否配置数据连接。若配置数据连接，设备间的Hello报文等将通过控制连接完成，数据同步等信息将通过数据连接完成。若不配置数据连接，设备间所有的同步信息将通过控制连接完成。

配置HA连接，需要首先指定HA连接接口，然后为接口指定IP地址。

指定HA连接接口

用户最多可以指定两个HA控制连接接口，后配置的HA连接接口可以作为先配置的HA连接接口的备份接口工作。当先配置的HA连接接口断开连接，后配置的HA连接接口会继续传输HA报文。

指定HA控制连接接口，在全局配置模式下，使用以下命令：

ha link interface *interface-name*

- *interface-name* - 指定接口名称。

指定HA数据连接接口，在全局配置模式下，使用以下命令：

```
ha link data interface interface-name
```

- **data** - 指定该连接接口为数据连接接口。指定后，会话信息将通过该HA数据连接接口同步完成。目前仅支持将物理接口和集聚接口配置为Data Link的接口。用户最多可以指定1个集聚接口为HA数据连接接口，或者最多指定2个物理接口为HA数据连接接口。
- *interface-name* - 指定接口名称。

在全局配置模式下，使用上述命令**no**的形式删除指定接口的配置。

指定HA数据连接接口工作模式

当HA数据连接接口配置为两个物理接口时，这两个物理接口可以工作在主备模式（Active-passiveMode）或者负载模式（Load-balance Mode）。指定HA数据连接接口工作模式，在全局配置模式下，使用以下命令：

```
ha data-link mode {active-passive | load-balance}
```

- **active-passive** - 指定HA数据连接接口工作模式为主备模式。指定后，先配置的HA数据连接接口为主接口，后配置的HA数据连接接口为备份接口。当主接口发生故障时，备份接口接替主接口工作；当主接口恢复正常后，主接口重新运行所有工作。
- **load-balance** - 指定HA数据连接接口工作模式为负载模式，该模式为系统默认模式。指定后，两个HA数据连接接口互为备份，且同时运行各自的工作。当其中一个接口发生故障时，另一个接口运行其自身的工作并且接管故障接口的工作；当故障接口恢复正常后，两个接口重新运行各自的工作。

在全局配置模式下，使用**no ha data-link mode**命令恢复系统默认配置，即负载模式。

指定HA连接接口IP地址

HA连接接口指定完毕，用户需要为HA连接接口配置IP地址。在全局配置模式下，使用以下命令：

```
ha link {ip ipv4-address/Mask | ipv6 ipv6-address/Prefix}
```

- **ip** *ipv4-address/Mask* - 指定HA连接接口的IPv4地址和网络掩码。支持两种子网掩码书写方式，可以为1.1.1.1/24，也可以为1.1.1.1 255.255.255.0。
- **ipv6** *ipv6-address/Prefix* - 指定HA连接接口的IPv6地址和前缀长度。前缀长度取值范围为1到128。

在全局配置模式使用该命令**no**的形式取消HA连接接口IP地址的配置：

```
no ha link {ip ipv4-address/Mask | ipv6 ipv6-address/Prefix}
```

指定HA辅助链路接口

在Active-Passive（A/P）模式中，用户可以指定HA辅助链路接口，用来接收和发送心跳报文（Hello报文），以确保在HA连接发生故障时HA设备维持正常的主备状态。

指定HA辅助链路接口，在全局配置模式下，使用以下命令：

```
ha assist-link interface interface-name
```

- *interface-name* - 指定接口名称。用户最多可以配置1个HA辅助链路接口。

在全局配置模式使用该命令**no**的形式删除对指定的HA辅助链路接口配置：

```
no ha assist-link interface interface-name
```



注意：

- 在HA连接恢复正常之前，HA辅助链路接口只能接收和发送心跳报文，不能同步数据报文信息，因此建议用户不要修改当前设备配置信息，在HA连接恢复后执行**exec ha sync rdo session**命令进行手动同步会话信息。
- HA辅助链路接口必须使用除HA连接接口以外的接口，并且已绑定到安全域。
- HA主备设备需将相同的接口指定为HA辅助链路接口，并确保主备设备的该接口属于同一个VLAN。

HA簇配置

为设备配置了HA组、HA组接口和HA连接接口后，用户需要将设备添加到HA簇中，才能够使设备的HA功能生效。如果网络中存在多对HA设备，用户需要为它们配置不同的HA簇ID，否则可能出现MAC地址冲突现象。配置HA簇，在全局配置模式下使用以下命令：

ha cluster *cluster-id*

- *cluster-id* - 指定HA簇ID。范围依据HA的虚MAC前缀而变化。

在全局配置模式下使用该命令no的形式关闭设备的HA功能：

no ha cluster

配置HA虚MAC前缀

当同一网段内需要配置8个以上的HA簇时，为了防止系统生成的HA虚MAC地址重复，用户可以配置HA虚拟基MAC的前缀，即HA虚MAC前缀。当前缀设置为七位时，您最多可以在同一网段内部署128个HA簇；当前缀设置为八位或者不设置时，您最多可以在同一网段内部署8个HA簇。配置完成后，系统将提示可能会生成的HA虚MAC的范围，重启后配置才能生效。配置HA虚MAC的前缀，在全局配置模式下，使用如下命令：

ha virtual-mac-prefix *prefix-addr*

- *prefix-addr* - 指定HA虚拟基MAC的前缀，格式为十六进制，且只能配置为七位或者八位。默认情况下，HA虚MAC的前缀为0x001C54FF。需要注意的是，全0、全F或者组播地址（即第二个十六进制数为奇数的MAC地址）前缀是无效的。

在全局配置模式下，执行**no ha virtual-mac-prefix**命令恢复默认前缀。

说明：开启HA功能后，如需修改HA虚MAC前缀，请先关闭HA功能。

查看虚MAC前缀信息

使用**show ha cluster**命令查看当前的HA虚MAC的前缀和当前支持的最大HA簇个数。

接口管理IP配置

为实现对HA备份设备的管理，用户需要为备份设备配置管理IP。配置管理IP地址，在接口配置模式下，使用以下命令：

manage ip *ip-address*

- *ip-address* - 指定管理IP地址。

配置三层接口Down-Up功能

用户可以配置三层接口down-up功能，该功能默认开启。关闭该功能后，当设备进行HA切换由主设备切换为备份设备时，以下类型的物理接口不进行down-up操作：

- 已绑定三层安全域的物理接口
- 属于冗余接口的物理接口，且该冗余接口已绑定三层安全域
- 属于集聚接口的物理接口，且该集聚接口已绑定三层安全域

开启/关闭三层接口down-up功能，在全局配置模式下，使用以下命令：

```
ha l3-port-force-down-up {enable | disable}
```

- **enable** - 开启三层接口down-up功能。
- **disable** - 关闭三层接口down-up功能。

查看三层接口down-up功能的配置信息，在任意配置模式下，使用以下命令：

```
show ha l3-port-force-down-up
```

手动同步HA信息

在某些特殊情况下，可能出现主备配置信息不同步现象。此时，需要用户手动同步主备设备的配置信息。用户可以通过以下方法判断是否需要手动同步：

1. 分别在主备设备上执行相应的show命令查看相关配置信息，或者执行 **exec ha sync configuration check** 命令查询主备设备配置信息是否一致。
2. 根据显示的配置信息，判断是否需要手动同步：
 - 如果显示的配置信息一致，则无需进行手动同步；
 - 如果显示的配置信息不一致，可以执行**exec ha sync configuration difference [all]**（**all**表示对比所有VSYS的配置信息）命令查看主备设备之间的配置信息差异，之后需要手动执行相应的命令完成配置信息同步（相关show命令和执行命令，参阅下表）。

**注意:**

- 本地配置信息不一致时，例如配置口超时时间等，不需要进行手动同步。
- 对于动态信息，例如会话等，只有当正常动态信息没有同步时，才需要进行手动同步，否则无需手动同步。

Figure 15-1 表5：手动同步配置命令列表

HA同步信息	show命令	手动同步命令
所有静态配置及动态数据	show ha sync state all	exec ha sync all
配置信息	show configuration	exec ha sync configuration
文件信息	show file	exec ha sync file <i>file-name</i>
ARP表项	show arp	exec ha sync rdo arp
DNS配置信息	show ip hosts	exec ha sync rdo dns
DNS rewrite规则信息	show dns-rewrite-rule	exec ha sync rdo dns-rewrite
会话信息	show session	exec ha sync rdo session
会话保持表	show slb persistence {14 17}	exec ha sync rdo persistence
DHCP配置信息	show dhcp	exec ha sync rdo dhcp
MAC地址表	show mac	exec ha sync rdo mac
PKI配置信息	show pki key	exec ha sync rdo pki
	show pki trust-domain	
会话信息	show session	exec ha sync rdo session
NTP信息	show ntp	exec ha sync rdo ntp
路由信息	show ip route	exec ha sync rdo route

HA同步信息	show命令	手动同步命令
IGMP信息	show ha sync statistic igmp	exec ha sync rdo igmp
	show ha sync state igmp	

启用/禁用HA会话自动同步

默认情况下，HA设备之间会自动同步会话信息。同步会话会产生一定流量，在高负载情况下可能会对设备性能造成影响。用户可以根据设备负载情况启用或禁用HA会话自动同步功能，以确保设备的稳定性。

启用或禁用HA会话自动同步功能，在全局配置模式下，使用以下命令：

- 启用：**ha sync rdo session**
- 禁用：**no ha sync rdo session**

启用/禁用HA配置信息定时比较功能

开启HA配置信息定时比较功能后，系统会每1小时对HA配置信息进行一次检查，如果发现配置信息发生变更，将会记录日志信息。默认情况下，HA配置信息定时比较功能为关闭状态。

启用/禁用HA配置信息定时比较功能，在全局配置模式下，使用以下命令：

- **ha configuration-consistency-check enable** - 启用该功能。
- **no ha configuration-consistency-check enable** - 禁用该功能。

手动切换HA设备的主备状态

用户可以在任何模式下使用以下命令进行主备设备的手动切换：

exec ha master switch-over

注意：仅支持在HA的主设备上执行此命令。

备设备配置模式

为提高主备设备配置信息的一致性，系统提供备设备配置模式。进入该模式后，用户可以根据备设备与主设备之间不一致的配置信息，使用对应功能的配置命令，手动修改备设备的配置。

在执行模式下，使用以下命令：

- **exec ha slave-force-config enable** - 进入备设备配置模式。
- **exec ha slave-force-config disable** - 退出备设备配置模式。

指定vADC的HA心跳口MAC地址

仅vADC支持该功能。HA心跳口MAC地址指HA设备向HA组中的其它设备发送心跳（Hello报文）时所使用的源MAC地址。默认情况下，系统使用默认的MAC地址发送心跳报文，用户也可指定控制连接接口的MAC或者自定义MAC作为HA心跳口的MAC地址。指定HA心跳口MAC地址，在全局配置模式下，使用以下命令：

ha link mac { 1st-interface-mac | mac-address }

- **1st-interface-mac** - 指定使用控制连接接口的MAC地址作为HA心跳口的MAC地址。当用户配置多个控制连接接口时，系统将使用第一个控制连接接口的MAC作为HA心跳口的MAC地址。
- **mac-address** - 指定使用自定义的MAC地址作为HA心跳口的MAC地址。

在全局配置模式使用**no ha link mac**恢复默认的HA心跳口的MAC地址：

配置vADC使用接口的真实MAC

该功能仅对于vADC的接口（除HA连接接口和配置了Local属性的接口）生效。默认情况下，设备接口使用系统分配的虚拟MAC进行正常的数据流量转发。配置该功能后，vADC将使用云平台分配给接口的真实MAC进行业务通信。配置vADC使用接口的真实的MAC，在全局配置模式下，使用以下命令：

no ha virtual-mac enable

使用**ha virtual-mac enable**命令恢复默认配置。



注意: 当设备被添加到HA簇后，将无法修改vADC接口所使用的MAC。如需修改，请先执行命令**no ha cluster**关闭设备HA功能。

配置通过二层单播方式进行HA协商通信

仅vADC支持该功能。默认情况下，HA环境中的两台设备使用组播方式进行协商通信，但在虚拟化环境中，部分云平台要求设备使用其分配的MAC地址进行通信，否则报文将被丢弃。系统支持通过二层单播的方式进行HA协商通信。在HA部署环境中，用户可以在两台设备上，分别配置对端HA连接接口的IP地址或同时配置对端HA连接接口的IP和MAC地址（即心跳口MAC地址），这样两台设备将采用二层单播的方式进行HA协商通信。配置HA对端的IP和MAC地址，在全局配置模式下，使用以下命令：

```
ha peer { ip ipv4-address | ipv6 ipv6-address } [mac mac-address]
```

- { **ip** *ipv4-address* | **ipv6** *ipv6-address* } - 指定对端设备的HA连接接口的IPv4或IPv6地址。
- **mac** *mac-address* - 指定对端设备的HA连接接口的MAC地址，即心跳口的MAC地址。用户需提前指定心跳口的MAC地址，具体参考[指定vADC HA心跳口MAC地址](#)。

在执行模式下，使用命令**no ha peer {ip | ipv6}**恢复默认配置。



注意: 当设备被添加HA簇后，将无法修改HA对端IP和MAC地址。如需修改，请先执行命令**no ha cluster**关闭设备HA功能。

指定HA连接接口的最大传输单元（MTU）

仅vADC支持该功能。HA连接接口指定完毕后，用户可按需为HA连接接口配置最大传输单元（MTU）值。当报文大小超过配置的HA接口MTU值时，发送端会将报文进行分片发送，接收端收到后会将报文进行重组，然后再进行后续处理。

指定HA连接接口的MTU值，在全局配置模式下，使用以下命令：

```
ha link mtu value
```

- *value* - 指定HA连接接口的最大传输单元的数值。默认为1500。

在执行模式使用该命令**no**的形式**no ha link mtu**取消HA连接接口MTU的配置。

配置Hello报文使用UDP协议

仅vADC支持该功能。默认情况下，HA Hello报文使用VRRP协议进行传输。在虚拟化环境中，核心交换机对VRRP报文的传输速率和报文大小均有限制，影响了HA主设备与备份设备之间的同步功能。用户可以配置Hello报文使用UDP协议进行传输，防止核心交换机对报文的限制，在全局配置模式下，使用以下命令：

```
ha transmit udp
```

使用**no ha transmit udp**命令恢复默认的VRRP协议传输。

当设备被添加到HA簇后，将无法修改Hello报文所使用的协议。如需修改，请先执行命令**no ha cluster**关闭设备HA功能。



注意：HA主设备和备设备须保证使用相同的传输协议。

开启/关闭阿里云HAVIP

仅部署在阿里云上的vADC支持。启用后，vADC可以使用阿里云上的HAVIP进行HA部署。若使用接口的辅助IP进行HA部署或不进行HA部署时，需关闭该功能。开启/关闭阿里云HAVIP簇，在配置模式下使用以下命令：

- 开启：**ha aliyun-deploy havip enable**
- 关闭：**ha aliyun-deploy havip disable**

在任意模式下，使用**show ha aliyun deploy-mode**查看开启状态。

指定访问阿里云的密钥ID及密码

仅部署在阿里云上的vADC支持。指定访问阿里云的密钥ID及密码,用于vADC的HA部署，在配置模式下，使用以下命令：

```
aliyun accesskeyid id accesskeysecret password
```

- *id* -指定阿里云上的AccessKey的ID。
- *password* - 指定阿里云上的AccessKey的密码。

在配置模式下，使用以下命令下使用 **no aliyun accesskeyid** 取消配置。

在任意模式下，使用**show aliyun accesskey**查看密钥的相关信息。



注意:

- 当设备配置HA簇ID后，表示设备的HA功能开启。开启后，如需修改HA配置，请先关闭设备HA功能。
- 对于vADC，当部署在阿里云环境中时，需保证系统可以访问阿里云服务，即能ping通 `vpc.aliyuncs.com`；
- 对于vADC，当部署在阿里云环境中时，需保证当前系统的时间与阿里云时间一致，同时注意时间误差范围小于15分钟以内。设置时间，请参考“设备管理 > 设备管理”。

HA簇配置

为设备配置了HA组、HA组接口和HA连接接口后，用户需要将设备添加到HA簇中，才能够使设备的HA功能生效。如果网络中存在多对HA设备，用户需要为它们配置不同的HA簇ID，否则可能出现MAC地址冲突现象。配置HA簇，在执行模式下使用以下命令：

```
ha cluster cluster-id [[ peer-mode node ID [ symmetric-routing ]] | node ID]
```

- *cluster-id* – 指定HA簇ID。范围依据HA的虚MAC前缀而变化。
- **peer-mode** *node ID* – 配置HA Peer模式，并标识该设备在HA簇中的角色。范围是0到1。默认情况下，HA Node ID为0的设备上的组0为主动状态，HA Node ID为1的设备上的组0为禁用状态。
- **symmetric-routing** - 若指定该参数，设备将工作在对称路由模式下。
- **node** *ID* - 为设备指定HA Node值，两台设备需指定不同的Node值。范围是0到1。如不指定该参数，设备将通过自动协商获取Node ID。

在执行模式下使用**no ha cluster**关闭设备的HA功能。

显示HA配置

系统提供相应的show命令，查看HA配置信息。

- 查看HA簇配置信息：`show ha cluster`
- 查看HA组配置信息：`show ha group {config | group-id}`
- 查看HA连接配置状态：`show ha link status`
- 查看HA同步状态：`show ha sync state {all | pki | dns | dhcp | ntp | vpn | config | flow | route | igmp | health-check | persistence}`
- 查看HA traffic状态：`show ha traffic`
- 查看HA同步统计信息：`show ha sync statistic {pki | dns | dhcp | ntp | config | route | igmp | health-check | persistence}`
- 显示接收和发送的HA协议统计信息：`show ha protocol statistics`
- 显示已同步或未同步的HA会话信息：`show session {sync | unsync}`
- 显示HA统计信息及RDO同步信息的版本号等相关信息：`show ha flow {statistics | rdo}`
 - **rdo** - 显示HA RDO同步信息的名称（name）、类型（type）、主版本号（major_version）、次版本号（minor_version）及消息长度（length）。主要用于HA部署环境下，通过查看上述信息，确认系统是否可以升级。

第15章 系统管理

系统的维护与管理主要包括以下各项：

- [配置主机名称](#)
- [配置系统信息显示语言](#)
- [配置系统管理员](#)
- [配置可信主机](#)
- [配置管理接口](#)
- [数据库修复](#)
- [配置存储管理](#)
- [配置文件管理](#)
- [切换接口工作模式](#)
- [查看当前对象的配置信息](#)
- [查看光模块状态信息](#)
- [配置Banner功能](#)
- [系统维护与调试](#)
- [配置系统重启](#)
- [系统版本升级](#)
- [升级IP地理库](#)
- [升级域名地理库](#)
- [升级ISP信息库](#)
- [许可证管理](#)

- [简单网络管理协议（SNMP）](#)
- [网络时间协议（NTP）](#)
- [HSCP协议](#)
- [配置时间表功能](#)
- [短信发送参数](#)
- [HSM代理](#)
- [连接到山石云平台](#)
- [Bypass](#)

配置主机名称

有些情况下，用户的网络环境中会配有一台以上设备，为区分这些设备，就需要为每一台设备指定不同的名称。设备的默认名称是其平台名称。通过CLI配置设备名称，在全局配置模式输入以下命令：

hostname *host-name*

- *host-name* - 指定设备名称。长度范围是1到63个字符。执行该命令后，命令行提示符也会变为新的设备的名称。在全局配置模式下使用no hostname命令恢复设备的默认名称。

以下是配置设备名称的命令示例：

```
hostname# configure （进入全局配置模式）  
hostname(config)# hostname hillstone  
hillstone(config)#
```

配置主机名称显示长度

用户可以配置系统可显示的主机名称长度，超过配置长度部分的主机名称用“~”来代替显示。配置主机名称显示长度，在全局配置模式下，使用以下命令：

hostname-display-length *length*

- *length* - 指定系统可显示的主机名称长度，取值范围为1到63个字符。默认值为16个字符，即当设备主机名称长度超过16个字符时，超过16个字符部分的主机名称用“~”来代替显示。

在全局配置模式下，使用`no hostname-display-length`命令恢复默认值。

查看主机名称显示长度

在任何模式下，使用以下命令查看主机名称显示长度：

```
show hostname-display-length
```

配置系统信息显示语言

系统信息包括日志信息、错误信息和提示信息。设备支持简体中文和英文两种系统信息显示语言，在全局配置模式下，使用以下命令设置显示语言：

```
language {en | zh_CN}
```

- **en** - 设置系统信息显示语言为英文。默认情况下，系统信息显示语言为英文。
- **zh_CN** - 设置系统信息显示语言为简体中文。

在全局配置模式下使用`no language`命令恢复显示语言为默认情况。

需要注意的是，该命令的设置不会影响Web管理界面的语言。

配置管理员

设备的管理员根据角色的不同，对系统可执行的管理和配置权限不同。系统支持预定义管理员角色和自定义管理员角色。

系统默认预定义如下四类管理员角色，这四类管理员角色不可被删除和编辑：

- 系统管理员（admin）：拥有读、执行和写权限，可以通过`show`命令查看当前或者历史配置信息、在执行模式下运行`import`、`export`和`save`等命令以及在任何模式下对设备所有功能模块进行配置。
- 系统管理员（只读）（admin-read-only）：拥有读和部分执行权限，可以通过`show`命令查看当前或者历史配置信息，可以在执行模式下运行`export`命令。

- 安全操作员（operator）：拥有读、执行和部分写权限，可以修改除管理员配置、重启设备、恢复出厂设置以及升级版本以外的其他功能模块配置，通过show命令查看当前或者历史配置信息、但是不能查看日志信息，以及在执行模式下运行部分执行命令。
- 安全审计员（auditor）：只可以对日志信息进行操作，包括查看、导出和清除。

下表为管理员的详细权限列表。

功能	权限			
	系统管理员	系统管理员（只读）	安全操作员	安全审计员
配置（包括保存配置）	✓	✗	✓	✗
管理员配置	✓	✗	✗	✗
恢复出厂配置	✓	✗	✗	✗
删除配置文件	✓	✗	✓	✗
回退起始配置信息	✓	✗	✓	✗
重启设备	✓	✗	✗	✗
查看配置信息	✓	✓	✓	✗
查看日志信息	✓	✓	✗	✓
修改当前管理员密码	✓	✓	✓	✓
import命令	✓	✗	✓（除系统升级外）	✗
export命令	✓	✓	✗	✓
clear命令	✓	✓	✓	✓
ping/traceroute命令	✓	✓	✓	✗
debug命令	✓	✓	✓	✗
exec命令	✓	✓	✓	✓
terminal width命令	✓	✓	✓	✓

功能	权限			
	系统管理员	系统管理员（只读）	安全操作员	安全审计员
令				



注意:

- Hillstone设备拥有一个默认系统管理员“hillstone”，用户可以对系统管理员“hillstone”进行编辑（只可编辑密码和访问方式）或删除。
- 除了系统管理员，其他角色的管理员不能编辑管理员的任何属性，只能修改自身密码。
- 安全审计员可以管理一种或多种日志信息，管理日志类型需要系统管理员配置。

管理员配置包括：

- 配置默认用户登录操作
- 新建管理员角色
- 指定管理员角色的权限
- 指定管理员角色的描述信息
- 创建管理员
- 配置管理员角色
- 配置管理员密码
- 配置管理员访问方式
- 配置安全审计员可管理日志类型
- 配置管理员登录限制
- 配置管理员的最大数量
- 显示管理员角色的配置
- 显示管理员配置

配置默认用户登录操作

系统拥有一个默认用户“hillstone”以及对应的默认密码“hillstone”，当管理员使用默认用户名和默认密码登录设备时，可能会存在被破解的风险。针对该问题，系统将会在管理员使用默认用户名和密码登录设备时，系统将跳出修改密码的提示，用户可以按照提示进行操作：

```
Administrator is logging in with default account and password, please change your password!
```

```
new password: *****
```

```
Please input the new password again: *****
```

```
SG-6000#
```



注意：在HA Active-Passive（A/P）模式下，备设备不支持该功能，可以使用默认用户直接登录。

新建管理员角色

新建管理员角色，在全局配置模式下，使用如下命令：

```
admin role role-name
```

- *role-name* – 指定管理员角色的名称。长度范围是4到95个字符。执行该命令后，系统创建指定名称的管理员角色，并且进入管理员角色配置模式；如果指定的管理员角色名称已经存在，则直接进入管理员配置模式。

使用**no admin role *role-name***命令删除指定的管理员角色。

指定管理员角色的权限

用户可自定义管理员角色，指定管理员角色对CLI的权限和WebUI的权限。

- 对CLI的权限包括“读写”和“不可用”。
- 针对WebUI的各个功能模块，用户可设定“读写”、“只读”、或“不可用”三个权限。

指定管理员角色的CLI权限，在管理员角色配置模式下，使用如下命令：

```
cli-privilege all {rw | none}
```

- **rw** | **none** – **rw**表示管理员角色对全部CLI具有读写权限；**none**表示管理员角色不具有CLI权限，不可使用CLI命令。

指定管理员角色的WebUI权限，在管理员角色配置模式下，使用如下命令：

ui-privilege *module-name* {**none** | **r** | **rw**}

- *module-name* – 指定模块名称。获取完整的模块列表，在**ui-privilege** 命令后输入问号(?)。
- **none** | **r** | **rw** – 对指定的模块设置相应的权限。**none**表示对模块无权限，管理员角色无法在WebUI查看到此模块；**r**表示对模块具有读权限，可在WebUI查看此模块配置，但无法修改配置；**rw**表示对模块具有读写权限，可在WebUI查看并修改模块的配置。

使用**no ui-privilege** *module-name*命令取消对此模块的权限设置。

指定管理员角色的描述信息

指定管理员角色的描述信息，在管理员角色配置模式下，使用如下命令：

description *description*

- *description* – 指定描述信息标示此管理员角色。长度范围是0到255个字符。

使用**no description**命令删除描述信息。

创建管理员

创建管理员并进入管理员配置模式，请在全局配置模式下输入以下命令：

admin user *user-name*

- *user-name* - 指定管理员名称。长度范围是4到31个字符。执行该命令后，系统创建指定名称的管理员，并且进入管理员配置模式；如果指定的管理员名称已经存在，则直接进入管理员配置模式。

在全局配置模式下使用**no admin user** *user-name*命令删除指定的管理员。

在管理员配置模式下，用户可以配置管理员角色、管理员密码、访问方式和系统审计员可管理日志类型。

配置管理员角色

配置管理员角色，在管理员配置模式下输入以下命令：

role {**admin** | **operator** | **auditor** | **admin-read-only**}

- **admin** - 指定管理员角色为系统管理员（Administrator）。
- **operator** - 指定管理员角色为系统操作员（Operator）。
- **auditor** - 指定管理员角色为系统审计员（Auditor）。
- **admin-read-only** - 指定管理员角色为系统管理员（只读）（Administrator-read-only）。

配置管理员密码

设备具有密码策略。请为管理员指定符合密码策略的密码。指定管理员密码，在管理员配置模式下，输入以下命令配置管理员的密码：

```
password password
```

- *password* - 指定管理员的密码。范围是4到31个字符。

在管理员配置模式下使用**no password**命令取消管理员密码的配置。

系统允许当前登录的系统操作员、系统审计员或系统管理员（只读）修改自身密码，在任意模式下使用以下命令：

```
exec admin user password update password
```

- *password* - 指定管理员的新密码，为4到31个字符的字符串。



注意：系统管理员可以修改所有管理员的密码。

配置管理员密码策略

管理员密码策略中可以配置管理员密码的复杂度。密码复杂度包括密码的总长度、密码中组成元素的长度以及密码的有效期。其中组成元素包括以下4种类型：

- 大写字母（从A到Z）。
- 小写字母（从a到z）。
- 数字（从0到9）。
- 其他可见字符。例如：分号（；）、斜杠（/）等字符（仅支持半角字符）。

管理员密码策略的配置需要在管理员密码策略配置模式下进行。进入管理员密码策略配置模式，在全局配置模式下，使用以下命令：

password-policy

如果系统默认的管理员密码复杂度设置无法满足安全性的需求，用户可以自定义密码复杂度。自定义密码复杂度前，用户必须先开启复杂度检测功能。

开启或关闭管理员密码的复杂度检测功能，在管理员密码策略配置模式下，使用以下命令：

admin complexity {enable | disable}

- **enable | disable** – 开启或关闭管理员密码的复杂度检测功能。默认情况下，管理员密码的复杂度检测功能为关闭状态。开启后，该功能默认要求密码中必须包含以下各项：两个大写字母、两个小写字母、两个数字和两个特殊字符（例如 “@” 等）。

用户自定义密码组成元素长度，在管理员密码策略配置模式下，使用以下命令：

admin {capital-letters | non-alphanumeric-letters | numeric-characters | small-letters} value

- **capital-letters value** – 指定管理员密码中大写字母的长度。默认值是1个字符，范围是0到16。
- **non-alphanumeric-letters value** – 指定管理员密码中其他可见字符的长度。默认值是2个字符，范围是0到16。
- **numeric-characters value** – 指定管理员密码中数字的长度。默认值是2个字符，范围是0到16。
- **small-letters value** – 指定管理员密码中小写字母的长度。默认值是2个字符，范围是0到16。

用户自定义管理员密码的最小长度，在管理员密码策略配置模式下，使用以下命令：

admin min-length length-value

- **min-length length-value** – 指定管理员密码的最小长度。默认值是4个字符，范围是4到16个字符。当开启管理员密码的复杂度检测功能时，最小长度的默认值为8个字符（两个大写字母、两个小写字母、两个数字和两个特殊字符），范围是8到16个字符。



注意：无论管理员密码的复杂度检测功能是否开启，用户都可以配置管理员密码的最小长度，以提高密码的安全性。

密码的有效期用来限制管理员密码的使用时间。当用户登录时，如果用户输入已经过期的密码，系统将提示重新设置密码，回车后再次输入新密码。如果输入的新密码不符合密码复杂度要求，或连续两次输入的新密

码不一致，系统将要求用户重新输入。连续输入三次不符合要求的密码系统将会断开连接，用户重新登录时系统仍要求用户设置新密码。用户设置的新密码可以和旧密码相同。用户自定义管理员密码的有效期，在管理员密码策略配置模式下，使用以下命令：

admin password-expiration value

- **password-expiration value** – 指定管理员密码的有效期。单位为天，范围是0到365天，默认值是0，表示不对有效期进行限制。在管理员密码策略配置模式下，使用no admin complexity命令恢复管理员密码的复杂度检测功能的默认情况。

显示管理员密码策略信息

用户可以在任何模式下，随时使用show命令查看管理员密码策略信息：

show password-policy

配置管理员访问方式

默认情况下，新建的管理员不可以访问Hillstone设备进行配置。用户需指定管理员的访问方式。系统只允许系统管理员指定其他角色的管理员的访问方式。在管理员配置模式下，输入以下命令配置管理员的访问方式：

access {console | http | https | ssh | telnet | any}

- **console** – 指定管理员通过Console访问。
- **http** – 指定管理员通过HTTP访问。
- **https** – 指定管理员通过HTTPS访问。
- **ssh** – 指定管理员通过SSH访问。
- **telnet** – 指定管理员通过Telnet访问。
- **any** – 指定管理员可以通过以上任何一种方式访问。

使用多条该命令为管理员指定多种访问方式。

使用no access {console | http | https | ssh | telnet | any}命令取消指定的访问方式。

配置安全审计员可管理日志类型

安全审计员只允许对日志信息进行查看、导出和清除，可管理的日志类型需要系统管理员来指定。在管理员配置模式下，输入以下命令配置安全审计员可管理日志类型：

```
log {config | event | network}
```

- **config** – 指定安全审计员可管理配置日志信息。
- **event** – 指定安全审计员可管理事件日志信息。
- **network** – 指定安全审计员可管理网络日志信息。

使用多条该命令为管理员指定多种可管理的日志类型。

使用**no log {config | event | network}**命令取消指定的安全审计员可管理日志类型。

配置管理员登录限制

当用户在客户端通过某种[登录方式](#)登录设备，输入密码的次数超过最大登录尝试数时，系统会在指定时间内禁止所有用户在该客户端使用上述登录方式再次登录设备。当用户剩余登录次数小于等于2次时，系统将给出提示“Permission denied, only x attempt(s) to login”，其中x表示该账户实际的剩余登录次数。

指定禁止访问时长，在全局配置模式下，使用以下命令：

```
admin lockout-duration time
```

- **lockout-duration time** – 指定禁止访问时长。单位为分钟。范围是1到65535。默认值是2分钟。

使用**no admin lockout-duration**命令恢复管理员登录时长默认配置。

指定密码输入错误最大次数，在全局配置模式下，使用以下命令：

```
admin max-login-failure times
```

- **max-login-failure times** – 指定管理员密码输入错误最大次数。默认值是3，范围是1到256。

使用**no admin max-login-failure**命令恢复管理员密码输入错误次数默认配置。



注意：只允许系统管理员配置管理员登录限制。

配置管理员的最大数量

系统支持配置管理员的最大数量。配置后，系统支持创建的管理员的最大数量将为指定数值，用户可根据需要进行调整。调整后，需将设备重启，指定值才能生效。配置管理员的最大数量，在全局配置模式下，使用以下命令：

capacity management max-administrative-users *capacity-num*

- *capacity-num* - 指定管理员最大数量的数值，取值范围为1-128。

使用**no capacity management max-administrative-users**命令恢复默认的管理员最大数量的数值。不同平台的默认值不同，请以实际为准。



注意: 该命令为本地配置命令，不支持HA同步。在HA环境下，若主设备与备设备上设置的管理员最大数量不同，HA状态显示正常，但系统会定时发出告警信息。

显示管理员角色的配置

显示管理员角色的配置：**show admin role** [*role-name*]

显示管理员配置

用户可以在任何模式下，随时使用show命令查看管理员配置：

- 显示管理员信息：**show admin user**
- 显示管理员具体配置信息：**show admin user** *user-name*
- 显示管理员禁止访问时长配置信息：**show admin logout-duration**
- 显示管理员密码输入错误最大次数配置信息：**show admin max-login-failure**

配置可信主机

设备使用可信主机来进一步保证系统安全。管理员可以指定一个IP地址范围，在该指定范围内的主机为可信主机。只有可信主机才可以对设备进行管理。

默认情况下，设备的可信主机范围是0.0.0.0/0，即所有主机都是可信主机。所有可信主机列表中可信主机范围都是有效的。因此，建议用户在创建好合适的可信主机后，将系统原有的“0.0.0.0/0”可信主机范围删除。



注意: 如果远程主机不能访问设备，请检查设备的可信主机配置。

配置系统的可信主机，在全局配置模式下，使用以下命令：

```
admin host {A.B.C.D A.B.C.D | range A.B.C.D A.B.C.D | A.B.C.D/M | any} {http | https | ssh | telnet| any | restful-api | restful-api-https}
```

- `A.B.C.D A.B.C.D | range A.B.C.D A.B.C.D | A.B.C.D/M | any` – 指定可信主机的IP地址范围，例如，1.1.1.1 255.255.0.0。`any`表示任何IP地址。
- `http | https | ssh | telnet | any | restful-api | restful-api-https` – 指定可信主机的登录类型。`any`表示可以使用HTTP、HTTPS、SSH、Telnet、RESTful-API和RESTful-API-HTTPS任意一种类型登录。

用户可以配置多条该命令添加多个可信主机范围。系统最多允许配置128条可信主机范围。

使用`no admin host A.B.C.D A.B.C.D`命令取消可信主机的指定。

使用`no admin host {A.B.C.D A.B.C.D | range A.B.C.D A.B.C.D | A.B.C.D/M | any} {http | https | ssh | telnet| any | restful-api | restful-api-https}`取消对可信主机特定登录类型的指定。

配置IPv6可信主机

管理员可以指定一个IPv6地址范围，在该指定范围内的主机为可信主机。

配置IPv6地址的可信主机，在全局配置模式下，使用以下命令：

```
admin ipv6-host {X:X:X:X::X/M | range X:X:X:X::X X:X:X:X::X | any} {http | https | ssh | telnet| any | restful-api | restful-api-https}
```

- `X:X:X:X::X/M | range X:X:X:X::X X:X:X:X::X | any` – 指定可信主机的IPv6地址范围。`any`表示任何IP地址。
- `http | https | ssh | telnet| any | restful-api | restful-api-https` – 指定可信主机的登录类型。`any`表示可以使用HTTP、HTTPS、SSH和Telnet任意一种类型登录。

用户可以配置多条该命令添加多个可信主机范围。系统最多允许配置128条可信主机范围。

使用`no admin ipv6-host X:X:X:X::X/M`命令取消可信主机的指定。

使用`no admin ipv6-host {X:X:X:X::X/M | range X:X:X:X::X X:X:X:X::X | any} {http | https | ssh | telnet| any | restful-api | restful-api-https}`取消对可信主机特定登录类型的指定。

显示可信主机配置

用户可以在任何模式下，随时使用show命令查看可信主机配置：

```
show admin host
```

配置管理接口

设备支持Console、Telnet、SSH以及WebUI方式的访问。用户可以配置各种访问方式的超时时间、端口号以及HTTPS的PKI信任域。

使用Telnet、SSH、HTTP或者HTTPS方式登录设备时，如果在一分钟内连续三次登录失败，系统会将登录失败的IP地址锁定两分钟。被锁定的IP地址在两分钟内不能建立与设备的连接。

配置Console管理接口

Console管理接口的配置包括波特率配置和超时时间配置。

配置波特率

在任何模式下，使用以下命令设置Console口的波特率：

```
exec console baudrate {9600 | 19200 | 38400 | 57600 | 115200}
```

- 9600 | 19200 | 38400 | 57600 | 115200 – 指定Console口波特率，单位为bps，默认值为9600bps。

需要注意的是，完成波特率配置后，用户在通过Console口登录设备时需保证波特率与设备Console口所作配置一致。

配置超时时间

如果在超时时间内未通过Console口进行任何配置，系统将断开此次Console连接。配置Console超时时间，在全局配置模式下，使用以下命令：

```
console timeout timeout-value
```

- *timeout-value* – 指定Console超时时间，单位为分钟。范围是0到60分钟，0表示无时间限制。默认值是10分钟。

在全局配置模式下，使用该命令no的形式恢复Console超时默认值：

no console timeout

配置Telnet管理接口

用户可以配置Telnet的超时时间以及Telnet端口号。使用Telnet方式连接设备时，使用的端口号必须与此处配置的端口号一致。同时，用户还可以配置Telnet最大登录次数。

如果已经建立的Telnet连接在超时时间内未发送Telnet请求，系统将断开此次Telnet连接。配置Telnet超时时间，在全局配置模式下，使用以下命令：

telnet timeout *timeout-value*

- *timeout-value* – 指定Telnet超时时间，单位为分钟。范围是1到60分钟。默认值是10分钟。

在全局配置模式下，使用该命令no的形式恢复Telnet超时默认值：

no telnet timeout

配置Telnet最大会话数，在全局配置模式下，使用以下命令：

telnet max-session *max-session*

- *max-session* – 指定Telnet最大会话数。范围是1到X，不同平台X的取值不同。默认值为X。

在全局配置模式下，使用该命令no的形式恢复Telnet默认会话数：

no telnet max-session

配置Telnet端口号，在全局配置模式下，使用以下命令：

telnet port *port-number*

- *port-number* – 指定Telnet端口号。范围是1到65535。默认值是23。

在全局配置模式下，使用该命令no的形式恢复Telnet默认端口号：

no telnet port

Telnet最大登录次数，是指允许用户连续失败登录的最大次数。如果连续登录失败次数超出该指定数值，系统将断开此次Telnet连接。配置Telnet最大登录次数，在全局配置模式下，使用以下命令：

telnet authorization-try-count *count-number*

- *count-number* – 指定最大连接次数。范围是1到10次。默认为3次。

在全局配置模式下，使用该命令no的形式恢复Telnet默认登录次数：

no telnet authorization-try-count

配置SSH管理接口

用户可以配置SSH超时时间以及端口号。并且可以指定SSH连接的间隔时间。

如果已经建立的SSH连接在超时时间内未发送SSH请求，系统将断开此次SSH连接。配置SSH超时时间，在全局配置模式下，使用以下命令：

ssh timeout *timeout-value*

- *timeout-value* – 指定SSH超时时间，单位为分钟。范围是1到60分钟。默认值是10分钟。

在全局配置模式下，使用该命令no的形式恢复SSH默认超时时间：

no ssh timeout

配置SSH最大会话数，在全局配置模式下，使用以下命令：

ssh max-session *max-session*

- *max-session* – 指定SSH最大会话数。范围是1到X，不同平台X的取值不同。默认值为X。

在全局配置模式下，使用该命令no的形式恢复SSH默认会话数：

no ssh max-session *max-session*

配置SSH端口号，在全局配置模式下，使用以下命令：

ssh port *port-number*

- *port-number* – 指定SSH端口号。范围是1到65535。默认值是22。

在全局配置模式下，使用该命令no的形式恢复SSH默认端口号：

no ssh port

用户可以指定设备处理SSH连接的时间间隔。建立一个SSH连接后，在时间间隔过后，设备才接受下一个SSH连接请求。配置SSH连接时间间隔，在全局配置模式下，使用以下命令：

ssh connection-interval *interval-time*

- *interval-time* – 指定时间间隔，单位是秒。范围是2到3600秒。默认值是2秒。

在全局配置模式下，使用该命令no的形式恢复SSH连接默认端时间间隔：

no ssh connection-interval

配置WebUI管理接口

用户可以配置通过HTTP或HTTPS方式访问设备，包括选择是否开启相同账号同时登录功能、配置超时时间和端口号等。

系统支持使用相同账号同时登录设备的功能，默认情况下，该功能为关闭状态。开启或关闭相同账号同时登录功能，在全局配置模式下，使用以下命令：

- 开启：**web same-account-login enable**
- 关闭：**web same-account-login disable**

配置WebUI超时时间，在全局配置模式下，使用以下命令：

web timeout *timeout-value*

- *timeout-value* – 指定WebUI超时时间，单位为分钟。范围是1到1440分钟。默认值是10分钟。

在全局配置模式下，使用该命令no的形式恢复WebUI超时默认值：

no web timeout

指定HTTP端口号，在全局配置模式下，使用以下命令：

http port *port-number*

- *port-number* – 指定HTTP端口号。当使用HTTP方式访问设备时，浏览器的HTTP端口号必须与此处指定的端口号一致。范围是1到65535。默认值是80。

在全局配置模式下，使用该命令no的形式，恢复默认HTTP端口号：

no http port

配置防跨站脚本攻击（anti-xss）服务，在全局配置模式下，使用以下命令：

http anti-xss { **disable** | **enable** | **mode** { **normal** | **strict** } }

- **disable** | **enable** – 启用和禁用防跨站脚本攻击服务。默认情况下，防跨站脚本攻击服务为启用状态。
- **mode** { **normal** | **strict** } – 指定防跨站脚本攻击服务模式。包括字符匹配模式（**normal**）和正则表达式匹配模式（**strict**）。

在全局配置模式下，使用该命令no的形式，恢复防跨站脚本攻击（anti-xss）服务默认值：

no http anti-xss { **disable** | **enable** | **mode** { **normal** | **strict** } }

指定HTTPS端口号，在全局配置模式下，使用以下命令：

https port *port-number*

- *port-number* – 指定HTTPS端口号。当使用HTTPS方式访问设备时，浏览器的HTTPS端口号必须与此处指定的端口号一致。范围是1到65535。默认值是443。

在全局配置模式下，使用该命令no形式恢复默认HTTPS端口号：

no https port

指定HTTPS方式访问时使用的PKI信任域，在全局配置模式下，使用以下命令：

https trust-domain *trust-domain-name*

- *trust-domain-name* – 指定已配置的PKI信任域的名称。当HTTPS启动时，HTTPS服务器将使用指定PKI信任域中的证书。默认情况下，系统将使用缺省PKI信任域trust_domain_default。

在全局配置模式下，使用该命令no的形式恢复默认PKI信任域：

no https trust-domain

显示管理接口配置

用户可以在任何模式下，随时使用show命令查看管理接口配置信息。命令如下：

- 显示Console配置：**show console**
- 显示Telnet配置：**show telnet**
- 显示SSH配置：**show ssh**
- 显示Web配置：**show http**

数据库修复

当数据库不能进行正常的操作时，可尝试通过修复数据库表项来解决。在任意模式下，使用以下命令：

exec database repair [*date*]

- *date* - 指定日期，格式为代表“月/日/年”，例如“1/20/2022”。指定日期后，可修复当天的数据库表项。若不指定，则修复全部数据库表项。

如果数据库表项修复未按预期修复数据库至正常状态，可重置数据库。在任意模式下，使用以下命令：



注意: 重置数据库后, 原有的数据库表将被删除, 请谨慎操作。

配置存储管理

系统提供对设备硬盘存储空间的管理功能, 当存储空间超过指定阈值时, 系统可以帮助用户删除旧日志或停止记录日志。

开启/关闭存储管理功能

开启/关闭设备硬盘存储空间的管理功能, 在全局配置模式下使用以下命令:

- `storage threshold enable`
- `no storage threshold enable`

配置存储管理

设备硬盘存储空间的管理功能开启后, 需要配置存储空间的阈值, 以及当实际存储达到或超过阈值时, 系统将采取的处理方式。

配置存储管理的相关参数, 在全局配置模式使用以下命令:

`storage threshold percent global-value {automatically-overwrite | stop-overwrite} [mode {by-log | global}]`

- `percent global-value` - 指定设备硬盘存储空间的告警阈值百分比, `global-value`取值范围是0.01到90, 即0.01%到90%。
- `automatically-overwrite | stop-overwrite` - 指定实际存储达到或超过阈值时, 系统将采取的处理方式。
 - `automatically-overwrite` - 系统将删除存储在设备硬盘上较早的日志信息, 并存储新的日志信息到硬盘。
 - `stop-overwrite` - 系统将停止存储新的日志信息到硬盘上。
- `mode {by-log | global}` - 指定实际存储阈值的计算方式。
 - `by-log` - 指定存储阈值按每个模块日志单独的存储空间计算。详细介绍, 请参阅“[自定义日志存储空间](#)”。

- **global** - 指定存储阈值按照所有模块日志的存储空间总和计算。当存储在设备硬盘内的所有日志数据占硬盘总空间的百分比达到或超过 *global-value* 时，系统会按照指定的处理方式进行处理。

自定义日志存储空间

当按照各模块日志单独的存储空间计算设备硬盘实际的存储阈值时，系统支持自定义不同模块日志的存储空间阈值。

自定义不同模块日志的存储空间阈值，在全局配置模式下使用以下命令：

```
storage threshold log { configuration | event | health-check | network | traffic gslb | traffic slb } log-value
```

- { **configuration** | **event** | **health-check** | **network** | **traffic gslb** | **traffic slb** } *log-value* - 配置指定模块的日志的存储空间阈值。*log-value*的取值范围是0.01到90，即0.01%到90%。

例如：设备硬盘的存储容量为100G，存储的告警阈值 *global-value* 设置为90（即90%），**configuration**模块的日志存储空间的阈值设置为1（即1%），那么，当 **configuration**模块日志的实际存储容量达到或超过 $100\text{G} \times 90\% \times 1\%$ 时，系统将会对**configuration**模块的日志执行指定的处理动作，并产生告警日志进行提醒。

开启/关闭存储空间告警

当实际的存储容量达到或超过指定阈值时，系统执行相应动作的同时，也将产生告警日志。用户也可以根据实际情况，关闭存储空间的告警提醒。

在全局配置模式下，使用以下命令开启/关闭存储空间的告警功能：

```
storage threshold alert-log { enable | disable }
```

- **enable** - 开启存储空间的告警功能。系统默认开启该功能。
- **disable** - 关闭存储空间的告警功能。

查看硬盘存储管理的配置信息

查看硬盘存储管理的配置信息，在任意配置模式下使用以下命令：

```
show storage threshold
```

配置文件管理

设备的配置信息都被保存在系统的配置文件中。用户通过运行相应的命令或者访问相应的WebUI页面查看设备的各种配置信息，例如设备的初始配置信息和当前配置信息等。配置文件以命令行的格式保存配置信息，并且也以这种格式显示配置信息。

配置设备配置信息

用户可以查看和保存设备的配置信息，也可以导出和导入配置信息。

查看配置信息

配置文件中保存的用来初始化设备的配置信息称作起始配置信息，设备通过读取起始配置信息进行启动时的初始化工作；如果找不到起始配置信息，设备则使用设备的缺省参数初始化。与起始配置信息相对应，设备运行过程中正在生效的配置称为当前配置信息。

系统起始配置信息包括系统的当前起始配置信息（系统启动时使用的配置信息），和系统的备份起始信息。系统纪录最近十次保存的配置信息，最近一次保存的配置信息会纪录为系统的当前起始配置信息，当前系统配置信息以“startup”作为标记。前九次的配置信息按照保存时间的先后以数字0到8作为标记。

查看设备的当前起始配置信息，在任何命令模式下输入以下命令：**show configuration [startup]**

查看设备的备份起始信息，在任何命令模式下使用以下命令：

show configuration backup *number*

- *number* - 备份起始信息的数字标记。

查看设备的当前配置信息，在任何命令模式下输入以下命令：

show configuration

查看设备的当前接口配置信息，在任何命令模式下输入以下命令：

show configuration interface *interface-name*

查看设备的备份起始信息记录，在任何命令模式下输入以下命令：

show configuration record

查看设备的当前运行的配置信息记录，在任何命令模式下输入以下命令：

show configuration running

查看设备的当前地址簿配置信息，在任何命令模式下输入以下命令：

show configuration address

查看设备的当前路由配置信息，在任何命令模式下输入以下命令：

show configuration vrouter

以xml方式输出当前配置信息，在任何命令模式下输入以下命令：

show configuration xml

回退起始配置信息

系统能够纪录最近十次保存的起始配置信息，用户可以根据需要回退到已保存的指定的起始配置信息。系统重启后，系统将会使用该命令指定的配置信息。在执行模式下，使用以下命令：

rollback configuration backup *number*

- *number* - 备份起始配置信息的数字标记。系统将在重启后使用这里指定的起始配置信息。

删除配置文件

用户可以删除设备的起始配置信息。删除起始配置信息，在执行模式下，使用以下命令：

delete configuration {startup | backup *number*}

- **startup** - 删除当前起始配置信息。
- **backup *number*** - 删除指定的备份起始配置信息，*number*为备份起始配置信息的数字标记。

保存配置信息

用户可以保存设备的当前配置信息使其成为设备下次启动时的起始配置。保存设备的当前配置信息，在任何命令模式下输入以下命令：

save [*string*]

- *string* - 对所保存配置信息的描述。如果不使用*string*对保存的配置文件进行描述，系统会直接覆盖原有配置文件。

自动备份配置文件

用户可以通过配置自动备份配置文件功能，能够实现设备定期检查配置文件，在当前配置文件发生变化时，系统会自动将当前的配置文件上传到FTP或TFTP服务器上。

指定自动备份配置文件到FTP服务器，在全局配置模式下，使用以下命令：

```
configuration auto-backup ftp ip-address [user user-name password password] [vrouter vrouter-name] path path [interval time-value]
```

- *ip-address* - 指定FTP服务器的IP地址。
- **user** *user-name* **password** *password* - 指定访问FTP服务器的用户名和密码。
- **vrouter** *vrouter-name* - 指定VRouter的名称。
- **path** *path* - 指定配置文件的上传路径。
- **interval** *time-value* - 指定自动备份配置文件的时间间隔。单位为小时，默认值是1小时。范围是1到7*24小时。如果不指定该参数，系统将每1小时检查配置文件，在发生变化时，自动备份到FTP服务器上。

在全局配置模式下，使用**no configuration auto-backup ftp**取消自动备份配置文件到FTP服务器。

指定自动备份配置文件到TFTP服务器，在全局配置模式下，使用以下命令：

```
configuration auto-backup tftp ip-address [vrouter vrouter-name] path path [interval time-value]
```

在全局配置模式下，使用**no configuration auto-backup tftp**取消自动备份配置文件到TFTP服务器。

查看自动备份配置文件信息

查看自动备份配置文件功能的信息，在任何命令模式下输入以下命令：

```
show configuration auto-backup
```

导出配置信息

用户可以导出系统的当前起始配置信息、备份配置信息及所有VSYN起始配置信息，也可以将可编程脚本、错误页面以及健康检查第三方脚本文件的配置信息与上述配置信息一起打包导出。系统支持用户将系统配置信息或打包后的配置信息（即打包文件）导出到FTP服务器、TFTP服务器或者U盘。

导出系统配置信息到FTP服务器，在执行模式下使用以下命令：

export configuration {**startup** | **backup** *number* | **all-vsys**} **to ftp server** *ip-address* [**vrouter** *vrouter-name*][**user** *user-name* **password** *password*] [*file-name*]

- **startup** | **backup** *number* | **all-vsys** - 指定导出的配置信息。**startup**为导出当前起始配置信息；*number*为导出以*number*为标识的备份配置信息；**all-vsys**为导出所有VSYs当前起始配置信息。
- *ip-address* - 指定FTP服务器的IP地址。
- *vrouter-name* - 导出指定VRouter的配置信息。
- **user** *user-name* **password** *password* - 指定访问FTP服务器的用户名和密码，若不指定，默认使用匿名。
- *file-name* - 指定导出的配置信息文件的名称。

导出打包文件到FTP服务器，在执行模式下使用以下命令：

export configuration-package {**startup** | **backup** *number* | **all-vsys**} **to ftp server** *ip-address* [**vrouter** *vrouter-name*]
[**user** *user-name* **password** *password*] [*file-name*]

导出系统配置信息到TFTP服务器，在执行模式下使用以下命令：

export configuration {**startup** | **backup** *number* | **all-vsys**} **to tftp server** *ip-address* [**vrouter** *vrouter-name*] [*file-name*]

导出打包文件到TFTP服务器，在执行模式下使用以下命令：

export configuration-package {**startup** | **backup** *number* | **all-vsys**} **to tftp server** *ip-address* [**vrouter** *vrouter-name*]
[*file-name*]

导出系统配置信息到U盘，在执行模式下使用以下命令：

export configuration {**startup** | **backup** *number*} **to** {**usb0** | **usb1**} [*file-name*]

导出打包文件到U盘，在执行模式下使用以下命令：

export configuration-package {**startup** | **backup** *number*} **to** {**usb0** | **usb1**} [*file-name*]

导入配置信息

用户可以通过FTP和TFTP服务器导入配置信息，也可以将配置信息放入U盘中，通过设备的USB口导入配置信息。此外，用户可以将系统的打包文件通过上述方式导入。

从FTP服务器导入配置信息，在执行模式下使用以下命令：

import configuration [**all-vsys**] **from ftp server** *ip-address* [**vrouter** *vrouter-name*] [**user** *user-name* **password** *password*]
file-name

- **all-vsyz** - 导入所有VSYS配置信息。
- *ip-address* - 指定FTP服务器的IP地址。
- *vrouter-name* - 为指定的VRouter导入配置信息。
- **user user-name password password** - 指定FTP服务器的用户名和密码，若不指定，默认使用匿名。
- *file-name* - 指定导入的配置信息文件的名称。

从FTP服务器导入打包文件，在执行模式下使用以下命令：

```
import configuration-package [all-vsyz] from ftp server ip-address [vrouter vrouter-name] [user user-name password password] file-name
```

从TFTP服务器导入配置信息，在执行模式下使用以下命令：

```
import configuration [all-vsyz] from tftp server ip-address [vrouter vrouter-name] file-name
```

从TFTP服务器导入打包文件，在执行模式下使用以下命令：

```
import configuration-package [all-vsyz] from tftp server ip-address [vrouter vrouter-name] file-name
```

从U盘导入配置信息，在执行模式下使用以下命令：

```
import configuration [all-vsyz] from {usb0 | usb1} file-name
```

从U盘导入打包文件，在执行模式下使用以下命令：

```
import configuration-package [all-vsyz] from {usb0 | usb1} file-name
```

启用/禁用自动导入USB中配置文件功能

默认情况下，当设备系统启动时，将会自动导入USB中的配置文件，即替换设备中已存在的所有配置文件，包括预定义配置文件和增量配置文件（在预定义配置信息基础上增加的配置信息），用户可以通过命令禁用该功能，取消系统自动从USB中导入配置文件。禁用或启用该功能，在全局配置模式下，使用以下命令：

- **configuration load-by-usb enable** - 启用该功能。
- **configuration load-by-usb disable** - 禁用该功能。



注意:

- 当设备以出厂配置启动时，系统会自动导入USB中的增量配置文件，该增量配置文件名格式必须为“sn-inject_XXX.cong”，其中“sn”表示为设备SN号，“XXX”表示为用户自定义字段，由英文字符、数字或下划线组成，最多不能超过128字节。自动导入后，将会在USB的根目录中记录导入日志信息。
- 自动导入的配置文件必须是UTF-8编码文件且最大不能超过16M。
- 自动导入的配置文件需存放在USB的根目录下。

恢复出厂配置

用户除使用设备上的CLR按键使系统恢复到出厂配置外，也可以使用命令恢复。恢复出厂配置，在任何模式下，使用以下命令：

```
unset all
```



注意: 小心使用该命令。执行该命令后，设备的所有配置将被清除。

切换接口工作模式

ADC设备扩展模块接口的工作模式包括40G、10G和1G接口模式。

当前设备支持10G接口切换到1G接口模式，实现10G接口与1G接口互联。支持切换的扩展模块包括：IOC-AX-2SFP+、IOC-AX-2SFP+-B、IOC-AX-4SFP+、IOC-AX-4SFP+-B、IOC-AX-2SFP+-H、IOC-AX-2SFP+-B-H以及IOC-AX-4SFP+-H模块。其中，IOC-AX-4SFP+-B、IOC-AX-4SFP+-H 模块通过自协商的方式切换接口工作模式。

其他扩展模块切换接口工作模式，需在接口配置模式下，使用以下命令将10G接口工作模式切换为1G：

```
channel-speed 1000
```

在接口配置模式下，使用**no channel-speed** 命令恢复接口默认的10G接口模式。



注意: 在指定接口工作模式前，需要删除接口相关配置。

查看当前对象的配置信息

当用户在某一配置模式下完成指定对象的配置之后，用户可以当前配置模式下，使用**show this**命令查看当前对象的配置信息。

查看光模块状态信息

查看光口模块状态信息，包括SN序列号、功率、温度、电压以及模块类型。在任何命令模式下输入以下命令：

```
show transceiver [interface-name]
```

- *interface-name* – 指定光口模块接口名称。

配置Banner功能

Banner用于显示登录后的声明信息，用户可以自定义Banner信息内容。在全局配置模式下，使用以下命令配置Banner功能：

```
admin login-banner Banner-content
```

- *Banner-content* – 指定Banner信息内容，长度范围是1到4096个字符。执行该命令后，系统创建指定内容的Banner信息；如果已存在Banner信息，则将Banner信息内容修改为指定内容。

使用**no admin login-banner**命令删除Banner信息内容，显示为空。



注意：

- 在编辑Banner信息内容时，如果需要换行，需输入“\n”；需要空格，需输入双引号“ ”。
- 仅支持在使用SSH、Telnet或者Console方式登录设备时显示Banner信息。

系统维护与调试

设备支持网络连接测试工具Ping和Traceroute，当网络出现问题时，用户可以用这些工具对网络进行测试，查找故障原因。设备同时具有调试功能，供用户查阅与分析。

Ping命令

Ping命令主要用于检查网络连接状态以及主机是否可达。用户可以随时在任何CLI命令模式下使用Ping命令，检查网络连接状态及主机是否可达。其使用方法为：

```
ping [ipv6] {ip-address | hostname} [count number] [size number] [source ip-address] [timeout time] [vrouter vrouter-name]
```

- **ipv6** - 指定检查IPv6类型的网络。
- *ip-address | hostname* - 指定接受Ping报文的目的地址，可以是IP地址，也可以是主机名称。在双栈系统固件下，可以是IPv6地址。
- **count number** - 指定发送Ping包的个数。范围是1到65535。默认情况下，系统不限制发送Ping包的个数。
- **size number** - 指定发送Ping包的大小。范围是28到65500字节（byte）。
- **source ip-address** - 指定发送Ping包的源地址，只能是接口名称。
- **timeout time** - 指定发送Ping包的超时时间。范围是0到3600秒。默认值是0，即为没有超时时间限制。
- **vrouter vrouter-name** - 指定发送Ping包的出接口所属的VRouter。默认为缺省VR，即trust-vr。

命令输出结果包括以下两部分：

- 对每个ping报文的响应情况。如果在超时时间到后仍没有收到响应报文，则输出Destination Host Not Responding等，否则显示响应报文中报文序号、TTL和响应时间；如果ping包没有到达目的路由或发送ping包的接口发生变化，则输出Network is unreachable；如果接受Ping报文的目的地址无法解析时，则输出unknown host hostname。
- 最后的统计信息，包括发送报文数、接收报文数、未响应报文百分比、命令执行时间和响应时间的最小、平均、最大和平均偏差值。

以下是Ping命令使用示例：

```
hostname(config)# ping 10.200.3.1

Sending ICMP packets to 10.200.3.1

Seq ttl time(ms)

1 128 2.53

2 128 1.48
```

```
3 128 1.48
4 128 1.47
5 128 1.46

statistics:

5 packets sent, 5 received, 0% packet loss, time 4006ms

rtt min/avg/max/mdev = 1.464/1.689/2.536/0.423 ms
```

Traceroute命令

Traceroute用于测试数据包从发送主机到目的地所经过的网关。它主要用于检查网络连接是否可达，以及分析网络什么地方发生了故障。Traceroute通常的执行过程是：首先发送一个TTL为1的数据包，因此第一跳发送回一个ICMP错误消息以指明此数据包不能被发送（因为TTL超时），之后此数据包被重新发送，TTL为2，同样第二跳返回TTL超时，这个过程不断进行，直到到达目的地。执行这些过程的目的是记录每一个ICMP TTL超时消息的源地址，以提供一个IP数据包到达目的地所经历的路径。

用户可以随时在任何CLI命令模式下使用Traceroute命令测试数据包经过的网关。其使用方法为：

```
traceroute [ipv6] {ip-address | hostname} [numeric] [port port-number] [probe probe-number] [timeout time] [ttl [min-ttl] [max-ttl]] [source interface] [use-icmp] [vrouter vrouter-name]
```

- **ipv6** - 指定对端IP地址的类型为IPv6。
- *ip-address* | *hostname* - 指定traceroute命令的目的地址，可以是IP地址，也可以是主机名称。
- **numeric** - 指定用数字的方式显示地址，而不对地址进行解析。
- **port** *port-number* - 指定UDP端口号。范围是1到65535。默认端口号为33434。
- **probe** *probe-number* - 指定traceroute命令在每一跳发出的探测包的数目。范围是1到65535。默认值是3。
- **timeout** *time* - 指定发送下一个探测包的超时时间。范围是1到3600秒。默认值是5秒。
- **ttl** [*min-ttl*] [*max-ttl*] - *min-ttl*用来指定最小TTL值，范围是1到255，默认值是1。*max-ttl*用来指定最大TTL值，范围是1到255，默认值是30。指定TTL值，用来显示*min-ttl*跳到*max-ttl*跳的回显。
- **source** *interface* - 指定发送traceroute探测包的源地址，只可以是源接口名称。
- **use-icmp** - 指定使用ICMP包进行探测。如不配置该参数，系统将使用UDP包进行探测。

- **vrouter** *vrouter-name* – 指定发送traceroute探测包的出接口所属的VRouter。默认为缺省VRouter，即trust-vr。

以下是使用traceroute命令分析网络情况的示例：

```
hostname(config)# traceroute 210.74.176.150

traceroute to 210.74.176.150 (210.74.176.150), 30 hops max, 52 byte packets
 1 10.200.3.1 (10.200.3.1) 0.572 ms 0.541 ms 0.359 ms
 2 192.168.3.1 (192.168.3.1) 0.601 ms 0.754 ms 0.522 ms
 3 202.106.149.177 (202.106.149.177) 1.169 ms 1.723 ms 1.104 ms
 4 61.148.16.133 (61.148.16.133) 2.272 ms 1.940 ms 2.370 ms
 5 61.148.4.17 (61.148.4.17) 2.770 ms 61.148.4.101 (61.148.4.101) 6.030 ms 61.148.4.21
   (61.148.4.21) 2.584 ms
 6 202.106.227.45 (202.106.227.45) 4.893 ms 5.010 ms 3.917 ms
 7 202.106.193.70 (202.106.193.70) 5.407 ms 202.106.193.126 (202.106.193.126) 4.247 ms
   202.106.193.70 (202.106.193.70) 6.954 ms
 8 61.148.143.30 (61.148.143.30) 3.459 ms 3.758 ms 2.853 ms
 9 * * *
10 * * *
```

从以上示例结果中可以看出，从源主机到目的主机经过了哪些网关，以及哪些网关出现了故障。

系统调试功能

系统调试功能可以帮助用户对错误进行诊断和定位。设备的各种协议和功能基本上都具有相应的调试功能。默认情况下，所有协议和功能的系统调试功能都是关闭的。用户只可以通过CLI对系统调试功能进行配置。

开启Hillstone设备的系统调试功能，请在任何模式下输入以下命令：

```
debug {all | function-name}
```

- **all** – 开启Hillstone设备所有协议和功能的系统调试功能。
- *function-name* – 开启Hillstone设备指定协议或功能的系统调试功能。

在任何配置模式输入以下命令关闭所有或指定功能的系统调试功：

undebug {all | *function-name*}

用户还可以通过双击“ESC”键关闭debug功能。由于部分信息被缓存，关闭过程可能会持续几分钟。

查看调试功能开启或者关闭状态，请在任何模式下输入以下命令：

show debug



注意：调试功能开启后，如果需要在终端输出debug信息，请开启系统的debug日志功能（执行 **logging debug on** 命令）。

查看指定模块内的计数信息，请在任何模式下输入以下命令：

show debug-counter *daemon-name* [clear]

- *daemon-name* - 查看指定模块内的计数信息。
- **clear** - 清除指定模块内的计数信息。

查看指定模块内的缓存信息，请在任何模式下输入以下命令：

show debug-cache *daemon-name* [clear]

- *daemon-name* - 查看指定模块内的debug缓存信息。
- **clear** - 清除指定模块内的debug缓存信息。

配置系统重启

在设备运行过程中，由于各种原因，如系统文件升级等，用户需要重启设备。用户可以通过下电再重新上电重启设备，也可以通过CLI或者WebUI重启设备。

重启设备，请在执行模式下使用reboot命令重启。请参阅以下示例：

```
hostname# reboot
```

```
System configuration has been modified. Save? [y]/n （键入字母“y”或者敲回车键，系统将保存配置；键入字母“n”，系统将不保存配置）
```

```
Building configuration..
```

```
Saving configuration is finished
```

```
System reboot, are you sure? y/[n] （键入字母“y”，系统将重启；键入字母“n”或者敲
```

回车键，系统将返回到执行模式)

执行**reboot**命令时，系统首先会提示用户是否保存先前所做的配置。请谨慎使用**reboot**命令，因为执行该命令会导致网络工作在短时间内中断。

系统版本升级

用户在使用设备的过程中，有时需要升级设备的系统固件系统的版本。本节介绍设备的启动系统以及系统的升级方法。

启动系统介绍

设备的启动系统分为三个部分，分别是Bootloader、Sysloader和OS。它们各自的作用如下：

- Bootloader - Hillstone设备上电后最先运行的程序。Bootloader装载执行StoneOS或者Sysloader。
- Sysloader - 升级OS。
- OS - 设备的操作系统软件。



注意: SG-6000-AX120S/SG-6000-AX120S-GM/SG-6000-AX220S/SG-6000-AX320S/SG-6000-AX320S-GM/SG-6000-AX520S/SG-6000-AX1200S/AX-6000-AX3200S设备无需运行Bootloader，上电后首先运行的是Sysloader。

系统启动后，Bootloader尝试启动系统或者Sysloader。Sysloader实现系统的更新和选择，支持FTP、TFTP以及直接通过USB Host接口升级。Sysloader本身的升级由Bootloader通过TFTP下载完成。

Bootloader的工作模式

Bootloader有两种工作模式，分别是**自动模式**和**交互模式**。

自动模式下Bootloader试图启动配置的系统，如果没有系统或者系统不合法，系统将终止运行，此时用户必须使用Sysloader升级系统。

用户在启动时根据提示按下“ESC”键后，Bootloader进入交互模式。交互模式的主要功能是启动Sysloader。在交互模式下，可以选择启动保存在Flash中的Sysloader，也可以通过TFTP下载新的Sysloader然后启动。

通过网络迅速升级系统（TFTP）

Sysloader可以从TFTP服务器获取系统升级文件，从而保证用户能够通过网络迅速升级。请按照以下步骤进行操作：

给设备上电并且进入Sysloader。参照以下操作提示：

```
HILLSTONE NETWORKS

Hillstone Bootloader 1.3.2 Aug 14 2008-19:09:37

DRAM: 2048 MB

BOOTROM: 512 KB

Press ESC to stop autoboot: 4 （5秒倒计时结束前按“ESC”键）

Run on-board sysloader? [y]/n: y （键入字母“y”或者敲回车键）

Loading: #####
```

从Sysloader的操作选择菜单选择通过TFTP升级StoneOS。参照以下操作提示：

```
Sysloader 1.2.13 Aug 14 2008 - 16:53:42

1 Load firmware via TFTP
2 Load firmware via FTP
3 Load firmware from USB disks (not available)
4 Select backup firmware as active
5 Show on-board firmware
6 Reset

Please select: 1 （在此处键入“1”并敲回车键）
```

依次配置Sysloader的IP地址、TFTP服务器的IP地址、网关IP地址以及系统名称。参照以下操作提示：

```
Local ip address []: 10.2.2.10/16 （输入Sysloader的IP地址并敲回车键）

Server ip address []: 10.2.2.3 （输入TFTP服务器的IP地址并敲回车键）
```

Gateway ip address []: 10.2.2.1（如果Sysloader与TFTP服务器的IP地址不属于同一个网段，输入网关的IP地址并敲回车键；否则直接敲回车键）

File name : SG6000-AX-5.5R6-2.6.img（输入系统名称并敲回车键，系统开始通过TFTP获取）

```
#####  
#####  
  
#####  
#####
```

保存。参照以下操作提示：

File total length 10482508

Checking the image...

Verified OK Save this image? [y]/n: y（键入字母“y”或者敲回车键，保存获得的系统）

Saving

Set SG6000-AX-5.5R6-2.6 as active boot image

重启。系统将使用新的系统文件SG6000-AX-5.5R6-2.6启动。参照以下操作提示：

Please reset board to boot this image

1 Load firmware via TFTP

2 Load firmware via FTP

3 Load firmware from USB disks (not available)

4 Select backup firmware as active

5 Show on-board firmware

6 Reset

Please select: 6（在此处键入“6”并敲回车键，系统开始重启）

设备的Flash中最多可以储存两个系统文件。如果Flash中已经保存了两个，请根据提示对储存的系统文件进行删除。

其它升级方式

通过网络从TFTP服务器获取系统进行升级是最常用的升级方式，同时设备还支持从FTP服务器获取系统。另外，用户还可以将系统文件放入U盘，通过设备的USB Host接口进行升级。

通过FTP服务器获取系统文件

请按照以下步骤在Sysloader中通过FTP升级系统：

1. 进入Sysloader后，从Sysloader的操作选择菜单中选择“2”并敲回车键。
2. 配置Sysloader的IP地址。在“Local ip address [:]”后输入为Sysloader配置的IP地址。敲回车键。
3. 配置FTP服务器的IP地址。在“Server ip address [:]”后输入FTP服务器的IP地址。敲回车键。
4. 如果Sysloader与FTP服务器的IP地址不属于同一个网段，请配置Sysloader的网关IP地址。在“Gateway ip address [:]”后输入网关的IP地址。敲回车键。
5. 在“User Name [anonymous:]”后输入FTP用户名。敲回车键。
6. 在“Password:”后输入用户名对应的密码。敲回车键。
7. 在“File name:”后输入系统文件名称。敲回车键。系统开始通过FTP获取指定的系统文件。
8. StoneOS传输完成后，系统将会询问是否保存该系统文件。键入字母“y”，系统将把该系统保存到设备的Flash中。
9. 保存成功后，系统再次出现Sysloader的操作选择菜单，选择“6”并敲回车键。系统开始使用新的系统文件重新启动。



注意：对于匿名FTP服务器，在“User Name [anonymous:]”和“Password:”后直接敲回车键（第5步和第6步）。

Sysloader菜单介绍

Sysloader使用菜单提示的方式帮助用户完成指定的操作。本节介绍Sysloader中各菜单项的功能。关于Sysloader的菜单选项和功能，请参阅下表：

菜单选项	功能
1 Load firmware via TFTP	通过TFTP升级系统
2 Load firmware via FTP	通过FTP升级系统
3 Load firmware from USB disks	通过U盘升级系统
4 Select backup firmware as active	选择系统中保存的备份系统作为当前的系统启动系统
5 Show on-board firmware	显示系统中保存的系统名称和状态
6 Reset	重新启动系统
7 Reset Administrator password	重置管理员密码。
8 Load sysloader via TFTP	通过TFTP升级sysloader。

在“Please select”提示后键入菜单选项相对应的数字，然后按回车键。按照提示进行操作。

通过CLI升级系统

除了可以在Sysloader中升级系统以外，用户还可以在CLI中通过FTP服务器、TFTP服务器或者U盘升级。

登录进入CLI后，在执行模式下，使用以下命令通过FTP服务器升级：

```
import image from ftp server ip-address [user user-name [password password] ] [vrouter vrouter-name] file-name
```

- *ip-address* – 指定FTP服务器的IP地址。
- **user** *user-name* **password** *password* – 指定FTP服务器的用户名和密码。
- *vrouter-name* - 通过指定的VRouter升级。
- *file-name* – 指定系统文件名称。

登录进入CLI后，在执行模式下，使用以下命令通过TFTP服务器升级：

```
import image from tftp server ip-address [vrouter vrouter-name] file-name
```

升级成功后，重启系统使新的系统文件生效。

配置热补丁升级功能

系统支持在保证业务不中断的情况下，对设备当前软件版本问题进行修复。用户可以通过FTP/TFTP服务器上传补丁文件，将补丁加载至进程中后，激活补丁使之生效。

通过FTP服务器将补丁文件导入到系统中，在全局模式下使用以下命令：

```
import patch from ftp server ip-address [vrouter vrouter] [user user-name password password] filename
```

- *ip-address* – 指定FTP服务器的IP地址。
- [**user** *user-name*] [**password** *password*] – 指定FTP服务器的用户名和密码。
- *filename* – 指定需要导入到系统中的补丁文件的名称。

通过TFTP服务器将补丁文件导入到系统中，在全局模式下使用以下命令：

```
import patch from tftp server ip-address [vrouter vrouter] filename
```

- *ip-address* – 指定TFTP服务器的IP地址。
- *filename* – 指定需要导入到系统中的补丁文件的名称。

将补丁文件导入至系统后，用户可以对补丁进行加载、激活、运行、删除等操作，在任何模式下，使用以下命令：

```
exec patch patch-name { load | unload | delete | activate | deactivate | run | norun }
```

- *patch-name* – 指定需要进行操作的补丁文件的名称。
- **load** – 加载指定名称的补丁文件。
- **unload** – 卸载指定名称的补丁文件。
- **delete** – 删除指定名称的补丁文件。只有处于未加载状态的补丁才能被删除。
- **activate** – 激活指定名称的补丁文件使之生效。若在48小时内重启设备，补丁状态将回退到未加载状态；否则，48小时后，该补丁将自动进入运行状态。
- **deactivate** – 将指定名称的补丁状态回退到去激活状态。
- **run** – 运行指定名称的补丁文件。设备重启后，补丁的状态仍然是运行状态。
- **norun** – 使得指定名称的补丁文件从运行状态变为激活状态。

查看补丁状态，在任何模式下，使用以下命令：

```
show patch
```

备份与恢复配置

当系统升级时，为避免因升级失败而导致数据丢失，系统支持数据备份与恢复功能。该功能可在升级时将数据进行备份；当升级失败后，手动导入数据对其进行恢复，以保证系统的正常运行。目前仅支持将数据备份至指定的FTP服务器。仅T系列平台支持该功能。

在执行模式下，输入以下命令备份数据到指定的FTP服务器：

```
export db-data to ftp server ip-address [vrouter VR-name] {user username password password filename | filename}
```

- *ip-address* - 指定FTP服务器的IP地址。
- **vrouter** *VR-name* - 通过指定的VR备份文件。
- **user** *username* **password** *password* - 指定FTP服务器的用户名和密码。
- *filename* - 指定导出数据文件的名称。如果不指定，则默认版本名称作为文件名。

在执行模式下，输入以下命令从FTP服务器恢复数据：

```
import db-data from ftp server ip-address [vrouter VR-name][user username password password]filename
```

- *ip-address* - 指定FTP服务器的IP地址。
- **vrouter** *VR-name* - 通过指定的VR备份文件。
- **user** *username* **password** *password* - 指定FTP服务器的用户名和密码。
- *filename* - 指定导入的数据文件名称。

升级IP地理库

在全局配置模式下，使用以下命令升级IP地理库：

```
geolocation-IP-signature update {mode {auto | manual} | proxy-server {backup | main} ip-address port | schedule  
{daily [HH:MM] | weekly {sun | mon | tue | wed | thu | fri | sat} [HH:MM] } | server1 {address | domain-name}  
[vrouter vrouter-name] | server2 {address | domain-name} [vrouter vrouter-name] | server3 {address | domain-name}  
[vrouter vrouter-name] }
```

- **mode** {**auto** | **manual**} - 指定升级IP地理库的方式，分为自动升级和手动升级。默认为自动升级。
- **proxy-server** {**backup** | **main**} *ip-address* *port* - 指定升级IP地理库的代理服务器。

- **schedule** {**daily** [*HH:MM*] | **weekly** {**sun** | **mon** | **tue** | **wed** | **thu** | **fri** | **sat**} [*HH:MM*]} - 指定自动升级IP地理库的升级周期。
- **server1** {*address* | *domain-name*} [**vrouter** *vrouter-name*] - 指定升级服务器1的域名、IP地址以及所属的虚拟路由器。
- **server2** {*address* | *domain-name*} [**vrouter** *vrouter-name*] - 指定升级服务器2的域名、IP地址以及所属的虚拟路由器。
- **server3** {*address* | *domain-name*} [**vrouter** *vrouter-name*] - 指定升级服务器3的域名、IP地址以及所属的虚拟路由器。

在执行模式下，使用以下命令，从导入文件升级IP地理库：

```
import geolocation-IP-signature from {ftp server address [user user-name password password | vrouter vrouter-name] | tftp server address [vrouter vrouter-name]} file-name
```

在任何模式下，使用以下命令，立即升级IP地理库：

```
exec geolocation-IP-signature update
```

在任何模式下，使用以下命令，查看升级配置信息：

```
show geolocation-IP-signature {update | info}
```

- **info** - 查看IP地理库信息。
- **update** - 查看IP地理库的升级信息。

在全局配置模式下，使用**no geolocation-IP-signature update {mode | proxy-server {backup | main} | server1 | server2 | server3}**删除IP地理库的升级配置。

配置更新传输协议

系统支持通过HTTP和HTTPS对IP地理库进行更新，默认使用HTTPS协议。配置IP地理库更新的传输协议为HTTP，在全局配置模式下，使用以下命令：

```
geolocation-IP-signature update protocol HTTP
```

在全局配置模式下，使用**no geolocation-IP-signature update protocol HTTP**命令恢复默认的HTTPS模式。

升级域名地理库

在全局配置模式下，使用以下命令升级域名地理库：

```
domain-geo update {mode {auto | manual} | proxy-server {backup | main } ip-address port | schedule {daily [HH:MM] | weekly {sun | mon | tue | wed | thu | fri | sat} [HH:MM]} | server1 {address | domain-name} [vrouter vrouter-name] | server2 {address | domain-name} [vrouter vrouter-name] | server3 {address | domain-name} [vrouter vrouter-name] }
```

- **mode {auto | manual}** - 指定升级域名地理库的方式，分为自动升级和手动升级。默认为自动升级。
- **proxy-server {backup | main } ip-address port** - 指定升级域名地理库的代理服务器。
- **schedule {daily [HH:MM] | weekly {sun | mon | tue | wed | thu | fri | sat} [HH:MM]}** - 指定自动升级域名地理库的升级周期。
- **server1 {address | domain-name} [vrouter vrouter-name]** - 指定升级服务器1的域名、IP地址以及所属的虚拟路由器。
- **server2 {address | domain-name} [vrouter vrouter-name]** - 指定升级服务器2的域名、IP地址以及所属的虚拟路由器。
- **server3 {address | domain-name} [vrouter vrouter-name]** - 指定升级服务器3的域名、IP地址以及所属的虚拟路由器。

在执行模式下，使用以下命令，从导入文件升级域名地理库：

```
import domain-geo-file from {ftp server address[user user-name password password | vrouter vrouter-name] | tftp server address[ vrouter vrouter-name]} file-name
```

在任何模式下，使用以下命令，立即升级域名地理库：

```
exec domain-geo update
```

在任何模式下，使用以下命令，查看域名地理库的升级配置信息：

```
show domain-geo {info | update}
```

- **info** - 查看域名地理库信息。
- **update** - 查看域名地理库的升级信息。

在全局配置模式下，使用`no domain-geo update {mode | proxy-server {backup | main} | server1 | server2 | server3}`删除域名地理库升级配置。

配置更新传输协议

系统支持通过HTTP和HTTPS对域名地理库进行更新，默认使用HTTPS协议。配置域名地理库更新的传输协议为HTTP，在全局配置模式下，使用以下命令：

```
domain-geo update protocol HTTP
```

在全局配置模式下，使用`no domain-geo update protocol HTTP`命令恢复默认的HTTPS模式。

升级ISP信息库

在全局配置模式下，使用以下命令升级ISP信息库：

```
isp-information update {mode {auto | manual} | proxy-server {backup | main} ip-address port | schedule {daily [HH:MM] | weekly {sun | mon | tue | wed | thu | fri | sat} [HH:MM]} | server1 {address | domain-name} [vrouter vrouter-name] | server2 {address | domain-name} [vrouter vrouter-name] | server3 {address | domain-name} [vrouter vrouter-name] }
```

- `mode {auto | manual}` - 指定升级ISP信息库的方式，分为自动升级和手动升级。默认为自动升级。
- `proxy-server {backup | main} ip-address port` - 指定升级ISP信息库的代理服务器。
- `schedule {daily [HH:MM] | weekly {sun | mon | tue | wed | thu | fri | sat} [HH:MM]}` - 指定自动升级ISP信息库的升级周期。
- `server1 {address | domain-name} [vrouter vrouter-name]` - 指定升级服务器1的域名、IP地址以及所属的虚拟路由器。
- `server2 {address | domain-name} [vrouter vrouter-name]` - 指定升级服务器2的域名、IP地址以及所属的虚拟路由器。
- `server3 {address | domain-name} [vrouter vrouter-name]` - 指定升级服务器3的域名、IP地址以及所属的虚拟路由器。

在执行模式下，使用以下命令，从导入文件升级域名地理库：

```
import ispfile from {ftp server address [user user-name password password | vrouter vrouter-name] | tftp server address [vrouter vrouter-name]} file-name
```

在任何模式下，使用以下命令，立即升级ISP信息库：

```
exec isp-information update
```

在任何模式下，使用以下命令，查看ISP信息库的配置信息：

```
show isp-information {info | update}
```

- **info** - 查看ISP信息库信息。
- **update** - 查看ISP信息库的升级信息。

在全局配置模式下，使用**no isp-information update {mode | proxy-server {backup | main} | server1 | server2 | server3}**删除ISP信息库升级配置。

配置更新传输协议

系统支持通过HTTP和HTTPS对ISP信息库进行更新，默认使用HTTPS协议。配置ISP信息库更新的传输协议为HTTP，在全局配置模式下，使用以下命令：

```
isp-information update protocol HTTP
```

在全局配置模式下，使用**no isp-information update protocol HTTP**命令恢复默认的HTTPS模式。

许可证管理

许可证（license）用来授权用户使用一些功能、服务，或者用来扩展性能。

ADC系统的许可证的分类和规则如下：

平台许可证	说明	许可证过期
平台试用许可证 (Platform Trial)	平台许可证是其他许可证运行的基础，如果平台许可证无效，其他许可证均不生效。 设备出厂时已预装15天的试用许可证，支持功能同正式许可证。	到期后，已有的配置不能修改，若设备重启，系统恢复出厂配置。
平台正式许可证 (Platform Base)	设备正式销售后，可以安装平台正式许可证。	到期后，设备仍可正常使用，但不能升级到期后的OS版本。
功能许可证	说明	许可证过期
功能试用许可证	提供GSLB、QoS、LLB等功能的试用。	-

(Feature Trial License)		
全局负载均衡正 式许可证 (GSLB License)	提供全局负载均衡功能。	永久有效。
QoS许可证 (QoS License)	提供QoS功能。	到期后，无法使用功能升级和维护服务。
虚拟系统许可证	授权VSYS的可用数量。	永久有效。
SSL扩展许可证 (SSL Performance License)	提升设备的SSL处理性能。	正式SSL扩展许可证不会过期。试用SSL扩展许可证过期后，如果系统未重启可以正常使用该功能，系统重启后该功能失效。
服务许可证	说明	许可证过期
APP DB 许可证	提供APP库升级功能。APP DB许可证不需要单独申请，随平台许可证一同发放，有效期也同平台许可证。	过期后不能升级APP特征库。

vADC许可证

vADC的许可证机制分为平台许可证、订阅类许可证和功能服务类许可证。平台许可证是功能服务类许可证运行的基础。

平台许可证安装后，设备的SN号将进行变更，即变为虚拟SN（简称“vSN”）。若用户想继续获取功能服务类或订阅类许可证，可通过该vSN号进行申请。vADC重新安装后，许可证不依赖于原系统的SN号，故原先申请的许可证仍可继续使用。同时，Hillstone提供公网许可证服务器，对许可证进行校验及许可证的管理，保证许可证的安全。



注意: 如果您在公有云平台上购买的vADC是内置许可证的版本，那么您无需额外购买许可证，也无需安装许可证，即可获得以下许可证所代表的所有功能。

vADC平台类许可证

vADC系统初始预装有一个免费的默认许可证（default license），无需申请。用户可根据需求申请平台订阅许可证和平台正式许可证。

- **默认许可证（Default）**

vADC预装了一个免费的默认许可证（default license），无需申请。装有默认许可证的系统支持所有的功能，但是性能受限，例如系统HTTP会话连接数仅支持500个等等。该许可证的有效期为30天。到期后，系统的所有功能将不能使用，且系统版本和所有的特征库将不能升级。

- **平台订阅许可证（Platform Sub）**

安装平台订阅许可证后，系统支持的功能和性能与正式许可证相同，但是使用期限较短。具体使用时间，根据申请时协议决定，该使用时间指的是绝对时间，例如2017年3月1日到2017年3月31日。到期后，已有的配置不能修改，重启后仅平台的功能可用，且性能受限。

- **平台正式许可证（Platform Base）**

产品正式销售后，可以安装平台正式许可证。正式许可证提供基础应用交付系统功能，并且vADC性能可达标称数值。到期后，系统仍可正常使用，但不能升级到到期后的系统版本。



注意:

平台许可证过期时，系统安装的订阅许可证和功能服务类许可证仍然有效，但不能升级到到期后的系统版本。

vADC订阅类许可证

订阅类许可证能够控制相关功能是否开启及其使用期限。

- **CPU订阅许可证**

授权vADC可配置的CPU的最大数量。CPU许可证有正式和试用两种类型，正式CPU许可证不会过期。试用许可证过期后，系统将会立即重启，重启后将恢复到最低型号SG-6000-AX02的配置，即2vCPU。

- **iQoS订阅许可证**

开启iQoS功能。许可证过期后，系统重启前iQoS的所有配置不会丢失。

vADC功能服务类许可证

只有购买并安装了各个功能服务类许可证，用户才能使用相应的功能，并能够获取特征库更新。

- 功能试用许可证 (Feature Trial License)

提供提供链路负载均衡功能、全局负载均衡功能、QoS功能的试用。永久有效。

- APP DB 许可证

提供APP库升级功能。APP DB许可证不需要单独申请，随平台许可证一同发放，有效期也同平台类许可证。过期后，不能升级APP特征库。

申请许可证

请遵循以下流程申请许可证：

生成申请许可证所需的许可证请求。在任何模式使用**exec license apply applicant *string***命令生成许可证请求。具体命令描述，请参考“许可证命令”。

将生成的请求发送给Hillstone代理商。

安装许可证

许可证为一串字符串。获得许可证后，用户需要将许可证安装到相应的设备。

在CLI中安装许可证，在任何模式下使用**exec license install *license-string***命令。具体命令描述，请参考“许可证命令”。许可证正确安装完后，用户需重启设备以使许可证生效。



注意: 系统允许用户卸载已安装的许可证。但是强烈建议用户不要对许可证进行卸载。

许可证命令

本节具体描述申请、安装和卸载许可证所需的命令。

生成许可证请求

生成申请许可证所需的许可证请求，请在任何模式下使用以下命令：

exec license apply applicant *string*

- *string* – 申请人名称。

安装/卸载许可证

获得许可证后，用户可在任何模式下通过使用以下命令安装许可证：

```
exec license install license-string
```

- *license-string* – 要安装的许可证字符串。

卸载许可证，在任何模式下使用以下命令：

```
exec license uninstall license-name
```

- *license-name* – 要卸载的许可证名称。

安装许可证后，输入命令**reboot**使系统重启。许可证将在重启后生效。

许可证校验

vADC安装许可证后，需连接到LMS（许可证管理系统），进行合法性校验，以防止许可证被克隆。目前系统支持两种校验方式，分别是通过互联网连接到公网LMS进行校验和通过局域网连接到内网LMS进行校验，用户可根据需要选择其中的一种方式。

- 通过公网LMS校验适用于小型私有云或公有云场景。vADC连接到公网LMS后，公网LMS将提供许可证的合法性校验（目前公网LMS暂不提供许可证的分发和管理）。若发现克隆许可证的行为，克隆设备（安装许可证较晚的设备）将会立即被重启。
- 通过局域网LMS校验适用于大型私有云或行业云场景。vADC连接到内网LMS后，内网LMS不仅能提供许可证的校验，还可提供许可证的自动分发和管理。若发现克隆许可证的行为，克隆设备（安装许可证较晚的设备）上的许可证将会被卸载，同时设备也将立即被重启。

若vADC未连接到LMS进行校验，设备将会每隔30天进行重启。

连接到LMS进行合法性验证，在任何模式下使用以下命令：

```
exec lms enable { public | private ip A.B.C.D port port-number }
```

- **public** – 指定云•界通过公网LMS进行许可证校验。
- **private ip** *A.B.C.D* – 指定云•界通过内网LMS进行许可证校验，并指定内网LMS的IP地址。
- **port** *port-number* – 指定连接内网LMS的端口号，取值范围为1到65535，默认为8001。

许可证将在设备重启后生效，若此前未重启过，连接LMS成功后，可输入命令**reboot**重启设备。

断开与LMS的连接，在任何模式下使用以下命令：

```
exec lms disable
```



注意：通过公网LMS进行许可证验证时，请保证连接公网LMS的接口在trust-vr安全域内并且通过trust-vr安全域可以访问互联网。

显示vADC与LMS的连接信息

在任意模式下，使用以下命令查看vADC与LMS的连接信息：

```
show lms
```

许可证灌装介绍

许可证灌装方法适用于需要给大批设备安装许可证的情况。使用许可证灌装可以简化大批量设备安装许可证的操作步骤，减少错误的发生。

许可证灌装操作

许可证灌装操作步骤如下：

1. 拥有大批量设备的用户提供设备序列号以及需要的许可证类型。具体许可证信息请咨询当地代理商。
2. 山石网科获得许可证信息后，生成相应的许可证文件，并将许可证文件通过适当的方式发送给客户，例如通过邮件。
3. 用户获得许可证文件后，将许可证文件拷贝到格式为FAT32的U盘中，拷贝路径为“\license”。目录名称“license”区分大小写（必须为全部小写）且不可更改。拷贝许可证文件时不可修改许可证书写格式，否则将无法安装许可证。
4. 用户利用存有许可证文件的U盘为所有设备安装许可证。具体安装步骤请参考下节内容。

许可证安装

用户将许可证文件拷贝到U盘的正确位置后，将U盘插入设备的USB口，设备将自动扫描U盘并安装许可证。用户可以根据指示灯状态判断许可证安装状态。具体步骤如下：

启动设备，进入运行状态（出现“login”提示符）。

将存有许可证文件的U盘插入设备的USB口。

设备扫描U盘信息，寻找与其序列号相同的许可证，找到后自动安装相应的许可证。通过设备的ALM指示灯可判断许可证安装状态，指示灯闪烁方式以及含义如下表所示：

设备说明	ALM指示灯状态
设备从U盘的“license”目录下中发现匹配的许可证	绿色闪烁持续到许可证安装完成
许可证安装完成	恢复之前状态
设备未从U盘的“license”目录下中发现匹配的许可证	红色闪烁保持10秒后恢复之前状态
设备未从U盘中找到“license”目录	保证原状态不变

许可证安装完毕取出U盘，然后用同样的方法为其他设备安装许可证。

U盘中所有和设备相匹配的许可证都会被自动安装到设备上，同时已经安装的许可证将被自动移动到U盘的“license_installed”目录（自动创建）下，避免重新插入U盘后再次扫描并安装重复的许可证。

重启设备，使许可证生效。

简单网络管理协议（SNMP）

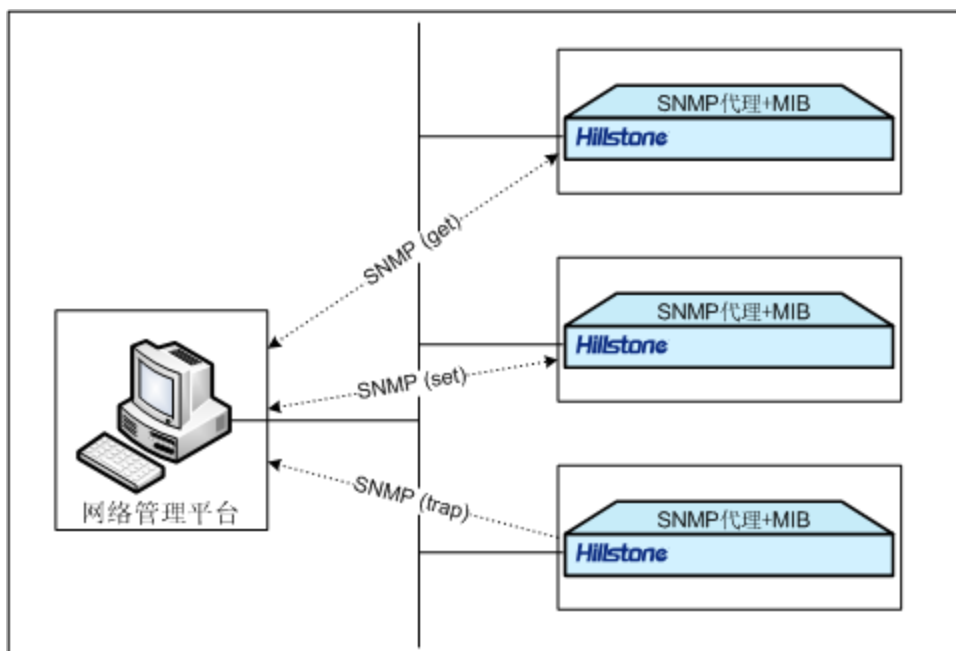
简单网络管理协议（SNMP，Simple Network Management Protocol）是应用层协议，它通过标准框架、公共语言和相对应的安全机制来监控和管理网络设备。SNMP的体系结构包括网络管理平台、SNMP代理、网络管理协议和管理信息库（MIB，Management Information Base）四部分。

- 网络管理平台：是一个通过网络管理软件（如adventnet、solarwinds等）向SNMP代理发出Get和Set报文并接收代理的应答，以达到管理和监控网络设备目的的系统。
- SNMP代理：是运行在被管理网络设备上的一个软件模块，用来维护被管理设备的信息数据并在需要时把管理数据发送给网络管理平台。
- 网络管理协议：网络管理平台 and SNMP代理之间是通过网络管理协议连接的，通过SNMP报文的形式来交换信息。协议主要支持Get、Set和Trap三种功能，Get用于管理平台获取代理的MIB对象值，Set用于管理平台去设置代理的MIB对象值，Trap用于代理向管理平台通告重要事件。

- 管理信息库（MIB）：是由SNMP代理维护的有关网络设备的信息数据库，信息库里的内容可供网络管理平台查询或设置其中变量的值。

山石网科设备的SNMP功能

山石网科设备拥有SNMP代理功能，该SNMP代理功能能够接受网络管理平台的操作请求并反馈网络和设备的相应信息。下图为SNMP管理框架在山石网科设备中实现的示意图：



SNMP版本

山石网科设备支持以下版本的SNMP：

- SNMPv1协议，具体描述请参阅RFC-1157，A Simple Network Management Protocol。
- SNMPv2协议，具体描述请参阅RFC-1901，Introduction to Community-based SNMPv2；RFC-1905，Protocol Operations for Version 2 of the Simple Network Management Protocol；RFC-1906，Transport Mappings for Version 2 of the Simple Network Management Protocol。
- SNMPv3协议，具体描述请参阅RFC2263，SNMPv3 Applications；RFC2264，User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)；RFC2265，View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)。

SNMPv1和SNMPv2c都使用了团体字的认证方式，可以限制网络管理平台获取设备信息。SNMPv3引入了基于用户的安全模型用于保证消息安全及基于视图的访问控制模型用于访问控制。

MIB信息库

山石网科设备支持RFC-1213中定义的所有相关的管理信息库组（Management Information Base for Network Management of TCP/IP-based Internets: MIB-II）和RFC-2233中定义的使用SMIv2的接口组MIB（The Interfaces Group MIB using SMIv2: IF-MIB）。此外，系统提供一个私有MIB库，MIB库中包含山石网科设备的系统信息、IPSec VPN信息以及系统统计信息，用户可以将其导入到管理主机的MIB浏览器，进行使用。

Trap报文信息

山石网科设备的SNMP代理功能在设备发生异常情况时，会主动向网络管理平台发送Trap报文报告所发生的事件。山石网科设备的SNMP代理可以生成以下各种trap信息：

- 热启动trap
- SNMP验证失败trap
- 端口状态改变trap
- VPN SA协商状态改变trap
- HA状态改变trap
- 系统状态改变trap，如CPU使用率超过80%的trap、风扇状态改变trap、内存过低trap等
- 网络攻击trap，如ARP欺骗攻击trap、IP地址欺骗攻击trap、SYN Flood攻击trap等
- 配置改变trap



注意：根VSYS支持所有私有Trap信息。非根VSYS支持部分私有Trap信息。

配置SNMP

设备的SNMP配置包括以下各项：

- 开启或者关闭SNMP代理功能
- 配置SNMP代理设备端口号
- 配置SNMP引擎ID
- 创建SNMPv3用户组
- 创建SNMPv3用户
- 配置管理主机地址
- 配置trap报文目标主机地址
- 配置管理员的标识及联系方法
- 配置山石网科设备位置
- 指定启用SNMP功能的虚拟路由器

开启或者关闭SNMP代理功能

默认情况下，系统的SNMP代理功能是关闭的。开启山石网科设备的SNMP代理功能，请在全局配置模式下使用以下命令。用该命令no的形式关闭SNMP代理功能。

- **snmp-server manager**
- **no snmp-server manager**

配置SNMP代理设备端口号

配置SNMP代理设备端口号，在全局配置模式下，使用以下命令：

snmp-server port *port-number*

- *port-number* – 指定SNMP代理设备的端口号。范围为1到65535。默认值为161。

配置SNMP引擎ID

SNMP引擎ID唯一标识一个引擎，SNMP引擎是SNMP实体（网络管理平台或者被管理网络设备）的重要组成部分，完成SNMP消息的收发、验证、提取PDU、组装消息与SNMP应用程序通信等功能。配置本地设备的

SNMP引擎ID，在全局配置模式下使用以下命令：

```
snmp-server engineID string
```

- *string* – 指定引擎ID号。取值范围为1到23个字符。

创建SNMPv3用户组

配置SNMPv3用户组，请在全局配置模式下使用以下命令：

```
snmp-server group group-name v3 {noauth | auth | auth-enc} [read-view read-view] [write-view writeview]
```

- *group-name* – 指定用户组的名称。取值范围为1到31个字符。
- **noauth** | **auth** | **auth-enc** – 指定用户组的安全级别。可以为noAuth、Auth或者Auth-Enc。安全级别决定了在处理一个SNMP数据包时所采用的安全机制。noAuth即无认证和加密；Auth提供基于MD5或SHA算法的认证；Auth-Enc提供基于MD5或SHA算法的认证和基于AES和DES的报文加密。
- **read-view** *read-view* – 指定该用户组的只读MIB视图名。如不指定该参数，系统默认为空。
- **write-view** *writeview* – 指定该用户组的可写MIB视图名。如不指定该参数，系统默认为空。

系统最多允许配置5个用户组，且每个用户组最多可包含5个用户。在全局配置模式下使用**no snmp-server group group-name**命令删除指定的用户组。

创建SNMPv3用户

配置SNMPv3用户，请在全局配置模式下使用以下命令：

```
snmp-server user user-name group group-name v3 remote remote-ip [auth-protocol {md5 | sha} auth-pass [enc-protocol {des | aes} enc-pass]]
```

- **user** *user-name* – 指定用户名称。取值范围为1到31个字符。
- **group** *group-name* – 为所创建的用户指定已经配置好的用户组。
- **remote** *remote-ip* – 指定远程管理主机的IP地址。
- **auth-protocol** {**md5** | **sha**} – 指定用户安全级别为需要认证且认证协议可以为MD5或SHA算法。如不输入此参数，则默认是无认证，无加密模式。

- *auth-pass* – 指定认证密码。取值范围为8到40个字符。
- **enc-protocol** {*des* | *aes*} – 指定用户安全级别为加密且加密协议为DES或者AES。
- *enc-pass* – 指定加密密码。取值范围为8到40个字符。

系统最多允许配置25个用户。在全局配置模式下使用**no snmp-server user** *user-name*命令删除指定的用户。

配置管理主机地址

配置管理主机地址，请在全局配置模式下使用以下命令：

```
snmp-server host { ip-address | ip-address/mask | range start-ip end-ip } {version [1 | 2c] community string [ro | rw] | version 3}
```

- *ip-address* | *ip-address/mask* | **range** *start-ip end-ip* – 指定管理主机的IP地址或IP地址范围。
- **version** [*1* | *2c*] – 指定SNMP的版本为SNMPv1或者SNMPv2C。
- **community string** – 团体字是管理进程和代理进程之间的口令，因此与Hillstone设备认可的团体字不符的SNMP报文将被丢弃。该参数指定主机的团体字，取值范围为一个最多31位的字符串，且仅当SNMP为v1和v2C版本时有效。
- **ro** | **rw** – 指定该团体字的读写权限。**ro**为只读，此类团体字只可读取MIB中的信息；**rw**为可读可写，此类团体字不仅可以读取MIB中的信息，还可以对信息进行修改。此项为可选，默认情况下，团体字的访问权限为只读。
- **version 3** – 指定SNMP的版本为SNMPv3。

全局配置模式下使用**no snmp-server host** {*host-name* | *ip-address* | *ip-address/mask* | **range** *start-ip end-ip*}命令删除指定的管理主机。

配置trap报文目标主机地址

用户可以配置接收SNMP trap报文的主机。配置SNMP trap报文目标主机地址，请在全局配置模式下使用以下命令：

```
snmp-server trap-host { host-ip } {version {1 | 2c} community string | version 3 user user-name engineID string } [port port-number]
```

- *host-ip* – 指定trap报文目标主机的IP地址。
- **port** *port-number* – 指定接收trap报文的目標主机端口号。取值范围为1到65535，默认值为162。
- **version** {1 | 2c} – 指定使用SNMPv1或者SNMPv2C发送trap报文。
- **community** *string* – 指定SNMPv1或者SNMPv2C的团体字。
- **version** 3 – 指定使用SNMPv3发送trap报文。
- **user** *string* – 指定已配置的SNMPv3用户名。
- **engineID** *string* – 指定trap报文目标主机的引擎ID号。
- **port** *port-number* – 指定接收trap报文的目標主机端口号。取值范围为1到65535，默认值为162。

在全局配置模式下使用**no snmp-server trap-host** {*host-name* | *ip-address*} 命令删除指定的trap报文目标主机。

配置管理员的标识及联系方法

sysContact即系统联络，是MIB II中系统组的一个管理变量，内容为被管理设备（此处为Hillstone设备）相关人员的标识及联系方法。用户可以通过配置此参数，将重要信息存储在Hillstone设备中，以便出现紧急问题时查询使用。配置管理员的标识及联系方法，请在全局配置模式下使用以下命令：

snmp-server contact *string*

- *string* – 描述系统联络信息的字符串。取值范围为1到255个字符。

在全局配置模式下使用**no snmp-server contact**命令该系统联系信息。

配置山石网科设备位置

sysLocation是MIB中系统组的一个管理变量，用于表示被管理设备（此处为山石网科设备）的位置。指定山石网科设备的位置，请在全局配置模式下使用以下命令：

snmp-server location *string*

- *string* – 描述山石网科设备位置的字符串。取值范围为1到255个字符。

在全局配置模式下使用**no snmp-server location**命令删除系统位置信息。

指定启用SNMP功能的VRouter

用户可以指定启用SNMP功能的VRouter。指定启用SNMP功能的VRouter，请在全局配置模式下使用以下命令：

```
snmp-server vrouter vrouter-name
```

- *vrouter-name* – 指定VRouter的名称。

在全局配置模式下使用**no snmp-server vrouter**命令关闭指定VRouter的SNMP功能。

配置设备历史最大会话数功能

启用设备历史最大会话数功能后，用户可以通过SNMP网络管理平台获取设备的历史会话数的最大值，即指定时间间隔内的最大会话数。

配置设备历史最大会话数功能，需先进入SNMP代理的配置模式，在全局配置模式下，使用以下命令：

- **snmp-agent** - 进入设备作为SNMP代理的配置模式。

在SNMP代理的配置模式下，使用以下命令，配置设备历史最大会话数功能：

```
session-history-max-number enable [interval value]
```

- **enable** - 启用设备历史最大会话数功能。
- *value* - 指定统计设备历史会话数最大值的时间间隔，取值范围是1到10080分钟，默认值为1分钟。

例如：启用该功能，并且指定*value*为5，那么从启用该功能的时刻开始，历史最大会话数初始值即为当前设备会话数，系统会实时更新当前设备会话数，并实时与历史最大会话数进行对比，记录下两者中的较大值即为历史最大会话数；经过设置的5分钟的时间间隔，设备将第六分钟初始时的当前设备会话数作为历史最大会话数初始值，重新执行以上流程，记录5分钟内的最大会话数，以此类推。

在SNMP代理的配置模式下，使用**no session-history-max-number enable** [*interval*]命令取消配置。

显示SNMP信息

用户可以在任何模式下通过以下命令查看SNMP的相关配置信息：

- 显示山石网科设备的SNMP配置信息：`show snmp-server`
- 显示山石网科设备的SNMPv3用户组信息：`show snmp-group`
- 显示山石网科设备的SNMPv3用户信息：`show snmp-user`

网络时间协议（NTP）

网络时间协议（Network Time Protocol），简称为NTP。NTP为整个网络传递统一、标准的时间。实现方法是在网络上指定若干时钟源，为用户提供授时服务，并且这些时钟服务器间能够相互对比以提高准确度。NTP协议采用UDP传输协议格式，使用专用端口123。



注意: 关于NTP确保时钟同步的精确性的算法，请参阅RFC1305规范。

设备的时间影响到设备的许多功能模块，例如VPN隧道的建立、时间表功能的实现以及自签名证书的使用等，因此系统时间的精确性十分重要。为保证设备系统能够一直保持精确时间，设备允许用户通过NTP来使系统时间与网络上的NTP服务器同步。设备支持两种设置时间的方式，分别是手动设置和通过NTP与服务器同步。



注意: 为保证自签名证书时间的正确性，避免证书使用错误，初次使用设备时，请务必将设备时间与PC时间同步。

手动配置时间

手动配置系统的时间，在全局配置模式下，使用以下命令：

clock time *HH:MM:SS Month Day Year*

- *HH:MM:SS Month Day Year* - 指定系统时间。*HH*、*MM*和*SS*分别表示小时、分钟和秒，*Month*、*Day*和*Year*分别表示月、日和年。

手动配置时区

系统提供多个预定义时区，同时，为实现更精确的时区配置，系统支持自定义时区配置，并且，用户可以为自定义时区指定夏令时。

系统的默认时区是东8区。为系统指定时区，在全局配置模式下，使用以下命令：

clock zone { *timezone-name* | *cus-timezone-name* *hours minutes* }

- *timezone-name* - 指定预定义时区名称。
- *cus-timezone-name* - 指定自定义时区名称，范围是1到6个字符。
- *hours minutes* - 为自定义时区指定相对UTC（Universal Time Coordinated，协调世界时）时间的偏移量。
hours的取值范围是-13到12；minutes的取值范围是0到59。

例如：

自定义时区为test，其相对UTC的偏移量是6小时30分：

```
hostname(config)# clock zone test 6 30
```

配置夏令时

夏令时（summer-time）是为节约能源而人为规定的地方时间制度。按国家法令，在夏季及其前后实施。一般在天亮早的夏季人为将时间提前一小时，夏季结束再将时间调回一小时。用户可以为系统自定义时区指定夏令时的绝对时间段和循环时间段。

为系统指定夏令时的绝对时间段，在全局配置模式下，使用以下命令：

clock summer-time *cus-timezone-name* **date** *start-date start-time end-date end-time* [*compensation-time*]

- *cus-timezone-name* - 指定自定义时区名称，范围是1到6个字符。
- **date** - 指定夏令时的绝对时间段。
- *start-date* - 指定夏令时起始日期。书写格式为“月/日/年”，例如7/20/2011。
- *start-time* - 指定夏令时起始时间。书写格式为“小时：分钟”，例如10:30。
- *end-date* - 指定夏令时终止日期。书写格式为“月/日/年”，例如7/20/2011。
- *end-time* - 指定夏令时终止时间。书写格式为“小时：分钟”，例如10:30。
- *compensation-time* - 指定夏令时生效时的时间补偿，默认值为0。例如夏令时开始时，某些地区时间须调快1小时30分；夏令时结束时，时间须调慢1小时30分。“1小时30分”即为夏令时生效时的时间补偿。书写格式为“小时：分钟”，例如1:30。

例如：

自定义时区test的夏令时从6/22/2011的10:30开始，到9/23/2011的10:00结束。夏令时期间的时间将比非夏令时期间的时间快2小时30：

```
hostname (config) # clock summer-time test date 6/22/2011 10:30 9/23/2011 10:00 2:30
```

为系统指定夏令时的循环时间段，即在每年的指定时间段内，执行夏令时。在全局配置模式下，使用以下命令：

```
clock summer-time cus-timezone-name recurring { [Mon] | [...] | [Sun] } {after | before} start-day start-month start-time { [Mon] | [...] | [Sun] } {after | before} end-day end-month end-time [compensation-time]
```

- *cus-timezone-name* – 指定自定义时区名称，范围是1到6个字符。
- **recurring** – 指定夏令时的循环时间段。
- { [Mon] | [...] | [Sun] } {after | before} *start-day start-month start-time* – 指定夏令时循环时间段的起始时间。例如命令关键字为Mon before 22 6 10:30，即夏令时起始时间为每年6月22日前的第一个周一的10:30。
- { [Mon] | [...] | [Sun] } {after | before} *end-day end-month end-time* – 指定夏令时循环时间段的终止时间。例如命令关键字为Fri after 23 9 10:00，即夏令时终止时间为每年9月23日后的第一个周五的10:00。
- *compensation-time* – 指定夏令时生效时的时间补偿，默认值为0。例如夏令时开始时，某些地区时间须调快1小时30分；夏令时结束时，时间须调慢1小时30分。“1小时30分”即为夏令时生效时的时间补偿。书写格式为“小时：分钟”，例如1:30。

例如：

自定义时区test的夏令时在从每年的6月22日前的第一个周一的10:30开始，到9月23日后的第一个周五的10:00结束。夏令时期间的时间将比非夏令时期间的时间快2小时30：

```
hostname (config) # clock summer-time test recurring Mon before 22 6 10:30 Fri after 23 9 10:00 2:30
```



注意：夏令时的配置会对日志和基于时间的功能模块产生影响。例如，当9/23/2011的10:00夏令时结束时，系统时间将自动调慢2小时30分，恢复为非夏令时期间的7:30。这样，9/23/2011的7:30到10:00在这一天会出现两次。

使用**no clock summer-time** *cus-timezone-name* **date**命令取消夏令时的配置。

查看系统时间配置信息

在CLI任何命令模式下使用**show clock**命令，查看当前的时区配置信息。

在CLI任何命令模式下使用**show config**命令，查看当前的夏令时配置信息。

配置NTP功能

通过NTP配置，可以使Hillstone设备的系统时间与时钟服务器同步。在Hillstone设备上可以做的NTP配置有以下各项：

- 开启/关闭NTP功能
- 配置NTP服务器
- 配置最大调整时间
- 配置查询间隔
- 开启/关闭身份验证功能
- 配置NTP身份验证功能

开启/关闭NTP功能

默认情况下，系统的NTP功能是关闭的。在Hillstone设备上开启或者关闭NTP功能，在全局配置模式下使用以下命令：

- 启用：**ntp enable**
- 禁用：**no ntp enable**

配置NTP时钟服务器

用户最多可以指定3个时钟服务器，同时可以使用**prefer**关键字指定主时钟服务器（Hillstone设备首先与主服务器进行时间同步）；如果没有为服务器指定**prefer**关键字，Hillstone设备会使用户最先配置的服务器做时间同步。

配置NTP时钟服务器，在全局配置模式下输入以下命令：

```
ntp server {ip-address | host-name} [key number] [source interface-name] [prefer] [vrouter vrouter-name]
```


- *ip-address | host-name* – 指定时钟服务器的IP地址或主机名称。主机名称取值范围为1到127个字符。
- *key number* – 指定可以通过该服务器的验证密钥。如果要在配置的时钟服务器上使用NTP身份验证功能，用户必须指定key参数值。
- *source interface-name* – 指定Hillstone设备上发送和接收NTP包的接口。
- *prefer* – 如果指定了多个时钟服务器，该关键字用来指定该服务器为主时钟服务器。Hillstone设备首先与主服务器进行时间同步，如果失败，再查找下一个时钟服务器。
- *vrouter-name* - 为指定的VRouter指定时钟服务器。

使用**no ntp server** *{ip-address | host-name}*命令取消指定时钟服务器的配置。

以下是时钟服务器配置示例：

```
hostname(config)# ntp server 10.160.64.5 prefer
```

配置最大调整时间

如果Hillstone设备和NTP时钟服务器的时间差在最大调整时间之内，就能成功进行时间同步，否则同步不成功。配置最大调整时间，在全局配置模式下，输入以下命令：

ntp max-adjustment *time-value*

- *time-value* – 最大调整时间值。范围是0到3600秒，0表示没有时间限制。默认值是10秒。

使用**no ntp max-adjustment**命令恢复最大调整时间的默认值。

配置查询间隔

设备每隔一个查询间隔就与时钟服务器做一次同步，保证设备系统时间的准确。配置查询间隔，在全局配置模式下，输入以下命令：

ntp query-interval *time-interval*

- *time-interval* – 查询间隔值。范围是1到60分钟。默认值是5分钟。

使用**no ntp query-interval**命令恢复查询间隔的默认值。

开启/关闭身份验证功能

默认情况下，系统的NTP身份验证功能是关闭的。在Hillstone设备上开启或者关闭NTP身份验证功能，在全局配置模式下使用以下命令：

- 启用：**ntp authentication**
- 禁用：**no ntp authentication**

配置NTP身份验证功能

使用NTP身份验证功能，用户需要配置MD5身份验证密钥ID和密钥。启动该功能后，设备只会与通过验证的服务器进行同步。配置NTP验证密钥ID和密钥，请在全局配置模式下，输入以下命令：

ntp authentication-key *number* md5 *string*

- *number* - 验证密钥ID，范围是从1到65535；
- *string* - MD5验证密钥，范围是1到31个字符。

在全局配置模式下，使用**no ntp authentication-key *number***命令取消验证密钥的配置。

查看NTP状态

NTP配置完成后，在任何模式下运行**show ntp status**命令可以查看当前的NTP配置信息和NTP状态。

查看NTP的调试信息

查看NTP的调试信息，在任何模式下，使用以下命令：

debug ntp {events | packet}

- **events** - 查看NTP的基本调试信息。
- **packet** - 查看NTP报文的调试信息。

配置时间表功能

设备支持时间表（Schedule）功能。时间表功能可以使策略规则在指定的时间生效，也可以控制PPPoE接口与因特网的连接时间。时间表包含绝对计划和周期计划。周期计划通过周期条目指定时间表的时间点或者时间段；而绝对计划决定周期计划的生效时间。每个周期计划最多可以拥有16条周期条目。

创建时间表

创建一个时间表，在全局配置模式下，使用以下命令：

```
schedule schedule-name
```

- *schedule-name* - 指定时间表的名称。范围是1到31个字符。

执行该命令后，系统创建指定名称的时间表并且进入时间表配置模式；如果指定的名称已存在，则直接进入时间表配置模式。在时间表配置模式下，用户可以配置时间表的周期和绝对时间。

使用**no schedule** *schedule-name*命令删除指定的时间表。删除时间表之前，请从其它模块中取消对该时间表的引用。

指定绝对计划

绝对计划是一个时间范围，指定的周期计划会在绝对计划的时间范围内生效。同时，用户也可以不启用绝对计划功能，此时周期计划会在被应用到系统中某项功能上时，立即生效。指定绝对计划，在时间表配置模式下，使用以下命令：

```
absolute {[start start-date start-time] [end end-date end-time]}
```

- **start** *start-date start-time* - 指定绝对计划的开始时间点，包括日期和具体时间。*start-date*为开始的日期，书写格式为“月/日/年”，例如10/23/2007；*start-time*为开始的具体时间，书写格式为“小时：分钟”，例如15：30。如果不指定该参数的值，开始时间为当前时间。
- **end** *end-date end-time* - 指定绝对计划的结束时间点，包括日期和具体时间。*end-date*为结束的日期，书写格式为“月/日/年”，例如11/05/2007；*end-time*为结束的具体时间，书写格式为“小时：分钟”，例如09：00。如果不指定该参数的值，则无结束时间，周期会从开始时间起，一直有效。

使用**no absolute**命令关闭绝对计划功能，使周期计划能够即时生效。

指定周期计划

周期计划的时间是该周期计划中周期条目的总和。一个周期计划中最多可以添加16个条周期条目。用户可以配置三种类型的周期条目：

- 每天：每天的指定时间。例如每天的9：00到18：00。
- 每周的某几天：一周中指定天的指定时间。例如每周一、周二和周六的9：00到13：30。
- 每周一段时间：一周中的一个连续时间段。例如从周一早上9：30到周三下午15：00。

指定“每天”或者“每周的某几天”类型周期条目，在时间表配置模式下，使用以下命令：

periodic {**daily** | **weekdays** | **weekend** | [**monday**] [...] [**sunday**]} *start-time to end-time*

- **daily** - 每一天（周一到周日）。
- **weekdays** - 工作日（周一到周五）。
- **weekend** - 周末（周六到周日）。
- **monday** [...] [**sunday**] - 选择需要的日期。例如选择周二、周三和周六，命令关键字为**tuesday wednesday saturday**。
- *start-time* - 开始时间。书写格式为“小时：分钟”，例如09：00。
- *end-time* - 结束时间。书写格式为“小时：分钟”，例如16：30。

使用多条该命令添加多个“每天”或者“每周的某几天”类型周期条目。

使用**no periodic** {**daily** | **weekdays** | **weekend** | [**monday**] [...] [**sunday**]} *start-time to end-time*命令删除指定的周期条目。

指定“每周一段时间”类型周期条目，在时间表配置模式下，使用以下命令：

periodic {[**monday**] | [...] | [**sunday**]} *start-time to* {[**monday**] | [...] | [**sunday**]} *end-time*

- [**monday**] | [...] | [**sunday**] - 开始日期，可以是周一到周日的任意一天。
- *start-time* - 开始时间。书写格式为“小时：分钟”，例如09：00。

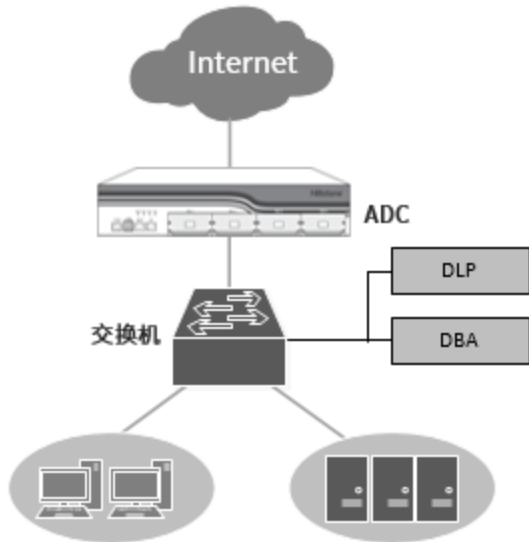
- `[monday] | [...] | [sunday]` - 结束日期，与开始日期相同或者晚于开始日期。
- `end-time` - 结束时间。书写格式为“小时：分钟”，例如16：30。

使用多条该命令添加多条“每周一段时间”类型周期条目。

使用`no periodic {[monday] | [...] | [sunday]} start-time to {[monday] | [...] | [sunday]} end-time`命令删除指定的周期条目。

HSCP协议

HSCP协议是山石网科私有协议。在部分网络场景中（例如下图所示），除了串接到网络中的安全设备（如防火墙、ADC、WAF、NIPS设备等）可以对流量进行安全阻断；旁路监听模式下的设备或其他安全产品（如DLP、DBA设备），由于网络流量不经其转发，无法对威胁主机、流量进行阻断。通过HSCP协议封装威胁报文信息发送给ADC设备，在ADC设备上添加对应的阻断规则，实现对此类设备的威胁阻断。



HSCP协议的配置包括本端和对端配置，本端只有1个，对端可存在多个。

- 本端：即ADC设备
- 对端：与ADC设备协作的其他网络安全产品

注意：使用HSCP协议，需同时开启接口的HSCP管理方式。

配置HSCP协议

配置HSCP协议，包括：

- **HSCP本端端口**：在全局配置模式下，使用`hscp port port-numbe`命令配置本端UDP端口。本端使用该UDP端口为源端口向对端发送消息，对端使用该UDP端口为目的端口向本端发送消息。取值范围为1至65535，默认值6000。
- **HSCP对端**：在全局配置模式下，使用`hscp peer peer-name`命令指定HSCP对端名称，并进入HSCP对端模式。
- **HSCP对端的IP地址和端口**：在HSCP对端模式下，使用`ip ip-address port port-numbe`命令指定对端的IP地址和端口，即HSCP报文的源IP和源端口。对端端口取值范围为1至65535，默认值5000。
- **HSCP共享密钥**：在HSCP对端模式下，使用`secret secret-value`命令指定共享密钥。本端和对端通信时，使用该密钥作为加密和解密的密钥，且两端共享密钥需保持一致。
- **开启防重放**：在HSCP对端模式下，使用`anti-replay leeway value`命令启用防重放功能，并配置时间戳。启用后，系统在接收消息时将检查时间戳。默认值为5秒，表示正负5秒内属于合法时间戳。

短信发送参数

配置短信猫

设备采用外置GSM短信猫或CDMA短信猫。配置短信发送参数前，请准备一张手机SIM卡、一个GSM短信猫或CDMA短信猫，并将短信猫正确连接到设备上。连接短信猫和设备，首先，将SIM卡正确插入短信猫内；然后，通过USB数据线将短信猫与设备的USB接口连接起来。我们推荐用户使用以下两种型号的短信猫：

型号	类型	芯片	接口
金笛GSM MODEM（M1203A、M1206B、M1206B-FT、M1806-NC5）	GSM	WAVECOM	USB接口
金笛CDMA MODEM（MC323）	CDMA	HUAWEI	USB接口

认证短信发送参数

管理员可以配置短信猫每小时和每天最多发送的短信数量。对超出数量限制的短信，系统将自动丢弃并记录日志信息。

在全局配置模式下，使用以下命令配置短信最大发送数量：

```
sms modem {num-per-hour | num-per-day} number
```

- **num-per-hour** *number* - 指定短信猫每小时最多发送的短信数量，取值范围是1到1000。
- **num-per-day** *number* - 指定短信猫每天最多发送的短信数量，取值范围是1到1000。

在全局配置模式下，使用**no sms modem {num-per-hour | num-per-day}**命令不限制短信最大发送数量。

短信发送测试

为验证设备能否正常发送短信，管理员可以向指定手机号码发送测试短信。发送测试短信，在任意模式下，使用以下命令：

```
exec sms send test-message to phone-number
```

- *phone-number* - 指定接收测试短信的手机号码。

如果测试短信发送成功，指定手机号码会收到系统发送的测试短信；如果测试短信发送失败，系统会记录日志并描述失败原因。

显示短信猫配置信息

在任意模式下，使用以下命令查看短信猫的配置信息，包括存在状态和短信最大发送数量：

```
show sms modem
```

配置短信网关

设备可通过运营商的短信网关或者其代理服务器向用户发送短消息。配置该功能前，用户需先向运营商索要短信网关的地址、发送短消息的设备ID等相关信息。

短信网关认证的配置包括：

1. 创建Service Provider（SP）实例。
2. 根据需要，配置SP实例。

指定短信网关默认协议类型

设备支持的短信网关协议类型包括SGIP、UMS、ACC和ALIYUNSMS。SGIP表示联通的SGIP协议，UMS表示使用联通企业信息平台，ACC表示电信的ACC协议，ALIYUNSMS表示使用阿里云短信服务平台。用户可以在

全局配置模式下，使用以下命令指定短信网关的默认协议类型：

```
sms service-provider default-protocol {sgip | ums | acc | aliyunsms}
```

- **sgip | ums | acc | aliyunsms** - 指定短信网关的默认协议类型。**sgip**表示联通的SGIP协议，**ums**表示使用联通企业信息平台，**acc**表示使用电信的ACC协议，**aliyunsms**表示使用阿里云短信服务平台。

在全局配置模式下，使用**no sms service-provider default-protocol**命令取消短信网关的默认协议类型的指定。

创建SP实例名称

创建SP实例，在全局配置模式下，使用以下命令：

```
sms service-provider sp-name [protocol {sgip | ums | acc | aliyunsms}]
```

- **sp-name** - 指定SP实例的名称，取值范围为1至31个字符。
- **protocol {sgip | ums | acc | aliyunsms}** - 指定SP实例运行的短信网关协议。指定SP实例运行的短信网关协议。**sgip**表示联通的SGIP协议，**ums**表示使用联通企业信息平台，**acc**表示使用电信的ACC协议，**aliyunsms**表示使用阿里云短信服务平台。

执行该命令后，系统创建指定名称的SP实例，并且进入SP实例配置模式；如果指定的名称已存在，则直接进入SP实例配置模式。对于每种协议类型的SP实例，系统最多可配置8个SP实例。

在全局配置模式下，使用该命令**no**的形式删除指定的SP实例：

```
no sms service-provider sp-name
```

在SP实例配置模式下，可以进行以下配置：

- 指定VRouter
- 指定UMS/ACC/ALIYUNSMS协议
- 指定短信网关的地址和端口号
- 设置发送认证短信的号码
- 指定设备ID
- 指定用户名和密码
- 配置短信最大发送数量

- 指定企业编码
- 指定AccessKeyId
- 指定AccessKeySecret

指定VRouter

系统有一个默认VRouter，即trust-vr，同时系统支持多VR。指定SP所属的VRouter，在SP实例配置模式下，使用以下命令：

```
vrouter vr-name
```

- *vr-name* – 指定已创建的VR名称。若不指定，默认属于trust-vr。

在SP实例配置模式下，使用该命令no的形式恢复为默认VR：

```
no vrouter
```

指定UMS/ALIYUNSMS/ACC协议

指定UMS/ALIYUNSMS/ACC的协议，在SP实例配置模式下，使用以下命令：

```
protocol {http | https}
```

- **http** | **https** – 指定UMS、ACC或者ALIYUNSMS的协议为HTTP或者HTTPS。UMS的默认协议为HTTPS，ACC及ALIYUNSMS的默认协议为HTTP。

在SP实例配置模式下，使用该命令no的形式恢复默认协议：

```
no protocol
```

指定短信网关的地址和端口号

指定短信网关的地址和端口号，在SP实例配置模式下，使用以下命令：

```
gateway {host hostname | ip ip-address} [port port-number]
```

- **host** *hostname* - 指定短信网关的主机名称，名称范围为1至31个字符。
- **ip** *ip-address* - 指定短信网关的IP地址。

- **port** *port-number* - 指定短信网关的端口号。当协议类型指定为“SGIP”时，默认端口号为8801；当协议类型指定为“UMS”时，默认端口号为9600；当协议类型指定为“XUANWU”或“CAS”时，默认端口号为8080。

多次执行此命令，最新一次执行的命令生效。

在SP实例配置模式下使用该命令no的形式删除短信网关的地址和端口号：

```
no gateway {host | ip }
```

设置发送认证短信的号码

开启短信口令认证功能后，系统会向已指定的用户手机号码发送认证码短信。在SP实例配置模式下，使用以下命令设置手机号码：

```
source-number phone-number
```

- *phone-number* - 指定用户的手机号码，取值范围为1至21个字符。

在SP实例配置模式下使用该命令no的形式取消用户手机号码的指定：

```
no source-number
```

指定设备ID

配置短信网关前，用户需向运营商索取允许发送短信的设备ID。在SP实例配置模式下，使用以下命令在设备端指定ID：

```
device-code code-number
```

- *code-number* - 指定设备的ID，取值范围为1至4294967295。

在SP实例配置模式下使用该命令no的形式取消ID号码的指定：

```
no device-code
```

指定用户名和密码

指定登录短信网关的用户名称及密码，在SP实例配置模式下，使用以下命令：

```
user username password password
```

- *username* - 指定登录短信网关的用户名称，名称范围是1至64个字符。
- *password* - 指定登录密码，名称范围是1至64个字符。

在SP实例配置模式下使用该命令no的形式取消用户名和密码的指定：

```
no user
```

配置短信最大发送数量

管理员可以配置短信网关每小时或者每天最多发送的短信数量。对超出数量限制的短信，系统将自动丢弃并记录日志信息。配置短信最大发送数量，在SP实例配置模式下，使用以下命令：

```
{num-per-hour | num-per-day} number
```

- *number* – 指定短信网关每小时（**num-per-hour**）或者每天（**num-per-day**）最多发送的短信数量。范围为1-65535条。

在SP实例配置模式下使用该命令no的形式取消短信最大发送数量的指定：

```
no {num-per-hour | num-per-day}
```

指定企业编码

当SP实例使用UMS协议类型时，用户可以指定在UMS平台上注册的企业编码，在SP实例配置模式下，使用以下命令：

```
spcode spcode-number
```

- *spcode-number* - 指定企业编码，取值范围为1至31位数字。

在SP实例配置模式下使用该命令no的形式取消企业编码的指定：

```
no spcode
```

指定AccessKeyId

当SP实例运行的短信网关协议为ALIYUNSMS时，用户需要指定在阿里云短信服务中申请的AccessKeyId，作为山石网科设备和阿里云短信网关之间相互认证时的用户名。指定AccessKeyId，在SP实例配置模式下，使用以下命令：

```
accesskeyid word
```

- *word* - 指定AccessKeyId，取值范围为1至64个字符。该参数需与在阿里云短信服务中申请的模板AccessKeyId保持一致。

在SP实例配置模式下，使用**no accesskeyid**命令取消AccessKeyId的指定。

指定AccessKeySecret

当SP实例运行的短信网关协议为ALIYUNSMS时，用户需要指定在阿里云短信服务中申请的AccessKeySecret，作为山石网科设备和阿里云短信网关之间相互认证时的密码。指定AccessKeySecret，在SP实例配置模式下，使用以下命令：

```
accesskeysecret word
```

- *word* - 指定AccessKeySecret，取值范围为1至63个字符。该参数需与在阿里云短信服务中申请的模板AccessKeySecret保持一致。

在SP实例配置模式下，使用**no accesskeysecret**命令取消AccessKeySecret的指定。

发送测试短信

为验证设备能否正常发送短信，管理员可以向指定手机号码发送测试短信。发送测试短信，在任意模式下，使用以下命令：

```
exec sms sp sp-name send test-message to phone-number
```

- *sp-name* - 指定SP实例的名称。
- *phone-number* - 指定接收测试短信的手机号码。

如果测试短信发送成功，指定手机号码会收到系统发送的测试短信；如果测试短信发送失败，系统会记录日志并描述失败原因。

显示短信网关配置信息

在任意模式下，使用以下命令查看短信网关的配置信息：

```
show sms service-provider [sp-name]
```

- *sp-name* - 指定已创建的SP实例。如不指定，则默认显示所有已创建的SP实例的配置信息。

HSM代理

Hillstone Security Management™，简称为HSM，是山石网科自主研发的集中网络安全管理系统，能够对网络中的多台Hillstone安全设备进行集中控制和管理。HSM系统分为三部分，即HSM代理、HSM服务器和HSM客户端。将这三部分合理部署到网络中，并且实现安全连接后，用户可以通过客户端程序，查看被管理安全设备的日志信息、统计信息、设备属性等，实时监控被管理设备的运行状态和流量信息。

每台Hillstone安全设备运行的StoneOS都包含HSM代理模块，在设备上正确配置了HSM代理功能后，就可以实现设备与HSM服务器的连接，进而实现服务器对设备的管理与控制。

用户可以通过命令行接口（CLI）和Web界面（WebUI）两种方式为Hillstone安全设备配置HSM代理功能（Hillstone SR系列安全路由器只支持WebUI配置方式）。Hillstone设备的HSM代理功能配置主要包括以下各项：

- 配置HSM服务器管理参数
- 开启/关闭HSM代理功能
- 显示HSM代理配置

配置HSM服务器管理参数

为实现设备与HSM服务器的连接，使服务器能够对设备进行管理，用户需要在设备上配置服务器的IP地址、连接端口号、连接出接口、设备注册模式、访问密码及启用HSM代理功能的VRouter。

配置HSM服务器的IP地址，在全局配置模式下，使用以下命令：

network-manager host *ip-address*

- *ip-address* – 指定HSM服务器的IP地址。此IP地址不能为“0.0.0.0”、“255.255.255.255”以及组播地址。

配置HSM服务器的连接端口号，在全局配置模式下，使用以下命令：

network-manager host port *port-number*

- *port-number* – 指定HSM服务器的连接端口号。范围是1到65535。默认值是9091。

配置HSM服务器的连接出接口，在全局配置模式下，使用以下命令：

network-manager host source *interface-name*

- **source *interface-name*** – 指定HSM服务器的连接出接口。

指定HSM服务器的设备注册模式为普通模式（即非加密模式），在全局配置模式下，使用以下命令：

network-manager host plain

在全局配置模式下，用该命令no的形式指定为加密模式：

no network-manager host plain

配置HSM服务器的访问密码，在全局配置模式下，使用以下命令：

network-manager host password *password*

- *password* – 指定HSM服务器的访问密码。服务器通过该密码对设备进行认证。范围是1到31个字符。

配置启用HSM代理功能的VRouter，在全局配置模式下，使用以下命令：

```
network-manager host vrouter vrouter-name
```

- *vrouter-name* – 指定VRouter的名称。

在全局配置模式下，使用以下命令取消对HSM服务器管理参数的配置：

```
no network-manager host
```

为保证设备与HSM服务器在NAT环境下能够正常通信，系统支持用户在设备上配置FTP服务器和日志服务器的IP地址和端口号。默认情况下，FTP服务器的IP地址为HSM服务器的IP地址，端口号为21；日志服务器的IP地址为HSM服务器的IP地址，端口号为514。

配置FTP服务器的IP地址和端口号，在全局配置模式下，使用以下命令：

```
network-manager host ftp-server ip-address [port port-number]
```

- *ip-address* – 指定FTP服务器的IP地址。
- *port-number* – 指定FTP服务器的端口号。

在全局配置模式下，使用以下命令恢复FTP服务器默认IP地址和端口号：

```
no network-manager host ftp-server [port]
```

配置日志服务器的IP地址和端口号，在全局配置模式下，使用以下命令：

```
network-manager host syslog-server ip-address [secure-tcp] [port port-number]
```

- *ip-address* – 指定日志服务器的IP地址。
- **secure-tcp** – 指定该参数后，安全设备和HSM服务器在日志传输时，日志信息将被加密传输。
- *port-number* – 指定日志服务器的端口号。

在全局配置模式下，使用以下命令恢复日志服务器默认IP地址和端口号：

```
no network-manager host syslog-server [secure-tcp] [port]
```

开启/关闭HSM代理功能

HSM服务器管理参数以及信任域配置完成以后，用户需要开启设备的HSM代理功能以实现设备与服务器的正常连接。默认情况下，设备的HSM代理功能是关闭的，启用此功能，在全局配置模式下，使用以下命令：

`network-manager enable`

在全局配置模式下，用该命令no的形式关闭此功能：

`no network-manager enable`

显示HSM代理配置

用户可以在任何模式下使用show命令查看设备上HSM代理的配置信息：

`show network-manager`

连接山石云平台

山石云平台是移动互联时代的云安全服务平台，主要提供山石云服务功能。山石云服务是山石的云端能力中心、云网融合的大脑。启用山石云服务后设备将与山石云端互联，借此您将获得更广的威胁情报，提升设备的防护能力，极大地提升网络安全性、可视性、易用性。

山石云平台提供的云服务应用包括：

- 云·景（CloudView）：是一款安全领域的SaaS产品，是移动互联时代的云安全服务平台。云·景部署在公有云上，为用户提供在线按需服务。设备注册到云平台，将设备信息、威胁事件、系统日志等上传到云平台，由云·景提供可视化的展示。用户可以通过Web方式或手机APP方式远程监控设备状态信息、获取报表并进行威胁分析。关于云·景（CloudView），请参阅“山石云·景常见问题”手册。

设备端配置

在设备端，配置包括以下内容：

- 配置云平台服务器
- 启用山石云·景
- 开启系统日志上传
- 开启威胁事件上传
- 一键断网
- 显示云·景服务器配置

配置云平台服务器

在连接云平台之前，用户需要配置云平台服务器地址、用户名、密码，当用户名密码验证通过后，将下发云平台服务器的配置信息。配置云平台服务器的地址、用户名及密码需要在Cloud Server配置模式下进行。

进入Cloud Server配置模式，在全局配置模式下，使用以下命令：

cloud server

配置云平台服务器地址，在Cloud Server配置模式下，使用以下命令：

address {*A.B.C.D* | *domain*}

- *A.B.C.D* | *domain* – 指定云平台服务器地址或域名，系统默认地址为cloud.hillstonenet.com.cn。

在Cloud Server配置模式下，使用**no address**命令取消云平台服务器地址或域名的指定。

配置云平台服务器的用户名及密码，在Cloud Server配置模式下，使用以下命令：

username *user-name* **password** *pass-word*

- **username** *user-name* – 指定云平台账号的注册用户名称，即可将设备注册到公有云指定的用户名下。
- **password** *pass-word* – 指定对应用户的密码。

在Cloud Server配置模式下，使用**no username**命令取消云平台服务器的用户名及密码的指定。

配置云平台服务器的虚拟路由器，在Cloud Server配置模式下，使用以下命令：

vrouter *vr-name*

- *vr-name* – 指定虚拟路由器名称。

在Cloud Server配置模式下，使用**no vrouter**命令取消云平台服务器的虚拟路由器的指定。

启用山石云·景

在设备端，云·景相关配置包括以下内容：

- 启用云·景
- 开启数据上传

启用云·景

启用云·景需要在Cloud View配置模式下进行。进入Cloud View配置模式，在Cloud Server配置模式下，使用以下命令：

```
cloud-view
```

启用云·景，在Cloud View配置模式下，使用以下命令：

```
enable
```

在Cloud View配置模式下，使用**no enable**命令关闭云·景。

开启数据上传

将设备的监控数据上传到云平台，在Cloud View配置模式下，使用以下命令：

```
upload-type {log-event | threat-event | slb | all}
```

- **log-event** - 指定将设备的事件日志上传到云平台，上传间隔默认为10分钟。开启该功能前，请先确保设备已开启事件日志功能（**logging event on**）。
- **threat-event** - 指定将设备的威胁事件上传到云平台，上传间隔默认为60分钟。
- **slb** - 指定将设备检测的所有SLB事件上传到云平台，上传间隔默认为10分钟。关于SLB的配置，请参阅具体[服务器负载均衡](#)功能配置章节。
- **all** - 指定将上述所有数据类型上传到云平台。

在Cloud View配置模式下，使用以下命令取消数据上传类型的指定：

```
no upload-type {log-event | threat-event | slb | all}
```

显示云平台服务器配置

显示云平台服务器的配置，在任意模式下，使用如下命令：

```
show cloud server
```

Bypass

在SSL透视镜场景下，若遇系统重启、异常或断电等不能正常转发流量的情况，设备可使用Bypass策略。互为Bypass的接口对在物理上直接连通，仍可以转发网络流量，从而保证了业务的可靠性。

对于SG-6000-AX3200S平台，设备有eth0/0-eth0/5共八个接口。两个相邻接口可组成一对bypass对，即eth0/0与eth0/1（pair 0）、eth0/2与eth0/3（pair 1）、eth0/4与eth0/5（pair 2）、eth0/6与eth0/7（pair 3）四对bypass对。

对于SG-6000-AX1200S平台，设备有eth0/0-eth0/5共八个接口。其中，相邻接口eth0/4与eth0/5（pair 0）、eth0/6与eth0/7（pair 1）共两对bypass对。

对于SG-6000-AX320S/AX320S-GM/AX520S平台，设备有eth0/0-eth0/15共十六个接口。其中，相邻接口eth0/12与eth0/13（pair 0）、eth0/14与eth0/15（pair 1）共两对bypass对。

对于SG-6000-AX120S/AX120S-GM平台，设备有eth0/0-eth0/7共八个接口。其中，相邻接口eth0/6与eth0/7（pair 0）组成1对bypass对。

对于SG-6000-AX500/AX1000/AX1000S平台，设备有eth0/0-eth0/5共六个接口。两个相邻接口可组成一对bypass对，即eth0/0与eth0/1（pair 0）、eth0/2与eth0/3（pair 1）、eth0/4与eth0/5（pair 2）三对bypass对。

对于SG-6000-AX2600-GC平台，设备支持插入IOC-AX-8GE-B-HG扩展模块（共8个千兆电口），该扩展模块上的上下两个相邻接口组成一对bypass对。



注意: 系统进入HA模式后，Bypass配置无法下发。

在全局配置模式下，使用以下命令，进入Bypass模式：

```
bypass slot slot-number pair pair-number
```

- *slot-number* - 指定扩展槽位号。用户可通过**show module**命令查看扩展模块的槽位号。
- *pair-number* - 指定Bypass接口对。

开启/关闭Bypass

进入Bypass模式后，使用以下命令开启或关闭该接口对的Bypass功能。开启后，系统正常运行期间Bypass不生效；当设备故障或重启过程中才生效。默认为关闭状态。

- 开启Bypass：**offtime-bypass enable**
- 关闭Bypass：**offtime-bypass disable**

开启强制Bypass

强制Bypass是指系统正常运行期间以及重启过程中，Bypass均生效。

进入Bypass模式后，使用以下命令开启强制Bypass：

force-bypass

在Bypass模式下，使用**no force-bypass**命令关闭强制Bypass。

注意：设备重启过程中，若系统配置信息未加载完成，设备处于Bypass状态。此时，SG-6000-AX2000/AX2000S/AX4060/AX4060S平台的Bypass生效，Bypass接口对正常转发流量。而SG-6000-AX500/AX1000/AX1000S平台仅光口模块Bypass生效，电口模块不生效。

查看Bypass信息

在任何模式下，输入**show bypass**命令可查看扩展槽信息、接口对、扩展模块型号、Bypass的开启状态。如：

```
SG-6000(M)(config-bypass)# show bypass

Slot Pair Module Type Mode Offtime-Bypass
-----
1 0 IOC-AX-8GE-B-H Auto Auto(Disable)
1 1 IOC-AX-8GE-B-H Auto Auto(Disable)
1 2 IOC-AX-8GE-B-H Auto Auto(Disable)
1 3 IOC-AX-8GE-B-H Auto Auto(Disable)
-----
```

配置举例

开启SG-6000-AX2000的扩展槽1中的eth0/0与eth0/1（pair 0）Bypass功能。

```
SG-6000(M)# conf

SG-6000(M)(config-bypass)# show module

Slot State Module Type Serial Number
-----
1 Online IOC-AX-8GE-B-H 0000000000000000
2 Online IOC-AX-4SFP+-H 0000000000000000
3 Empty
```

4 Empty

SG-6000(M)(config)# **bypass slot 1 pair 0**

SG-6000(M)(config-bypass)# **offtime-bypass enable**

第16章 虚拟系统

虚拟系统（Virtual System），简称为VSYS，能够将一台物理设备在逻辑上划分成多个虚拟设备，每个虚拟设备都可以被看成是一台完全独立的设备，可以拥有独立的系统资源，且能够实现设备的大部分功能。每个虚拟设备之间相互独立，不允许直接相互通信。

VSYS具有以下特征：

- 每个VSYS拥有独立的管理员；
- 每个VSYS拥有独立的虚拟路由器、安全域、地址簿、服务簿等；
- 每个VSYS可以拥有独立的物理接口或者逻辑接口；
- 每个VSYS拥有独立的安全策略；
- 每个VSYS拥有独立的日志。

不同型号的设备支持的最大VSYS个数不同，如果想增加支持的VSYS个数，请向代理商购买相应的许可证。

配置VSYS

VSYS配置包括：

- [创建非根VSYS](#)
- [创建VSYS Profile](#)
- [启用/禁用CPU资源配额](#)
- [查看VSYS的CPU资源占用](#)
- [绑定Profile到VSYS](#)
- [进入根VSYS](#)
- [进入非根VSYS](#)
- [配置共享属性](#)
- [导入/导出物理接口](#)

- [分配逻辑接口](#)
- [绑定监测对象](#)
- [监测指定VSYS状态](#)
- [回退配置信息（非根VSYS）](#)
- [配置VSYS日志功能](#)
- [配置跨VSYS流量转发功能](#)
- [显示VSYS信息](#)
- [显示VSYS Profile信息](#)

创建非根VSYS

根系统管理员能够创建非根VSYS。创建非根VSYS，在根VSYS的全局配置模式下使用以下命令：

vsys *vsys-name*

- *vsys-name* – 指定需要创建的VSYS名称，为1到23个字符的字符串，名称不能为root（root为保留名称），且不能包含“\”字符。

执行该命令后，系统创建指定名称的非根VSYS，并且进入该VSYS的配置模式。如果指定的名称已存在，则直接进入该VSYS的配置模式。在根VSYS的全局配置模式下使用**no vsys vsys-name**命令删除指定的VSYS。

配置非根VSYS的描述信息

用户可根据需要，为非根VSYS配置描述信息。在非根VSYS的配置模式下，使用以下命名：

description *string*

- *string* – 指定描述信息内容。

在非根VSYS的配置模式下，使用该命令**no**的形式取消描述信息的指定：

no description

创建VSYS Profile

每个VSYS在功能上相互独立，但共享系统资源，如虚拟服务器数、服务池数、健康检查数、真实服务数、会话数、LLB 模板数、LLB规则数、安全域数、策略数、SNAT规则数、DNAT规则数等。根系统管理员可以创建VSYS Profile，并通过Profile设置VSYS中各项系统资源的预留配额和最大配额。预留配额即系统为每个VSYS预留的资源值；最大配额即每个VSYS可获得的最大资源值。各个VSYS中实际配置的每种资源总和不能超过系统的整体限制（Capacity）。

创建VSYS Profile，在根VSYS全局配置模式下使用以下命令：

```
vsys-profile vsys-profile-name
```

- *vsys-profile-name* – 指定需要创建的VSYS Profile名称，为1到31个字符的字符串。

执行该命令后，系统创建指定名称的VSYS Profile，并且进入VSYS Profile配置模式；如果指定的名称已存在，则直接进入VSYS Profile配置模式。在根VSYS全局配置模式下使用该命令no的形式删除指定的VSYS Profile：

```
no vsys-profile vsys-profile-name
```



注意：

- 根VSYS的默认Profile（root-vsys-profile）和非根VSYS的默认Profile（default-vsys-profile）都不可以被删除和编辑。
- 删除VSYS Profile之前必须删除所有引用该Profile的VSYS。

配置QoS

根系统RXW管理员可以通过VSYS Profile来配置是否开启QoS功能，然后将其绑定到VSYS，从而控制非根VSYS是否支持QoS功能。管理员还可以配置根管道的最大配额和预留配额。

VSYS Profile中的QoS功能需要在VSYS Profile Qos 模式下进行配置。进入VSYS Profile Qos 模式，在VSYS Profile配置模式下使用以下命令：

```
iqos
```

在VSYS Profile Qos配置模式下，使用以下命令在VSYS Profile中开启或关闭QoS功能：

- 开启：**enable**
- 关闭：**no enable**

设置VSYS Profile中根管道的配额，请在VSYS Profile Qos配置模式下使用以下命令：

```
root-pipe max max-num reserve reserve-num
```

- **max max-num reserve reserve-num** - 指定VSYS Profile中根管道数的最大配额（**max max-num**）和预留配额（**reserve reserve-num**）。最大配额的取值范围为0~20。预留配额不能超过最大配额。

设置资源配额

用户可对VSYS资源的最大配额和预留配置进行配置。资源配额包括VSYS中真实服务数（**real-server**）、虚拟服务器数（**virtual-server**）、服务池数（**server-pool**）、健康检查数（**health-check**）、CPU（**cpu**）、会话数（**session**）、LLB 模板数（**llb-profile**）、LLB规则数（**llb-rule**）、安全域个数（**zone**）、策略数（**policy**）、策略组数（**policy-group**）、SNAT规则数（**snat**）、DNAT规则数（**dnat**）、会话限制规则数（**session-limit**）、日志数（**log**）、统计集（**statistic-set**）、IPSec VPN隧道数（**tunnel-ipsec**）和新建连接速率（**cps**）。

设置资源配额，在VSYS Profile配置模式下使用以下命令：

```
{ cpu | iqos | real-server | server-pool | virtual-server | health-check | session | llb-profile | llb-rule | zone | policy | policy-group | snat | dnat | session-limit | log | statistic-set { non-session-based | session-based } | tunnel-ipsec | cps } max max-num [reserve reserve-num] [alarm alarm-num]
```

- **max max-num** - 指定VSYS资源的最大资源配额。最大配额和预留配额根据不同平台取值范围不同。预留配额不能超过最大配额。各资源的最大配额取值范围以及预留配额的最小值请参见下表。
- **reserve reserve-num** - 指定VSYS资源的预留配额。
- **alarm alarm-num** - 该参数为CPU专用。配置该参数后，当CPU使用率超过指定百分比时，系统产生报警日志。取值范围为50到99。

系统资源	最大配额（max max-num）取值范围	预留配额（reserve reserve-num）最小值
CPU	1 - 10000 以1/10000为单位，10000表示100%	0
虚拟服务器数	0 - capacity	0
服务池数	0 - capacity	0
真实服务数	0 - capacity	0

系统资源	最大配额（max max-num）取值范围	预留配额（reserve reserve-num）最小值
健康检查数	0 - capacity	0
会话数	min (capacity /2, 256) - capacity	0
LLB调度策略数	0 - 20	0
LLB规则数	0 - 16	0
安全域数	1 - capacity	0
策略数	0 - capacity	0
策略组数	0 - 1000	0
SNAT规则数	0 - capacity	0
DNAT规则数	0 - capacity	0
会话限制规则数	- 根VSYS Profile：固定值128 - 非根VSYS Profile：0 - 118	- 根VSYS Profile：固定值10 - 非根VSYS Profile：0
统计集	0 - 32	0
IPSec VPN隧道数	0 - capacity	0
iQoS管道数	0 - 20	0
新建连接速率	10 - 50000000	--
日志	0 - capacity	0

例如：

当为某VSYS设置CPU资源配额时，CPU最大配额指定为5000（即50%），预留配额指定为3000（即30%）、告警阈值指定为70（即70%），使用以下命令：

```
hostname[DBG](M)(config)# vsys-profile test
```

```
hostname[DBG](M)(config-vsys-profile)# cpu max 5000 reserve 3000 alarm 70
```

那么，当CPU利用率超过（5000/10000）*70%时，系统将会产生CPU告警日志。

在VSYS Profile配置模式下使用该命令no的形式恢复默认配额：

```
no {real-server | server-pool | virtual-server | health-check | cpu | session | llb-profile | llb-rule | zone | policy |  
policy-group | snat | dn timer | session-limit | statistic-set {non-session-based | session-based} | tunnel-ipsec | cps} max  
max-num [reserve reserve-num] [alarm alarm-num]
```

设置日志的缓存配额

配置将日志信息输出到内存缓存后，根系统管理员可以通过Profile为VSYS设置各类日志占用内存缓存的预留配额和最大配额。预留配额即系统为每个VSYS的各类型日志预留的日志缓存值；最大配额即每个VSYS的各类型日志可获得的最大日志缓存值。如果VSYS中日志的容量超过其最大配额，那么新增加的日志将覆盖掉缓存中最早的日志。

设置VSYS中日志的缓存配额，在VSYS Profile配置模式下使用以下命令：

```
log {configuration | operation | event | network | threat | traffic {session | nat | pbr | urlfilter}} buffer-size max  
max-num reserve reserve-num
```

- **max** max-num **reserve** reserve-num - 指定VSYS中配置日志、操作日志、事件日志、网络日志、威胁日志和流量日志（会话日志、NAT日志和上网日志）的最大配额（**max** max-num）和预留配额（**reserve** reserve-num）。最大配额取值范围是0到2097152。预留配额不能超过最大配额。

启用/禁用CPU资源配额

默认情况下，配置完成的CPU资源配额会在系统中立即生效。用户可以通过命令关闭VSYS CPU资源的检查，也就是已配置的CPU资源配额不生效，每个VSYS来抢占系统中CPU的资源值。禁用或者启用CPU资源配额，在根VSYS全局配置模式下，使用以下命令：

- 禁用：**vsys-resource cpu disable**
- 启用：**vsys-resource cpu enable**

查看VSYS的CPU资源占用

在根VSYS中，查看非根VSYS的CPU资源占用情况：

- 查看非根VSYS的CPU资源占用百分比，在根VSYS任意模式下使用以下命令：
show cpu vsys vsys-name

在指定非根VSYS中，查看该非根VSYS的CPU资源占用情况：

- 查看该非根VSYS的CPU资源占用百分比，在非根VSYS任意模式下使用以下命令：

```
show cpu
```

绑定Profile到VSYS

将已经创建的VSYS Profile绑定到VSYS，在VSYS配置模式下使用以下命令：

```
profile vsys-profile-name
```

- *vsys-profile-name* – 指定绑定的VSYS Profile名称。

在VSYS配置模式下使用**no profile**命令恢复默认绑定。



注意:

- 当将一个Profile绑定到VSYS时，如果所有VSYS的预留配额之和超过当前系统Capacity，则绑定失败。
- 被绑定的VSYS Profile只有在解除绑定后，才可以进行删除。

进入根VSYS

进入根VSYS，请按照以下步骤进行操作：

1. 在本地PC上启动一个终端仿真程序，输入设备的管理IP和端口号后与系统建立连接。
2. 根据提示输入用户名和密码后进入根VSYS，可以是根系统管理员或者根系统中配置的认证服务器（本地服务器/Radius服务器/TACACS+服务器）用户的用户名和密码。

进入非根VSYS

用户可直接通过管理IP访问非根VSYS，也可从根VSYS系统中进入非根VSYS（仅根系统管理员具有该权限）。

方式一：直接访问非根VSYS

1. 在本地PC上启动一个终端仿真程序，输入设备的管理IP和端口号后与系统建立连接。
2. 根据提示输入非根用户名和密码。如：根VSYS的管理IP为10.90.89.1，输入用户名“hillstone”和密码“hillstone”，即可进入根VSYS。创建非根VSYS“vsys1”后，同样输入管理IP 10.90.89.1，输入非根系统管理员

的用户名“vsys1\admin”和密码“vsys1-admin”，即可直接进入非根VSYs。关于管理员配置的详细信息，参见《系统管理》的“[配置管理员](#)”章节。



注意: 若通过以上方式直接进入非根VSYs，用户将无法使用**exit-vsys**命令返回根VSYs，需退出设备后，再次进入根VSYs。

方式二：从根VSYs进入非根VSYs（仅根系统管理员具有该权限），并对该非根VSYs进行配置。

在根VSYs执行模式或者全局配置模式下使用以下命令：

```
enter-vsys vsys-name
```

- **vsys-name** – 指定进入的非根VSYs名称。

在非根VSYs执行模式或者全局配置模式下，使用**exit-vsys**命令退出当前的非根VSYs，进入根VSYs对应的执行模式或者全局配置模式。

方式三：在非根VSYs中配置认证服务器，用户通过认证服务器登录非根VSYs。

1. 通过上述任意方式进入非根VSYs。
2. 在非根VSYs的全局配置模式下，使用**aaa-server** *aaa-server-name* [**type** {**local** | **radius** | **ldap** | **tacacs+**}] 命令创建AAA服务器（本地服务器/Radius服务器/LDAP服务器/TACACS+服务器）并进行服务器参数配置。关于AAA服务器的详细信息，请参阅“[配置AAA服务器](#)”。
3. 在非根VSYs全局配置模式下，使用**admin auth-server** *server-name*命令指定系统管理员认证服务器。关于指定系统管理员认证服务器的详细信息，参见“用户认证 > 配置AAA服务器 > 指定系统管理员认证服务器”部分。
4. 在本地PC上启动一个终端仿真程序，输入设备的管理IP和端口号后与系统建立连接。
5. 根据提示输入认证服务器中配置的用户名和密码后进入非根VSYs。

配置共享属性

为根VSYs的VRouter、VSwitch或者安全域对象配置共享属性，分别在根VSYs的VRouter配置模式、VSwitch配置模式或者安全域配置模式下使用以下命令：

```
vsys-shared
```

在根VSYS的VRouter配置模式、VSwitch配置模式或者安全域配置模式下，使用**no vsys-shared**命令取消共享属性配置。

导入/导出物理接口

所有物理接口都默认属于根VSYS。根系统管理员可以将根VSYS中的物理接口导入到非根VSYS，也可以将非根VSYS中的物理接口导出到根VSYS。导入或者导出的物理接口不能属于安全域，不能为BGroup接口、集聚接口、和冗余接口成员，且无子接口。导入到非根VSYS中的物理接口的相关接口（如子接口）只能在该非根VSYS中使用。

将物理接口导入到非根VSYS，在接口配置模式下使用以下命令：

```
export-to vsys-name
```

- *vsys-name* – 指定物理接口导入到的VSYS名称。

在接口配置模式下，使用**no export-to**命令将非根VSYS中的物理接口导出到根VSYS。

分配逻辑接口

根系统管理员可以将根VSYS中的逻辑接口分配给非根VSYS，也可以将已分配的逻辑接口恢复到根VSYS。

将逻辑接口分配到非根VSYS，在接口配置模式下使用以下命令：

```
vsys vsys-name
```

- *vsys-name* – 指定将接口分配到的VSYS名称。

在接口配置模式下，使用**no vsys**命令将已分配的逻辑接口恢复到根VSYS。

绑定监测对象

用户可以将非根VSYS绑定一个监测对象，来监控该非根VSYS的状态。配置非根VSYS绑定监测对象，在指定非根VSYS配置模式下，使用以下命令：

```
vsys-track-status track track-name
```

- *track-name* – 指定在此非根VSYS中已配置的监测对象的名称。

在指定非根VSYS配置模式下使用该命令**no**的形式解除绑定监测对象：

```
no vsys-track-status track track-name
```



注意:

- 被绑定的监测对象只有在解除绑定后，才可以进行删除。
- 关于如何配置监测对象，请参阅的“[配置监测对象](#)”部分。

监测指定VSYS状态

在根VSYS下可以监测指定VSYS的状态，根据被监测的VSYS状态改变，采取相应的措施。监测指定的VSYS状态，在根VSYS的监测对象的配置模式下，使用以下命令：

```
vsys vsys-name weight value
```

- *vsys-name* – 指定被监测的VSYS名称。
- **weight** *value* – 指定该条监测失败对整个监测对象失败贡献的权重值。取值范围是1到255。默认值是255。



注意: 监测指定VSYS状态只能适用于HA场景下。

回退配置信息（非根VSYS）

系统可对根VSYS和非根VSYS回退配置信息，支持以下两种方式：

第一种：在执行模式下，使用以下命令回退起始配置信息。系统能够纪录最近十次保存的起始配置信息，用户可以根据需要回退到已保存的指定的起始配置信息。系统将在重启后使用指定的起始配置信息。

```
rollback configuration backup number
```

- *number* – 备份起始配置信息的数字标记。

第二种：在配置回滚模式下，使用以下命令回退配置信息并退出配置回滚模式。用户不需要重启设备，该配置直接生效。

```
exec configuration rollback
```



注意:

- 在执行模式下，使用**exec configuration start**进入配置回滚模式。



- 开启配置回滚模式后和结束之前，用户无法切换VSYS。
- 每个VSYS可以独立的开启和结束回滚模式，互不影响。
- 每个VSYS同一时刻只允许一个用户开启配置回滚模式，并且仅该用户可以结束配置回滚模式。
- 根VSYS开启配置回滚模式后，系统将无法执行：切换HA状态、切换主备设备、创建或删除HA Cluster、创建或删除VSYS、修改VSYS资源配额。

示例：

```
hostname# exec configuration start （进入配置回滚模式）  
hostname[TRN]# configure （进入全局配置模式）  
…… （进行任意配置，且所做配置即时生效）  
hostname[TRN](config)# exec configuration rollback （回退配置并退出配置回滚模式）  
hostname#
```

退出配置回滚模式

直接退出配置回滚模式，系统支持以下两种方式：

第一种：在配置回滚模式下，使用以下命令直接退出配置回滚模式：

exec configuration commit

示例：

```
hostname# exec configuration start （进入配置回滚模式）  
hostname[TRN]# configure （进入全局配置模式）  
…… （进行任意配置，且所做配置即时生效）  
hostname[TRN](config)# exec configuration commit （直接退出配置回滚模式）  
hostname#
```

第二种：在配置回滚模式下，使用**exit**命令直接退出登录终端，从而退出配置回滚模式。



提示:

- 当不同用户同时登录设备时，先进入配置回滚模式的用户可以继续配置操作，其他用户无法进行配置操作。
- 当相同用户通过不同访问方式登录设备时，先进入配置回滚模式的某访问方式的用户可以继续配置操作，其他访问方式的用户无法进行配置操作，但其可以使用**exec configuration commit**或者**exec configuration rollback**命令强制使进入配置回滚模式的某用户退出配置回滚模式。

配置退出配置回滚模式的动作

当使用**exit**命令退出配置回滚模式时，默认情况下，系统会直接退出配置回滚模式。回退配置后退出配置回滚模式，在全局配置模式下，使用以下命令：

cli-exit-action rollback

恢复直接退出配置回滚模式，在全局配置模式下，使用以下命令：

cli-exit-action commit



注意: 每个VSYS可以独立使用该命令，指定自己的退出配置回滚模式的动作。

配置VSYS日志功能

目前系统支持对VSYS中的AAA、NAT、策略、路由、攻击防护、接口、DNS、服务、DHCP和系统管理事件生成日志。有关配置和查看日志的更多详细信息，请参考《监控》的“[日志](#)”。



注意: 在非根VSYS中，系统不支持生成调试、IPS和数据安全类型日志。

配置跨VSYS转发功能

为了实现设备的跨VSYS转发功能，系统引入了Simple-Switch的概念，即一种特殊的VSwitch，仅进行MAC地址学习、转发已知单播包或者泛洪。用户通过新建VWANIF接口，并且分配给指定的VSYS，不同的VSYS即可通过VWANIF接口进行相互通信，从而实现在设备内部直接转发跨越不同VSYS之间流量数据包。

通常情况下，配置跨VSYS转发功能，需要以下步骤：

1. 开启跨VSYS转发功能。
2. 配置Simple-Switch。
包括创建Simple-Switch、二层安全域以及绑定该二层安全域到Simple-Switch。
3. 创建VWANIF接口。
创建新的VWANIF接口后，系统都会自动生成一个配对的VPort接口。
4. 配置VPort接口。
将VPort接口绑定到已加入Simple-Switch的二层安全域。
5. 配置VWANIF接口。
将VWANIF接口导入到自定义VSYS，并配置所属的三层安全域和IP地址。

开启跨VSYS转发功能

默认情况下，该功能是关闭的。开启跨VSYS转发功能，在全局配置模式下，使用以下命令：

```
vsys-switch-mode
```

使用**no vsys-switch-mode**关闭跨VSYS转发功能。

配置Simple-Switch

Simple-Switch，即一种特殊的VSwitch，仅进行MAC地址学习、转发已知单播包或者泛洪。可以创建多个Simple-Switch，每一个Simple-Switch都是一个独立的广播域。

创建Simple-Switch

创建Simple-Switch，在全局配置模式下，使用以下命令：

```
vswitch vswitch Number [simple-switch]
```

- *Number* – 指定VSwitch的数字标识。Number的取值范围根据平台不同而不同。不可指定为VSwitch1。
- **simple-switch** – 指定该参数，创建Simple-Switch，并且进入Simple-Switch配置模式。

在全局配置模式下，使用以上命令**no**的形式删除指定的Simple-Switch：

```
no vswitch vswitch Number
```

绑定二层安全域到Simple-Switch

绑定二层安全域到Simple-Switch需要进行两步配置。

首先，创建二层安全域，在全局配置模式下，使用以下命令：

```
zone zone-name l2
```

- *zone-name* - 创建域的名称。
- **l2** - 指定所创建域为二层域。

然后，在安全域配置模式下，输入以下命令将该二层安全域绑定到Simple-Switch：

```
bind vswitch-name
```

- *vswitch-name* - 指定将二层域绑定到的Simple-Switch所属的VSwitch名称。

创建VWANIF接口

VWANIF接口是三层接口，每新建一个VWANIF接口，系统都会自动生成一个配对的VPort接口，通过VWANIF接口和VPort接口可以实现不同VSYS的互通。

创建VWANIF接口，在全局配置模式下，使用以下命令：

```
interface vwanif id
```

- *id* - 指定将要创建的VWANIF接口的编号。如果指定编号的VWANIF接口不存在，则创建VWANIF接口并进入VWANIF接口配置模式；如果指定编号的VWANIF接口已存在，则直接进入VWANIF接口配置模式。

在全局配置模式下使用**no interface vwanif *id***命令删除指定的VWANIF接口。

配置VPort接口

创建VWANIF接口之后，同时需要将VPort接口绑定到已加入Simple-Switch的二层安全域。在VPort接口配置模式下，使用以下命令：

```
zone zone-name
```

- *zone-name* - 指定将接口绑定到已加入Simple-Switch的二层安全域名称。

配置VWANIF接口

为了实现不同VSYS的三层互通，用户还需要将VWANIF接口导入到自定义VSYS，并配置所属的三层安全域和IP地址（IPv4或IPv6）。



注意: 关于配置VWANIF接口配所属安全域以及IP地址（IPv4或IPv6），请参阅“[配置接口](#)”章节。

分配VWANIF接口

创建VWANIF接口之后，需要将VWANIF接口分配到非根VSYS，在接口配置模式下使用以下命令：

```
vsys vsys-name
```

- *vsys-name* – 指定将接口分配到的VSYS名称。

显示跨VSYS转发功能信息

查看设备是否开启了跨VSYS转发功能，在任意模式使用以下命令：

```
show vsys-switch-mode
```

显示VWANIF接口配置信息

显示指定VWANIF接口信息，在任意模式下，使用以下命令：

```
show [ ipv6 ] interface vwanif id
```

显示VSYS信息

显示系统中VSYS信息，在根VSYS任意模式使用以下命令：

```
show vsys [vsys-name]
```

vsys-name – 指定需要查看的VSYS的名称。若不指定，则显示系统所有VSYS的信息。

显示VSYS Profile信息

显示系统中VSYS Profile信息，在根VSYS任意模式使用以下命令：

show vsys-profile [*vsys-profile-name*]

- *vsys-profile-name* – 指定需要查看的VSYN Profile的名称。若不指定，则显示系统所有VSYN Profile的信息。

第17章 SLB脚本编程手册

ADC产品通过Web界面和CLI命令行，提供了丰富的负载均衡参数可供配置，满足绝大多数用户的需求。对于需求比较复杂的用户，ADC提供可编程脚本的接口，满足用户自己编写脚本控制流量的需求，更加方便、灵活。

当前，可编程脚本仅支持TCP、HTTP、HTTPS、SSL-OVER-TCP和RADIUS类型的虚拟服务器（Virtual Server，VS）。详细信息，请查阅[ADC SLB脚本编程手册](#)。