

CN9000/CN6000 系列  
/S6820/S6550E/S6220/S5560V2 系列  
命令行手册

浪潮思科网络科技有限公司（以下简称“浪潮网络”）为客户提供全方位的技术支持和服务。直接向浪潮网络购买产品的用户，如果在使用过程中有任何问题，可与浪潮网络各地办事处或用户服务中心联系，也可直接与公司总部联系。

读者如有任何关于浪潮网络产品的问题，或者有意进一步了解公司其他相关产品，可通过下列方式与我们联系：

公司网址：<http://www.inspur.com/>  
技术支持热线：400-691-1766  
技术支持邮箱：[inspur\\_network@inspur.com](mailto:inspur_network@inspur.com)  
客户投诉热线：400-691-1766  
公司总部地址：山东省济南市历下区浪潮路 1036 号  
邮政编码：250000

---

## 声 明

**Copyright ©2021**

浪潮思科网络科技有限公司

版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。

**inspur 浪潮** 是浪潮思科网络科技有限公司的注册商标。

对于本手册中出现的其它商标，由各自的所有人拥有。

此为 A 级产品，在生活环境中，该产品可能会造成无线电干扰。在这种情况下，可能需要用户对其干扰采取切实可行的措施。

由于产品版本升级或其它原因，本手册内容会不定期进行更新。除非另有约定，本手册仅作为使用指导，本手册中的所有陈述、信息和建议不构成任何明示或暗示的担保。

# 前言

## 概述

本文档系统介绍了以太网交换机设备支持的各种功能的配置命令。主要内容包括基础配置、以太网、设备管理、网络管理、组播、安全性、IP 业务、IP 路由、流量管理、IPV6、VPN、可靠性、EVPN、堆叠配置等相关命令。

从命令语法、命令模式、默认值、使用说明、实例说明五个方面进行介绍，阅读本文档有助于读者系统掌握设备功能特性的配置命令。

该手册适用于以下交换机系列型号，包括：

数据中心 CN9000 系列（含 CN9408H/CN9300-48Y8C/CN9008-48YC-S/CN9100-48X8C；不含 CN93240）、CN6000 系列（含 CN61108PC-V-H；不含 CN61108PC-V、CN6132、CN61108TC-V 等设备）

园区网 S6820 系列（S6820-24XQ-E）、S6550E 系列（含 S6550E-48T4X-C/S6550E-48TS4X-C/S6550E-48S4X-C）、S6220 系列（含 S6220-24TQ-S-PWR/S6220-48TQ-S-PWR/S6220-24TQ-S/S6220-48TQ-S/S6220-24S4X-S）、S5560V2 系列（含 S5560V2-48T4X-S/ S5560V2-48T4S-S/S5560V2-24T4X-S/S5560V2-24T4S-S/S5560V2-24TS-L-PWR/S5560V2-24T4X-HS）；

注：每款产品所支持特性有差异，具体请以产品实际支持功能为准。





## 版本更新说明

手册版本	更新说明
V1.0	手册第一次发行
V1.1	<ul style="list-style-type: none"><li>● 新增了部分 POE、TACACS+、TELEMETRY、基础命令、OSPF、RIP、VXLAN、L2 组、堆叠和 IP 路由相关命令；</li><li>● 更新隧道配置命令小节</li></ul>

## 约定

### 符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

符号	说明
 <b>警告</b>	以本标志开始的文本表示有潜在危险，如果不能避免，可能导致人员伤害。
 <b>注意</b>	以本标志开始的文本表示有潜在风险，如果忽视这些文本，可能导致设备损坏、数据丢失、设备性能降低或不可预知的结果。
 <b>说明</b>	以本标志开始的文本是正文的附加信息，是对正文的强调和补充
 <b>窍门</b>	以本标志开始的文本能帮助您解决某个问题或节省您的时间。

### 通用格式约定

格式	说明
宋体	正文采用宋体表示。
黑体	一级标题、二级标题、三级标题、Block 采用黑体表示。
楷体	警告、提示等内容用楷体表示。
“Lucida Console” 格式	“Lucida Console” 格式表示屏幕输出信息。此外，屏幕输出信息中夹杂的用户从终端输入的信息采用加粗字体表示。

### 命令行格式约定

格式	说明
<b>粗体</b>	命令行关键字（命令中保持不变、必须照输的部分）采用 <b>粗体</b> 表示。
<i>斜体</i>	命令行参数（命令中必须由实际值进行替代的部分）采用 <i>斜体</i> 表示。
[ ]	表示用 “[ ]” 括起来的部分在命令配置时是可选的。
{ x   y   ... }	表示从两个或多个选项中选取一个。
[ x   y   ... ]	表示从两个或多个选项中选取一个或者不选。



---

格式	说明
{ x   y   ... } *	表示从两个或多个选项中选择多个，最少选取一个，最多选取所有选项。
[ x   y   ... ] *	表示从两个或多个选项中选择多个或者不选。

# 目录

前言.....	i
概述.....	i
版本更新说明.....	i
约定.....	ii
符号约定 .....	ii
通用格式约定 .....	ii
命令行格式约定.....	ii
目录.....	1
1 基础命令行参考.....	1
1.1 系统管理配置命令 .....	1
1.1.1 hostname .....	1
1.1.2 management ip address .....	2
1.1.3 management route .....	3
1.1.4 management interface shutdown.....	4
1.1.5 show management ip address.....	4
1.1.6 show management interface.....	5
1.1.7 clear counters mgmt-if.....	5
1.1.8 enable password .....	6
1.1.9 terminal length .....	7
1.1.10 service terminal-length.....	8
1.1.11 banner motd.....	8
1.1.12 banner exec .....	9
1.1.13 banner login .....	10
1.1.14 show version .....	11
1.1.15 line vty maximum .....	11
1.1.16 exec-timeout.....	12
1.1.17 transport input .....	13
1.1.18 access-class in .....	13
1.1.19 reboot .....	14
1.1.20 schedule reboot at.....	15
1.1.21 schedule reboot delay.....	16

---

1.1.22 boot system .....	16
1.1.23 show boot .....	17
1.1.24 show boot images .....	18
1.1.25 show memory .....	18
1.1.26 show cpu traffic-limit .....	21
1.1.27 show processes cpu sorted .....	22
1.1.28 show processes cpu history .....	23
1.1.29 show processes memory sorted .....	24
1.1.30 terminal monitor .....	26
1.1.31 configure terminal .....	26
1.1.32 disable .....	27
1.1.33 enable .....	28
1.1.34 end .....	28
1.1.35 exit (global) .....	29
1.1.36 exit (EXEC) .....	30
1.1.37 quit .....	30
1.1.38 cd .....	31
1.1.39 copy .....	32
1.1.40 delete .....	33
1.1.41 dir .....	34
1.1.42 ls .....	35
1.1.43 more .....	36
1.1.44 mkdir .....	36
1.1.45 rename .....	37
1.1.46 rmdir .....	38
1.1.47 tar create .....	39
1.1.48 tar table .....	39
1.1.49 tar xtract .....	40
1.1.50 tar diagnostic-information .....	41
1.1.51 format .....	41
1.1.52 umount .....	42
1.1.53 cut_through_forwarding enable (10G-40G-100G  1G-10G-100G  1G-10G-40G) .....	43
1.1.54 show cut-through-forwarding mode .....	44
1.2 用户管理配置 .....	44
1.2.1 username .....	44
1.2.2 username password [8] .....	45
1.2.3 username secret .....	46
1.2.4 username privilege .....	46
1.2.5 username privilege password .....	47
1.2.6 username service-type .....	48
1.2.7 re-username newname .....	49
1.2.8 cipher detect .....	49

---

---

1.2.9 cipher detect length .....	50
1.2.10 username retry-times .....	51
1.2.11 username unlock.....	52
1.2.12 username active-period .....	52
1.2.13 username lock-time .....	53
1.3 FTP 配置 .....	54
1.3.1 ftp .....	54
1.3.2 ftpvrf .....	55
1.3.3 ftp username .....	55
1.3.4 ftp password.....	56
1.3.5 ftp passive .....	57
1.3.6 show ftp.....	58
1.4 FTP Server 配置.....	58
1.4.1 service ftpd.....	58
1.4.2 ftpd username password.....	59
1.5 TFTP 配置.....	60
1.5.1 copy GFILENAME GURLNAME .....	60
1.5.2 Copy GURLNAME GFILENAME .....	61
1.5.3 copy running-config mgmt-if.....	61
1.5.4 copy startup-config mgmt-if .....	62
1.5.5 copy mgmt-if startup-config .....	63
1.6 Telnet 配置 .....	64
1.6.1 service telnet .....	64
1.6.2 telnet.....	64
1.6.3 telnet server source address.....	65
1.6.4 telnet server sourceport .....	66
1.6.5 telnet server source mgmt-ifport .....	67
1.7 Netconf 配置 .....	68
1.7.1 netconf ssh {enable disable} .....	68
1.7.2 netconf super-user .....	68
1.8 SSH 配置.....	69
1.8.1 ip ssh server.....	69
1.8.2 ip ssh server authentication-retries.....	70
1.8.3 ip ssh server authentication-timeout.....	70
1.8.4 ip ssh server authentication-type .....	71
1.8.5 ip ssh server host-key rsa key.....	72
1.8.6 ip ssh server rekey-interval .....	73
1.8.7 ip ssh server version .....	74
1.8.8 ip ssh server source address .....	75
1.8.9 ip ssh server source port.....	75
1.8.10 ip ssh server source mgmt-ifport.....	76

---

1.8.11 show ip ssh server session .....	77
1.8.12 show ip ssh server status .....	77
1.8.13 rsa key .....	78
1.8.14 key format .....	79
1.8.15 key string end .....	80
1.8.16 key type .....	80
1.8.17 reset .....	81
1.8.18 validate .....	82
1.8.19 KEYLINE .....	82
1.8.20 rsa key export .....	83
1.8.21 rsa key import .....	84
1.8.22 show rsa key .....	85
1.8.23 show rsa keys .....	86
1.8.24 ssh .....	86
1.9 时间配置命令 .....	88
1.9.1 clock set datetime .....	88
1.9.2 clock set timezone .....	89
1.9.3 clock set summer-time .....	90
1.9.4 show clock .....	91
1.9.5 show timezones .....	91
1.10 证书命令 .....	92
1.10.1 generate device identifier .....	92
1.10.2 show license .....	93
1.11 HTTP 配置 .....	94
1.11.1 service http .....	94
1.11.2 service https .....	94
1.11.3 http server load .....	95
1.11.4 http timeout .....	96
1.12 周期定时任务配置 .....	97
1.12.1 kron policy-list .....	97
1.12.2 command .....	97
1.12.3 kron occurrence policy-list at .....	98
1.12.4 enable kron policy-list .....	99
1.12.5 show kron policy-list .....	100
2 以太网命令行参考 .....	101
2.1 接口命令 .....	101
2.1.1 bandwidth .....	101
2.1.2 clear counters .....	102
2.1.3 description .....	102
2.1.4 duplex .....	103
2.1.5 speed .....	104

---

2.1.6 interface .....	105
2.1.7 interface range.....	106
2.1.8 interface range create vlan .....	107
2.1.9 jumboframe .....	108
2.1.10 media-type.....	108
2.1.11 unidirectional .....	109
2.1.12 shutdown.....	110
2.1.13 split interface.....	111
2.1.14 load-interval .....	112
2.1.15 vlan dot1q tag native .....	112
2.1.16 show interface .....	113
2.1.17 show interface status .....	115
2.1.18 show interface hybrid.....	116
2.1.19 show interface trunk.....	116
2.1.20 show interface summary .....	117
2.1.21 show ip interface .....	118
2.1.22 switchport.....	119
2.1.23 switchport access vlan.....	120
2.1.24 switchport mode access.....	120
2.1.25 switchport mode trunk .....	121
2.1.26 switchport mode hybrid .....	122
2.1.27 switchport mode dot1q-tunnel.....	122
2.1.28 switchport trunk allowed.....	123
2.1.29 switchport trunk native vlan.....	124
2.1.30 switchport hybrid allowed.....	125
2.1.31 switchport hybrid native vlan.....	126
2.1.32 mtu .....	126
2.1.33 subif .....	127
2.1.34 carrier {up-delay down-delay} .....	128
2.2 接口 Errdisable 命令.....	129
2.2.1 errdisable detect .....	129
2.2.2 errdisable recovery interval.....	129
2.2.3 errdisable fdb-loop .....	130
2.2.4 errdisable recovery reason.....	131
2.2.5 errdisable flap.....	132
2.2.6 no errdisable.....	133
2.2.7 show errdisable detect .....	134
2.2.8 show errdisable recovery .....	135
2.2.9 show errdisable flap .....	136
2.3 MAC Address Table 命令 .....	136
2.3.1 mac-address-table ageing-time.....	136
2.3.2 mac-address-table forward.....	137

---

---

2.3.3 mac-address-table discard .....	138
2.3.4 clear mac address-table .....	139
2.3.5 show mac address-table ageing-time.....	140
2.3.6 show mac address-table .....	140
2.3.7 show mac address-table hardware.....	142
2.3.8 show mac address-table count.....	143
2.3.9 show mac address-table add-fdb-fail.....	143
2.3.10 show mac-filter address-table .....	144
2.3.11 show resource mac-filter .....	145
2.3.12 show resource static-fdb.....	145
2.4 VLAN 命令.....	146
2.4.1 vlan database.....	146
2.4.2 vlan.....	147
2.4.3 vlan port.....	148
2.4.4 vlan VLAN_LIST .....	148
2.4.5 show vlan .....	149
2.4.6 show vlan all .....	150
2.4.7 show vlan brief.....	151
2.4.8 show interface switchport .....	151
2.4.9 switchport hybrid allowed.....	152
2.4.10 switchport hybrid native vlan.....	153
2.4.11 switchport access vlan.....	154
2.4.12 switchport mode hybrid .....	154
2.4.13 switchport mode access.....	155
2.4.14 switchport mode trunk .....	156
2.4.15 switchport trunk allowed.....	156
2.4.16 switchport trunk native.....	157
2.4.17 vlan bridge disable .....	158
2.4.18 vlan statistics enable.....	159
2.4.19 vlan statistics interval.....	160
2.4.20 clear vlan statistics .....	160
2.4.21 show vlan statistics.....	161
2.5 VOICE VLAN 命令.....	162
2.5.1 voice vlan.....	162
2.5.2 voice vlan security enable .....	163
2.5.3 voice vlan set cos to .....	163
2.5.4 voice vlan mac-address .....	164
2.5.5 voice vlan enable.....	165
2.5.6 show voice vlan state .....	165
2.6 VLAN Classification 命令.....	166
2.6.1 vlan classifier activate.....	166
2.6.2 vlan classifier group.....	167

---

---

2.6.3	vlan classifier rule .....	168
2.6.4	show vlan classifier group.....	170
2.6.5	show vlan classifier interface .....	170
2.6.6	show vlan classifier rule.....	171
2.6.7	show resource vlan-classification .....	172
2.7	VLAN Mapping 命令 .....	173
2.7.1	ethernet evc .....	173
2.7.2	dot1q mapped-vlan.....	173
2.7.3	dot1q mapped-double-vlan .....	174
2.7.4	vlan mapping table .....	175
2.7.5	raw vlan group .....	176
2.7.6	raw-vlan .....	176
2.7.7	dot1q ethertype.....	177
2.7.8	show vlan mapping table.....	178
2.7.9	show vlan mapping table applied-interface.....	179
2.7.10	switchport mode.....	180
2.7.11	switchport dot1q-tunnel type.....	180
2.7.12	switchport dot1q-tunnel native.....	181
2.7.13	switchport dot1q-tunnel allow vlan.....	182
2.7.14	switchport dot1q-tunnel vlan mapping table.....	183
2.7.15	switchport dot1q-tunnel vlan mapping miss-forward .....	184
2.7.16	switchport trunk vlan-translation .....	184
2.7.17	switchport trunk vlan-translation mapping table.....	185
2.7.18	switchport trunk vlan-translation miss-forward .....	185
2.7.19	vlan dot1q tag native .....	186
2.7.20	show resource vlan-mapping.....	187
2.8	Link Aggregation 命令 .....	187
2.8.1	channel-group .....	187
2.8.2	static-channel-group.....	188
2.8.3	lacp port-priority .....	189
2.8.4	lacp timeout.....	190
2.8.5	lacp system-priority.....	191
2.8.6	lacp system-mac .....	191
2.8.7	lacp device-id .....	192
2.8.8	lacp max-bundle.....	193
2.8.9	port-channel load-balance hash-field-select.....	193
2.8.10	port-channel load-balance hash-arithmetic .....	195
2.8.11	port-channel <i>channel-group-number</i> load-balance-mode dynamic.....	195
2.8.12	port-channel <i>channel-group-number</i> load-balance-mode round-robin .....	196
2.8.13	port-channel <i>channel-group-number</i> self-healing .....	197
2.8.14	show channel-group summary .....	198
2.8.15	show channel-group detail .....	199

---



---

2.8.16 show lacp internal .....	200
2.8.17 show lacp internal detail .....	201
2.8.18 show lacp neighbor .....	203
2.8.19 show lacp neighbor detail .....	205
2.8.20 show channel-group port.....	207
2.8.21 show lacp counters .....	210
2.8.22 show lacp sys-id.....	211
2.8.23 clear lacp counters.....	212
2.8.24 lacp force-up .....	213
2.9 MSTP 命令 .....	213
2.9.1 spanning-tree enable .....	213
2.9.2 spanning-tree priority .....	214
2.9.3 spanning-tree instance priority .....	215
2.9.4 spanning-tree forward-time .....	215
2.9.5 spanning-tree hello-time .....	216
2.9.6 spanning-tree max-age .....	217
2.9.7 spanning-tree max-hops .....	218
2.9.8 spanning-tree transmit-holdcount.....	219
2.9.9 spanning-tree edgeport bpdu-guard.....	219
2.9.10 spanning-tree edgeport bpdu-filter .....	220
2.9.11 spanning-tree port.....	221
2.9.12 spanning-tree port-priority .....	221
2.9.13 spanning-tree pathcost-standard.....	222
2.9.14 spanning-tree path-cost .....	223
2.9.15 spanning-tree link-type .....	224
2.9.16 spanning-tree edgeport.....	224
2.9.17 spanning-tree edgeport bpdu-guard.....	225
2.9.18 spanning-tree edgeport bpdu-filter .....	226
2.9.19 spanning-tree guard root .....	227
2.9.20 spanning-tree guard loop.....	228
2.9.21 spanning-tree force-version.....	228
2.9.22 spanning-tree restricted-tcn.....	229
2.9.23 spanning-tree restricted-role.....	230
2.9.24 spanning-tree tc-protection.....	231
2.9.25 spanning-tree tc-protection threshold.....	231
2.9.26 spanning-tree mode .....	232
2.9.27 spanning-tree instance priority .....	233
2.9.28 spanning-tree instance path-cost .....	233
2.9.29 spanning-tree instance restricted-tcn.....	234
2.9.30 spanning-tree instance restricted-role.....	235
2.9.31 spanning-tree mst configuration.....	236
2.9.32 instance .....	237

---

---

2.9.33 region .....	237
2.9.34 revision.....	238
2.9.35 clear spanning-tree detected protocols .....	239
2.9.36 clear spanning-tree disabled-port .....	240
2.9.37 show spanning-tree .....	240
2.9.38 show spanning-tree interface.....	241
2.9.39 show spanning-tree brief.....	243
2.9.40 show spanning-tree disabled-port .....	244
2.9.41 show spanning-tree mst.....	244
2.9.42 show spanning-tree mst config.....	245
2.9.43 show spanning-tree mst detail .....	246
2.9.44 show spanning-tree mst instance.....	247
2.9.45 show spanning-tree mst interface.....	248
2.9.46 show spanning-tree mst brief .....	249
2.9.47 spanning-tree instance forward .....	251
2.10 Flow control 命令 .....	252
2.10.1 flowcontrol send.....	252
2.10.2 flowcontrol receive .....	252
2.10.3 show flowcontrol .....	253
2.11 Priority-based flow control 命令.....	254
2.11.1 priority-based flowcontrol enable .....	254
2.11.2 priority-flow-control enable priority .....	255
2.11.3 show priority-flow-control .....	255
2.11.4 show priority-flow-control statistics .....	256
2.12 Layer 2 Protocols Tunneling 命令 .....	257
2.12.1 l2protocol enable.....	257
2.12.2 l2protocol tunnel-dmac .....	257
2.12.3 l2protocol mac 1 .....	258
2.12.4 l2protocol mac <2-6>.....	259
2.12.5 l2protocol .....	260
2.12.6 l2protocol uplink enable.....	261
2.12.7 show l2protocol.....	262
2.12.8 l2protocol cos.....	262
2.12.9 l2protocol full-mac.....	263
2.13 Storm Control 命令 .....	264
2.13.1 storm-control .....	264
2.13.2 show storm-control .....	265
2.13.3 ipg storm-control enable .....	266
2.14 Loopback Detection 命令.....	266
2.14.1 Loopback-detect enable .....	266
2.14.2 loopback-detect packet-interval .....	267

---

2.14.3 loopback-detect action .....	268
2.14.4 loopback-detect packet vlan .....	269
2.14.5 show loopback-detect .....	269
2.15 MLAG 命令 .....	270
2.15.1 mlag configuration .....	270
2.15.2 peer-address .....	271
2.15.3 peer-link .....	272
2.15.4 timers mlag .....	272
2.15.5 reload-delay .....	273
2.15.6 sync-orphan .....	274
2.15.7 mlag .....	274
2.15.8 clear mlag count .....	275
2.15.9 show mlag .....	276
2.15.10 show mlag peer .....	277
2.15.11 show mlag interface .....	278
2.16 PoE 命令 .....	278
2.16.1 power inline enable .....	278
2.16.2 power inline enable .....	279
2.16.3 power inline legacy .....	280
2.16.4 power inline max .....	280
2.16.5 power inline port max .....	281
2.16.6 power inline policy .....	282
2.16.7 power inline priority .....	282
2.16.8 power inline high-inrush .....	283
2.16.9 power inline admin disable time-range .....	284
2.16.10 power inline pd-description .....	284
2.17 PoE 检测和调试命令 .....	285
2.17.1 show power inline .....	285
2.17.2 show power inline .....	287
2.17.3 show environment .....	288
3 设备管理命令行参考 .....	1
3.1 STM 命令 stm prefer .....	1
3.1.1 stm prefer .....	1
3.1.2 show stm prefer .....	2
3.2 日志管理命令 .....	3
3.2.1 clear logging buffer .....	3
3.2.2 logging alarm-trap .....	4
3.2.3 logging file .....	5
3.2.4 logging level file .....	5
3.2.5 logging buffer .....	6
3.2.6 logging level module .....	7

---

---

3.2.7 logging merge .....	8
3.2.8 logging sync .....	9
3.2.9 logging operate.....	10
3.2.10 logging server.....	11
3.2.11 logging server address .....	11
3.2.12 logging server facility .....	12
3.2.13 logging server severity .....	13
3.2.14 logging timestamp.....	15
3.2.15 show logging .....	15
3.2.16 show logging buffer .....	16
3.3 Mirror 命令 .....	17
3.3.1 monitor session destination interface .....	17
3.3.2 monitor session destination cpu .....	18
3.3.3 monitor session destination group.....	19
3.3.4 member .....	20
3.3.5 monitor session source interface .....	21
3.3.6 monitor session source vlan .....	22
3.3.7 monitor session source cpu .....	24
3.3.8 monitor session destination remote .....	25
3.3.9 monitor mac escape.....	26
3.3.10 show monitor .....	27
3.3.11 show monitor mac escape .....	29
3.3.12 monitor destination forwarding enable .....	29
3.3.13 monitor cpu set packet buffer.....	30
3.3.14 monitor cpu capture strategy .....	31
3.3.15 show monitor cpu packet .....	31
3.3.16 clear monitor cpu packet all .....	32
3.3.17 show monitor cpu packet buffer-size .....	33
3.3.18 show monitor cpu capture strategy .....	33
3.3.19 cpu-traffic-limit reason mirror-to-cpu .....	34
3.4 设备管理命令 .....	35
3.4.1 temperature .....	35
3.4.2 show environment.....	35
3.4.3 boot system .....	36
3.4.4 show transceiver.....	37
3.4.5 update bootrom .....	39
3.4.6 update epld.....	40
3.4.7 Show reboot-info .....	40
3.5 Bootrom 命令.....	42
3.5.1 version.....	42
3.5.2 setenv .....	42
3.5.3 saveenv.....	43

---

---

3.5.4 printenv .....	44
3.5.5 reset.....	44
3.5.6 ping .....	45
3.5.7 ls.....	46
3.5.8 boot_tftp.....	46
3.5.9 boot_tftp_nopass .....	47
3.5.10 boot_flash.....	48
3.5.11 boot_flash_nopass .....	49
3.5.12 upgrade_uboot.....	49
3.6 Bootup Diagnostic 命令 .....	50
3.6.1 diagnostic bootup level .....	50
3.6.2 show diagnostic bootup level .....	51
3.6.3 show diagnostic bootup result .....	51
3.7 Bootstrap 命令 .....	52
3.7.1 bootstrap.....	52
3.7.2 show smart-config config.....	53
4 网络管理命令行参考.....	55
4.1 网络诊断命令.....	55
4.1.1 ping .....	55
4.1.2 traceroute .....	56
4.2 NTP 命令 .....	57
4.2.1 ntp ace.....	57
4.2.2 ntp authentication.....	59
4.2.3 ntp broadcast client .....	59
4.2.4 ntp broadcastdelay .....	60
4.2.5 ntp disable .....	61
4.2.6 ntp key.....	62
4.2.7 ntp interface reload.....	62
4.2.8 ntp max-distance .....	63
4.2.9 ntp peer .....	64
4.2.10 ntp refclock .....	65
4.2.11 ntp server.....	66
4.2.12 ntp trustedkey.....	67
4.2.13 show ntp .....	67
4.2.14 show ntp ace.....	68
4.2.15 show ntp associations.....	69
4.2.16 show ntp key .....	70
4.2.17 show ntp status .....	70
4.2.18 show ntp statistics .....	71
4.2.19 clear ntp statistics .....	72
4.3 Phy Loopback 命令 .....	73

---

---

4.3.1 loopback phy .....	73
4.3.2 loopback port .....	73
4.3.3 no loopback.....	74
4.3.4 show phy loopback .....	75
4.3.5 l2 ping .....	76
4.3.6 l2 ping response .....	77
4.3.7 show l2ping response .....	77
4.3.8 show l2ping state.....	78
4.3.9 l2 ping stop.....	79
4.3.10 l2 ping forward enable .....	79
4.3.11 debug l2ping.....	80
4.3.12 show debugging l2ping .....	81
4.4 SNMP 命令 .....	81
4.4.1 snmp-server access.....	81
4.4.2 snmp-server community.....	83
4.4.3 snmp-server context .....	83
4.4.4 snmp-server enable .....	84
4.4.5 snmp-server engineID .....	85
4.4.6 snmp-server group .....	86
4.4.7 snmp-server notify .....	86
4.4.8 snmp-server system-contact .....	87
4.4.9 snmp-server system-location.....	88
4.4.10 snmp-server target-address.....	89
4.4.11 snmp-server trap enable .....	90
4.4.12 snmp-server trap delay .....	91
4.4.13 snmp-server trap target-address .....	91
4.4.14 snmp-server inform target-address.....	92
4.4.15 snmp-server usm-user .....	93
4.4.16 snmp-server version .....	94
4.4.17 snmp-server view .....	95
4.4.18 snmp-server access-group NAME in .....	96
4.4.19 show snmp .....	97
4.4.20 show snmp-server access .....	98
4.4.21 show snmp-server community .....	98
4.4.22 show snmp-server context.....	99
4.4.23 show snmp-server engineID.....	100
4.4.24 show snmp-server group .....	100
4.4.25 show snmp-server notify .....	101
4.4.26 show snmp-server sys-info.....	102
4.4.27 show snmp-server trap-receiver .....	103
4.4.28 show snmp-server usm-user.....	103
4.4.29 show snmp-server version.....	104

---

---

4.4.30 show snmp-server view.....	105
4.5 SFLOW 命令 .....	106
4.5.1 sflow enable .....	106
4.5.2 sflow agent .....	106
4.5.3 sflow collector.....	107
4.5.4 sflow counter interval.....	108
4.5.5 sflow counter-sampling enable.....	109
4.5.6 sflow flow-sampling rate .....	109
4.5.7 sflow flow-sampling enable .....	110
4.5.8 show sflow .....	111
4.6 LLDP 命令 .....	112
4.6.1 lldp enable(全局) .....	112
4.6.2 lldp enable(接口) .....	113
4.6.3 lldp system-name .....	113
4.6.4 lldp system-description .....	114
4.6.5 lldp management .....	115
4.6.6 lldp msg-tx-hold.....	116
4.6.7 lldp timer msg-tx-interval .....	117
4.6.8 lldp timer reinit-delay.....	117
4.6.9 lldp timer tx-delay.....	118
4.6.10 lldp tlv basic .....	119
4.6.11 lldp tlv 8021-org-specific .....	120
4.6.12 lldp tlv 8021-org-specific vlan-name-value .....	121
4.6.13 lldp tlv 8023-org-specific .....	122
4.6.14 lldp tlv med .....	123
4.6.15 lldp tlv med location-id.....	124
4.6.16 debug lldp.....	125
4.6.17 show lldp local .....	126
4.6.18 show lldp neighbor.....	127
4.6.19 show lldp statistics .....	128
4.6.20 clear lldp statistics.....	129
4.6.21 lldp ignore-pvid-inconsistency.....	130
4.7 TELEMETRY 命令.....	130
4.7.1 sensor-group.....	130
4.7.2 sensor-path .....	131
4.7.3 destination-group .....	132
4.7.4 ipv4-address port protocol grpc .....	133
4.7.5 subscription.....	134
4.7.6 subs-sensor-group sample-interval.....	134
4.7.7 subs-destination-group .....	135
4.7.8 telemetry-sample enable .....	136

---

4.7.9 show telemetry sensor-path.....	137
4.7.10 show telemetry sensor.....	138
4.7.11 show telemetry destination.....	139
4.7.12 show telemetry subscription.....	140
4.8 Restconf 配置.....	141
4.8.1 service restconf enable.....	141
5 组播命令行参考.....	142
5.1 组播路由命令.....	142
5.1.1 ip multicast-routing.....	142
5.1.2 ip multicast route-limit.....	143
5.1.3 ip mroute-rpf.....	143
5.1.4 show ip mroute.....	144
5.1.5 show ip mvif.....	145
5.1.6 show ip multicast groups count.....	146
5.1.7 show ip mroute-rpf.....	147
5.1.8 show resource mcast.....	148
5.1.9 clear ip mroute.....	149
5.2 IGMP 命令.....	149
5.2.1 ip igmp access-group.....	149
5.2.2 ip igmp immediate-leave group-list.....	150
5.2.3 ip igmp last-member-query-count.....	151
5.2.4 ip igmp last-member-query-interval.....	152
5.2.5 ip igmp limit.....	153
5.2.6 ip igmp mroute-proxy.....	154
5.2.7 ip igmp proxy-service.....	154
5.2.8 ip igmp querier-timeout.....	155
5.2.9 ip igmp query-interval.....	156
5.2.10 ip igmp query-max-response-time.....	157
5.2.11 ip igmp robustness-variable.....	158
5.2.12 ip igmp version.....	158
5.2.13 ip igmp static-group.....	159
5.2.14 ip igmp ssm-map enable.....	160
5.2.15 ip igmp ssm-map static.....	161
5.2.16 clear ip igmp.....	161
5.2.17 clear ip igmp interface.....	162
5.2.18 show ip igmp groups.....	163
5.2.19 show ip igmp groups interface.....	164
5.2.20 show ip igmp groups count.....	165
5.2.21 show ip igmp interface.....	165
5.3 IGMP Snooping 命令.....	166
5.3.1 ip igmp snooping.....	166

---



---

5.3.2 ip igmp snooping fast-leave .....	167
5.3.3 ip igmp snooping last-member-query-interval .....	168
5.3.4 ip igmp snooping global source-address .....	169
5.3.5 ip igmp snooping max-member-num .....	170
5.3.6 ip igmp snooping query-interval .....	170
5.3.7 ip igmp snooping query-max-response-time .....	171
5.3.8 ip igmp snooping report-suppression .....	172
5.3.9 ip igmp snooping version .....	173
5.3.10 ip igmp snooping discard-unknown .....	174
5.3.11 ip igmp snooping querier tcn .....	175
5.3.12 ip igmp snooping vlan access-group .....	175
5.3.13 ip igmp vlan mrouter interface .....	176
5.3.14 ip igmp vlan mrouter-aging-interval .....	177
5.3.15 ip igmp snooping vlan querier .....	178
5.3.16 ip igmp snooping vlan querier address .....	178
5.3.17 ip igmp snooping vlan querier-timeout .....	179
5.3.18 ip igmp snooping vlan static-group .....	180
5.3.19 clear ip igmp snooping group .....	181
5.3.20 clear ip igmp snooping vlan .....	181
5.3.21 show ip igmp snooping global .....	182
5.3.22 show ip igmp snooping groups .....	183
5.3.23 show ip igmp snooping groups vlan .....	183
5.3.24 show ip igmp snooping groups count .....	184
5.3.25 show ip igmp snooping querier .....	185
5.3.26 show ip igmp snooping mrouter .....	186
5.3.27 show ip igmp snooping vlan .....	187
5.3.28 show resource l2mcast .....	188
5.4 PIM 命令 .....	189
5.4.1 ip pim accept-register .....	189
5.4.2 ip pim anycast-rp .....	189
5.4.3 ip pim bsr-candidate .....	190
5.4.4 ip pim bsr-border .....	191
5.4.5 ip pim dr-priority .....	192
5.4.6 ip pim exclude-genid .....	192
5.4.7 ip pim hello-interval .....	193
5.4.8 ip pim ignore-rp-set-priority .....	194
5.4.9 ip pim jp-timer .....	194
5.4.10 ip pim neighbor-filter .....	195
5.4.11 ip pim register-rate-limit .....	196
5.4.12 ip pim register-source .....	197
5.4.13 ip pim register-rp-reachability .....	198
5.4.14 ip pim register-suppression .....	198

---

---

5.4.15 ip pim rp-address.....	199
5.4.16 ip pim rp-candidate .....	200
5.4.17 ip pim rp-register-kat.....	201
5.4.18 ip pim spt-switch-threshold infinity .....	202
5.4.19 ip pim cisco-register-checksum.....	202
5.4.20 ip pim sparse-mode .....	203
5.4.21 ip pim dense-mode .....	204
5.4.22 ip pim hello-holdtime.....	205
5.4.23 ip pim propagation-delay .....	205
5.4.24 ip pim state-refresh origination-interval.....	206
5.4.25 ip pim unicast-bsm .....	207
5.4.26 ip pim ssm.....	208
5.4.27 show ip pim sparse-mode bsr-router .....	208
5.4.28 show ip pim sparse-mode interface.....	209
5.4.29 show ip pim sparse-mode local-member.....	210
5.4.30 show ip pim sparse-mode mroute .....	211
5.4.31 show ip pim sparse-mode neighbor.....	212
5.4.32 show ip pim sparse-mode rp mapping.....	213
5.4.33 show ip pim sparse-mode rp-hash.....	214
5.4.34 show ip pim sparse-mode spt-threshold .....	214
5.4.35 show ip pim dense-mode interface.....	215
5.4.36 show ip pim dense-mode mroute .....	216
5.4.37 show ip pim dense-mode neighbor .....	217
5.4.38 show ip pim dense-mode nexthop.....	217
5.4.39 ip pim virtual address enable.....	218
5.5 MVR 命令 .....	219
5.5.1 mvr.....	219
5.5.2 mvr vlan .....	219
5.5.3 mvr group.....	220
5.5.4 mvr source-address .....	221
5.5.5 mvr type .....	222
5.5.6 show mvr.....	222
5.5.7 show mvr interface.....	223
5.5.8 show mvr group .....	224
5.5.9 show mvr group static .....	224
5.5.10 show resource mvr .....	225
6 安全性命令行参考.....	227
6.1 端口安全命令.....	227
6.1.1 clear port-security address-table static .....	227
6.1.2 switchport port-security .....	228
6.1.3 switchport port-security mac-address.....	228

---

---

6.1.4 switchport port-security maximum .....	229
6.1.5 switchport port-security violation .....	230
6.1.6 switchport port-security sticky .....	231
6.1.7 switchport port-security sticky mac-address .....	231
6.1.8 show port-security address-table .....	232
6.1.9 show port-security current mac-num interface .....	233
6.1.10 show port-security interface .....	234
6.1.11 show port-security maximum mac-num interface .....	235
6.2 VLAN 安全命令 .....	236
6.2.1 vlan mac-limit maximum .....	236
6.2.2 vlan mac-limit action .....	236
6.2.3 vlan mac learning .....	237
6.2.4 show vlan-security .....	238
6.3 Time Range 命令 .....	239
6.3.1 time-range .....	239
6.3.2 absolute .....	240
6.3.3 periodic .....	241
6.3.4 show time-range .....	242
6.4 ACL 命令 .....	243
6.4.1 mac access-list .....	243
6.4.2 sequence-num .....	243
6.4.3 deny src-mac .....	245
6.4.4 permit src-mac .....	246
6.4.5 remark .....	248
6.4.6 show access-list mac .....	248
6.4.7 ip access-list .....	249
6.4.8 deny .....	250
6.4.9 deny tcp .....	252
6.4.10 deny udp .....	254
6.4.11 deny icmp .....	255
6.4.12 deny igmp .....	256
6.4.13 deny gre .....	256
6.4.14 deny nvgre .....	257
6.4.15 permit .....	258
6.4.16 permit tcp .....	259
6.4.17 permit udp .....	260
6.4.18 permit icmp .....	261
6.4.19 permit igmp .....	262
6.4.20 permit gre .....	262
6.4.21 permit nvgre .....	263
6.4.22 show access-list ip .....	264
6.5 Extend ACL 命令 .....	265

---

---

6.5.1 ip access-list extend .....	265
6.5.2 sequence-num .....	266
6.5.3 deny src-mac .....	267
6.5.4 permit src-mac .....	268
6.5.5 deny.....	269
6.5.6 deny tcp.....	271
6.5.7 deny udp.....	273
6.5.8 deny icmp.....	274
6.5.9 deny igmp .....	275
6.5.10 deny gre.....	275
6.5.11 deny nvgre.....	276
6.5.12 permit.....	277
6.5.13 permit tcp .....	278
6.5.14 permit udp .....	279
6.5.15 permit icmp .....	280
6.5.16 permit igmp.....	281
6.5.17 permit gre .....	281
6.5.18 permit nvgre .....	282
6.5.19 remark .....	283
6.5.20 show access-list ip extend .....	284
6.6 ACLv6 命令 .....	284
6.6.1 ipv6 access-list .....	284
6.6.2 sequence-num .....	285
6.6.3 remark .....	286
6.6.4 deny.....	287
6.6.5 deny tcp.....	288
6.6.6 deny udp.....	290
6.6.7 deny icmp.....	290
6.6.8 deny gre.....	291
6.6.9 deny nvgre.....	292
6.6.10 permit.....	293
6.6.11 permit tcp .....	295
6.6.12 permit udp .....	296
6.6.13 permit icmp .....	297
6.6.14 permit gre .....	298
6.6.15 permit nvgre .....	298
6.6.16 show access-list ipv6.....	299
6.7 IEEE 802.1x 命令 .....	300
6.7.1 dot1x system-auth-ctrl.....	300
6.7.2 dot1x initialize .....	301
6.7.3 dot1x max-req .....	302
6.7.4 dot1x port-control .....	303

---

---

6.7.5 dot1x protocol-version .....	304
6.7.6 dot1x timeout quiet-period .....	304
6.7.7 dot1x reauthentication .....	305
6.7.8 dot1x re-authenticate .....	306
6.7.9 dot1x timeout .....	307
6.7.10 dot1x guest-vlan .....	308
6.7.11 show dot1x .....	309
6.7.12 debug dot1x .....	310
6.7.13 clear dot1x .....	311
6.7.14 dot1x re-activate radius-server .....	311
6.7.15 dot1x mandatory-domain .....	312
6.7.16 radius scheme .....	313
6.7.17 authentication server .....	313
6.7.18 domain .....	314
6.7.19 authentication radius-scheme .....	315
6.7.20 domain default enable .....	315
6.7.21 show radius-server-group all .....	316
6.7.22 dot1x auth-free .....	317
6.7.23 clear dot1x statistics .....	317
6.8 Arp Inspection 命令 .....	318
6.8.1 show ip arp inspection .....	318
6.8.2 show ip arp inspection interfaces .....	319
6.8.3 show ip arp inspection log .....	320
6.8.4 show ip arp inspection statistics .....	321
6.8.5 show ip arp inspection vlan .....	322
6.8.6 show debugging arp inspection .....	323
6.8.7 debug arp inspection .....	323
6.8.8 ip arp inspection filter .....	324
6.8.9 ip arp inspection log-buffer entries .....	325
6.8.10 ip arp inspection log-buffer logs interval .....	326
6.8.11 ip arp inspection validate .....	326
6.8.12 ip arp inspection vlan .....	327
6.8.13 ip arp inspection vlan WORD logging acl-macth .....	328
6.8.14 ip arp inspection vlan logging dhcp-bindings (all none permit) .....	329
6.8.15 clear ip arp inspection log-buffer .....	330
6.8.16 clear ip arp inspection statistics .....	330
6.8.17 ip arp inspection trust .....	331
6.8.18 arp access-list .....	332
6.8.19 ip mac .....	332
6.8.20 no sequence-num .....	333
6.8.21 show access-list arp .....	334
6.9 DHCP Snooping 命令 .....	335

---

---

6.9.1 clear dhcp snooping .....	335
6.9.2 dhcp snooping .....	336
6.9.3 dhcp snooping binding .....	337
6.9.4 dhcp snooping database .....	338
6.9.5 dhcp snooping information option .....	338
6.9.6 dhcp snooping information option allow-untrusted .....	339
6.9.7 dhcp snooping trust .....	340
6.9.8 dhcp snooping verify.....	341
6.9.9 dhcp snooping vlan .....	342
6.9.10 dhcp snooping vlan information option format-type circuit-id string .....	343
6.9.11 dhcp snooping information option format remote-id .....	343
6.9.12 show dhcp snooping binding.....	344
6.9.13 debug dhcp snooping .....	345
6.9.14 show dhcp snooping config.....	346
6.9.15 show dhcp snooping statistics .....	347
6.9.16 show dhcp snooping trusted-sources.....	348
6.10 IP Source Guard 命令 .....	348
6.10.1 ip source binding.....	348
6.10.2 no ip source binding.....	350
6.10.3 ip source maximal binding.....	350
6.10.4 ip verify source .....	351
6.10.5 show ip source binding .....	352
6.11 AAA 命令 .....	353
6.11.1 aaa new-model .....	353
6.11.2 aaa authentication login.....	354
6.11.3 aaa authorization exec .....	354
6.11.4 aaa accounting exec.....	355
6.11.5 aaa accounting commands.....	356
6.11.6 aaa privilege mapping .....	357
6.11.7 login authentication .....	357
6.11.8 authorization exec .....	358
6.11.9 accounting exec .....	359
6.11.10 accounting commands .....	359
6.11.11 show aaa method-lists authentication .....	360
6.11.12 show aaa status .....	361
6.11.13 show aaa privilege mapping .....	361
6.12 RADIUS 认证命令 .....	362
6.12.1 radius-server deadtime .....	362
6.12.2 radius-server host .....	363
6.12.3 radius-server retransmit.....	364
6.12.4 radius-server timeout.....	365
6.12.5 radius-server key .....	366

---

---

6.12.6 show radius-server .....	366
6.13 TACACS+认证命令 .....	367
6.13.1 clear tacacs statistics .....	367
6.13.2 show tacacs .....	368
6.13.3 tacacs-server host .....	369
6.14 Port-Isolate 命令 .....	370
6.14.1 port-isolate group .....	370
6.14.2 port-isolate mode .....	370
6.14.3 show port-isolate .....	371
6.15 私有 Vlan 命令 .....	372
6.15.1 switchport mode private-vlan .....	372
6.15.2 switchport private-vlan .....	373
6.15.3 show private-vlan .....	374
6.16 DDOS 命令 .....	375
6.16.1 ip icmp intercept .....	375
6.16.2 ip smurf intercept .....	376
6.16.3 ip fraggle intercept .....	376
6.16.4 ip udp intercept .....	377
6.16.5 ip tcp intercept .....	378
6.16.6 ip small-packet intercept .....	379
6.16.7 ip maceq intercept .....	380
6.16.8 ip ipeq intercept .....	380
6.16.9 show ip-intercept config .....	381
6.16.10 show ip-intercept statistics .....	382
6.16.11 clear ip-intercept statistics .....	383
6.17 Key Chain 命令 .....	384
6.17.1 key chain .....	384
6.17.2 key .....	384
6.17.3 key-string .....	385
6.17.4 accept-lifetime .....	386
6.17.5 send-lifetime .....	387
6.17.6 show key chain .....	388
6.18 Port Block 命令 .....	389
6.18.1 port-block .....	389
6.18.2 show port-block .....	390
6.19 设备管理安全命令 .....	391
6.19.1 telnet server acl .....	391
6.19.2 ssh server acl .....	392
7 IP 业务命令行参考 .....	393
7.1 ARP 命令 .....	393
7.1.1 arp .....	393

---

---

7.1.2 arp retry-interval .....	394
7.1.3 arp timeout .....	394
7.1.4 clear arp-cache .....	395
7.1.5 clear ip arp.....	396
7.1.6 clear ip arp statistics.....	397
7.1.7 show ip arp.....	397
7.1.8 show ip arp summary .....	398
7.1.9 debug arp.....	399
7.1.10 show debugging arp .....	400
7.1.11 proxy-arp enable.....	401
7.1.12 local-proxy-arp enable .....	402
7.1.13 gratuitous-arp-learning enable .....	402
7.2 DHCP Client 命令.....	403
7.2.1 ip address dhcp.....	403
7.2.2 management ip address dhcp .....	404
7.2.3 dhcp client request .....	405
7.2.4 dhcp client client-id.....	406
7.2.5 dhcp client class-id.....	407
7.2.6 dhcp client lease .....	408
7.2.7 dhcp client hostname.....	409
7.2.8 dhcp client default-router distance .....	410
7.2.9 dhcp client broadcast-flag .....	411
7.2.10 debug dhcp client .....	411
7.2.11 show dhcp client.....	412
7.2.12 show dhcp client statistics.....	413
7.2.13 clear dhcp client statistics.....	414
7.3 DHCP Relay 命令 .....	415
7.3.1 dhcp relay.....	415
7.3.2 dhcp-server(全局).....	416
7.3.3 dhcp-server (接口).....	416
7.3.4 dhcp relay information check.....	417
7.3.5 dhcp relay information option.....	418
7.3.6 dhcp relay information policy .....	419
7.3.7 dhcp relay information trust-all.....	419
7.3.8 dhcp relay information trusted .....	420
7.3.9 dhcp relay gateway.....	421
7.3.10 service dhcp .....	422
7.3.11 debug dhcp relay .....	422
7.3.12 show dhcp-server .....	423
7.3.13 show dhcp relay interfaces .....	424
7.3.14 show dhcp relay information config.....	425
7.3.15 show dhcp relay information trusted-sources.....	425

---



---

7.3.16 show dhcp relay statistics .....	426
7.3.17 clear dhcp relay statistics .....	427
7.4 DHCP Server 命令 .....	428
7.4.1 service dhcp .....	428
7.4.2 dhcp server(全局) .....	428
7.4.3 dhcp server (接口) .....	429
7.4.4 dhcp server database {enable disable} .....	430
7.4.5 dhcp server database auto-save interval .....	430
7.4.6 dhcp ping packets .....	431
7.4.7 dhcp ping timeout .....	432
7.4.8 dhcp pool .....	433
7.4.9 static-bind .....	434
7.4.10 dns-server address .....	435
7.4.11 domain-name .....	435
7.4.12 bootfile-name .....	436
7.4.13 tftp-server-address .....	437
7.4.14 gateway address .....	438
7.4.15 netbios-name-server .....	439
7.4.16 netbios-node-type .....	439
7.4.17 network .....	440
7.4.18 lease .....	441
7.4.19 option .....	442
7.4.20 dhcp excluded-address .....	443
7.4.21 show dhcp server conflict .....	443
7.4.22 show dhcp server binding .....	444
7.4.23 show dhcp server statistics .....	445
7.4.24 show dhcp server config .....	446
7.4.25 clear dhcp server conflict .....	446
7.4.26 clear dhcp server binding .....	447
7.4.27 clear dhcp server statistics .....	448
7.5 DNS 命令 .....	449
7.5.1 ip host .....	449
7.5.2 dns domain .....	449
7.5.3 dns server .....	450
7.5.4 show dns .....	451
7.5.5 show ip host .....	452
7.5.6 ip dns server .....	453
7.6 DNS 调试命令 .....	453
7.6.1 show ip dns servers .....	453
7.7 NAT 配置命令 .....	455
7.7.1 ip nat inside .....	455

---

7.7.2 ip nat outside .....	455
7.7.3 ip nat-sa outside-ip .....	456
7.7.4 ip nat-da protocol .....	457
7.7.5 ip nat-da inside .....	457
7.7.6 clear ip nat session .....	458
7.7.7 arp scan for-nat.....	459
7.7.8 nat session max-count .....	459
7.7.9 nat session aging-timer.....	460
7.7.10 nat session sync.....	460
7.8 NAT 调试命令.....	461
7.8.1 show ip nat session.....	461
7.8.2 show ip nat session statistics .....	462
7.8.3 show resource nat.....	463
8 IP 路由命令行参考 .....	464
8.1 IP Unicast-Routing 命令 .....	464
8.1.1 ip address .....	464
8.1.2 ip icmp error-interval .....	465
8.1.3 ip redirects.....	466
8.1.4 ip unreachable.....	467
8.1.5 ip verify unicast reverse-path.....	467
8.1.6 router-id (global).....	468
8.1.7 ip route .....	469
8.1.8 ip host-collect.....	470
8.1.9 show ip route.....	470
8.1.10 show ip route database .....	472
8.1.11 show ip protocols .....	473
8.1.12 show ip route summary .....	473
8.1.13 show ip route add-fib-fail.....	474
8.1.14 max-static-routes.....	475
8.1.15 show resource fib .....	476
8.1.16 ecmp load-balance-mode dynamic.....	476
8.1.17 ecmp load-balance-mode dynamic (efd-only tcp-only).....	477
8.1.18 ecmp load-balance-mode static .....	478
8.1.19 ecmp load-balance-mode static self-healing .....	478
8.1.20 ecmp load-balance-mode round-robin .....	479
8.1.21 ecmp hash-field-select.....	480
8.1.22 show ecmp information.....	480
8.1.23 ecmp load-balance hash-arithmetic .....	481
8.2 RIP 命令.....	482
8.2.1 aggregate-address.....	482
8.2.2 default-information originate (RIP) .....	483

---

---

8.2.3 default-metric (RIP) .....	483
8.2.4 distance (RIP).....	484
8.2.5 ip rip authentication .....	486
8.2.6 ip rip authentication mode.....	486
8.2.7 ip rip receive version.....	487
8.2.8 ip rip receive-packet.....	488
8.2.9 ip rip send version .....	489
8.2.10 ip rip send-packet.....	490
8.2.11 ip rip split-horizon.....	490
8.2.12 network (RIP).....	491
8.2.13 neighbor (RIP) .....	492
8.2.14 offset-list (RIP) .....	493
8.2.15 passive-interface (RIP).....	494
8.2.16 redistribute (RIP) .....	495
8.2.17 router rip .....	496
8.2.18 timers basic (RIP) .....	496
8.2.19 show ip rip database.....	497
8.2.20 show ip rip interface.....	498
8.2.21 version (RIP).....	499
8.2.22 distribute-list .....	500
8.2.23 address-family.....	501
8.2.24 show ip protocol rip .....	501
8.2.25 debug rip .....	502
8.2.26 show debugging rip.....	503
8.2.27 show ip rip database database-summary .....	504
8.2.28 show resource rip .....	505
8.3 OSPF 命令 .....	505
8.3.1 area authentication .....	505
8.3.2 area default-cost .....	507
8.3.3 area filter-list.....	508
8.3.4 area range .....	509
8.3.5 area stub .....	510
8.3.6 auto-cost.....	511
8.3.7 clear ip ospf.....	512
8.3.8 compatible rfc1583 .....	512
8.3.9 default-information originate (OSPF).....	513
8.3.10 default-metric (OSPF).....	514
8.3.11 distance (OSPF) .....	515
8.3.12 distribute-list (OSPF).....	516
8.3.13 ip ospf authentication .....	517
8.3.14 ip ospf authentication-key .....	518
8.3.15 ip ospf cost.....	519

---

---

8.3.16 ip ospf database-filter all out.....	520
8.3.17 ip ospf dead-interval.....	520
8.3.18 ip ospf hello-interval .....	521
8.3.19 ip ospf message-digest-key md5 .....	522
8.3.20 ip ospf mtu .....	523
8.3.21 ip ospf mtu-ignore.....	524
8.3.22 ip ospf priority.....	525
8.3.23 ip ospf retransmit-interval.....	526
8.3.24 ip ospf transmit-delay.....	526
8.3.25 ip ospf network .....	527
8.3.26 neighbor (OSPF) .....	528
8.3.27 network area (OSPF).....	529
8.3.28 overflow database external.....	530
8.3.29 passive-interface (OSPF) .....	531
8.3.30 redistribute (OSPF) .....	532
8.3.31 router-id (OSPF) .....	533
8.3.32 router ospf.....	534
8.3.33 summary-address (OSPF) .....	535
8.3.34 show ip ospf.....	536
8.3.35 show ip ospf border-routers .....	537
8.3.36 show ip ospf database .....	538
8.3.37 show ip ospf interface .....	540
8.3.38 show ip ospf neighbor .....	540
8.3.39 show ip ospf summary-address .....	541
8.3.40 show ip ospf database database-summary.....	542
8.3.41 show ip ospf route summary .....	543
8.3.42 show ip protocols ospf .....	544
8.3.43 show ip ospf processes-count.....	545
8.3.44 timers spf.....	545
8.3.45 max-concurrent-dd.....	546
8.3.46 maximum-area .....	547
8.3.47 refresh timer .....	548
8.3.48 debug ospf.....	548
8.3.49 debug ospf events.....	549
8.3.50 debug ospf ifsm.....	550
8.3.51 debug ospf nfsm.....	551
8.3.52 debug ospf lsa .....	551
8.3.53 debug ospf packet .....	552
8.3.54 debug ospf route.....	553
8.3.55 show debugging ospf .....	554
8.3.56 show resource ospf.....	555
8.3.57 area nssa .....	555

---

---

8.3.58 show ip ospf database .....	556
8.4 Route-map 命令 .....	557
8.4.1 route-map .....	557
8.4.2 match as-path .....	559
8.4.3 match community.....	560
8.4.4 match interface.....	561
8.4.5 match ip address.....	562
8.4.6 match ip address prefix-list .....	563
8.4.7 match ip next-hop .....	564
8.4.8 match ip next-hop prefix-list.....	565
8.4.9 match local-preference .....	566
8.4.10 match metric.....	567
8.4.11 match origin .....	568
8.4.12 match route-type external.....	569
8.4.13 match tag .....	570
8.4.14 set aggregator .....	571
8.4.15 set as-path.....	572
8.4.16 set atomic-aggregate .....	573
8.4.17 set comm-list delete .....	574
8.4.18 set community .....	575
8.4.19 set dampening .....	576
8.4.20 set extcommunity .....	577
8.4.21 set ip next-hop.....	579
8.4.22 set ip nex-hop load-share .....	579
8.4.23 set local-preference .....	580
8.4.24 set metric.....	581
8.4.25 set metric-type.....	582
8.4.26 set origin .....	583
8.4.27 set originator-id .....	584
8.4.28 set tag .....	585
8.4.29 set vpnv4 next-hop .....	586
8.4.30 set weight .....	587
8.4.31 show route-map.....	588
8.5 Prefix-list 命令 .....	589
8.5.1 ip prefix-list.....	589
8.5.2 ip prefix-list description .....	591
8.5.3 ip prefix-list sequence-number.....	591
8.5.4 show ip prefix-list .....	592
8.5.5 clear ip prefix-list .....	593
8.6 PBR 命令 .....	594
8.6.1 ip policy route-map .....	594
8.6.2 show ip policy route-map.....	595

---

---

8.6.3 show resource pbr .....	596
8.7 BGP 命令 .....	596
8.7.1 address-family .....	596
8.7.2 advertise l2vpn .....	597
8.7.3 aggregate-address .....	598
8.7.4 bgp always-compare-med .....	599
8.7.5 bgp bestpath as-path ignore .....	599
8.7.6 bgp bestpath compare-confed-aspath .....	600
8.7.7 bgp bestpath compare-routerid .....	601
8.7.8 bgp bestpath med .....	601
8.7.9 bgp client-to-client reflection .....	602
8.7.10 bgp cluster-id .....	603
8.7.11 bgp confederation identifier .....	604
8.7.12 bgp confederation peers .....	605
8.7.13 bgp dampening .....	606
8.7.14 bgp default ipv4-unicast .....	607
8.7.15 bgp default local-preference .....	607
8.7.16 bgp deterministic med .....	608
8.7.17 bgp enforce-first-as .....	609
8.7.18 bgp fast-external-failover .....	610
8.7.19 bgp log-neighbor-changes .....	610
8.7.20 bgp router-id .....	611
8.7.21 bgp scan-time .....	612
8.7.22 clear ip bgp * .....	613
8.7.23 clear ip bgp A.B.C.D .....	614
8.7.24 clear ip bgp dampening .....	615
8.7.25 clear ip bgp flap-statistics .....	616
8.7.26 clear ip bgp ASN .....	617
8.7.27 clear ip bgp external .....	618
8.7.28 clear ip bgp peer-group .....	619
8.7.29 clear ip bgp vrf .....	621
8.7.30 debug bgp .....	622
8.7.31 distance .....	623
8.7.32 exit-address-family .....	624
8.7.33 ip as-path access-list .....	624
8.7.34 ip community-list .....	625
8.7.35 ip community-list expanded .....	627
8.7.36 ip community-list standard .....	628
8.7.37 neighbor activate .....	629
8.7.38 neighbor advertisement-interval .....	630
8.7.39 neighbor allowas-in .....	631
8.7.40 neighbor attribute-unchanged .....	632

---

---

8.7.41 neighbor capability dynamic .....	633
8.7.42 neighbor capability orf prefix-list .....	633
8.7.43 neighbor capability route-refresh .....	634
8.7.44 neighbor default-originate .....	635
8.7.45 neighbor description .....	636
8.7.46 neighbor distribute-list .....	637
8.7.47 neighbor ebgp-multihop .....	638
8.7.48 neighbor filter-list .....	639
8.7.49 neighbor maximum-prefix .....	640
8.7.50 neighbor next-hop-self .....	641
8.7.51 neighbor override-capability .....	642
8.7.52 neighbor passive .....	643
8.7.53 neighbor peer-group (adding a neighbor) .....	644
8.7.54 neighbor peer-group (creating a peer-group) .....	645
8.7.55 neighbor prefix-list .....	645
8.7.56 neighbor remote-as .....	647
8.7.57 neighbor remove-private-AS .....	647
8.7.58 neighbor route-reflector-client .....	648
8.7.59 neighbor send-community .....	649
8.7.60 neighbor shutdown .....	650
8.7.61 neighbor soft-reconfiguration inbound .....	651
8.7.62 neighbor strict-capability-match .....	652
8.7.63 neighbor timers .....	653
8.7.64 neighbor unsuppress-map .....	654
8.7.65 neighbor update-source .....	655
8.7.66 neighbor weight .....	656
8.7.67 neighbor fake-as .....	657
8.7.68 network .....	657
8.7.69 network synchronization .....	659
8.7.70 synchronization .....	659
8.7.71 router bgp .....	660
8.7.72 redistribute (BGP) .....	661
8.7.73 show debugging bgp .....	662
8.7.74 show ip bgp .....	663
8.7.75 show ip bgp attribute-info .....	663
8.7.76 show ip bgp cidr-only .....	664
8.7.77 show ip bgp community .....	665
8.7.78 show ip bgp community-info .....	666
8.7.79 show ip bgp community-list .....	666
8.7.80 show ip bgp dampening .....	667
8.7.81 show ip bgp filter-list .....	668
8.7.82 show ip bgp inconsistent-as .....	669

---

---

8.7.83 show ip bgp neighbors .....	670
8.7.84 show ip bgp paths.....	671
8.7.85 show ip bgp prefix-list .....	671
8.7.86 show ip bgp quote-regexp .....	672
8.7.87 show ip bgp regexp .....	673
8.7.88 show ip bgp scan.....	674
8.7.89 show ip bgp summary .....	674
8.7.90 show ip bgp vpnv4 all .....	675
8.7.91 show ip bgp vpnv4 rd.....	676
8.7.92 show ip bgp vpnv4 vrf .....	677
8.7.93 timers .....	678
<b>9 流量管理命令行参考.....</b>	<b>680</b>
<b>9.1 QOS 命令.....</b>	<b>680</b>
9.1.1 bandwidth.....	680
9.1.2 class type qos .....	681
9.1.3 class type qos class-default .....	681
9.1.4 class type traffic-class .....	682
9.1.5 class-map type qos .....	683
9.1.6 class-map type traffic-class .....	683
9.1.7 clear qos aggregate-policer statistics.....	684
9.1.8 clear qos interface statistics policer flow .....	685
9.1.9 clear qos interface statistics policer port .....	685
9.1.10 clear qos interface statistics queue .....	686
9.1.11 match cos.....	687
9.1.12 match dscp .....	687
9.1.13 match precedence.....	689
9.1.14 match access-group .....	690
9.1.15 acl-statistics exclude-drop enable .....	691
9.1.16 match traffic-class .....	691
9.1.17 policy-map type qos.....	692
9.1.18 policy-map type traffic-class.....	693
9.1.19 pause buffer-size .....	693
9.1.20 priority level.....	694
9.1.21 flow-policer number.....	695
9.1.22 qos aggregate-policer .....	696
9.1.23 aggregate-policer (policy-map).....	697
9.1.24 policer(policy-map).....	697
9.1.25 qos policer(port).....	698
9.1.26 qos shape rate(port).....	699
9.1.27 shape rate(queue) .....	700
9.1.28 queue-limit .....	701

---



---

9.1.29 queue-limit dynamic .....	702
9.1.30 random-detect .....	702
9.1.31 set cos.....	703
9.1.32 set dscp.....	704
9.1.33 set precedence .....	704
9.1.34 set traffic-class .....	705
9.1.35 service-policy type qos.....	706
9.1.36 service-policy type traffic-class .....	706
9.1.37 show qos aggregate-policer statistics .....	707
9.1.38 show qos interface.....	708
9.1.39 show qos interface statistics policer flow.....	708
9.1.40 show qos interface statistics policer port.....	709
9.1.41 show qos interface statistics queue .....	710
<b>10 IPv6 安全命令行参考.....</b>	<b>712</b>
10.1 DHCPv6 Snooping 命令 .....	712
10.1.1 clear dhcpv6 snooping bindings learning.....	712
10.1.2 clear dhcpv6 snooping statistics.....	713
10.1.3 dhcpv6 snooping .....	713
10.1.4 dhcpv6 snooping binding .....	714
10.1.5 dhcpv6 snooping database.....	715
10.1.6 dhcpv6 snooping trust .....	716
10.1.7 dhcpv6 snooping vlan .....	716
10.1.8 show dhcpv6 snooping binding.....	717
10.1.9 debug dhcpv6 snooping .....	718
10.1.10 show dhcpv6 snooping config.....	719
10.1.11 show dhcpv6 snooping trusted-sources.....	720
10.1.12 show dhcpv6 snooping statistics .....	721
<b>11 IPv6 路由命令行参考.....</b>	<b>722</b>
11.1 OSPFv3 命令 .....	722
11.1.1 router ipv6 ospf.....	722
11.1.2 area default-cost .....	723
11.1.3 area range .....	723
11.1.4 area stub .....	724
11.1.5 auto-cost.....	725
11.1.6 clear ipv6 ospf.....	726
11.1.7 default-information originate (OSPFv3) .....	727
11.1.8 default-metric (OSPFv3).....	728
11.1.9 distance (OSPFv3) .....	729
11.1.10 distribute-list (OSPFv3) .....	730
11.1.11 enable db-summary-opt.....	731
11.1.12 ipv6 ospf cost .....	732

---

---

11.1.13 ipv6 ospf dead-interval.....	733
11.1.14 ipv6 ospf hello-interval .....	733
11.1.15 ipv6 ospf mtu-ignore .....	734
11.1.16 ipv6 ospf priority.....	735
11.1.17 ipv6 ospf retransmit-interval .....	736
11.1.18 ipv6 ospf transmit-delay.....	737
11.1.19 passive-interface (OSPFv3).....	738
11.1.20 redistribute (OSPFv3) .....	739
11.1.21 router-id (OSPFv3).....	740
11.1.22 summary-address (OSPFv3) .....	741
11.1.23 show ipv6 ospf .....	742
11.1.24 show ipv6 ospf database.....	743
11.1.25 show ipv6 ospf interface .....	744
11.1.26 show ipv6 ospf neighbor .....	745
11.1.27 show ipv6 ospf database database-summary .....	746
11.1.28 show ipv6 ospf route .....	747
11.1.29 show ipv6 ospf route summary .....	748
11.1.30 show ipv6 protocols ospf.....	749
11.1.31 timers spf.....	750
11.1.32 max-concurrent-dd .....	751
11.1.33 debug ipv6 ospf.....	752
11.1.34 debug ipv6 ospf events.....	752
11.1.35 debug ipv6 ospf ifsm .....	753
11.1.36 debug ipv6 ospf nfsm .....	754
11.1.37 debug ipv6 ospf lsa.....	755
11.1.38 debug ipv6 ospf packet.....	756
11.1.39 debug ipv6 ospf route.....	757
11.1.40 show debuggin ipv6 ospf.....	757
11.1.41 show resource ipv6 ospf.....	758
RIPng 命令.....	759
11.1.42 router ipv6 rip.....	759
11.1.43 ipv6 router rip.....	760
11.1.44 ipv6 rip metric-offset.....	760
11.1.45 ipv6 rip split-horizon.....	761
11.1.46 default-information originate .....	762
11.1.47 default-metric .....	763
11.1.48 distance.....	763
11.1.49 neighbor .....	765
11.1.50 offset-list .....	766
11.1.51 passive-interface.....	767
11.1.52 redistribute .....	767
11.1.53 timers basic .....	768

---

---

11.1.54 distribute-list .....	769
11.1.55 aggregate-address .....	770
11.1.56 route map.....	771
11.1.57 maximum-prefix.....	772
11.1.58 show ipv6 rip database .....	773
11.1.59 show ipv6 rip interface.....	774
11.1.60 show ipv6 rip database database-summary .....	774
11.1.61 show ipv6 protocol rip .....	775
11.1.62 debug ipv6 rip .....	776
11.1.63 show debugging ipv6 rip .....	777
11.1.64 show resource ipv6 rip .....	777
11.1.65 clear ipv6 rip router .....	778
11.2 IPv6 单播配置 .....	779
11.2.1 ipv6 enable .....	779
11.2.2 max-static-v6routes .....	780
11.2.3 ipv6 route .....	780
11.2.4 ipv6 address.....	782
11.2.5 show ipv6 route .....	783
11.2.6 show ipv6 interface .....	785
11.2.7 ipv6 verify unicast reverse-path .....	786
11.2.8 ipv6 icmp error-interval .....	787
11.3 Ipv6 Prefix-list 命令 .....	788
11.3.1 ipv6 prefix-list.....	788
11.3.2 ipv6 prefix-list description .....	790
11.3.3 ipv6 prefix-list sequence-number .....	790
11.3.4 show ipv6 prefix-list .....	791
11.3.5 clear ipv6 prefix-list .....	792
11.4 Route-map 命令 .....	793
11.4.1 route-map .....	793
11.4.2 match as-path .....	795
11.4.3 match community.....	796
11.4.4 match interface .....	797
11.4.5 match ipv6 address.....	798
11.4.6 match ipv6 address prefix-list .....	799
11.4.7 match ipv6 next-hop.....	800
11.4.8 match ipv6 next-hop prefix-list .....	801
11.4.9 match local-preference .....	802
11.4.10 match metric.....	803
11.4.11 match origin.....	804
11.4.12 match route-type external.....	805
11.4.13 match tag.....	806
11.4.14 set ipv6 aggregator .....	807

---

---

11.4.15 set as-path.....	808
11.4.16 set atomic-aggregate.....	809
11.4.17 set comm-list delete.....	810
11.4.18 set community .....	811
11.4.19 set dampening.....	813
11.4.20 set extcommunity .....	814
11.4.21 set ipv6 next-hop.....	815
11.4.22 set ipv6 next-hop load-share .....	816
11.4.23 set local-preference .....	817
11.4.24 set metric .....	818
11.4.25 set metric-type.....	819
11.4.26 set origin.....	820
11.4.27 set ipv6 originator-id .....	821
11.4.28 set tag .....	822
11.4.29 set vpnv6 next-hop.....	823
11.4.30 set weight .....	824
11.4.31 show route-map.....	825
<b>12 IPv6 业务命令行.....</b>	<b>827</b>
12.1 隧道配置命令.....	827
12.1.1 interface .....	827
12.1.2 tunnel mode ipv6ip.....	828
12.1.3 tunnel source .....	829
12.1.4 tunnel destination .....	830
12.1.5 tunnel enable .....	830
12.1.6 tunnel gre key.....	831
12.1.7 tunnel dscp .....	832
12.1.8 ipv6 mtu .....	833
12.1.9 show interface tunnel .....	833
12.1.10 show resource tunnel.....	834
12.2 NDP 配置.....	835
12.2.1 ipv6 neighbor .....	835
12.2.2 clear ipv6 neighbors.....	836
12.2.3 ipv6 hop-limit.....	837
12.2.4 ipv6 nd ra hop-limit.....	838
12.2.5 ipv6 nd dad attempts .....	838
12.2.6 ipv6 nd ns-interval .....	839
12.2.7 ipv6 nd ra suppress.....	840
12.2.8 ipv6 nd ra mtu suppress .....	841
12.2.9 ipv6 nd ra interval .....	842
12.2.10 ipv6 nd ra lifetime .....	842
12.2.11 ipv6 nd reachable-time.....	843

---

12.2.12 ipv6 nd managed-config-flag .....	844
12.2.13 ipv6 nd other-config-flag .....	845
12.2.14 ipv6 nd prefix .....	845
12.2.15 show ipv6 interface IFNAME prefix .....	847
12.2.16 show ipv6 neighbors .....	847
12.2.17 debug ipv6 nd.....	848
12.3 DHCPv6 Relay 命令 .....	849
12.3.1 dhcpv6 relay.....	849
12.3.2 dhcpv6-server(全局).....	850
12.3.3 dhcpv6-server (接口).....	851
12.3.4 dhcpv6 relay remote-id option .....	851
12.3.5 dhcpv6 relay remote-id format.....	852
12.3.6 dhcpv6 relay pd route.....	853
12.3.7 dhcpv6 relay pd route distance.....	854
12.3.8 service dhcpv6 .....	854
12.3.9 debug dhcpv6 relay .....	855
12.3.10 show dhcpv6-server .....	856
12.3.11 show dhcpv6 relay interfaces .....	856
12.3.12 show dhcpv6 relay pd client.....	857
12.3.13 show dhcpv6 relay statistics.....	858
12.3.14 clear dhcpv6 relay statistics .....	859
12.3.15 clear dhcpv6 relay pd route .....	859
13 IPv6 组播命令行参考.....	861
13.1 IPv6 组播路由命令 .....	861
13.1.1 ipv6 multicast-routing .....	861
13.1.2 ipv6 multicast route-limit.....	862
13.1.3 ipv6 mroute-rpf.....	862
13.1.4 show ipv6 mroute.....	863
13.1.5 show ipv6 mif .....	865
13.1.6 show ipv6 multicast groups count.....	865
13.1.7 show ipv6 mroute-rpf.....	866
13.1.8 show resource mcast6 .....	867
13.2 MLD 命令 .....	868
13.2.1 ipv6 mld access-group .....	868
13.2.2 ipv6 mld immediate-leave group-list .....	869
13.2.3 ipv6 mld last-member-query-count.....	870
13.2.4 ipv6 mld last-member-query-interval.....	870
13.2.5 ipv6 mld limit.....	871
13.2.6 ipv6 mld mroute-proxy .....	872
13.2.7 ipv6 mld proxy-service .....	873
13.2.8 ipv6 mld querier-timeout.....	874

---

---

13.2.9 ipv6 mld query-interval.....	874
13.2.10 ipv6 mld query-max-response-time .....	875
13.2.11 ipv6 mld robustness-variable .....	876
13.2.12 ipv6 mld version .....	877
13.2.13 ipv6 mld static-group .....	878
13.2.14 ipv6 mld ssm-map enable .....	879
13.2.15 ipv6 mld ssm-map static .....	879
13.2.16 clear ipv6 mld .....	880
13.2.17 clear ipv6 mld interface.....	881
13.2.18 show ipv6 mld groups .....	882
13.2.19 show ipv6 mld groups interface .....	883
13.2.20 show ipv6 mld groups count .....	884
13.2.21 show ipv6 mld interface .....	884
13.3 MLD Snooping 命令 .....	885
13.3.1 ipv6 mld snooping.....	885
13.3.2 ipv6 mld snooping fast-leave .....	886
13.3.3 ipv6 mld last-member-query-interval.....	887
13.3.4 ipv6 mld snooping global source-address .....	888
13.3.5 ipv6 mld snooping max-member-num .....	889
13.3.6 ipv6 mld snooping query-interval .....	889
13.3.7 ipv6 mld snooping query-max-response-time .....	890
13.3.8 ipv6 mld snooping report-suppression .....	891
13.3.9 ipv6 mld snooping version .....	892
13.3.10 ipv6 mld snooping discard-unknown .....	893
13.3.11 ipv6 mld snooping querier tcn.....	894
13.3.12 ipv6 mld snooping vlan access-group .....	894
13.3.13 ipv6 mld vlan mrouter interface .....	895
13.3.14 ipv6 mld vlan mrouter-aging-interval .....	896
13.3.15 ipv6 mld snooping vlan querier.....	897
13.3.16 ipv6 mld snooping vlan querier address.....	897
13.3.17 ipv6 mld snooping vlan querier-timeout .....	898
13.3.18 ipv6 mld snooping vlan static-group .....	899
13.3.19 clear ipv6 mld snooping group.....	900
13.3.20 clear ipv6 mld snooping vlan group .....	900
13.3.21 show ipv6 mld snooping global .....	901
13.3.22 show ipv6 mld snooping groups .....	902
13.3.23 show ipv6 mld snooping groups vlan.....	902
13.3.24 show ipv6 mld snooping groups count.....	903
13.3.25 show ipv6 mld snooping querier .....	904
13.3.26 show ipv6 mld snooping mrouter .....	905
13.3.27 show ipv6 mld snooping vlan .....	906
13.3.28 show resource l2mcast .....	907

---

---

13.4 PIMv6 命令.....	908
13.4.1 ipv6 pim accept-register.....	908
13.4.2 ipv6 pim anycast-rp.....	909
13.4.3 ipv6 pim bsr-candidate.....	909
13.4.4 ipv6 pim bsr-border.....	910
13.4.5 ipv6 pim dr-priority.....	911
13.4.6 ipv6 pim exclude-genid.....	912
13.4.7 ipv6 pim hello-interval.....	912
13.4.8 ipv6 pim ignore-rp-set-priority.....	913
13.4.9 ipv6 pim jp-timer.....	914
13.4.10 ipv6 pim neighbor-filter.....	914
13.4.11 ipv6 pim register-rate-limit.....	915
13.4.12 ipv6 pim register-source.....	916
13.4.13 ipv6 pim register-rp-reachability.....	917
13.4.14 ipv6 pim register-suppression.....	918
13.4.15 ipv6 pim rp-address.....	918
13.4.16 ipv6 pim rp-candidate.....	919
13.4.17 ipv6 pim rp-register-kat.....	920
13.4.18 ipv6 pim spt-switch-threshold infinity.....	921
13.4.19 ipv6 pim cisco-register-checksum.....	922
13.4.20 ipv6 pim sparse-mode.....	922
13.4.21 ipv6 pim unicast-bsm.....	923
13.4.22 ipv6 pim ssm.....	924
13.4.23 show ipv6 pim sparse-mode bsr-router.....	925
13.4.24 show ipv6 pim sparse-mode interface.....	925
13.4.25 show ipv6 pim sparse-mode local-member.....	926
13.4.26 show ipv6 pim sparse-mode mroute.....	927
13.4.27 show ipv6 pim sparse-mode neighbor.....	928
13.4.28 show ipv6 pim sparse-mode rp mapping.....	929
13.4.29 show ipv6 pim sparse-mode rp-hash.....	930
13.4.30 show ipv6 pim sparse-mode spt-threshold.....	930
13.5 MVR6 命令.....	931
13.5.1 mvr6.....	931
13.5.2 mvr6 vlan.....	932
13.5.3 mvr6 group.....	933
13.5.4 mvr6 source-address.....	933
13.5.5 mvr6 type.....	934
13.5.6 show mvr6.....	935
13.5.7 show mvr6 interface.....	936
13.5.8 show mvr6 group.....	936
13.5.9 show mvr6 group static.....	937
13.5.10 show resource mvr6.....	938

---

---

14 VPN 命令行参考 .....	939
14.1 VRF 命令 .....	939
14.1.1 ip vrf.....	939
14.1.2 为租户绑定 VXLAN 路由的 VNI.....	940
14.1.3 show ip vrf .....	940
14.1.4 ip vrf forwarding .....	941
14.1.5 ip route vrf.....	942
14.1.6 arp vrf.....	943
14.1.7 show ip arp vrf .....	944
14.1.8 clear ip arp vrf.....	944
14.1.9 ping vrf.....	945
14.1.10 traceroute vrf.....	946
14.1.11 telnet vrf .....	947
14.1.12 rd .....	947
14.1.13 route-target .....	948
14.1.14 import map .....	949
14.1.15 export map .....	950
14.1.16 router-id.....	950
14.1.17 description.....	951
14.2 IPv4 GRE 隧道配置命令.....	952
14.2.1 interface .....	952
14.2.2 tunnel mode gre.....	953
14.2.3 tunnel source .....	953
14.2.4 tunnel destination .....	954
14.2.5 tunnel enable .....	955
14.2.6 tunnel gre key.....	956
14.2.7 tunnel dscp .....	957
14.2.8 keepalive .....	957
14.2.9 show interface tunnel .....	958
14.2.10 show resource tunnel.....	959
14.2.11 show tunnel keepalive statistics .....	960
14.2.12 clear tunnel keepalive statistics.....	960
14.2.13 clear tunnel statistics .....	961
15 可靠性命令行参考.....	963
15.1 BHM 命令.....	963
15.1.1 sysmon enable .....	963
15.1.2 show sysmon.....	963
15.1.3 heart-beat-monitor enable .....	964
15.1.4 heart-beat-monitor reactivate .....	965
15.1.5 show heart-beat-monitor .....	965
15.1.6 cpu-limit percent .....	966

---



---

15.2 CFM 命令 .....	967
15.2.1 ethernet cfm enable .....	967
15.2.2 ethernet cfm domain level .....	968
15.2.3 service .....	969
15.2.4 ethernet cfm mep .....	970
15.2.5 ethernet cfm mep crosscheck mpid .....	971
15.2.6 ethernet cfm mip .....	972
15.2.7 ethernet cfm cc enable domain .....	973
15.2.8 ethernet cfm cc domain priority .....	974
15.2.9 ethernet cfm loopback .....	974
15.2.10 ethernet cfm loopback mac .....	976
15.2.11 ethernet cfm errors enable domain .....	977
15.2.12 clear ethernet cfm errors .....	978
15.2.13 ethernet cfm ais status enable .....	978
15.2.14 ethernet cfm ais suppress alarm enable domain .....	980
15.2.15 ethernet cfm server-ais status enable level .....	980
15.2.16 show ethernet cfm domain .....	981
15.2.17 show ethernet cfm maintenance-points .....	982
15.2.18 show ethernet cfm maintenance-points local .....	982
15.2.19 show ethernet cfm maintenance-points remote .....	983
15.2.20 show ethernet cfm cc config .....	984
15.2.21 show ethernet cfm errors .....	985
15.2.22 show ethernet cfm ais mep .....	986
15.2.23 show ethernet cfm .....	986
15.2.24 ethernet cfm linktrace rmepid .....	987
15.2.25 ethernet cfm linktrace mac .....	988
15.2.26 ethernet cfm linktrace cache enable .....	989
15.2.27 ethernet cfm linktrace cache size .....	990
15.2.28 ethernet cfm linktrace cache holdtime .....	990
15.2.29 show ethernet cfm linktrace cache .....	991
15.2.30 clear ethernet cfm linktrace cache .....	992
15.2.31 ethernet cfm mip ccm-database size .....	992
15.2.32 ethernet cfm mip ccm-database holdtime .....	993
15.2.33 show ethernet cfm mip ccm-database .....	994
15.2.34 clear ethernet cfm mip ccm-database .....	994
15.2.35 ethernet cfm sf-reason .....	995
15.2.36 ethernet cfm mode .....	996
15.2.37 ethernet cfm lm enable dual-ended .....	997
15.2.38 ethernet cfm lm enable single-ended .....	998
15.2.39 ethernet cfm lm single-ended .....	999
15.2.40 show ethernet cfm lm .....	1000
15.2.41 ethernet cfm sd-reason .....	1001

---

---

15.2.42 ethernet cfm (1dm dmm).....	1002
15.2.43 ethernet cfm delaymeasurement cache enable .....	1003
15.2.44 ethernet cfm delaymeasurement cache size.....	1004
15.2.45 show ethernet cfm delaymeasurement cache .....	1005
15.2.46 clear ethernet cfm delaymeasurement cache .....	1005
15.2.47 ethernet cfm csf.....	1006
15.2.48 show ethernet cfm csf .....	1007
15.2.49 ethernet cfm lck enable .....	1008
15.2.50 show ethernet cfm lck .....	1009
15.2.51 show ethernet cfm lm brief .....	1009
15.2.52 ethernet cfm tst transmission enable .....	1010
15.2.53 ethernet cfm tst start/stop .....	1011
15.2.54 ethernet cfm tst reception enable.....	1012
15.2.55 show ethernet cfm tst .....	1013
15.2.56 clear ethernet cfm tst counters.....	1014
15.3 CPU Traffic Limit 命令.....	1015
15.3.1 cpu-traffic-limit total rate .....	1015
15.3.2 cpu-traffic-limit reason rate.....	1016
15.3.3 cpu-traffic-limit reason class.....	1018
15.3.4 show cpu traffic-limit.....	1019
15.4 CPU Traffic Statistics 命令 .....	1021
15.4.1 cpu-traffic-statistics time.....	1021
15.4.2 no cpu-traffic-statistics time.....	1021
15.4.3 show cpu traffic- statistics receive .....	1022
15.4.4 show cpu traffic-statistics receive all .....	1024
15.4.5 show cpu traffic-statistics transmit.....	1025
15.5 UDLD 命令.....	1026
15.5.1 udld enable.....	1026
15.5.2 udld port.....	1027
15.5.3 udld message interval.....	1027
15.5.4 udld reset.....	1028
15.5.5 show udld.....	1029
15.5.6 show udld neighbors .....	1029
15.5.7 debug udld.....	1030
15.5.8 show debugging udld .....	1031
15.6 Smart-Link 命令.....	1032
15.6.1 smart-link group.....	1032
15.6.2 smart-link relay enable.....	1032
15.6.3 interface .....	1033
15.6.4 protected mstp instance .....	1034
15.6.5 load-balance instance .....	1035
15.6.6 restore time.....	1036

---

---

15.6.7 restore enable .....	1037
15.6.8 flush send .....	1038
15.6.9 group enable.....	1039
15.6.10 smart-link flush receive.....	1039
15.6.11 smart-link tcn enable .....	1040
15.6.12 smart-link tcn query-count .....	1041
15.6.13 smart-link tcn query-interval.....	1042
15.6.14 show smart-link.....	1042
15.6.15 show smart-link group .....	1043
15.6.16 clear smart-link statistic .....	1044
15.6.17 debug smart-link .....	1044
15.7 Multi-Link 命令 .....	1045
15.7.1 multi-link group .....	1045
15.7.2 multi-link relay enable .....	1046
15.7.3 interface .....	1046
15.7.4 protected mstp instance.....	1048
15.7.5 load-balance instance .....	1049
15.7.6 restore time.....	1050
15.7.7 restore enable .....	1051
15.7.8 flush send .....	1051
15.7.9 group enable.....	1052
15.7.10 multi-link flush receive .....	1053
15.7.11 multi-link tcn enable .....	1054
15.7.12 multi-link tcn query-count.....	1055
15.7.13 multi-link tcn query-interval .....	1055
15.7.14 show multi-link .....	1056
15.7.15 show multi-link group.....	1057
15.7.16 clear multi-link statistic.....	1058
15.7.17 debug multi-link.....	1058
15.7.18 multilink-enhance interface.....	1059
15.7.19 multilink-enhance receive .....	1060
15.7.20 multilink-enhance send-interval.....	1060
15.7.21 multilink-enhance timeout .....	1061
15.8 Monitor Link 命令 .....	1062
15.8.1 monitor-link group .....	1062
15.8.2 monitor-link uplink interface .....	1062
15.8.3 monitor-link uplink smart-link group.....	1063
15.8.4 no monitor-link uplink .....	1064
15.8.5 monitor-link downlink interface.....	1065
15.8.6 monitor-link recover-time .....	1065
15.8.7 show monitor-link group.....	1066
15.8.8 debug monitor-link.....	1067

---

---

15.9 VRRP 命令.....	1068
15.9.1 advertisement-interval.....	1068
15.9.2 advertisement-interval msec.....	1069
15.9.3 interface (VRRP).....	1069
15.9.4 learnmaster-mode.....	1070
15.9.5 preempt-mode.....	1071
15.9.6 preempt delay.....	1072
15.9.7 priority(VRRP).....	1073
15.9.8 router vrrp.....	1073
15.9.9 track (VRRP).....	1074
15.9.10 enable /disable.....	1075
15.9.11 virtual-ip.....	1076
15.9.12 show vrrp.....	1077
15.10 Track 命令.....	1078
15.10.1 delay up.....	1078
15.10.2 delay down.....	1079
15.10.3 frequency.....	1079
15.10.4 ip sla monitor.....	1080
15.10.5 description string.....	1081
15.10.6 show ip sla monitor ip sla monitor schedule.....	1082
15.10.7 timeout.....	1082
15.10.8 threshold.....	1083
15.10.9 interval.....	1084
15.10.10 ttl.....	1085
15.10.11 tos.....	1085
15.10.12 data-size.....	1086
15.10.13 data-pattern.....	1087
15.10.14 fail-percent.....	1088
15.10.15 packets-per-test.....	1088
15.10.16 statistics (packet  test).....	1089
15.10.17 clear ip sla statistics.....	1090
15.10.18 show ip sla monitor track.....	1090
15.10.19 track interface linkstate.....	1091
15.10.20 track rtr reachability.....	1092
15.10.21 track rtr state.....	1093
15.10.22 track bfd.....	1094
15.10.23 type icmp-echo.....	1095
15.10.24 show ip sla monitor.....	1096
15.10.25 show track.....	1096
15.10.26 vrf.....	1097
15.11 VARP 命令.....	1098
15.11.1 ip virtual-router mac.....	1098

---

---

15.11.2 ip virtual-router address .....	1099
15.12 IP 双向转发检测配置.....	1100
15.12.1 bfd interval.....	1100
15.12.2 bfd NAME peer-ip interface .....	1101
15.12.3 bfd NAME peer-ip .....	1102
15.12.4 bfd set interval.....	1103
15.12.5 bfd global dscp.....	1104
15.12.6 bfd set dscp .....	1105
15.12.7 ip route .....	1105
15.12.8 ip ospf bfd .....	1106
15.12.9 bfd .....	1107
15.12.10 show bfd.....	1108
15.12.11 show bfd static configurations.....	1109
15.12.12 show bfd session .....	1109
15.12.13 show bfd interface.....	1111
16 EVPN 相关命令行参考.....	1113
16.1 Overlay 命令 .....	1113
16.1.1 vlan overlay enable .....	1113
16.1.2 overlay .....	1114
16.1.3 overlay 负载分担模式.....	1114
16.1.4 overlay 映射.....	1115
16.1.5 overlay 源 vtep.....	1116
16.1.6 overlay 动态隧道功能.....	1116
16.1.7 overlay 上联口.....	1117
16.1.8 show overlay .....	1118
16.2 VXLAN 命令 .....	1119
16.2.1 vxlan.....	1119
16.2.2 vxlan vni .....	1120
16.2.3 vtep reachability protocol bgp.....	1120
16.2.4 remote-vtep virtual-mac .....	1121
16.2.5 vxlan remote-vtep .....	1122
16.2.6 mac-address-table forward remote-vtep vxlan .....	1122
16.2.7 encapsulation mode.....	1123
16.2.8 encapsulation vxlan.....	1124
16.2.9 show overlay .....	1125
16.2.10 interface vxlan.....	1126
16.3 EVPN 命令 .....	1127
16.3.1 address-family l2vpn evpn .....	1127
16.3.2 neighbor activate .....	1127
16.3.3 neighbor send-community.....	1128
16.3.4 evpn.....	1129

---

---

16.3.5 vni .....	1130
16.3.6 rd .....	1131
16.3.7 route-target .....	1131
16.3.8 export map .....	1132
16.3.9 import map .....	1133
16.3.10 overlay host-collect .....	1134
16.3.11 suppress-arp .....	1134
16.3.12 show bgp evpn .....	1135
16.3.13 show bgp evpn neighbors .....	1136
16.3.14 show overlay host-information .....	1137
16.3.15 show overlay suppress-arp .....	1138
16.3.16 debug overlay evpn .....	1139
<b>17 堆叠配置命令 .....</b>	<b>1140</b>
17.1 SCF 命令 .....	1140
17.1.1 scf domain .....	1140
17.1.2 scf member .....	1141
17.1.3 scf priority .....	1141
17.1.4 interface scf .....	1142
17.1.5 port-member interface .....	1143
17.1.6 switch convert mode scf .....	1143
17.1.7 scf sync image to .....	1144
17.1.8 show scf upgrade progress .....	1145
17.1.9 reboot .....	1145
17.1.10 scf redundancy switch .....	1146
17.1.11 show scf .....	1147
17.1.12 show scf topology .....	1148
17.1.13 show running-config scf .....	1149
17.1.14 show scf config .....	1150
17.1.15 scf clear config .....	1151

# 1 基础命令行参考

## 1.1 系统管理配置命令

### 1.1.1 hostname

全局配置模式下使用 **hostname** 命令配置或修改主机名。

使用 **no** 命令将主机名恢复至缺省值。

#### 命令语法

**hostname** *name*

**no hostname**

name	新主机名
------	------

#### 命令模式

全局配置模式

#### 默认

主机名的缺省值为 Switch。

#### 使用说明

主机名将会在提示符和缺省配置文件中出现。

主机名必须符合 ARPANET 网络关于主机名的约定。包括英文字符，数字，连字号以及下划线。字数不能超过 64 个字符。

#### 举例说明

修改主机名为 `sandbox`。

```
Switch (config)# hostname sandbox
sandbox(config)#
```

## 1.1.2 management ip address

本命令设置交换机管理口的 IP 地址。

本命令的 **no** 格式用来删除管理口 IP 地址。

### 命令语法

**management ip address** { *ipv4-address/M* | *ipv4-address mask-ipv4-address* } [ **gateway** *gateway-ipv4-address* ]

**no management ip address**

**management ipv6 address** { *ipv6-address/M* | *ipv6-address mask-ipv6 address* } [ **gateway** *gateway-ipv6-address* ]

**no management ipv6 address**

ipv4-address/M	配置带掩码长度的 IPv4 地址
ipv4-address	配置 IPv4 地址
mask-ipv4-address	IPv4 地址的子网掩码
ipv6-address/M	配置带掩码长度的 IPv6 地址
ipv6-address	配置 IPv6 地址
mask-ipv6-address	IPv6 地址的子网掩码
gateway	配置网关
gateway-ipv4-address	配置网关 IPv4 地址
gateway-ipv6-address	配置网关 IPv6 地址

### 命令模式

全局配置模式

### 默认

无

### 使用说明

无

### 举例说明

设置交换机管理口的 IPv4 地址：

```
Switch(config)# management ip address 192.168.100.100/24
```

删除管理口 IPv4 地址：



```
Switch(config)# no management ip address
```

设置交换机管理口的 IPv6 地址:

```
Switch(config)# management ipv6 address 2001:1000::1000/96
```

删除管理口的 IPv6 地址:

```
Switch(config)# no management ipv6 address
```

### 1.1.3 management route

本命令可以用来设置交换机管理口的网关地址。

#### 命令语法

```
management route { add | del } gateway gateway-ipv4-address
```

```
management ipv6 route { add | del } gateway gateway-ipv6-address
```

add	添加路由
del	删除路由
ipv6	配置 IPv6 路由
gateway	配置网关
gateway-ipv4-address	网关 IPv4 地址
gateway-ipv6-address	网关 IPv6 地址

#### 命令模式

全局配置模式

#### 默认

无

#### 使用说明

无

#### 举例说明

设置交换机管理口的网关 IPv4 地址:

```
Switch(config)# management route add gateway 192.168.100.254
```

设置交换机管理口的网关 IPv6 地址:

```
Switch(config)# management ipv6 route add gateway 2001:1000::1
```

## 1.1.4 management interface shutdown

本命令关闭管理口。本命令的 no 格式用开启管理口。

### 命令语法

```
management interface shutdown
no management interface shutdown
```

### 命令模式

全局配置模式

### 默认

no shutdown

### 使用说明

无

### 举例说明

```
Switch(config)# management interface shutdown
Switch(config)# no management interface shutdown
```

### 相关命令

无

## 1.1.5 show management ip address

本命令显示交换机管理口 IP 地址。

### 命令语法

```
show management ip address
show management ipv6 address
```

### 命令模式

特权模式

### 默认

无

### 使用说明

无

## 举例说明

```
Switch# show management ip address
Management IP address is: 192.168.100.100/24
Gateway: 192.168.100.254
Switch# show management ipv6 address
Management IPv6 address is: 2001:1000::1000/96
Gateway: 2001:1000::1
```

## 相关命令

无

### 1.1.6 show management interface

本命令显示交换机管理口配置以及统计值。

## 命令语法

```
show management interface
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch# show management interface
Management Interface current state: DOWN
Description:
Link encap: Ethernet      HWaddr: 94:EB:AB:88:2A:B4
Inet addr: 192.168.100.102 Mask: 255.255.255.0
Bcast: 192.168.100.255    MTU: 1500
Speed: 10                  Duplex: Half
Auto-negotiation: Enable
Received:                   2 Packets,          128 Bytes (128.0 b)
Transmitted:                 1 Packets,          78 Bytes (78.0 b)
```

## 相关命令

**clear counters mgmt-if**

### 1.1.7 clear counters mgmt-if

本命令清除交换机管理口的统计值。

## 命令语法

```
clear counters mgmt-if
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch# clear counters mgmt-if
```

## 相关命令

无

## 1.1.8 enable password

本命令设置用户进入特权模式时的密码。

## 命令语法

```
enable password (privilege privilege_level | )(8| )LINE
```

```
no enable password
```

<b>privilege</b>	设置用户的特权等级
<b>privilege_level</b>	用户的特权等级，范围是 1~4
<b>8</b>	指定隐藏密码
<b>LINE</b>	设置密码

## 命令模式

全局配置模式

## 默认

无

## 使用说明

配置该命令后，用户进去特权模式需要输入密码。

## 举例说明

```
Switch(config)# enable password 123
Switch(config)# exit
Switch # disable
Switch> enable
Password:
Switch #
```

## 相关命令

无

### 1.1.9 terminal length

特权模式下，命令 `terminal length` 用来设置用户终端屏幕的显示行数。本命令的 `no` 格式用来将配置恢复至缺省值。

## 命令语法

```
terminal length screen-length
```

```
terminal no length
```

<b>screen-length</b>	用户终端上的显示行数。取值范围 0 至 512。0 表示不限制显示长度
----------------------	-------------------------------------

## 命令模式

特权模式

## 默认

自动检查终端显示行数。

## 使用说明

无

## 举例说明

```
Switch# terminal length 0
```

## 相关命令

**service terminal-length**

## 1.1.10 service terminal-length

全局配置模式下，命令 `service terminal-length` 用来设置当前终端下所有会话的显示行数。本命令的 `no` 格式用来将配置恢复至缺省值。

### 命令语法

**service terminal-length** *screen-length*

**no service terminal-length**

<b>screen-length</b>	设置屏幕上的显示行数。取值范围 0 至 512，0 表示不限制显示长度
----------------------	-------------------------------------

### 命令模式

全局配置模式

### 默认

无

### 使用说明

无

### 举例说明

```
Switch(config)# service terminal-length 0
```

### 相关命令

**terminal length**

## 1.1.11 banner motd

全局配置模式下，命令 `banner motd` 用来创建每日提示信息，这些信息将会显示在已登录的用户的终端上。本命令的 `no` 格式用来将配置恢复至缺省值。

### 命令语法

**banner motd** *LINE*

**no banner motd**

<b>LINE</b>	指定用户输入的提示信息的结束字符
-------------	------------------

## 命令模式

全局配置模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch(config)# banner motd #
Enter TEXT message. End with the character '#'.
this is a example message#
```

## 相关命令

**banner exec**

**banner login**

### 1.1.12 banner exec

全局配置模式下，命令 **banner exec** 用来设置用户登录到 EXEC 模式下的提示信息。本命令的 **no** 格式用来将配置恢复至缺省值。

## 命令语法

**banner exec** *LINE*

**no banner exec**

<b>LINE</b>	指定用户输入的提示信息的结束字符
-------------	------------------

## 命令模式

全局配置模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch(config)# banner exec #
Enter TEXT message. End with the character '#'.
this is a example message#
```

## 相关命令

**banner motd**

**banner login**

### 1.1.13 banner login

全局配置模式下，命令 **banner login** 用来设置用户登录到系统时的提示信息。本命令的 **no** 格式用来将配置恢复至缺省值。

## 命令语法

**banner login** *LINE*

**no banner login**

<b>LINE</b>	指定用户输入的提示信息的结束字符
-------------	------------------

## 命令模式

全局配置模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch(config)# banner login #
Enter TEXT message. End with the character '#'.
this is a example message#
```



## 相关命令

**banner motd**

**banner exec**

### 1.1.14 show version

特权模式下，使用 `show version` 命令查看硬件和固件的版本信息。

## 命令语法

**show version** (slot *id* | )

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch# show version
```

## 相关命令

无

### 1.1.15 line vty maximum

全局配置模式下，命令 `line vty maximum` 用来设置最大用户 VTY 登录数量。本命令的 `no` 格式用来将配置恢复至缺省值。

## 命令语法

**line vty maximum***vty\_id*

**no line vty maximum**

<b>vty_id</b>	设置范围为 0-8。默认为 8
---------------	-----------------

## 命令模式

全局配置模式

## 默认

8

## 使用说明

无

## 举例说明

```
Switch(config)# line vty 5
```

## 相关命令

无

### 1.1.16 exec-timeout

`exec-timeout` 用来设置用户多久未执行任何操作后被强制退出。`no` 用来将配置恢复至缺省值。

## 命令语法

**exec-timeout minutes seconds**

**no exec-timeout**

<b>minutes</b>	设置范围为<0-35791>
<b>seconds</b>	设置范围是<0-2147483>

## 命令模式

config-line 配置模式

## 默认

600 秒

## 使用说明

只有当用户重新登录时才会起作用。

## 举例说明

```
Switch(config)# line vty 0
Switch(config-line)# exec-timeout 3 200
```

## 相关命令

无

### 1.1.17 transport input

transport input 用来设置终端允许承载的服务类型。

## 命令语法

**transport input (ssh | telnet | none | all)**

<b>ssh</b>	<b>SSH 服务</b>
<b>telnet</b>	<b>Telnet 服务</b>
<b>none</b>	不支持任何服务
<b>all</b>	支持 telnet 和 ssh 服务

## 命令模式

config-line 配置模式

## 默认

all

## 使用说明

无

## 举例说明

```
Switch(config)# line vty 0
Switch(config-line)# transport input telnet
```

## 相关命令

无

### 1.1.18 access-class in

access-class in 用来设置终端绑定的 ACL 条目。no 用来将配置恢复至缺省值。

## 命令语法

**access-class** *WORD* in

<b>WORD</b>	ACL 模块中配置的 ACL 条目名称
-------------	---------------------

## 命令模式

config-line 配置模式

## 默认

无

## 使用说明

该命令用到的 ACL 只能是 IPv4 访问控制列表

## 举例说明

```
Switch(config)# line vty 0
Switch(config-line)# access-class test in
```

## 相关命令

无

## 1.1.19 reboot

特权模式下，使用 reboot 命令重启系统。

## 命令语法

reboot

## 命令模式

特权模式

## 默认

无

## 使用说明

reboot 命令重启系统。重启系统前，请先保存好系统的配置。

## 举例说明

```
Switch# reboot
```

## 相关命令

**reload**

### 1.1.20 schedule reboot at

全局配置模式下，使用 schedule reboot at 命令设置系统重启时间。该命令的 no 格式取消设置的重启时间。

## 命令语法

**schedule reboot atHH:MM(MM/DD | MM/DD/YYYY | YYYY/MM/DD)**

**no schedule reboot**

<b>HH:MM</b>	设置小时与分钟。时间范围 00:00 – 23:59
<b>MM/DD</b>	设置重启时间(以月/年)格式
<b>MM/DD/YYYY</b>	设置重启时间(以月/日/年。其中年份范围[2000, 2037])格式
<b>YYYY/MM/DD</b>	设置重启时间(以年/月/日/年，其中年份范围[2000, 2037])格式

## 命令模式

全局配置模式

## 默认

无重启时间

## 使用说明

如果指定月份和日期，系统将在指定的月份和日期内的指定时间重启。如果没有指定月份和日期，系统将在当日的指定时间重启。

## 举例说明

```
Switch(config)# schedule reboot at 12:12 2008/12/25
```

## 相关命令

**schedule reboot delay**

### 1.1.21 schedule reboot delay

全局配置模式下，使用 `schedule reboot delay` 命令设置系统延期重启时间。该命令的 `no` 格式取消设置的重启时间。

## 命令语法

**schedule reboot delay** (*HH:MM* | *minutes*)

**no schedule reboot**

<b>HH:MM</b>	设置小时与分钟。时间范围 <b>00:00~23:59</b>
<b>minutes</b>	设置分钟。范围 <b>1~720</b>

## 命令模式

全局配置模式

## 默认

无重启时间

## 使用说明

无

## 举例说明

```
Switch(config)# schedule reboot delay 300
```

## 相关命令

**schedule reboot at**

### 1.1.22 boot system

特权模式下，使用命令 `boot system` 指定系统启动时的 `image` 文件。

## 命令语法

**boot system** (tftp: mgmt-if *SERVERIP* | flash:/) *file-name*

<b>tftp</b>	定启动时用 <b>tftp</b> 方式
<b>flash:/</b>	指定启动时用 <b>flash</b> 方式
<b>mgmt-if</b>	指定管理口
<b>SERVERIP</b>	<b>tftp</b> 服务器的 ip 地址
<b>file-name</b>	启动时用到的 <b>image</b> 文件名

## 命令模式

特权模式

## 默认

无

## 使用说明

使用 TFTP 方式启动时，`startup-config` 文件中的管理口 IP 地址将作为源地址。

## 举例说明

```
Switch# boot system flash:/boot/Internal-1.0.0.25.bin
```

## 相关命令

**show boot**

### 1.1.23 show boot

特权模式下，使用 `show boot` 命令查看系统当前使用的 `image` 文件和下次启动时的 `image` 文件设置。

## 命令语法

```
show boot
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch# show boot
The current boot image version is: E330-3.0.0.23.it
The current running image is: tftp://10.10.29.160/humberOS-e330-ma-
v3.0.0.23.it.r.bin
The next running image is: tftp://10.10.29.160/humberOS-e330-ma-v3.0.0.23.it.r.bin
```

## 相关命令

**show boot images**

### 1.1.24 show boot images

特权模式下，使用 `show boot images` 显示系统 flash 中所有的 image 文件。

## 命令语法

**show boot images**

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch# show boot images
System image files list:
Current boot image version: 1.0.0.25
      Create Time      Version      File name
=====
* 2011-07-25 10:58:29  v3.0.0.22it  Internal-.00.22.bin
```

## 相关命令

**show boot**

### 1.1.25 show memory

特权模式下，使用 `show memory` 命令显示系统中进程的内存使用情况。



## 命令语法

**show memory** (all | bgp | bhm | chsm | dhclient | dot1x | imi | ipv6 | lacp | ldp | lib | mstp | nsm | oamd | onmd | ospf | pim | ptp | rip | rsvp | shal | summary)

<b>all</b>	所有内存信息
<b>bgp</b>	边界网关协议 (BGP)
<b>bhm</b>	系统监控
<b>chsm</b>	Chassis 管理
<b>dhclient</b>	DHCP client
<b>dhcpcd</b>	动态主机配置协议
<b>dhcprelay</b>	DHCP relay
<b>dot1x</b>	IEEE 802.1X
<b>imi</b>	集成管理接口 (IMI)
<b>ipv6</b>	Ipv6
<b>lacp</b>	链路聚合控制协议 (LACP)
<b>ldp</b>	标签分发协议 (LDP)
<b>lib</b>	公共库
<b>mstp</b>	生成树协议 (STP/RSTP/MSTP)
<b>nsm</b>	网络服务模块 (NSM)
<b>oamd</b>	双向转发检测(BFD)
<b>onmd</b>	LLDP and EFM_OAM
<b>ospf</b>	开放最短路径优先(OSPF)
<b>pim</b>	协议无关组播 (PIM)
<b>ptp</b>	精确时间同步协议 (PTP)
<b>rip</b>	路由信息协议 (RIP)
<b>rsvp</b>	资源预留协议 (RSVP)
<b>shal</b>	Hal server monitoring
<b>summary</b>	内存概要信息
<b>monitor</b>	监视器

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch# show memory bgp
Library memories for BGP
Memory type                Alloc cells  Alloc bytes
=====
Temporary memory          :          6596      322216
Hash                      :           10         320
Hash index                :           10      40960
Hash bucket               :           55         880
Link list                 :           13         400
Link list node            :          115      1840
Show                      :            1         512
Show page                 :            1      8192
Show server               :            1          64
Prefix IPv4               :            6          48
Route table               :            6          48
Route node                :           309     19776
Vector                   :          3383    324768
Vector index              :          3383    48824
SNMP subtree              :            8      6144
Host config               :            1          16
Message of The Day        :            1      128
IMI Client                 :            2     1056
VTY master                :            1          16
VTY if                    :           52    39936
VTY connected             :            3      192
Message handler           :            2      128
Host                      :            1          96
Log information           :            2      128
Context                   :            1         512
Memories for BGP
Memory type                Alloc cells  Alloc bytes
=====
BGP structure             :            1          768
BGP VR structure          :            1          384
BGP global structure      :            1          64
BGP peer                  :            1     2048
Ext community             :            1          16
BGP as list master        :            1          32
Community list handler    :            1          32
BGP Damp Reuse List Array :            1     2048
```

BGP table	:	31	248
BGP VRF list	:	1	64

## 相关命令

**show processes memory sorted**

### 1.1.26 show cpu traffic-limit

特权模式下，使用 show cpu traffic-limit 显示 CPU traffic-limit 的配置信息。

## 命令语法

```
show cpu traffic-limit
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch# show cpu traffic-limit
reason                rate (pps)  class
-----                -
bpdu                  64          3
cfm                   512         2
slow-protocol         128         1
eapol                 128         0
erps                  128         2
smart-link            128         2
udld                  128         3
arp                   640         1
dhcp                  128         0
rip                   64          1
ldp                   512         1
ospf                  256         1
pim                   128         1
vrrp                  512         1
rsvp                  512         1
ipda                  1024        0
icmp-redirect         128         0
mcast-rpf-fail       128         1
macsa-mismatch        128         0
port-security-discard 128         0
vlan-security-discard 128         0
mtu-dontfrag          64          0
```

mtu-frag	64	0
ptp	512	2
ip-option	512	0
ucast-ttl-fail	64	0
mpls-ttl-fail	64	0
igmp	128	2
sflow-ingress	128	0
sflow-egress	128	0
fwd-to-cpu	64	0
mpls-tp-pwoam	128	2
Total rate:	2048 (pps)	

## 相关命令

无

### 1.1.27 show processes cpu sorted

特权模式下，使用 `show processes cpu sorted` 命令显示各进程的 `cpu` 利用情况，这里的 CPU 利用率指的是从进程启动一直到这条命令被执行这个时间段内，这个进程所占用 CPU 的时间片。

## 命令语法

**show processescpu sorted**

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch# show processes cpu sorted
PID      TIME %CPU TTY      COMMAND
 924 00:20:03  2.0 ?      hsrvd
 956 00:07:17  0.7 ?      nsm
1007 00:02:44  0.2 ?      imi
 959 00:01:24  0.1 ?      snmpd
1317 00:00:01  0.1 pts/0   imish
   5 00:00:45  0.0 ?      events/0
 983 00:00:23  0.0 ?      mstpd
 985 00:00:15  0.0 ?      onmd
 966 00:00:15  0.0 ?      lacpd
 963 00:00:12  0.0 ?      bhm
 929 00:00:12  0.0 ?      chsm
```

```

    964 00:00:11 0.0 ?      oamd
    919 00:00:10 0.0 ?      ntpd
1003 00:00:08 0.0 ?      pimd
    942 00:00:08 0.0 ?      sshd
    957 00:00:08 0.0 ?      dhcrelay
    973 00:00:07 0.0 ?      authd
1005 00:00:07 0.0 ?      ldpd
    977 00:00:07 0.0 ?      rmond
1021 00:00:07 0.0 ?      ripd
1027 00:00:07 0.0 ?      ospfd
1032 00:00:07 0.0 ?      bgpd
     1 00:00:05 0.0 ?      init
    779 00:00:04 0.0 ?      jffs2_gcd_mtd1
1106 00:00:01 0.0 ?      imish
     3 00:00:00 0.0 ?      ksoftirqd/0
    916 00:00:00 0.0 ?      syslog-ng
     65 00:00:00 0.0 ?      bdi-default
    965 00:00:00 0.0 ?      ptpd
    917 00:00:00 0.0 ?      crond
     63 00:00:00 0.0 ?      sync_supers
1096 00:00:00 0.0 ?      telnetd
     6 00:00:00 0.0 ?      khelper
    105 00:00:00 0.0 ?      khungtaskd
     2 00:00:00 0.0 ?      kthreadd
     4 00:00:00 0.0 ?      watchdog/0
     9 00:00:00 0.0 ?      netns
    10 00:00:00 0.0 ?      async/mgr
    66 00:00:00 0.0 ?      kblockd/0
    73 00:00:00 0.0 ?      kseriod
    88 00:00:00 0.0 ?      rpciod/0
   106 00:00:00 0.0 ?      kswapd0
   157 00:00:00 0.0 ?      aio/0
   164 00:00:00 0.0 ?      nfsiod
   171 00:00:00 0.0 ?      crypto/0
   712 00:00:00 0.0 ?      mtblockd
   741 00:00:00 0.0 ?      kpsmoused
   789 00:00:00 0.0 ?      PETH/Tx
   912 00:00:00 0.0 ?      angel
1098 00:00:00 0.0 ?      telnetd
1414 00:00:00 0.0 pts/0    imish
1415 00:00:00 0.0 pts/0    more
1416 00:00:00 0.0 ?      ps

```

## 相关命令

无

### 1.1.28 show processes cpu history

特权模式下，使用 `show processes cpu history` 命令显示 `cpu` 总体历史利用情况，可以显示最近 5s, 1min, 5min 的利用情况。

## 命令语法

**show processescpuhistory**

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch# show processes cpuhistory  
CPU usage for five seconds: 4.7%; one minute: 3.0%; five minutes: 3.68%
```

## 相关命令

无

## 1.1.29 show processes memory sorted

特权模式下，使用 show processes memory sorted 命令显示各进程的内存使用情况。

## 命令语法

**show processes memory sorted (core | physical | virtual)**

<b>core</b>	进程使用的物理内存页面大小
<b>physical</b>	进程使用的非交换物理内存
<b>virtual</b>	进程使用的虚拟内存

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch# show processes memory sorted
Total: 256108; Used: 89644; Free: 166464; Buffers: 0
  PID TTY      RSS   VSZ   SZ COMMAND
1317 pts/0    9516 13104 3276 imish
1106 ?        9428 13104 3276 imish
1463 pts/0    7436 13104 3276 imish
  956 ?        6836 14644 3661 nsm
 1007 ?        5948  9624 2406 imi
  924 ?        5912 17652 4413 hsrvd
  959 ?        3336  8076 2019 snmpd
 1032 ?        2724  8204 2051bgpd
 1027 ?        2488  7140 1785 ospfd
1003 ?        2472  7152 1788 pimd
  957 ?        2340  6572 1643 dhcrelay
  983 ?        2336  6592 1648 mstpd
1021 ?        2324  6600 1650 ripd
1005 ?        2320  6732 1683 ldpd
  942 ?        2284  6772 1693 sshd
  985 ?        2208  6592 1648 onmd
  929 ?        2132  7168 1792 chsm
  966 ?        2028  6140 1535 lacpd
  973 ?        2028  6284 1571 authd
  965 ?        2024  6408 1602 ptpd
  964 ?        1952  6364 1591 oamd
  977 ?        1948  6200 1550 rmond
  963 ?        1708  5980 1495 bhm
  919 ?        1120  3792  948 ntpd
  916 ?        1060  2300  575 syslog-ng
1465 pts/0    764   2516  629 ps
  917 ?        668   3040  760 crond
   1 ?        656   2928  732 init
1464 pts/0    472   1668  417 more
1096 ?        416   2928  732 telnetd
1098 ?        272   2928  732 telnetd
  912 ?        172  1496  374 angel
   2 ?          0     0     0 kthreadd
   3 ?          0     0     0 ksoftirqd/0
   4 ?          0     0     0 watchdog/0
   5 ?          0     0     0 events/0
   6 ?          0     0     0 khelper
   9 ?          0     0     0 netns
  10 ?          0     0     0 async/mgr
  63 ?          0     0     0 sync_supers
  65 ?          0     0     0 bdi-default
  66 ?          0     0     0 kblockd/0
  73 ?          0     0     0 kseriod
  88 ?          0     0     0 rpciod/0
 105 ?          0     0     0 khungtaskd
 106 ?          0     0     0 kswapd0
```

157 ?	0	0	0 aio/0
164 ?	0	0	0 nfsiod
171 ?	0	0	0 crypto/0
712 ?	0	0	0 mtblockd
741 ?	0	0	0 kpsmoused
779 ?	0	0	0 jffs2_gcd_mtd1
789 ?	0	0	0 PETH/Tx

## 相关命令

无

### 1.1.30 terminal monitor

特权模式下，使用 `terminal monitor` 命令显示系统的调试信息。

## 命令语法

`terminalmonitor`

`terminal no monitor`

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch# terminal monitor
Jan 1 16:09:30 DUT1 IMISH-6: ready to service
```

## 相关命令

无

### 1.1.31 configure terminal

特权模式下，使用 `configure terminal` 命令进入全局配置模式。

## 命令语法

`configure terminal`



## 命令模式

特权模式

## 默认

无

## 使用说明

使用本命令进入全局配置模式。全局配置模式下的用户配置将会被保存到 `running configuration` 文件，并且命令提示行也会由特权模式下的 `<switch-name>#` 变为 `<switch-name>(config)#`，提醒用户系统当前处于全局配置模式，`end` 命令或使用组合键 `Ctrl-Z` 离开本模式。

## 举例说明

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
```

## 相关命令

**enable**

**disable**

### 1.1.32 disable

特权模式下，使用 `disable` 命令退出特权模式进入用户模式。

## 命令语法

**disable**

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch> enable
Password: <password>
Switch# disable
```

```
Switch>
```

## 相关命令

**enable**

### 1.1.33 enable

用户模式下，使用 **enable** 命令进入特权模式。

## 命令语法

```
enable
```

## 命令模式

用户模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch> enable
Password: <password>
Switch# disable
Switch>
```

## 相关命令

**disable**

### 1.1.34 end

全局配置模式下，使用 **end** 命令退出当前配置会话并返回到特权模式。

## 命令语法

```
end
```

## 命令模式

全局配置模式

## 默认

无

## 使用说明

该命令将直接返回到特权模式，无论用户当前在那个模式下。

该命令可在所有配置模式下使用。

做完所有的系统配置后，用户可以使用该命令返回特权模式查看配置信息。

## 举例说明

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# end
Switch# show interface eth-0-1
```

## 相关命令

exit

### 1.1.35 exit (global)

任何模式下，都可使用 exit 命令退出当前模式，返回到当前模式的下一级模式。

## 命令语法

exit

## 命令模式

所有配置模式

## 默认

无

## 使用说明

exit 可让用户退出当前模式并返回到当前模式的下一级模式。

用户可以在全局配置模式下使用该命令退回到特权模式，或在接口配置模式，路由配置模式下使用该命令退回到全局配置模式。

## 举例说明

```
Switch(config-if)# exit
Switch(config)#
```

## 相关命令

**end**

**exit (EXEC)**

### 1.1.36 exit (EXEC)

用户模式下，使用 **exit** 命令关闭会话退出交换机。

## 命令语法

**exit**

## 命令模式

所有配置模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch(config)# exit
Switch# disable
Switch> exit
```

## 相关命令

**quit**

### 1.1.37 quit

用户模式下，使用 **quit** 命令关闭会话退出交换机。

## 命令语法

**quit**

## 命令模式

所有配置模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch(config)# quit
Switch# disable
Switch> quit
```

## 相关命令

**Exit**

### 1.1.38 cd

特权模式下，使用 `cd` 命令改变当前路径。

## 命令语法

`cd(dir |)`

<b>dir</b>	(可选)文件系统路径。末尾加一个冒号(:)表示。比如， <b>Flash:</b> 改变当前路径为 <b>flash:</b> <b>udisk:</b> 改变当前路径为 <b>udisk</b> 。如果当前没有 USB 设备， <b>cd udisk</b> 命令将无法执行
------------	--

## 命令模式

特权模式

## 默认

系统的初始当前路径为 **flash:**如果用户没有设置当前路径。那么系统的缺省当前路径就是文件系统的根路径 **flash:**。

## 使用说明

所有特权模式下带有文件路径参数的命令，如果用户在命令中省略该参数，系统会使用由 `cd` 命令指定的当前路径作为缺省参数。比如 `dir` 命令，该命令将当前路径下的文件列表显示给用户。

## 举例说明

设置当前路径为 **flash:**。

```
DUT1# cd
```

```
DUT1# pwd
flash:/
```

设置当前路径为 USB。

```
storage device
DUT1# cd udisk:
DUT1# pwd
udisk:/
```

## 相关命令

**dir**

**ls**

**pwd**

## 1.1.39 copy

特权模式下，使用 **copy** 命令拷贝文件。

## 命令语法

copysource-name destination-name

<b>source-nam</b>	源文件的 <b>URL</b> 。源文件可以是本地或远程文件
<b>destination-name</b>	目的文件的 <b>URL</b> 。目的文件可以是本地或远程文件

## 命令模式

特权模式

## 默认

无

## 使用说明

源和目的文件的 **URL** 的具体值取决于文件所在位置。可以是一个相对路径或者是一个满足文件系统要求的绝对路径(filesystem:[/filepath][/filename])。

## 举例说明

通过带内管理口从 tftp 服务器拷贝 image。

```
Switch# copy tftp://192.168.0.1/image flash:/boot/image
Download from URL to temporary file.
Get file from tftp://192.168.0.1/image
.....
.....
```

```
Received 15591515 bytes in 16.6 seconds
Copy the temporary file to its destination.
.....
.....
15591515 bytes in 69.8 seconds, 218 kbytes/second
```

通过带外管理口从 tftp 服务器拷贝 image。

```
Switch# copy mgmt-if tftp://192.168.0.1/image flash:/boot/image
```

## 相关命令

**delete**

### 1.1.40 delete

特权模式下，使用 delete 命令删除 flash 上的文件。

## 命令语法

**delete file-name**

<b>file-name</b>	准备删除的文件名
------------------	----------

## 命令模式

特权模式

## 默认

无

## 使用说明

如果用户删除的是系统的配置文件或 image 文件，系统会提示用户是否确定删除。同样，如果用户删除系统中某些特定文件，比如 DHCP 的配置文件，系统也会有同样提示。

## 举例说明

删除 flash 上的 test 文件。

```
Switch# delete flash:/test
Are you sure to delete flash:/test? [confirm]:y
```

## 相关命令

**copy**

## 1.1.41 dir

特权模式下，使用 `dir` 命令显示当前路径下的文件列表。

### 命令语法

**dir** (**flash:** | **udisk:** | ) (*directory-name* | ) (*file-name* | )

<b>flash:</b>	<b>flash</b> 文件系统
<b>udisk:</b>	<b>USB</b> 存储设备。如果系统没有 <b>USB</b> 存储设备。该命令将无法执行
<b>directory-name</b>	<b>flash</b> 或 <b>USB</b> 存储设备的路径
<b>file-name</b>	文件名字

### 命令模式

特权模式

### 默认

无

### 使用说明

无

### 举例说明

`dir` 命令的输出结果。

```
Switch# dir
Directory of flash:/
total 42
drwxr-xr-x  2    0 Jul 30 15:42 boot
drwxr-xr-x  3    0 Jan  1  1970 conf
drwxr-xr-x  2    0 Jan  1  1970 log
-rw-r----- 1 1020 Jul 29 19:18 startup-config.conf
-rw-r--r--  1 10270 Jul 30 10:10 syslog
-rw-r--r--  1  6886 Jul 29 23:59 syslog.1.gz
63.0M bytes total (30.4M bytes free)
Switch # cd udisk:
Switch # dir
Directory of udisk:/
total 12
drwxrwxrwx 2 4096 Jun  2  2011test
drwxrwxrwx 2 4096 Jun  8  2011test1
drwxrwxrwx 2 4096 Jun  7  2011test2
```



3.7G bytes total (3.7G bytes free)

## 相关命令

**ls**

### 1.1.42 ls

特权模式下，使用 ls 命令显示当前路径下的文件列表。

## 命令语法

**ls (flash: | udisk: |) (directory-name |)(file-name |)**

<b>flash:</b>	<b>flash</b> 文件系统
<b>udisk:</b>	<b>USB</b> 存储设备。如果系统没有 <b>USB</b> 存储设备。该命令将无法执行
<b>directory-name</b>	<b>flash</b> 或 <b>USB</b> 存储设备的路径
<b>file-name</b>	文件名字

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

ls 命令的输出结果。

```
Switch# ls
Directory of flash:/
total 42
drwxr-xr-x  2    0 Jul 30 15:42 boot
drwxr-xr-x  3    0 Jan  1  1970 conf
drwxr-xr-x  2    0 Jan  1  1970 log
-rw-r----- 1 1020 Jul 29 19:18 startup-config.conf
-rw-r--r--  1 10270 Jul 30 10:10 syslog
-rw-r--r--  1  6886 Jul 29 23:59 syslog.1.gz
63.0M bytes total (30.4M bytes free)
```

## 相关命令

**dir**

### 1.1.43 more

特权模式下，使用 `more` 命令显示文件内容。

## 命令语法

**more** (**flash:**| **udisk:**) (*directory-name*)*file-name*

<b>flash:</b>	<b>flash</b> 文件系统
<b>udisk:</b>	USB 存储设备。如果系统没有 USB 存储设备。该命令将无法执行
<b>directory-name</b>	<b>flash</b> 或 USB 存储设备的路径
<b>file-name</b>	文件名字

## 命令模式

特权模式

## 默认

无

## 使用说明

系统一次只能以 ASCII 形式显示一个文件。

## 举例说明

显示 flash 上 startup-config 文件的内容。

```
Switch# more flash:/startup-config.conf
```

## 相关命令

**dir**

**ls**

### 1.1.44 mkdir

特权模式下，使用 `mkdir` 命令创建一个新的路径。

## 命令语法

**mkdir directory-name**

<b>directory-name</b>	新路径名
-----------------------	------

## 命令模式

特权模式

## 默认

无

## 使用说明

该命令只对本地文件系统有效。

## 举例说明

在 flash 上创建一个名为 newdir 的路径。

```
Switch# mkdir flash:/newdir
```

在 USB 上创建一个名为 newdir 的路径。

```
Switch# mkdir udisk:/newdir
```

## 相关命令

**rmdir**

**dir**

## 1.1.45 rename

特权模式下，使用 **rename** 命令改变一个文件名。

## 命令语法

**rename old-filename new-filename**

<b>old-filename</b>	原文件名
<b>new-filename</b>	新文件名

## 命令模式

特权模式

## 默认

无

## 使用说明

该命令只对本地文件系统有效。

## 举例说明

将文件 `rtup-config.conf-bak` 更名为 `startup-config.conf-bak2`:

```
DUT1# rename udisk:/ startup-config.conf-bak udisk:/ startup-config.conf-bak2
Are you sure to rename udisk:/ startup-config.conf-bak? [confirm]
```

## 相关命令

无

## 1.1.46 rmdir

特权模式下，使用 `rmdir` 命令删除一个路径。

## 命令语法

**rmdir**directory-name

<b>directory-name</b>	删除的路径名
-----------------------	--------

## 命令模式

特权模式

## 默认

无

## 使用说明

该命令只对本地文件系统有效。

## 举例说明

删除一个名为 `newdir` 的路径。

```
Switch# rmdir flash:/newdir
Are you sure to delete newdir? [yes/no]: y
```

## 相关命令

**mkdir**

**dir**

### 1.1.47 tar create

特权模式下，使用 **tar create** 命令创建一个 tar 文件。

## 命令语法

**tar createtar-file-name source-directory**

<b>tar-file</b>	新 tar 文件名
<b>source-directory</b>	源路径

## 命令模式

特权模式

## 默认

无

## 使用说明

源路径必须是一个存在的路径。

## 举例说明

```
DUT1# tar create udisk:/tar1 udisk:/wu
```

## 相关命令

**tar table**

**tar xtract**

### 1.1.48 tar table

特权模式下，使用 **tar table** 命令查看 tar 文件中具体内容。

## 命令语法

**tar createtar-file-name**

<b>tar-file</b>	tar 文件名
-----------------	---------

## 命令模式

特权模式

## 默认

无

## 使用说明

tar 文件必须是一个已存在的文件。

## 举例说明

```
DUT1# tar table udisk:/tar1
```

## 相关命令

**tar create**

**tar xtract**

### 1.1.49 tar xtract

特权模式下，使用 tar xtract 命令解压 tar 文件。

## 命令语法

**tar xtract tar-file destination-directory**

<b>tar-file</b>	目的 tar 文件名
<b>destination-directory</b>	目的路径

## 命令模式

特权模式

## 默认

无

## 使用说明

目的路径必须是一个已存在的路径，你可以用 mkdir 创建一个新路径。

## 举例说明

```
Switch# tar xtract flash:/tar1 flash:/mydir
```

## 相关命令

**tar create**

**tar table**

### 1.1.50 tar diagnostic-information

特权模式下，使用 `tar diagnostic-information` 将 `diagnostic-information` 信息打包成 `tar` 文件，并放到 `flash`、`udisk`、`ftp` 服务器或 `tftp` 服务器上。目前的诊断信息有 `image` 版本信息，设备时钟信息，`running-config`，`startup-config`，端口信息，内存信息，`flash` 上文件信息，`logging buffer` 信息，`core` 文件，`syslog` 文件等信息。

## 命令语法

**tardiagnostic-information(mgmt-if | )destination-directory/ tar-file**

<b>destination-director</b>	目的路径，可以是 <b>flash</b> ， <b>udisk</b> ， <b>tftp</b> 服务器， <b>ftp</b> 服务器
<b>tar-file</b>	目的 <b>tar</b> 文件名

## 命令模式

特权模式

## 默认

无

## 使用说明

目的路径必须可达且磁盘空间充足。

## 举例说明

```
Switch# tar diagnostic-information flash:/diag.tar.gz
```

## 相关命令

无

### 1.1.51 format

配置模式下，使用 `format` 命令格式化 `udisk`。

## 命令语法

**format**[*udisk*]:

<b>udisk</b>	<b>USB 存储设备。如果系统中没有 USB 设备，命令将无法执行</b>
--------------	--

## 命令模式

全局配置模式

## 默认

无

## 使用说明

目的路径必须存在。

## 举例说明

```
DUT1(config)# format udisk:
    WARNING: All data on udisk: will be lost!!!
And format operation may take a while.
Are you sure to process with format? [yes/no]: yes
```

## 相关命令

无

## 1.1.52 umount

配置模式下，使用 **umount** 命令卸载 USB 设备。将 USB 设备从交换机拔下前需要先卸载它。

## 命令语法

**umount** *udisk*:

<b>udisk</b>	<b>USB 存储设备。如果系统中没有 USB 设备，命令将无法执行</b>
--------------	--

## 命令模式

全局配置模式

## 默认

无



## 使用说明

USB 设备必须已挂载到系统中，使用 `umount` 命令卸载 USB 设备。

## 举例说明

```
DUT1(config)# umount udisk:
After this operation, you can not use USB disk.
Are you sure to continue? [yes/no]: yes
```

## 相关命令

无

### 1.1.53 cut\_through\_forwarding enable (10G-40G-100G | 1G-10G-100G | 1G-10G-40G |)

全局配置模式下，使能 Cut-Through 模式，在 GG 分支上可以配置支持的速率。

## 命令语法

**cut\_through\_forwarding enable (10G-40G-100G| 1G-10G-100G| 1G-10G-40G|)**

<b>enbale</b>	<b>使能 Cut-Through 模式</b>
<b>(10G-40G-100G  1G-10G-100G  1G-10G-40G )</b>	<b>配置 cut_through 支持的速率，默认为 10G-40G-100G</b>

## 命令模式

全局配置模式

## 默认

使能 Cut-Through 模式默认速率为 10G-40G-100G

## 使用说明

GG 上可以配置速率，Duet2 上则只能使能 cut through 模式。

## 举例说明

```
DUT4#cut-through-forwarding enable 1G-10G-40G
% Configuration about cutting through forwarding mode has been stored, but cannot
take effect until the next reload.
```

## 相关命令

无

## 1.1.54 show cut-through-forwarding mode

本命令用于查看系统启动当前工作的模式。

### 命令语法

```
show cut-through-forwarding mode
```

### 命令模式

特权模式

### 默认

无

### 使用说明

无

### 举例说明

```
DUT1# show cut-through-forwarding mode
```

### 相关命令

无

## 1.2 用户管理配置

### 1.2.1 username

本命令创建或删除一个本地交换机上的账户。

### 命令语法

```
username WORD
```

```
no username WORD
```

<b>username</b>	创建用户账户
<b>WORD</b>	用户账户名

## 命令模式

全局配置模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch (config)#username testName
```

## 相关命令

无

## 1.2.2 username password [8]

本命令增加用户账户和密码。

## 命令语法

```
username WORD password (8|) LINE
```

<b>WORD</b>	用户账户名
<b>Password</b>	账户密码
<b>8</b>	指定后面配置的密码为加密密码
<b>LINE</b>	用户密码字符串

## 命令模式

全局配置模式

## 默认

无

## 使用说明

配置”8”选项后，后面配置的密码必须为加密过的密码，否则配置失败。加密密码可见于用命令”username secret”配置后的用户密码。

## 举例说明

```
Switch(config)#username testName password 123456
```

## 相关命令

```
username secret
```

### 1.2.3 username secret

本命令创建用户账户和加密的账户名密码。

## 命令语法

```
username WORD secret LINE
```

<b>WORD</b>	用户账户名
<b>secret</b>	指定密码加密
<b>LINE</b>	用户密码字符串

## 命令模式

全局配置模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch(config)#username testName secret 123456
```

## 相关命令

无

### 1.2.4 username privilege

本命令创建具有特权等级的用户账户。

## 命令语法

```
username WORD privilege <1-4>
```

<b>username WORD</b>	用户账户名
<b>privilege&lt;1-4&gt;</b>	设置账户特权等级，特权等级<1-4>

## 命令模式

全局配置模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch(config)#username testName privilege 2
```

## 相关命令

无

## 1.2.5 username privilege password

本命令创建具有特权等级和密码的账户。

## 命令语法

```
username WORD privilege<1-4>password (8)LINE
```

<b>WORD</b>	用户账户名
<b>privilege &lt;1-4&gt;</b>	设置账户特权等级，特权等级<1-4>
<b>8</b>	指定密码隐藏
<b>LINE</b>	用户密码

## 相关命令

全局配置模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch(config)#username testName privilege 2 password 123456
```

## 相关命令

无

## 1.2.6 username service-type

本命令配置用户可用于的服务类型。

## 命令语法

```
username WORD service-type ({telnet|ssh|web|rpc-api}|all|none)
```

<b>WORD</b>	用户账户名
<b>telnet</b>	<b>Telnet 服务</b>
<b>ssh</b>	<b>SSH 服务</b>
<b>web</b>	<b>WEB 服务</b>
<b>rpc-api</b>	<b>RPC 服务</b>
<b>all</b>	所有服务
<b>none</b>	不支持任何服务

## 相关命令

全局配置模式

## 默认

all

## 使用说明

无

## 举例说明

```
Switch(config)# username hell service-type telnet
```

## 相关命令

无

## 1.2.7 re-username newname

本命令恢复用户名。

## 命令语法

```
re-username WORD newname WORD
```

<b>re-username</b> <b><i>WORD</i></b>	原用户名
<b>newname</b> <b><i>WORD</i></b>	新用户名

## 命令模式

全局配置模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch(config)#re-username testName newname newname
```

## 相关命令

无

## 1.2.8 cipher detect

本命令设置密码的安全等级。

## 命令语法

cipher detect (strong| normal | none)

<b>strong</b>	密码必须包含数字，普通字符和自定义字符
<b>normal</b>	密码必须包含数字和普通字符
<b>none</b>	关闭安全检查

## 命令模式

全局配置模式。

## 默认

无

## 使用说明

无

## 举例说明

```
Switch(config)#cipher detect strong
```

注意:本命令会清除所有强度不够的密码。

## 相关命令

无

## 1.2.9 cipher detect length

本命令设置安全等级为 normal 或者 strong 时密码的最小长度。

## 命令语法

**cipher detect length** *length-value*

<b>length-value</b>	密码最小长度
---------------------	--------

## 命令模式

全局配置模式



## 默认

8

## 使用说明

该命令配合 **cipher detect** 命令使用，在配置 **cipher detect** 模式为 normal 或者 strong 时该限制生效。

## 举例说明

设置安全等级为 normal 或者 strong 时密码的最小长度：

```
Switch(config)#cipher detect length 10
```

## 1.2.10 username retry-times

本命令设置用户允许登录失败最大次数。

使用 **no** 命令解除限制。

## 命令语法

```
username WORD retry-times times-value
```

```
no username WORD retry-times
```

WORD	用户账户名
times-value	允许用户登录失败最大次数范围为 1~99

## 命令模式

全局配置模式

## 默认

没有限制

## 使用说明

配置该命令后，用户登录失败次数超过配置的上限则会锁定用户。用户锁定后可以使用命令 **username unlock** 解除锁定状态。

## 举例说明

设置用户允许登录失败最大次数：

```
Switch(config)#username testName retry-times 3
```

## 1.2.11 username unlock

本命令用来解除已经被锁定的用户。

### 命令语法

**username** *WORD* **unlock**

WORD	用户账户名
------	-------

### 命令模式

全局配置模式

### 默认

无

### 使用说明

用户登录失败次数超过配置的登录失败最大次数上限，被锁定后使用该命令解除锁定状态。

### 举例说明

解除已经被锁定的用户：

```
Switch(config)#username testName unlock
```

## 1.2.12 username active-period

本命令设置用户密码的有效周期。

### 命令语法

**username** *WORD* **active-period** *time-value*

WORD	用户账户名
time-value	用户密码有效周期，取值范围为 1~129600，单位：分钟

### 命令模式

全局配置模式

### 默认

没有限制

## 使用说明

用户创建并配置该命令后，若管理员在配置时间内未修改密码，会导致密码超时不可用。修改用户密码后重新开始计时。

## 举例说明

设置用户密码的有效周期：

```
Switch(config)#username testName active-period 129600
```

## 1.2.13 username lock-time

本命令设置用户登录失败被锁定后的时长。

## 命令语法

**username** *WORD* **lock-time** *time-value*

WORD	用户账户名
time-value	用户登录失败被锁定后的时长，取值范围为 5~1440，单位：分钟

## 命令模式

全局配置模式

## 默认

默认锁定时间是 30 分钟

## 使用说明

当设置了用户的 `retry-times` 后，用户登录失败的次数超过了 `retry-times`，用户会被锁定。默认锁定时间是 30 分钟，设置了 `lock-time` 后，锁定时长超过这个时间就会解除锁定。

## 举例说明

设置用户登录失败被锁定后的时长：

```
Switch(config)# username xxx lock-time 50
```

## 1.3 FTP 配置

### 1.3.1 ftp

ftp 命令用来在本地主机和远程 ftp 服务器间交换文件。

#### 命令语法

ftp (mgmt-if | )host

<b>mgmt-if</b>	使用管理口
<b>host</b>	远程主机的 IPv4, IPv6 地址或主机名

#### 命令模式

特权模式

#### 默认

无

#### 使用说明

使用 ftp 命令从远程 ftp 服务器上传或下载文件。

#### 举例说明

```
Switch# ftp mgmt-if 10.10.29.160
Connected to 10.10.29.160.
220----- Welcome to Pure-FTPd -----
220-You are user number 1 of 50 allowed.
220-Local time is now 09:00. Server port: 21.
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
Name (10.10.29.160:root): root
331 User root OK. Password required
Password:
230-User root has group access to: wheel disk adm sys daemon
230- bin root
230 OK. Current directory is /root
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
Switch# ftp mgmt-if 2001:1000::2
Connected to 2001:1000::2 (2001:1000::2).
220 Serv-U FTP Server v10.2 ready...
Name (2001:1000::2:root): centec
331 User name okay, need password.
```

```

Password:
230 User logged in, proceed.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>

```

## 相关命令

无

### 1.3.2 ftpvrf

特权模式下，使用 `ftp vrf` 命令在本地主机和远程 VPN 内的 ftp 服务器间交换文件。

## 命令语法

```
ftp vrf WORD
```

<b>vrf</b>	VNP 路由/转发实例
<b>WORD</b>	VNP 路由/转发实例名字

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch# ftp vrftestvrf
```

## 相关命令

无

### 1.3.3 ftp username

全局配置模式下，使用 `FTP username` 命令创建一个 ftp user name。本命令的 `no` 格式用来删除 ftp user name。

## 命令语法

```
ftp username username
```

```
no ftp username
```

<b>username</b>	远程 FTP 服务器的用户名
-----------------	----------------

## 命令模式

全局配置模式

## 默认

无用户名

## 使用说明

用户名必须以字母开头，包括英文字母，数字和下划线，不多于 31 个字符。

## 举例说明

```
Switch(config)# ftp username abc
```

## 相关命令

```
ftp password
```

```
ftp passive
```

### 1.3.4 ftp password

全局配置模式下，使用 ftp password 命令为 ftp 用户创建密码。本命令的 no 格式用来删除 ftp 用户密码。

## 命令语法

```
ftp password(password | 8 password)
```

```
no ftp password
```

<b>8</b>	指定隐藏密码
<b>password</b>	远程 FTP 服务器的用户密码

## 命令模式

全局配置模式

## 默认

无用户密码

## 使用说明

如果 `service password-encryption` 功能被启用。 `running-config` 文件中的密码将会以加密形式显示。

## 举例说明

```
Switch(config)# ftp password abc
```

## 相关命令

`ftp username`

`ftp passive`

## 1.3.5 ftp passive

全局配置模式下，使用 `ftp passive` 命令设置 FTP 为 `passive` 模式。本命令的 `no` 格式用来恢复到缺省模式。

## 命令语法

`ftp passive`

`no ftp passive`

## 命令模式

全局配置模式

## 默认

FTP 工作在 `Active` 模式。

## 使用说明

无

## 举例说明

```
Switch(config)# ftp passive
```

## 相关命令

ftp username

ftp password

### 1.3.6 show ftp

特权模式下，使用 show ftp 命令显示 ftp 的配置信息。

## 命令语法

```
show ftp
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch# show ftp
ftp passive mode: on
ftp username: root
ftp password: unencrypted, abc
Switch#
```

## 相关命令

**ftp username**

**ftp password**

**ftp passive**

## 1.4 FTP Server 配置

### 1.4.1 service ftpd

使用此命令启用或者禁用 ftp server 服务。

## 命令语法

```
service ftpd { enable | disable }
```



enable	开启 ftp 服务
disable	关闭 ftp 服务

## 命令模式

全局配置模式

## 默认

关闭

## 使用说明

无

## 举例说明

开启 ftp server 服务：

```
Switch(config)# service ftpd enable
```

## 1.4.2 ftpd username password

本命令配置 ftp server 用户账户和密码。

使用 **no** 命令删除 ftp server 用户账户。

## 命令语法

**ftpd username** *WORD* **password** [ **8** ] *LINE*

**no ftpd username** *WORD*

WORD	用户账户名
password	账户密码
8	指定后面配置的密码为加密密码
LINE	用户密码字符串

## 命令模式

全局配置模式

## 默认

无

## 使用说明

配置”8”选项后，后面配置的密码必须为加密过的密码，否则配置失败。使用 **username secret** 命令配置后的用户密码。配置用户后，在运行的 FTP Client 端输入相应的用户名及密码登入设备。

## 举例说明

配置 ftp server 用户账户和密码：

```
Switch(config)#ftpd username testName password 123456
```

## 1.5 TFTP 配置

### 1.5.1 copy GFILENAME GURLNAME

使用本命令拷贝本地文件至 tftp 服务器。

## 命令语法

```
copyGFILENAME (mgmt-if | )GURLNAME
```

<b>mgmt-if</b>	使用管理口
<b>GFILENAME</b>	本地文件名
<b>GURLNAME</b>	目的 URL

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch#copy flash:/test.c tftp://1.1.1.1/running-config
```

## 相关命令

无

## 1.5.2 Copy GURLNAME GFILENAME

使用本命令从 tftp 服务器拷贝文件至本地。

### 命令语法

copy (mgmt-if) GURLNAME GFILENAME

<b>mgmt-if</b>	使用管理口
<b>GFILENAME</b>	本地文件名
<b>GURLNAME</b>	源 URL

### 命令模式

特权模式

### 默认

无

### 使用说明

无

### 举例说明

```
Switch#copy tftp://1.1.1.1/test.c flash:test1.c
get file from tftp://1.1.1.1/test.c
Received 225 bytes in 0.3 seconds
```

### 相关命令

无

## 1.5.3 copy running-config mgmt-if

使用本命令拷贝 running-config 文件至 tftp 服务器。

### 命令语法

copy running-config (mgmt-if) *GURLNAME*

<b>mgmt-if</b>	使用管理口
----------------	-------

<b>running-config</b>	系统当前的配置文件
<b>GURLNAME</b>	目的 URL

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch#copy running-config tftp://1.1.1.1/running-config
Building configuration...
send file to tftp://1.1.1.1/running-config
...
Sent 40198 bytes in 8.3 seconds
```

## 相关命令

无

## 1.5.4 copy startup-config mgmt-if

使用本命令拷贝 startup-config 文件至 tftp 服务器。

## 命令语法

**copy startup-config(mgmt-if) *GURLNAME***

<b>mgmt-if</b>	使用管理口
<b>startup-config</b>	系统当前的配置文件
<b>GURLNAME</b>	目的 URL

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch#copy startup-config tftp://1.1.1.1/startup-config
send file to tftp://1.1.1.1/startup-config
..
Sent 32252 bytes in 6.4 seconds
```

## 相关命令

无

# 1.5.5 copy mgmt-if startup-config

使用本命令从 tftp 服务器拷贝 `startup-config` 文件至本地。

## 命令语法

```
copy(mgmt-if) GURLNAME startup-config
```

<b>mgmt-if</b>	使用管理口
<b>GURLNAME</b>	目的 URL
<b>startup-config</b>	拷贝至本地的 <code>startup-config</code> 文件

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch#copy tftp://1.1.1.1/startup-configstartup-config
get file from tftp://1.1.1.1/startup-config
```

```
..  
Sent 32252 bytes in 6.4 seconds
```

## 相关命令

无

# 1.6 Telnet 配置

## 1.6.1 service telnet

使用此命令启用或者禁用 SSH 服务。

## 命令语法

**service telnet (enable | disable)**

<b>enable</b>	开启 Telnet 服务
<b>disable</b>	关闭 Telnet 服务

## 命令模式

全局配置模式

## 默认

关闭

## 使用说明

无

## 举例说明

交换机上开启 Telnet 服务：

```
Switch(config)# service telnet enable
```

## 相关命令

无

## 1.6.2 telnet

本命令可让交换机访问网络上其他的设备。

## 命令语法

**telnet** (-a *WORD*)( vrf *WORD*| **mgmt-if**)*WORD*(*PORT* |)

<b>-a WORD</b>	<b>Telnet 时指定源 IP</b>
<b>vrfWORD</b>	<b>VPN 路由转发实例名</b>
<b>mgmt-if</b>	<b>使用管理口</b>
<b>WORD</b>	<b>远程设备的 IPv4, IPv6 地址或主机名</b>
<b>PORT</b>	<b>TCP 端口号</b>

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch# telnet mgmt-if 10.10.29.247
Entering character mode
Escape character is '^]'.
TestOS, Version 2.3(62), fcs
Switch# telnet 2001:1000::1
Entering character mode
Escape character is '^]'.
DUT1#
```

## 相关命令

无

### 1.6.3 telnet server source address

本命令可修改交换机上 telnet 服务器的源地址。

## 命令语法

**telnet server source address** (vrf *NAME*) *A.B.C.D*

**no telnet server source address**

<b>vrf NAME</b>	指定提供 telnet 服务的 vrf
<b>A.B.C.D</b>	配置带内 telnet 服务器的源 IP 地址

## 命令模式

全局配置模式

## 默认

无

## 使用说明

该命令可以修改 telnet 服务器默认的源地址，并可以指定提供 telnet 服务的 vrf。源地址只能是 loopback 口的地址或者 0.0.0.0，当配置为 0.0.0.0 表示不指定 ip 作为 telnet 服务器地址。

## 举例说明

```
Switch(config)# telnet server source address vrf vpn1 10.10.10.1
```

## 相关命令

无

## 1.6.4 telnet server sourceport

本命令可修改交换机上带内 telnet 服务器的源端口。

## 命令语法

**telnet server sourceport** NUMBER

**no telnet server sourceport**

<b>portNUMBER</b>	配置带内 telnet 服务器的源端口号，有效值范围[1025,65535]
-------------------	--

## 命令模式

全局配置模式

## 默认

无



## 使用说明

no telnet server sourc port 会配置带内 telnet 服务器的源端口号为默认值 23。

## 举例说明

```
Switch(config)# telnet server source port 2323
```

## 相关命令

无

## 1.6.5 telnet server source mgmt-ifport

本命令可修改交换机上带外 telnet 服务器的源端口。

## 命令语法

**telnetserver source**mgmt-ifport*NUMBER*

**no telnet server source**mgmt-ifport

<b>mgmt-ifport</b> <i>NUMBER</i>	配置带外 telnet 服务器的源端口号，有效值范围[1025,65535]
-------------------------------------	--

## 命令模式

全局配置模式

## 默认

无

## 使用说明

no telnet server sourc mgmt-ifport 会配置带外 telnet 服务器的源端口号为默认值 23。

## 举例说明

```
Switch(config)# telnet server source mgmt-ifport 2323
```

## 相关命令

无

## 1.7 Netconf 配置

### 1.7.1 netconf ssh {enable|disable}

使用此命令启用或者禁用 Netconf 的 ssh 端口 830 监听服务。

#### 命令语法

**netconf ssh { enable | disable }**

enable	开启 SSH 服务
disable	关闭 SSH 服务

#### 命令模式

全局配置模式

#### 默认

关闭

#### 使用说明

无

#### 举例说明

开启 netconf ssh 服务：

```
Switch(config)# netconf ssh enable
```

### 1.7.2 netconf super-user

本命令指定或取消 Netconf 管理功能超级用户。

#### 命令语法

**netconf super-user WORD**

**no netconf super-user**

WORD	超级用户名
------	-------

#### 命令模式

全局配置模式

## 默认

无

## 使用说明

无

## 举例说明

指定 Netconf 管理功能超级用户为 admin:

```
Switch (config)#netconf super-user admin
```

# 1.8 SSH 配置

## 1.8.1 ip ssh server

使用此命令启用或者禁用 SSH 服务。

## 命令语法

**ip ssh server (enable | disable)**

<b>enable</b>	开启 SSH 服务
<b>disable</b>	关闭 SSH 服务

## 命令模式

全局配置模式

## 默认

开启

## 使用说明

无

## 举例说明

交换机上开启 SSH 服务:

```
Switch(config)# ip ssh server enable
```

## 相关命令

**show ip ssh server status**

### 1.8.2 ip ssh server authentication-retries

使用此命令设置使用 SSH 登录时，如果认证失败，可以在尝试的次数。

使用关键字 **no** 恢复当认证失败时可以尝试的次数为默认值。

## 命令语法

**ip ssh server authentication-retries** *integer*

**no ip ssh server authentication-retries**

<b>integer</b>	设置认证失败时还可以尝试登录的次数，最大 6 次
----------------	--------------------------

## 命令模式

全局配置模式

## 默认

默认 6 次

## 使用说明

无

## 举例说明

设置认证失败时还可以尝试登录的次数为 3 次：

```
Switch(config)# ip ssh server authentication-retries 3
```

## 相关命令

**show ip ssh server status**

### 1.8.3 ip ssh server authentication-timeout

使用此命令设置使用 SSH 登录后，无操作时系统断开连接的等待时间。

使用关键字 **no** 恢复此项设置为默认值。

## 命令语法

**ip ssh server authentication-timeout** *seconds*

**no ip ssh server authentication-timeout**

<b>seconds</b>	设置无操作时系统断开连接的等待时间；以秒为单位
----------------	-------------------------

**命令模式**

全局配置模式

**默认**

120 秒

**使用说明**

无

**举例说明**

设置无操作时系统断开连接的等待时间：

```
Switch(config)# ip ssh server authentication-timeout 100
```

**相关命令****show ip ssh server status****1.8.4 ip ssh server authentication-type**

使用此命令设置使用 SSH 登录时所支持的认证方式。

使用关键字 no 恢复此项设置为默认值。

**命令语法****ip ssh server authentication-type** (all | {password | public-key | rsa})**no ip ssh server authentication-type**

<b>all</b>	启用所有认证方式
<b>password</b>	启用密码认证方式
<b>public-key</b>	启用 SSHv2 公钥认证方式
<b>rsa</b>	启用 SSHv1RSA 认证方式

## 命令模式

全局配置模式

## 默认

缺省在登录时支持所有认证方式。

当使用 SSH 协议进行登录时，在开始建立连接时会协商所使用的加密方式；如果某一端设置所使用的加密方式为 all，则协商的结果由对端所使用的加密方式来决定。

## 使用说明

无

## 举例说明

启用所用认证方式：

```
Switch(config)# ip ssh server authentication-type password all
```

## 相关命令

**show ip ssh server status**

### 1.8.5 ip ssh server host-key rsa key

使用此命令设置交换机的 host-key。

使用关键字 no 恢复此项设置为默认值。

## 命令语法

**ip ssh server host-key rsa key***key*

**no ip ssh server host-key rsa**

<b>key</b>	所设置的交换机的 <b>host-key</b>
------------	--------------------------

## 命令模式

全局配置模式

## 默认

host-key 主要用来在连接建立时和公钥一起生成会话 ID；如果在 SSH 登录后修改 host-key，则此次 SSH 登录会立即断开。

## 使用说明

无

## 举例说明

设置交换机的 host-key:

```
Switch(config)# ip ssh serverhost-key rsa key KEY1
```

## 相关命令

**show ip ssh server status**

## 1.8.6 ip ssh server rekey-interval

使用此命令设置交换机的 rekey-interval。

使用关键字 no 恢复此项设置为默认值。

## 命令语法

**ip ssh server rekey-interval***minute*

**no ip ssh server rekey-interval**

<b>minute</b>	<b>rekey-interval 值；以分钟为单位，最大 1440 分钟</b>
---------------	---

## 命令模式

全局配置模式

## 默认

默认时间间隔 60 分钟。

## 使用说明

无

## 举例说明

设置交换机的 rekey-interval 为 30 分钟:

```
Switch(config)# ip ssh server rekey-interval 30
```

## 相关命令

**show ip ssh server status**

## 1.8.7 ip ssh server version

使用此命令设置 SSH 协议的版本。

使用关键字 no 恢复此设置为默认值。

### 命令语法

**ip ssh server version(1 | 2 | all)**

**no ip ssh server version**

<b>1</b>	设置交换机使用 SSH 协议的 <b>version 1</b> 版
<b>2</b>	设置交换机使用 SSH 协议的 <b>version 2</b> 版
<b>all</b>	设置交换机支持 <b>version 1</b> 和 <b>version 2</b>

### 命令模式

全局配置模式

### 默认

版本 2

### 使用说明

缺省交换机使用 version 2 版本。

当使用 SSH 协议登录时，客户端和服务端在开始建立连接时会协商所使用的协议版本；如果协商失败，则不会建立连接；如果某一端设置所使用的 SSH 协议为 all，则协商的结果以对端所支持的 SSH 协议的最高版本来决定。

### 举例说明

设置交换机使用 version 1:

```
Switch(config)# ip ssh server version 1
```

设置交换机使用 version 2:

```
Switch(config)# ip ssh server version 2
```

恢复默认 SSH 的版本:

```
Switch(config)# no ip ssh server version
```

### 相关命令

```
show ip ssh server status
```



## 1.8.8 ip ssh server source address

使用此命令设置 SSH 服务器的源地址。

使用关键字 `no` 恢复此设置为默认值。

### 命令语法

```
ip ssh server source address {vrf NAME} A.B.C.D
```

```
no ip ssh server source address
```

<b>vrf <i>NAME</i></b>	指定提供 SSH 服务的 <b>vrf</b>
<b>ip <i>A.B.C.D</i></b>	配置带内 SSH 服务器的源 IP 地址

### 命令模式

全局配置模式

### 默认

无

### 使用说明

该命令可以修改 SSH 服务器的源地址，指定提供 SSH 服务的 `vrf`。源地址只能是 `loopback` 口的地址或者 `0.0.0.0`，当配置为 `0.0.0.0` 表示不指定 `ip` 作为 SSH 服务器地址。

### 举例说明

设置 SSH 服务器的带内地址为 `vpn1` `vrf` 内的地址 `10.10.10.1`：

```
Switch(config)# ip ssh server source address vrf vpn1 10.10.10.1
```

### 相关命令

`ip ssh server`

## 1.8.9 ip ssh server source port

使用此命令配置带内 SSH 服务器的源端口号。

使用关键字 `no` 恢复此设置为默认值。

### 命令语法

```
ip ssh server source portNUMBER
```

**no ip ssh server sourceport**

<b>portNUMBER</b>	配置带内 SSH 服务器的源端口号，有效值范围[1025,65535]
-------------------	-------------------------------------

**命令模式**

全局配置模式

**默认**

无

**使用说明**

no ip ssh server source port 会配置带内 SSH 服务器的源端口号为默认值 22。

**举例说明**

```
Switch(config)# ip ssh server source port 2222
```

**相关命令**

```
ip ssh server
```

## 1.8.10 ip ssh server source mgmt-ifport

使用此命令配置带外 SSH 服务器的源端口号。

使用关键字 no 恢复此设置为默认值。

**命令语法**

```
ip ssh server source mgmt-ifportNUMBER
```

```
no ip ssh server source mgmt-ifport
```

<b>mgmt-ifport NUMBER</b>	配置带外 SSH 服务器的源端口号，有效值范围[1025,65535]
-------------------------------	-------------------------------------

**命令模式**

全局配置模式

## 默认

无

## 使用说明

no ip ssh server source mgmt-ifport 会配置带外 SSH 服务器的源端口号为默认值 22。

## 举例说明

```
Switch(config)# ip ssh server source mgmt-ifport 2222
```

## 相关命令

ip ssh server

### 1.8.11 show ip ssh server session

使用此命令查看当前 SSH 会话信息

## 命令语法

```
show ip ssh server session
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

查看当前的 SSH 会话信息：

```
Switch# show ip ssh server session
Version Encryption  Hmac      User      IP          State
=====
2.0      aes128-cbc  hmac-md5  abc       10.10.29.22  Session started
```

## 相关命令

show ip ssh server status

### 1.8.12 show ip ssh server status

使用此命令查看 SSH 配置信息。

## 命令语法

```
show ip ssh server status
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

使用此命令查看 SSH 配置信息：

```
Switch# show ip ssh server status
SSH server enabled
Version: 1.99
Authentication timeout: 33 second(s)
Authentication retries: 6 time(s)
Server key lifetime: 60 minute(s)
Authentication type: password, public-key
```

## 相关命令

```
show ip ssh server session
```

### 1.8.13 rsa key

使用此命令创建 key 并且进入 key 的自定义配置模式。

## 命令语法

```
rsa keykeyname
```

<b>keyname</b>	指定要创建的 key 名称
----------------	---------------

## 命令模式

全局配置模式

## 默认

无

## 使用说明

无

## 举例说明

创建 key1 并进入 key1 的自定义配置模式：

```
Switch(config)# rsa key KEY1  
Switch(config-rsa-key)#
```

## 相关命令

show rsa keys

## 1.8.14 key format

使用此命令设置生成的 key 的格式。

## 命令语法

**key format** (der | pem)

<b>der</b>	设置生成的 key 的格式为 der 格式
<b>pem</b>	设置生成的 key 的格式为 pem 格式

## 命令模式

RSA key 配置模式

## 默认

默认是 Der 格式

## 使用说明

无

## 举例说明

设置此 key 的格式为 pem 格式：

```
Switch(config)# rsa key KEY1
```

```
Switch(config-rsa-key)# key format der
```

## 相关命令

**rsa key**

### 1.8.15 key string end

退出当前 key 配置模式并且应用所有修改。

## 命令语法

**key string end**

## 命令模式

## 命令语法

## 默认

无

## 使用说明

无

## 举例说明

退出当前 key 配置模式并且应用所有修改：

```
Switch(config)# rsa key KEY1
Switch(config-rsa-key)# key string end
Switch(config)#
```

## 相关命令

**rsa key**

### 1.8.16 key type

使用此命令设置 key 的模式。

## 命令语法

**key type** (public | private)

<b>public</b>	生成公钥
<b>private</b>	生成私钥

## 命令模式

RSA key 配置模式

## 默认

无

## 使用说明

无

## 举例说明

设置生成公钥:

```
Switch(config)# rsa key KEY1  
Switch(config-rsa-key)# key type public
```

## 相关命令

**rsa key**

### 1.8.17 reset

使用此命令清除在当前 key 配置模式中所作的所有修改。

## 命令语法

**reset**

## 命令模式

RSA key 配置模式

## 默认

无

## 使用说明

无

## 举例说明

清除在当前 key 配置模式中所作的所有修改:

```
Switch(config)# rsa key KEY1  
Switch(config-rsa-key)# reset
```

## 相关命令

**rsa key**

### 1.8.18 validate

使用此命令检查给当前 key 的配置是否有效。

## 命令语法

**validate**

## 命令模式

RSA key 配置模式

## 默认

无

## 使用说明

无

## 举例说明

检查在当前 key 配置模式中所修改的配置是否有效：

```
Switch(config)# rsa key KEY1  
Switch(config-rsa-key)# validate
```

## 相关命令

**rsa key**

### 1.8.19 KEYLINE

使用此命令给当前 key 添加密钥内容。

## 命令语法

**KEYLINE**

## 命令模式

RSA key 配置模式

## 默认

无



## 使用说明

此命令通过直接在屏幕上粘贴密钥文件的内容并设置对应的格式以生成 key。

## 举例说明

粘贴密钥文件内容：

```
Switch(config)# rsa key KEY1
Switch(config-rsa-key)# 00302017 4A7D385B 1234EF29 335FC973
Switch(config-rsa-key)# 2DD50A37 C4F4B0FD 9DADE748 429618D5
```

## 相关命令

**validate**

### 1.8.20 rsa key export

使用此命令使用指定 key 导出密钥文件。

## 命令语法

**rsa key keyname export url destination-file(public | private)(der | der-hex | pem | ssh1 | ssh2)**

<b>keyname</b>	指定要导出密钥文件所使用的 key
<b>destination-file</b>	指定导出的密钥文件存放的位置
<b>public</b>	导出公钥文件
<b>private</b>	导出私钥文件
<b>(der   der-hex   pem   ssh1   ssh2)</b>	指定导出的密钥文件的格式

## 命令模式

全局配置模式

## 默认

无

## 使用说明

指定导出的密钥文件的格式

## 举例说明

使用 key1 生成公钥文件：

```
Switch(config)# rsa key KEY1 export url flash:/key1.pub public ssh2
```

使用 key2 生成私钥文件：

```
Switch(config)# rsa key KEY2 export url flash:/key1 private ssh1
```

## 相关命令

**rsa key generate**

**rsa key import**

### 1.8.21 rsa key import

使用此命令使用指定密钥文件导入 key。

## 命令语法

```
rsa key keyname import url source-file(public | private) (der | der-hex | pem | ssh1 | ssh2)
```

<b>keyname</b>	指定要导入的 key 名称
<b>source-file</b>	指定要使用的密钥文件存放的位置
<b>public</b>	从公钥文件导入 key
<b>private</b>	从私钥文件导入 key
<b>der   der-hex   pem   ssh1   ssh2</b>	指定要使用的密钥文件的格式

## 命令模式

全局配置模式

## 默认

无

## 使用说明

通过密钥文件生成密钥 key，不能与系统现在存在的 key 名称相同，否则提示操作失败。

## 举例说明

使用 key1 公钥文件生成公钥 key：

```
Switch(config)# rsa key KEY1 import url flash:/key1.pub public ssh2
```

使用 key2 私钥文件生成私钥 key:

```
Switch(config)# rsa key KEY2 import url flash:/key1 private ssh1
```

## 相关命令

```
rsa key generate
```

```
rsa key export
```

## 1.8.22 show rsa key

使用此命令查看 key 的详细信息。

## 命令语法

```
show rsa key keyname
```

<b>keyname</b>	要查看的 key 名称
----------------	-------------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

查看 key1 的详细信息:

```
Switch# show rsa key KEY1
RSA key information:
=====
Name: KEY1
Type: private
Modulus: 1024 bit
Usage count: 0
Private key DER code:
30820258
    0201
    00
    028180
```

9B3E9726 6405BD54 692F172A901F3879 C947366E 5703D282 AA31707F 214D38C9

## 相关命令

**show rsa keys**

### 1.8.23 show rsa keys

使用此命令查看交换机所有 key 的简要信息。

## 命令语法

show rsa keys

## 命令模式

特权模式

## 默认

无

## 使用说明

查看交换机所有 key 的简要信息。

## 举例说明

查看交换机所有 key 的简要信息：

```
Switch# show rsa keys
Name                               Type      用法      Modulus
=====
key1                               private  0         1024
key2                               public   0         1024
```

## 相关命令

**show rsa key**

### 1.8.24 ssh

使用此命令登录到远程 SSH 服务器。

## 命令语法

```
ssh -l NAME ({-i KEYNAME | -p DPORT | -v (1|2) | -c {3des|des|3des-cbc|aes128-cbc|aes192-cbc|aes256-cbc} | -m {hmac-md5-128|hmac-md5-96|hmac-sha1-160|hmac-sha1-96} | -o numberofpasswordprompts NUM | -a A.B.C.D}) (mgmt-if) (A.B.C.D|X::X::X::X|HOST)
```

<b>-l NAME</b>	指定登录用户名
<b>-i KEYNAME</b>	RSA 私钥名称
<b>-p DPORT</b>	指定远程 SSH 服务器端口
<b>-v (1 2)</b>	指定 SSH 协议版本
<b>-c</b>	选择加密算法
<b>3des</b>	Triple DES (仅 SSHv1 使用)
<b>des</b>	DES (仅 SSHv1 使用)
<b>3des-cbc</b>	Triple DES (仅 SSHv2 使用)
<b>aes128-cbc</b>	AES 128 bits (仅 SSHv2 使用)
<b>aes192-cbc</b>	AES 192 bits (仅 SSHv2 使用)
<b>aes256-cbc</b>	AES 256 bits (仅 SSHv2 使用)
<b>-m</b>	选择 HMAC 算法
<b>hmac-md5-128</b>	基于 MD5 的 HMAC (128 bits, 仅 SSHv2 使用)
<b>hmac-md5-96</b>	基于 MD5 的 HMAC (96 bits, 仅 SSHv2 使用)
<b>hmac-sha1-160</b>	基于 SHA1 的 HMAC (160 bits, 仅 SSHv2 使用)
<b>hmac-sha1-96</b>	基于 SHA1 的 HMAC (96 bits, 仅 SSHv2 使用)
<b>-o numberof- passwordprompts NUM</b>	指定密码重试次数, 有效值为[1, 7]
<b>-a A.B.C.D</b>	Ssh 时指定源 IP
<b>mgmt-if</b>	使用管理口连接
<b>A.B.C.D</b>	指定 SSH 服务器的 IPv4 地址
<b>X:X::X:X</b>	指定 SSH 服务器的 IPv6 地址
<b>HOST</b>	指定 SSH 服务器的主机名称

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

配置交换机登录到地址为 1.1.1.1 的 SSH 服务器：

```
Switch# ssh -l aaa -v 2 1.1.1.1
aaa@1.1.1.1's password:
Switch#
```

## 相关命令

ip ssh server

# 1.9 时间配置命令

## 1.9.1 clock set datetime

全局配置模式下使用该命令来修改系统时间。

## 命令语法

**clock set datetimehh:mm:ssmonth day year**

<b>hh:mm:ss</b>	当前时间，hh 取值范围为 0~23, mm 和 ss 取值范围为 0~59。
<b>month</b>	设置当前月份，范围为 1 到 12
<b>day</b>	设置当前日期，范围为 1 到 31
<b>year</b>	设置当前年份，范围为 1993 到 2035

## 命令模式

全局配置模式

## 默认

缺省为 UTC 时间。

## 使用说明

在需要严格获取绝对时间的应用环境中，必须设定设备当前日期和时钟。

## 举例说明

```
Switch (config)# clock set 13:32:00 23 7 2014
```

## 相关命令

show clock

### 1.9.2 clock set timezone

全局配置模式下使用该命令来修改系统时区。

## 命令语法

clock set timezone ZONE (add | minus) hours-offset [minutes-offset] [seconds-offset]

no clock set timezone

<b>ZONE</b>	设置时区名字，时区名字长度必须大于等于 3 并且小于 32，同时只支持[a-zA-Z_], 时区名的首字母和末字母不能为”_”。
<b>add</b>	比 UTC (Universal Time Coordinated, 通用协调时间) 标准时间增加
<b>minus</b>	比 UTC 标准时间减少
<b>hours-offset</b>	设置时区的小时偏移量
<b>minutes-offset</b>	设置时区的分钟偏移量
<b>seconds-offset</b>	设置时区的秒偏移量

## 命令模式

全局配置模式

## 默认

缺省为 UTC 时间。

## 使用说明

无。

## 举例说明

设置本地时区名称为 ZZZ，比 UTC 标准时间增加 5 小时

```
Switch (config)# clock set timezone ZZZ add 5
```

## 相关命令

show clock

## 1.9.3 clock set summer-time

全局配置模式下使用该命令来设置夏令时。

### 命令语法

```
clock set summer-time ZONE recurring start-time end-time offset
```

```
clock set summer-time ZONE date start-time end-time offset
```

```
no clock set summer-time
```

<b>ZONE</b>	设置时区名字，时区名字长度必须大于等于 3 并且小于 32，同时只支持[a-zA-Z_], 时区名的首字母和末字母不能为”_”。
<b>recurring</b>	表示对从某一年开始的以后每年的夏令时时间的设置
<b>date</b>	表示仅对某一年的夏令时时间进行设置
<b>start-time</b>	起始时间和日期，对于 recurring 模式，格式为 <i>month, day, hh:mm:ss</i> ，对于 date 模式，格式为 <i>month, day, year, hh:mm:ss</i>
<b>end-time</b>	结束时间和日期，对于 recurring 模式，格式为 <i>month, day, hh:mm:ss</i> ，对于 date 模式，格式为 <i>month, day, year, hh:mm:ss</i>
<b>offset</b>	增加的时间，以分钟为单位，默认为 60 分钟

### 命令模式

全局配置模式

### 默认

夏令时默认不使能。

### 使用说明

夏令时的第一部分用来说明起始时间和日期，第二部分用来说明结束时间和日期。所有的时间都是基于当前时区。开始时间是基于当前的标准时间，而结束时间是基于夏令时的。如果设置的开始时间大于结束时间，说明你处于南半球。

### 举例说明

下面的例子显示了夏令时开始的时间是每年的 6 月 1 日 2 点钟，结束于每年的 10 月 31 日 2 点钟。

```
Switch (config)# clock set summer-time recurring 6 1 02:00:00 10 31 02:00:00 120
```

### 相关命令

```
show clock
```



## 1.9.4 show clock

显示当前系统的时间和日期。

### 命令语法

```
show clock
show clock detail
```

### 命令模式

特权模式

### 默认

无。

### 使用说明

无。

### 举例说明

```
Switch#show clock detail
10:43:00 beijing Fri Oct 25 2013
Time zone: (GMT + 08:00:00) beijing
```

### 相关命令

```
show clock
```

## 1.9.5 show timezones

显示所有的时区。

### 命令语法

```
show timezones
```

### 命令模式

特权模式

### 默认

无。

### 使用说明

无。

## 举例说明

```
Switch#show timezones
(GMT+00:06:04)   Europe/Andorra
(GMT+03:41:12)   Asia/Dubai
(GMT+04:36:48)   Asia/Kabul
(GMT-04:07:12)   America/Antigua
(GMT-04:12:16)   America/Anguilla
(GMT+01:19:20)   Europe/Tirane
(GMT+02:58:00)   Asia/Yerevan
(GMT-04:36:00)   America/Curacao
(GMT+00:52:56)   Africa/Luanda
(GMT+11:06:24)   Antarctica/McMurdo   McMurdo Station, Ross Island
=====
(GMT+00:00:00)   Antarctica/South_Pole Amundsen-Scott Station, South Pole
(GMT-04:32:32)   Antarctica/Rothera   Rothera Station, Adelaide Island
(GMT-04:16:24)   Antarctica/Palmer    Palmer Station, Anvers Island
```

## 相关命令

show clock

## 1.10 证书命令

### 1.10.1 generate device identifier

特权模式下使用该命令来生成建立证书所需的设备唯一标识符。

## 命令语法

generate device identifier (mgmt-if | )*GURLNAME*

generate device identifier (*GFILENAME*)

<b>mgmt-if</b>	管理端口
<b>GURLNAME</b>	目的 URL 地址
<b>GFILENAME</b>	本地文件名

## 命令模式

特权模式

## 默认

无

## 使用说明

该命令用于生成交换机的设备唯一标识符(UDI)，使用对应交换机的 UDI，可以向设备商申请该交换机可用的各类证书。

## 举例说明

```
Switch# generate device identifier mgmt-if tftp://10.10.38.160/device.udi
```

## 相关命令

无

## 1.10.2 show license

特权模式下使用该命令来显示交换机上的证书。

## 命令语法

```
show license (GFILENAME)
```

GFILENAME	本地文件名
-----------	-------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch# show lincese
License files:
=====
flash:/ma.lic:
  Created Time: Fri Dec 6 17:22:23 CST 2013
  Vendor:      centec
  Customer:    centec
  Device MAC:  00:1E:08:09:03:00
  Feature Set: QINQ MVR ERPS MEF ETHOAM
               VPWS VPLS HVPLS SMLK TPOAM
               OSPF PIM_SM IGMP VRF MPLS
```

```
LDP BGP RSVP OSPF_TE EXTEND_ACL  
PTP BFD SSM IPV6 OSPF6  
PIM_SM6 MVR6 RIPNG TUNNEL_V6
```

## 相关命令

无

## 1.11 HTTP 配置

### 1.11.1 service http

本命令可让交换机启用 HTTP 服务。

## 命令语法

```
service http (enable | disable)
```

<b>enable</b>	开启 HTTP 服务
<b>disable</b>	关闭 HTTP 服务

## 命令模式

全局配置模式

## 默认

关闭

## 使用说明

使能 HTTP 服务需要先加载 WEB 镜像。

## 举例说明

```
Switch(config)# server http enable
```

## 相关命令

```
http server load
```

```
http timeout
```

### 1.11.2 service https

本命令可让交换机启用 HTTPS 服务。

## 命令语法

service https (enable | disable)

<b>enable</b>	开启 HTTPS 服务
<b>disable</b>	关闭 HTTPS 服务

## 命令模式

全局配置模式

## 默认

关闭

## 使用说明

使能 HTTPS 服务需要先加载 WEB 镜像。

## 举例说明

```
Switch(config)# server https enable
```

## 相关命令

**http server load**

**http timeout**

### 1.11.3 http server load

用来加载 WEB 镜像。

## 命令语法

http server load *FILENAME*

no http server load

<b><i>FILENAME</i></b>	<b>WEB 镜像名称</b>
------------------------	-----------------

## 命令模式

全局配置模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch(config)# http server load flash:/webImage.bin
```

## 相关命令

**service http enable**

**service https enable**

**http timeout**

### 1.11.4 http timeout

配置 Web 服务器的超时时间。

## 命令语法

```
http timeout timeout
```

<b><i>timeout</i></b>	指定在线用户的 Web 服务器超时时间。取值范围是 1~60，单位是分钟。
-----------------------	---------------------------------------

## 命令模式

全局配置模式

## 默认

20min

## 使用说明

无

## 举例说明

```
Switch(config)# http timeout 30
```

## 相关命令

**http server load**

```
service http enable
service https enable
```

## 1.12 周期定时任务配置

### 1.12.1 kron policy-list

全局配置模式下，使用 **kron policy-list** 命令创建 kron policy 策略并进入该 kron policy 模式。

使用 **no** 命令删除该策略。

#### 命令语法

```
kron policy-list name
no kron policy-list name
```

name	策略名称
------	------

#### 命令模式

全局配置模式

#### 默认

无

#### 使用说明

kron polciy 名称必须符合命名规定。包括英文字符，数字，连字号以及下划线。字数不能超过 64 个字符。并且 kron policy 策略最多同时存在 20 条。

#### 举例说明

创建 kron policy 策略并进入该 kron policy 模式：

```
Switch (config)# kron policy-list 123
Switch(config-kron-policy)#
```

### 1.12.2 command

在 kron policy 模式下，使用 **command** 命令执行 EXEC 模式下的命令。

使用 **no** 关键字用来删除该命令。

#### 命令语法

```
command LINE
```

**no command** *LINE*

LINE	交换机 EXEC 模式下的命令
------	-----------------

**命令模式**

kron policy 配置模式

**默认**

无

**使用说明**

用户必须保证该 **command** 命令有效并且能在 EXEC 下执行。命令本身不会对用户输入进行检查，需用户保证该命令的可靠性。且一个 **kron policy** 策略最多支持配置 5 条 **command** 规则。

**举例说明**

执行 EXEC 模式下的命令：

```
Switch (config)# kron policy 123
Switch(config-kron-policy)#command show ftp
Switch(config-kron-policy)#
```

**1.12.3 kron occurrence policy-list at**

在全局配置模式下，使用该命令指定某个 **kron policy** 策略执行的周期。

本命令的 **no** 格式用来删除该配置。

**命令语法**

**kron occurrence policy-list** *name at time* { **daily** | **weekly** *week-range* | **monthly** *month-range* }

**no kron occurrence policy-list** *name*

name	kron policy 策略名称
time	配置执行策略的时间（小时：分钟）
daily	每天执行一次
weekly	每周执行一次
week-range	星期一至星期日，取值范围为 1~7
monthly	每月执行一次
month-range	具体日期，取值范围为 1~31



## 命令模式

全局配置模式

## 默认

无

## 使用说明

用户在使能 `kron policy` 策略前需要配置该策略的周期，配置周期的时间以交换机的时间为准，若该月份无 31 或 30 号则会跳过该月。

## 举例说明

设置名为 123 的 `kron policy` 策略每天 12 点执行一次：

```
Switch (config)# kron occurrence policy-list 123 at 12:00 daily
```

## 1.12.4 enable kron policy-list

全局配置模式下，使用 `enable kron policy-list` 命令使能 `kron policy` 策略。

使用 `no` 命令去使能该策略。

## 命令语法

```
enable kron policy-list name
```

```
no enable kron policy-list name
```

name	策略名称
------	------

## 命令模式

全局配置模式

## 默认

无

## 使用说明

使能该 `kron policy` 策略前，必须要配置执行周期和至少一条 `command` 规则。

## 举例说明

使能 `kron policy` 策略：

```
Switch (config)# enable kron policy-list 123
```

## 1.12.5 show kron policy-list

显示配置 kron policy 的策略信息。

### 命令语法

```
show kron policy-list [ name ]
```

name	策略名称
------	------

### 命令模式

特权模式

### 默认

无

### 使用说明

无

### 举例说明

显示配置 kron policy 的策略信息：

```
Switch# show kron policy-list
kron policy list count      : 1
kron policy list enable count : 1

kron policy list name      : test
kron policy list status    : enable
kron policy list rule      :
  rule 1                    : write
  rule 2                    : copy flash:/startup-config.conf mgmt-if
ftp://admin:123456@10.69.65.112:21/startup-config.conf
kron occurrence rule recurring at 12:00 daily
```

# 2 以太网命令行参考

## 2.1 接口命令

### 2.1.1 bandwidth

使用此命令设置端口带宽。使用关键词 **no** 设置带宽到默认值。

#### 命令语法

**bandwidth** bandwidth

**no bandwidth**

bandwidth	<1-100000000> 端口带宽，单位：kbps
-----------	----------------------------

#### 命令模式

端口配置模式

#### 默认

无

#### 使用说明

无

#### 举例说明

- 下面的例子显示了如何设置带宽为 1M 字节：

```
Switch(config)# interface eth-0-1
Switch(config-if)# bandwidth 1000
```

- 下面的例子显示了如何设置带宽到默认值：

```
Switch(config-if)# no bandwidth
```

#### 相关命令

duplex

speed

## 2.1.2 clear counters

使用此命令清除端口的报文统计信息。

### 命令语法

```
clear counters (IFNAME |)
```

IFNAME	端口名称；可以为物理端口，也可以为汇聚端口；如果此项为空，则清除所有端口的报文统计信息
--------	---

### 命令模式

特权模式

### 默认

无

### 使用说明

在某些情况下，需要统计一定时间内某端口的流量，这就需要在统计开始前清除该端口原有的统计信息，重新进行统计。如果不指定端口类型和端口号，则清除所有端口的统计信息；如果仅指定端口类型，则清除所有该类型端口的统计信息。

### 举例说明

- 下面的例子显示了如何清除所有端口的统计信息：

```
Switch# clear counters
```

- 下面的例子显示了如何清除物理口 eth-0-1 的统计信息：

```
Switch# clear counters eth-0-1
```

- 下面的例子显示了如何清除聚合端口 aggl 的统计信息：

```
Switch# clear counters aggl
```

### 相关命令

无

## 2.1.3 description

使用该命令为端口设置描述信息。

使用关键词 **no** 删除端口描述信息。

## 命令语法

description *LINE*

no description

LINE	端口描述信息，必须小于等于 64 个字符，字符类型必须是 “0-9A-Za-z.-_” 这样的格式
------	---

## 命令模式

端口配置模式

## 默认

无

## 使用说明

无

## 举例说明

- 下面的例子显示了如何配置端口 eth-0-1 上的描述信息：

```
Switch(config)# interface eth-0-1
Switch(config-if)# description Ethernet
```

- 下面的例子显示了如何清除端口上的描述信息：

```
Switch(config-if)# no description
```

## 相关命令

无

### 2.1.4 duplex

使用此命令设置端口的工作方式。

使用关键词 no 设置工作方式为默认值。

## 命令语法

duplex (auto |full |half)

no duplex

auto	自协商模式，端口根据它所连接的设备自动检测应该处于全双工还是半双工状态
------	-------------------------------------

full	全双工模式
half	半双工模式,只能配置在 10M,100M 的端口

## 命令模式

端口配置模式

## 默认

自动

## 使用说明

此命令不能在 10G 端口以及复用端口(combo port)上使用。

## 举例说明

- 设置端口模式为自协商：  
Switch(config)# interface eth-0-1  
Switch(config-if)# duplex auto
- 设置端口模式为全双工：  
Switch(config-if)# duplex full
- 将端口双工模式设为默认值：  
Switch(config-if)# no duplex

## 相关命令

bandwidth

speed

### 2.1.5 speed

使用该命令设置端口速率。使用该命令的 no 形式恢复速率为默认值。

## 命令语法

speed (10 |100 |1000 |auto|100G|10G|2G5|40G|5G)

no speed

auto	端口自动检测协商速率
10	强制端口速率为 10Mb/s
100	强制端口速率为 100Mb/s

1000	强制端口速率为 1000Mb/s
100G	强制端口速率为 100Gb/s
10G	强制端口速率为 10Gb/s
2G5	强制端口速率为 2.5Gb/s
40G	强制端口速率为 40Gb/s
5G	强制端口速率为 5Gb/s

## 命令模式

端口配置模式

## 默认

自动

## 使用说明

此命令不能在 10G 端口以及复用端口(combo port)上使用。

## 举例说明

- 强制设置端口速率为 1000Mb/s:

```
Switch(config)# interface eth-0-1
Switch(config-if)# speed 1000
```

- 恢复端口速率为自协商:

```
Switch(config-if)# no speed
```

## 相关命令

bandwidth

duplex

## 2.1.6 interface

使用该命令进入端口配置模式。

## 命令语法

```
interface IFNAME
```

IFNAME	接口名称, 比如 eth-0-1, agg1, vlan1, loopback1
--------	--

## 命令模式

全局配置模式

## 默认

无

## 使用说明

无

## 举例说明

- 进入物理端口 **eth-0-1**:  
Switch(config)# interface eth-0-1
- 进入聚合端口 **agg1**:  
Switch(config)# interface agg1
- 进入逻辑口 **vlan2**:  
Switch(config)# interface vlan2

## 相关命令

exit

## 2.1.7 interface range

使用该命令进入接口范围模式。

## 命令语法

interface range *IFNAME*

IFNAME	用“,”或“-”区分的界面范围集
--------	------------------

## 命令模式

全局配置模式

## 默认

无



## 使用说明

无

## 举例说明

- 下面的例子显示了如何操作一系列物理接口：

```
Switch(config)# interface range eth-0-1 - 24
Switch(config-if-range)# shutdown
```

- 下面的例子显示了如何操作一系列逻辑接口：

```
Switch(config)# interface range vlan 1 - 20
Switch(config-if-range)# shutdown
```

- 下面的例子显示了如何操作一系列聚合端口：

```
Switch(config)# interface range agg 10 - 20
Switch(config-if-range)# shutdown
```

- 下面的例子显示了如何操作一系列环回接口：

```
Switch(config)# interface range loopback 0 - 5
Switch(config-if-range)# shutdown
```

## 相关命令

无

## 2.1.8 interface range create vlan

使用此命令创建一系列的 `vlanif` 并进入 `vlan` 接口模式。

## 命令语法

```
interface range create vlan vid-range
```

<code>vid-range</code>	VLAN ID 范围，可以用 “,” 或 “-” 来分隔
------------------------	------------------------------

## 命令模式

全局配置模式

## 默认

无

## 使用说明

无

## 举例说明

下面的例子显示了如何一次性创建 10 个 vlan 界面：

```
Switch(config)# interface range create vlan 10 - 20
Switch(config-if-range)# shutdown
```

## 相关命令

无

## 2.1.9 jumboframe

使用该命令允许长帧通过以太网端口。使用该命令的 **no** 形式关闭该功能。

## 命令语法

```
jumboframe enable
no jumboframe enable
```

## 默认

无

## 命令模式

端口配置模式

## 使用说明

默认情况下接口上不允许长帧通过，最大可以通过的报文的长度是 1632 字节。使能 **jumboframe** 后，端口上最大允许通过的报文长度为 9600 字节。

## 举例说明

- 下面的例子显示了如何使能 **jumboframe** 功能：

```
Switch(config)# interface eth-0-1
Switch(config-if)# jumboframe enable
```

- 下面的例子显示了如何关闭 **jumboframe** 功能：

```
Switch(config-if)# no jumboframe enable
```

## 相关命令

无

## 2.1.10 media-type

使用该命令设置端口的介质类型。使用该命令的 **no** 形式恢复默认值。

## 命令语法

media-type (auto-select|rj45|sfp)

auto-select	自动检测选择端口介质类型
rj45	端口介质类型为 RJ45
sfp	端口介质类型为 SFP

## 命令模式

端口配置模式

## 默认

自动选择端口介质类型

## 使用说明

无

## 举例说明

- 下面的例子显示了如何设置端口的介质类型为 RJ45：

```
Switch(config)# interface eth-0-1
Switch(config-if)# media-type rj45
```

- 下面的例子显示了如何设置端口的介质类型为自动选择：

```
Switch(config-if)# no media-type
```

## 相关命令

无

## 2.1.11 unidirectional

使用该命令使能/关闭端口的单通功能。

## 命令语法

unidirectional (enable|disable)

enable	使能端口的单通功能
disable	关闭端口的单通功能

## 命令模式

端口配置模式

## 默认

关闭单通功能

## 使用说明

使能单通功能会导致该端口的发送强制可用，而接收强制不可用。  
仅光口支持单通功能，且 1000M 速率下需要将 duplex 强制为 full。

## 举例说明

- 下面的例子显示了如何使能端口的单通功能：

```
Switch(config)# interface eth-0-1
Switch(config-if)# unidirectional enable
```

- 下面的例子显示了如何关闭端口的单通功能：

```
Switch(config-if)# unidirectional disable
```

## 相关命令

无

## 2.1.12 shutdown

使用该命令手动关闭端口。使用该命令的 no 形式打开端口。

## 命令语法

```
shutdown
no shutdown
```

## 命令模式

端口配置模式

## 默认

无

## 使用说明

无

## 举例说明

- 下面的例子显示了如何关闭一个端口：

```
Switch(config)# interface eth-0-1
Switch(config-if)# shutdown
```

- 下面的例子显示了如何打开一个端口：

```
Switch(config-if)# no shutdown
```

## 相关命令

无

### 2.1.13 split interface

使用该命令可以拆分 40G 或者 100G 的端口。使用该命令的 `no` 形式取消拆分。

## 命令语法

```
split interface IFNAME (10giga|40giga)
```

```
no split interface
```

IFNAME	需要拆分的物理口
10giga	把端口拆分成 4 个 10G 口
40giga	把端口拆分成 1 个 40G 口

## 命令模式

全局配置模式

## 默认

无

## 使用说明

拆分命令配置或者取消配置后，先要保存配置并重启才生效。

## 举例说明

- 下面的例子显示了如何将口拆分成 4 个 10G 口：

```
Switch(config)# split interface eth-0-1 10giga
```

## 相关命令

无

## 2.1.14 load-interval

使用该命令设置计算端口速率时的时间范围。使用该命令的 **no** 形式恢复时间范围为默认值。

### 命令语法

```
load-interval seconds
```

```
no load-interval
```

seconds	时间范围，30 秒到 600 秒
---------	------------------

### 命令模式

端口配置模式

### 默认

300 秒

### 使用说明

时间范围必须是 30 的整数倍。默认值是 300 秒。

### 举例说明

- 下面的例子显示了如何将端口的 **load interval** 设为 600 秒：

```
Switch(config)# interface eth-0-1  
Switch(config-if)# load-interval 600
```

- 下面的例子显示了如何将端口的 **load interval** 恢复为默认值：

```
Switch(config-if)# no load-interval
```

### 相关命令

```
show interface
```

## 2.1.15 vlan dot1q tag native

使用该命令来配置边缘交换机使得所有从 **trunk** 口出去的报文都是带标签的。

### 命令语法

```
vlan dot1q tag native
```

```
no vlan dot1q tag native
```

## 命令模式

端口配置模式

## 默认

无

## 使用说明

如果在交换机上的 trunk 口上配置了该命令，那么交换机可以接收所有不带标签的报文，但是从该端口出去的报文一定是打上标签的。默认情况下该功能不开启。

## 举例说明

- 下面的例子显示如何让所有从 eth-0-1 口出去的报文都带标签：

```
Switch(config)# interface eth-0-1
Switch(config-if)# vlan dot1q tag native
```

- 下面的例子显示了如何禁用 tag native 功能：

```
Switch(config-if)# no vlan dot1q tag native
```

## 相关命令

无

### 2.1.16 show interface

使用该命令显示指定端口或者所有端口的配置以及统计值。

## 命令语法

```
show interface (IFNAME | subif subnumber)
```

<i>IFNAME</i>	接口名称 eth: 物理端口 agg: Agg 端口 loopback: 环回端口 vlan: Vlan 端口 tunnel: Tunnel 端口 null: Null 端口
<i>subnumber</i>	子接口编号

## 命令模式

特权模式

## 默认

无

## 使用说明

OAM 的统计值只有在端口是 10G 模式的时候才能显示出来。

## 举例说明

下面的例子显示了接口 eth-0-1 上的信息：

```
Switch# show interface eth-0-1
```

```
Interface eth-0-1
  Interface current state: Administratively DOWN
  Hardware is Ethernet, address is bc3e.60b2.1601 (bia bc3e.60b2.1601)
  Bandwidth 1000000 kbits
  Index 1 , Metric 1 , Encapsulation ARPA
  Speed - 1000Mb/s , Duplex - Full , Media type is 1000BASE_T
  Link speed type is autonegotiation, Link duplex type is autonegotiation
  Input flow-control is off, output flow-control is off
  The Maximum Frame Size is 1534 bytes
  VRF binding: not bound
  Label switching is disabled
  No virtual circuit configured
  ARP timeout 01:00:00, ARP retry interval 1s
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes
    Received 0 unicast, 0 broadcast, 0 multicast
    0 runts, 0 giants, 0 input errors, 0 CRC
    0 frame, 0 overrun, 0 pause input
    0 input packets with dribble condition detected
    0 packets output, 0 bytes
    Transmitted 0 unicast, 0 broadcast, 0 multicast
    0 underruns, 0 output errors, 0 pause output
```

下面的例子显示了接口 eth-0-1 上的子接口信息：

```
Switch# show interface eth-0-1 subif 5
```

```
Interface eth-0-1 subif 5
  Interface current state: UP
  Hardware is Subif, address is d886.0b00.09d5 (bia d886.0b00.09d5)
  Encapsulation-dot1q 5
  Bandwidth 1000000 kbits
  Index 16901 , Metric 1 , Encapsulation ARPA
  The maximum transmit unit (MTU) is 1500 bytes
  VRF binding: not bound
  VRRP master of : VRRP is not configured on this interface
```



```
ARP timeout 01:00:00, ARP retry interval 1s
ARP Proxy is disabled, Local ARP Proxy is disabled
```

## 相关命令

show interface status

### 2.1.17 show interface status

使用该命令显示物理端口和聚合端口的摘要信息。

## 命令语法

show interface (*IFNAME*) status

IFNAME	接口名称
--------	------

## 命令模式

特权模式

## 默认

无

## 使用说明

该命令不能显示 VLAN 接口和 TUNNEL 接口的信息。

## 举例说明

下面的例子显示了所有物理口和汇聚端口的摘要信息：

Switch# show interface status

```
Port      Status    Duplex    Speed    Mode    Type        Description
-----
eth-0-1   down      a-full    a-1000   ACCESS  1000BASE_T
eth-0-2   down      a-full    a-1000   ACCESS  1000BASE_T
eth-0-3   admin down auto      auto     ACCESS  1000BASE_T
eth-0-4   admin down auto      auto     ACCESS  1000BASE_T
eth-0-5   up        a-full    a-1000   routed  1000BASE_T
eth-0-6   up        a-full    a-100    ACCESS  1000BASE_T
eth-0-7   admin down auto      auto     ACCESS  1000BASE_T
eth-0-8   admin down auto      auto     ACCESS  1000BASE_T
eth-0-9   down      a-full    a-1000   ACCESS  1000BASE_T
eth-0-10  down      a-full    a-1000   ACCESS  1000BASE_T
eth-0-11  admin down auto      auto     ACCESS  1000BASE_T
eth-0-12  admin down auto      auto     ACCESS  1000BASE_T
eth-0-13  admin down auto      auto     ACCESS  1000BASE_T
eth-0-14  admin down auto      auto     ACCESS  1000BASE_T
eth-0-15  admin down auto      auto     ACCESS  1000BASE_T
```

```
eth-0-16  admin down auto    auto    ACCESS  1000BASE_T
eth-0-17  admin down auto    auto    ACCESS  1000BASE_T
eth-0-18  admin down auto    auto    ACCESS  1000BASE_T
eth-0-19  admin down auto    auto    ACCESS  1000BASE_T
eth-0-20  admin down auto    auto    ACCESS  1000BASE_T
```

## 相关命令

无

## 2.1.18 show interface hybrid

使用该命令显示所有 Hybrid 端口的统计信息。

## 命令语法

```
show interface hybrid
```

## 命令模式

特权模式

## 默认

无

## 使用说明

该命令以列表的形式显示 Hybrid 接口的统计信息。

## 举例说明

下面的例子显示了所有 Hybrid 接口的信息：

```
Switch# show interface hybrid
```

```
Port      Native VLAN  VLANs is allowed on hybrid
-----
eth-0-10  10           10,20,30
```

## 相关命令

show interface

## 2.1.19 show interface trunk

使用该命令显示所有 Trunk 端口的统计信息。

## 命令语法

```
show interface trunk
```

## 命令模式

特权模式

## 默认

无

## 使用说明

该命令以列表的形式显示 Trunk 接口的统计信息。

## 举例说明

下面的例子显示了所有 Trunk 接口的信息：

```
Switch# show interface trunk
```

Port	Encapsulation	Status	Native VLAN
eth-0-20	802.1q	trunking	20

Port	VLANs is allowed on trunk
eth-0-20	1,10,20,30

## 相关命令

show interface

### 2.1.20 show interface summary

使用该命令显示指定端口或者所有端口的统计信息。

## 命令语法

```
show interface (IFNAME) summary
```

IFNAME	接口名称
--------	------

## 命令模式

特权模式

## 默认

无

## 使用说明

该命令以列表的形式显示物理端口和 AGG 接口的统计信息。

## 举例说明

下面的例子显示了物理口 eth-0-1 的统计信息：

```
Switch# show interface eth-0-1 summary
```

```
RXBS: rx rate (bits/sec)          RXPS: rx rate (pkts/sec)
TXBS: tx rate (bits/sec)          TXPS: tx rate (pkts/sec)
Interface  Link    RXBS    RXPS    TXBS    TXPS
-----
eth-0-1    DOWN   2        0        0        0
```

## 相关命令

show interface

### 2.1.21 show ip interface

使用该命令显示 3 层接口的信息。

## 命令语法

```
show ip interface (IFNAME |)
```

```
show ip interface brief
```

IFNAME	接口名称
--------	------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面的例子显示了接口 vlan10 的信息：

```
Switch# show interface vlan10
```

```
Interface vlan10
  Interface current state: DOWN
  Hardware is VLAN, address is 8633.d260.6500 (bia 8633.d260.6500)
  Bandwidth 1000000 kbits
  Index 4098 , Metric 1 , Encapsulation ARPA
  The maximum transmit unit (MTU) is 1500 bytes
  VRF binding: not bound
  Label switching is disabled
  No virtual circuit configured
  VRRP master of : VRRP is not configured on this interface
  ARP timeout 01:00:00, ARP retry interval 1s
```

## 相关命令

无

## 2.1.22 switchport

使用该命令使端口在 2 层口和 3 层路由口之间切换。

## 命令语法

```
switchport
no switchport
```

## 命令模式

端口配置模式

## 默认

2 层口

## 使用说明

端口默认是一个 2 层口。当您使用该命令切换端口模式的时候，所有端口上原来的配置将会消失并且不能恢复。

## 举例说明

- 下面的例子显示了如何将端口设为 2 层口：

```
Switch(config)# interface eth-0-1
Switch(config-if)# switchport
```
- 下面的例子显示了如何将端口设为 3 层路由口：

```
Switch(config-if)# no switchport
```

## 相关命令

无

## 2.1.23 switchport access vlan

设置 access 端口的默认 VLAN。使用该命令的 no 形式恢复端口默认 VLAN 为 1。

### 命令语法

```
switchport access vlan vid
```

```
no switchport access vlan
```

vid	VLAN 标志符
-----	----------

### 命令模式

端口配置模式

### 默认

1

### 使用说明

使用该命令前，端口必须已经设置为 access 类型。端口的默认 VLAN 为 1。

### 举例说明

- 下面的例子将端口默认 VLAN 改为 10:

```
Switch(config)# interface eth-0-1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
```

- 下面的例子将端口默认 VLAN 恢复为 1:

```
Switch(config-if)# no switchport access vlan
```

### 相关命令

```
switchport trunk native
```

## 2.1.24 switchport mode access

使用该命令设置端口工作在 access 模式。

### 命令语法

```
switchport mode access
```

## 命令模式

端口配置模式

## 默认

Access 口

## 使用说明

当端口模式变化的时候，端口上所有的动态 FDB 都会被清掉。

## 举例说明

下面的例子显示了如何将端口配置为 access 模式：

```
Switch(config)# interface eth-0-1
Switch(config-if)# switchport mode access
```

## 相关命令

switchport mode trunk

## 2.1.25 switchport mode trunk

使用该命令设置端口工作在 trunk 模式。

## 命令语法

switchport mode trunk

## 命令模式

端口配置模式

## 默认

Access 模式

## 使用说明

当端口模式变化的时候，端口上所有的动态 FDB 都会被清掉。

## 举例说明

下面的例子显示了如何使端口工作在 trunk 模式：

```
Switch(config)# interface eth-0-1
Switch(config-if)# switchport mode trunk
```

## 相关命令

switchport mode access

### 2.1.26 switchport mode hybrid

使用该命令设置端口工作在 hybrid 模式。

## 命令语法

switchport mode hybrid

## 命令模式

端口配置模式

## 默认

Access 模式

## 使用说明

当端口模式变化的时候，端口上所有的动态 FDB 都会被清掉。

## 举例说明

下面的例子显示了如何将端口配置为 hybrid 模式：

```
Switch(config)# interface eth-0-1
```

```
Switch(config-if)# switchport mode hybrid
```

## 相关命令

switchport mode access

switchport mode trunk

### 2.1.27 switchport mode dot1q-tunnel

使用该命令设置端口为 QINQ。

## 命令语法

switchport mode dot1q-tunnel

## 命令模式

端口配置模式



## 默认

Access 端口

## 使用说明

当端口模式变化的时候，端口上所有的动态 FDB 都会被清掉。

## 举例说明

下面的例子显示了如何使端口工作在 QINQ 模式：

```
Switch(config)# interface eth-0-1
Switch(config-if)# switchport mode dot1q-tunnel
```

## 相关命令

switchport mode trunk

### 2.1.28 switchport trunk allowed

使用该命令允许指定 VLAN 的报文通过 trunk 端口。

## 命令语法

switchport trunk allowed vlan (add *vid* | remove *vid* | all | none)

add vid	允许指定 VLAN 的报文通过该端口
remove vid	禁止指定 VLAN 的报文通过该端口
all	允许所有的报文通过该端口
none	禁止所有的报文通过该端口

## 命令模式

端口配置模式

## 默认

1

## 使用说明

无

## 举例说明

- 下面的例子设置只允许指定 VLAN 的报文通过该端口：

```
Switch(config)# interface eth-0-1
Switch(config-if)# switchport trunk allowed vlan add 10
```

- 下面的例子设置允许所有的报文通过该端口：

```
Switch(config-if)# switchport trunk allowed vlan all
```

- 下面的例子显示禁止所有的报文通过该端口：

```
Switch(config-if)# switchport trunk allowed vlan none
```

## 相关命令

`switchport access allowed vlan (add | remove) vid`

### 2.1.29 switchport trunk native vlan

使用该命令设置 trunk 端口的默认 VLAN。

## 命令语法

`switchport trunk native vlan vid`

vid	VLAN 标志符，范围是 2-4094
-----	---------------------

## 命令模式

端口配置模式

## 默认

1

## 使用说明

使用该命令前，端口必须已经被配置为 trunk 口。

## 举例说明

下面的例子设置 trunk 口 eth-0-1 的默认 VLAN 为 10：

```
Switch(config)# interface eth-0-1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk native vlan 10
```

## 相关命令

`switchport access vlan vid`

### 2.1.30 switchport hybrid allowed

使用该命令允许指定 VLAN 的报文通过 hybrid 端口。

## 命令语法

`switchport hybrid allowed vlan (add vid | remove vid) (untagged | tagged)`

`switchport hybrid allowed vlan (all | none)`

add vid	允许指定 VLAN 的报文通过该端口
remove vid	禁止指定 VLAN 的报文通过该端口
untagged	指定 VLAN 的报文输出不带 TAG
tagged	指定 VLAN 的报文输出带上 TAG
all	允许所有的报文通过该端口
none	禁止所有的报文通过该端口

## 命令模式

端口配置模式

## 默认

1

## 使用说明

无

## 举例说明

- 下面的例子设置只允许指定 VLAN 的报文通过该端口：

```
Switch(config)# interface eth-0-1
Switch(config-if)# switchport hybrid allowed vlan add 10 tagged
```

- 下面的例子设置允许所有的报文通过该端口：

```
Switch(config-if)# switchport hybrid allowed vlan all
```

- 下面的例子显示禁止所有的报文通过该端口：

```
Switch(config-if)# switchport hybrid allowed vlan none
```

## 相关命令

`switchport trunk allowed vlan (add | remove) vid`

### 2.1.31 switchport hybrid native vlan

使用该命令设置 hybrid 端口的默认 VLAN。

## 命令语法

`switchport hybrid native vlan vid`

vid	VLAN 标志符，范围是 2-4094
-----	---------------------

## 命令模式

端口配置模式

## 默认

1

## 使用说明

使用该命令前，端口必须已经被配置为 hybrid 口。

## 举例说明

下面的例子设置 hybrid 口 eth-0-1 的默认 VLAN 为 10:

```
Switch(config)# interface eth-0-1
```

```
Switch(config-if)# switchport mode hybrid
```

```
Switch(config-if)# switchport hybrid native vlan 10
```

## 相关命令

`switchport trunk native vlan vid`

### 2.1.32 mtu

使用该命令改变接口的 MTU 值。

## 命令语法

**mtu** value

value	MTU 范围为 68~9000
-------	-----------------

## 命令模式

端口配置模式

## 默认

1500

## 使用说明

该命令只能配置在 3 层接口上。

## 举例说明

下面的例子设置 3 层接口 `vlan10` 的 MTU 值为 1600:

```
Switch(config)# interface vlan10
Switch(config-if)#mtu 1600
```

## 相关命令

无

## 2.1.33 subif

进入子接口，配置子接口封装的 VLAN ID

## 命令语法

**subif** *Sub\_Number* **encapsulation-dot1q** *VLAN\_ID*

<i>Sub_Number</i>	Sub number 范围为<1-256>
<i>VLAN_ID</i>	VLAN ID 范围为<1-4094>

## 命令模式

端口配置模式

## 默认

无

## 使用说明

该命令只能配置在 3 层 Ethernet、Agg 接口上。

## 举例说明

下面的例子在 3 层接口 Ethernet-0-1 创建编号为 10 的子接口，并封装 VLAN ID 为 10:

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# subif 10 encapsulation-dot1q 10
```

## 相关命令

无

## 2.1.34 carrier {up-delay|down-delay}

使用此命令配置接口上报 up/down 状态变化的延时时间。

使用 **no** 命令格式恢复默认值。

## 命令语法

**carrier** { **up-delay** | **down-delay** } *interval*

**no carrier** { **up-delay** | **down-delay** }

interval	延时时间，范围为 0~120，单位：ms
----------	----------------------

## 命令模式

接口配置模式

## 默认

0

## 使用说明

配置接口上报状态变化延时时间后，在延时时间内，接口物理状态之间的切换不会被系统感知；超过设定的延时时间后，如果接口物理状态还没有恢复，再向系统报告物理状态的变化。该命令只能在物理接口上配置。

## 举例说明

配置上报 UP 事件延迟时间为 10 秒:

```
Switch(config)# interface eth-0-1
Switch(config-if)# carrier up-delay 10
```

## 2.2 接口 Errdisable 命令

### 2.2.1 errdisable detect

使用此命令使能对端口的链路错误状态检测功能。使用 `no` 命令格式恢复默认值。

#### 命令语法

```
errdisable detect reason (link-flap | fdb-flap | udld)
```

```
no errdisable detect reason (link-flap | fdb-flap | udld)
```

link-flap	启用链路震荡检测功能
fdb-flap	启用 fdb 针对检查功能
udld	启用链路的单向链路检测功能

#### 命令模式

全局配置模式

#### 默认

上述三种检测功能都开启

#### 使用说明

无

#### 举例说明

- 下面的例子显示如何启用链路震荡检测功能：

```
Switch(config)# errdisable detect reason link-flap
```

- 下面的例子显示如何禁用链路震荡检测功能：

```
Switch(config)# no errdisable detect reason link-flap
```

#### 相关命令

```
show errdisable detect
```

### 2.2.2 errdisable recovery interval

使用此命令设置链路从错误状态恢复的时间。

使用关键词 `no` 恢复时间段为默认值。

## 命令语法

errdisable recovery interval *RANGE*

no errdisable recovery interval

RANGE	从错误状态恢复的时间间隔，以秒为单位，间隔范围 30~86400
-------	----------------------------------

## 命令模式

全局配置模式

## 默认

300 秒

## 使用说明

默认时间间隔为 300 秒。

当边缘端口启用 BPDU 保护功能后，如果此端口收到 BPDU 报文，则此端口会进入错误关闭状态。如果没有开启错误关闭自动恢复功能，则需要管理员打开被错误关闭的端口；如果开启了错误关闭自动恢复功能，则等待错误关闭恢复时间后，自动打开此端口。此命令用于设置错误关闭恢复时间。

## 举例说明

设置错误状态恢复的时间间隔为 30 秒：

```
Switch(config)# errdisable recovery interval 30
```

恢复时间间隔为默认值：

```
Switch(config)# no errdisable recovery interval
```

## 相关命令

errdisable recovery reason

show errdisable recovery

### 2.2.3 errdisable fdb-loop

使用此命令设置 FDB 检测环路值。

使用关键词 no 恢复默认值。

## 命令语法

errdisable fdb-loop *MAXSIZE RATE*



no errdisable fdb-loop

MAXSIZE	漏桶中令牌最大数目，建议配置为 FDB 最大条目数，防止因正常的 FDB 端口更新导致的误 errdisable
RATE	漏桶中每秒令牌增加数目，建议配置为默认值 200

## 命令模式

全局配置模式

## 默认

MAXSIZE 默认值为 60000，RATE 默认值为 200

## 使用说明

无

## 举例说明

设置配置的漏桶中令牌最大数目为 60000 增加速率为 100:

```
Switch(config)# errdisable fdb-loop 1000 100
```

## 相关命令

errdisable recovery reason

show errdisable recovery

## 2.2.4 errdisable recovery reason

使用该命令启用指定原因的错误恢复功能。

使用关键词 no 禁用此项功能。

## 命令语法

```
errdisable recovery reason (all|bpduguard | bpduloop| port-security|link-flap| link-monitor-failure | oam-remote-failure|udld|fdb-loop| loopback-detection)
```

```
no errdisable recovery reason (all|bpduguard | bpduloop| port-security|link-flap| link-monitor-failure | oam-remote-failure|udld|fdb-loop| loopback-detection)
```

all	使能所有原因的错误恢复功能
bpduguard	使能从 BPDU 防护错误状态恢复功能
bpduloop	使能 BPDU 环回错误状态恢复功能
port-security	使能端口绑定错误恢复功能
link-flap	使能链路震荡错误恢复功能
link-monitor-failure	使能链路监测错误恢复功能
oam-remote-failure	使能从 OAM 错误恢复功能
udld	使能 UDLD 错误恢复功能
fdb-loop	使能 FDB 环路恢复功能
loopback-detection	使能 loopback detection 错误状态恢复功能

## 命令模式

全局配置模式

## 默认

关闭

## 使用说明

修改链路错误状态恢复时间不会影响那些已经进入错误状态的端口。

## 举例说明

- 下面的例子显示了如何使能链路震荡错误恢复功能：  
Switch(config)# errdisable recovery reason link-flap
- 下面的例子显示如何禁用链路震荡错误恢复功能：  
Switch(config)# no errdisable recovery reason link-flap

## 相关命令

```
errdisable recovery interval
show errdisable recovery
```

### 2.2.5 errdisable flap

使用该命令设置链路震荡的参数。使用该命令的 no 形式恢复默认值。

## 命令语法

```
errdisable flap reason link-flap count seconds
no errdisable flap reason link-flap count seconds
```

link-flap	链路震荡检测
count	将端口置为 <code>errdisable</code> 前最大可以震荡的次数，范围 1~100
seconds	将端口置为 <code>errdisable</code> 前每秒钟可以震荡的次数，范围 1~120

## 命令模式

全局配置模式

## 默认

最大震荡次数：10  
每秒可以震荡的次数：10

## 使用说明

如果链路震荡错误检测功能被开启，那么端口可能会进入 `errdisable` 状态，否则就算链路震荡次数达到了指定值，系统只会记录 `log`。

## 举例说明

- 下面的例子显示如何设置链路震荡参数：  
Switch(config)# `errdisable flap reason link-flap 20 60`
- 下面的例子显示如何恢复链路震荡参数为默认值：  
Switch(config)# `no errdisable flap reason link-flap`

## 相关命令

```
show errdisable flap
```

### 2.2.6 no errdisable

使用该命令指定某一个特定的端口在发生 `mac flap` 的时候不被关闭

## 命令语法

```
no errdisable
```

## 命令模式

接口模式

## 默认

开启

## 使用说明

在指定的端口下执行该命令，发生 mac flap 的时候该端口不会被关闭

## 举例说明

- 在端口下执行该命令，使得该端口在发生 mac flap 的时候不被关闭：  
`switch(config-if)#no errdisable`
- 在端口下执行该命令，使得该端口在发生 mac flap 的时候能够被关闭：  
`switch(config-if)#errdisable`

## 2.2.7 show errdisable detect

该命令用于显示错误检测是否开启。

## 命令语法

```
show errdisable detect
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

```
DUT1# show errdisable detect
```

ErrDisable Reason	Detection status
-----	-----
bpduguard	Enabled

bpduloop	Enabled
link-monitor-failure	Enabled
oam-remote-failure	Enabled
port-security	Enabled
link-flap	Enabled
monitor-link	Enabled
udld	Enabled
fdb-loop	Enabled
loopback-detection	Enabled
reload-delay	Enabled

## 相关命令

errdisable detect

## 2.2.8 show errdisable recovery

该命令用于显示错误状态恢复功能是否开启。

## 命令语法

```
show errdisable recovery
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch# show errdisable recovery
```

```
ErrDisable Reason      Timer Status
-----
bpduguard              Disabled
bpduloop               Disabled
link-monitor-failure   Disabled
oam-remote-failure     Disabled
port-security          Disabled
link-flap              Disabled
udld                   Disabled
fdb-loop               Disabled
loopback-detection     Disabled
Timer interval: 300 seconds
```

## 相关命令

errdisable recovery interval

errdisable recovery reason

## 2.2.9 show errdisable flap

该命令用于显示链路震荡错误检测的参数。

## 命令语法

```
show errdisable flap
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch# show errdisable flap
ErrDisable Reason      Flaps      Time (sec)
-----
link-flap              10         10
```

## 相关命令

errdisable flap

## 2.3 MAC Address Table 命令

### 2.3.1 mac-address-table ageing-time

在 MAC 地址表中的条目使用或更新后，可以使用全局配置命令 `mac-address-table ageing-time` 设置 MAC 表中动态条目的老化时间，使用 `no` 命令将老化时间还原到默认值。老化时间适用于所有 VLAN 中的 MAC 地址条目。

## 命令语法

```
mac-address-table ageing-time ageing-time
```

```
no mac-address-table ageing-time
```

ageing-time	MAC 表老化时间，范围：0，10-1000000 秒，0 表示 MAC 表不老化
-------------	---

## 命令模式

全局配置模式

## 默认

300 秒

## 使用说明

如果没有连续的收到报文，用户可以增加老化时间的值使得设备能够保留更长的时间的动态条目。增加老化时间可以减少主机重复发送报文而引起广播风暴的可能性。

## 举例说明

以下例子说明了对所有的 VLAN 将老化时间设置成 200 秒。

```
Switch(config)# mac-address-table ageing-time 200
```

## 相关命令

```
show mac address-table ageing-time
```

## 2.3.2 mac-address-table forward

使用全局配置命令 `mac-address-table forward` 在 MAC 表中增加静态条目，使用 `no` 命令从 MAC 表中移除指定的静态条目。

## 命令语法

```
mac-address-table mac-addr forward interface-id[eps]|remote-vtep|smart-link vlan vlan-id
```

```
no mac-address-table mac-addr forward interface-id[eps]|remote-vtep|smart-link vlan vlan-id
```

mac-addr	目的 MAC 位址（单播或多播），特定 VLAN 中带有目的 MAC 位址的报文将通过特定的接口转发出去
interface-id	报文转发出去的界面。有效的接口包括物理接口和聚合接口
vlan-id	特定的 VLAN。带有特定 MAC 地址的报文所属的 VLAN。范围：1-4094
eps	EPS 保护组，取值范围<1-2048>
remote-vtep	远端 vtep，取值范围<1-65535>

smart-link	Smart-link 组，取值范围<1-16>
------------	-------------------------

## 命令模式

全局配置模式

## 默认

无

## 使用说明

通过该命令配置的静态条目不受老化时间限制。

## 举例说明

以下例子说明了添加静态条目 c2f3.220a.12f4 到 MAC 地址表中。当在 VLAN4 中收到一条这样的 MAC 目的地址的报文后，该报文将会从指定的界面转发出去：

```
Switch(config)# mac-address-table c2f3.220a.12f4 forward eth-0-1 vlan 4
```

## 相关命令

show mac address-table

### 2.3.3 mac-address-table discard

使用全局配置命令 `mac-address-table discard` 允许在交换机上对单播 MAC 地址过滤和对特定的源 MAC 位址或目的 MAC 位址停止转发。使用 `no` 命令还原到默认配置。

## 命令语法

`mac-address-table mac-addr discard`

`no mac-address-table mac-addr discard`

mac-addr	加入到地址过滤表中的源 MAC 位址或目的 MAC 位址 (单播地址)
----------	-------------------------------------

## 命令模式

全局配置模式

## 默认

无



## 使用说明

当使用该命令时需要遵循以下原则：

该命令不支持多播 MAC 地址、广播 MAC 地址和路由 MAC 地址。转发到 CPU 上的报文同样不支持。

## 举例说明

以下例子说明了在设备上启用单播地址过滤功能，设备将对源 MAC 位址或目的 MAC 位址为 c2f3.220a.12f4 的报文丢弃：

```
Switch(config)# mac-address-table c2f3.220a.12f4 discard
```

## 相关命令

mac-address-table forward

### 2.3.4 clear mac address-table

使用命令 `clear mac address-table` 可以删除所有的动态(或静态或组播)条目或根据接口/MAC 位址/VLAN 删除部分动态(或静态或组播)条目。

## 命令语法

```
clear mac address-table (static | dynamic| multicast) (address mac-addr | interface interface-id | vlan vlan-id)
```

<b>dynamic</b>	删除动态条目
<b>static</b>	删除静态条目
<b>multicast</b>	删除多播条目
<b>address mac-addr</b>	删除特定 MAC 地址的条目
<b>interface interface-id</b>	删除所有特定物理接口或聚合接口上的所有条目
<b>vlan vlan-id</b>	删除特定 VLAN 的所有条目，范围为 1- 4094

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

以下例子说明了删除特定 MAC 地址的所有动态条目：

```
Switch# clear mac address-table dynamic address 0008.0070.0007
```

## 相关命令

show mac address-table

### 2.3.5 show mac address-table ageing-time

使用特权命令 show mac address-table ageing-time 显示所有 VLAN 中所有条目的老化时间。

## 命令语法

```
show mac address-table ageing-time
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

以下例子说明了使用 show mac address-table ageing-time 命令查看条目的老化时间：

```
Switch# show mac address-table ageing-time
```

```
MAC address table ageing time is 300 seconds
```

## 相关命令

mac-address-table ageing-time

### 2.3.6 show mac address-table

使用特权命令 show mac address-table 显示特定 MAC 地址的静态和动态条目或特定接口特定 VLAN 的静态条目和动态条目。

## 命令语法

show mac address-table (dynamic | static | multicast | ) (address *mac-addr* | interface *interface-id* | vlan *vlan-id* | )

dynamic	显示动态条目
static	显示静态条目
multicast	显示多播条目
<b>address</b> <i>mac-addr</i>	显示特定 MAC 地址的条目
<b>interface</b> <i>interface-id</i>	显示特定物理接口或聚合接口上的所有条目
<b>vlan</b> <i>vlan-id</i>	显示特定 VLAN 中的所有条目. 范围为 1 - 4094

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

以下例子说明了使用 show mac address-table 命令查看条目输出:

```
Switch # show mac address-table
          Mac Address Table
-----
(*) - Security Entry
Vlan    Mac Address      Type           Ports
----    -
1       0000.0000.0001   static         eth-0-2
1       0000.0001.0003   static (*)     eth-0-1
1       0000.0001.0002   static (*)     eth-0-1
2       26fc.72e5.0100   dynamic (*)    eth-0-9
1       0100.0000.0001   static         eth-0-2
                                     eth-0-1
```

## 相关命令

mac-address-table

## 2.3.7 show mac address-table hardware

使用特权命令 `show mac address-table` 显示硬件中特定 MAC 地址的静态和动态条目或特定接口特定 VLAN 的静态条目和动态条目。

### 命令语法

`show mac address-table hardware (dynamic | static | ) (address mac-addr | interface interface-id | vlan vlan-id | )`

<b>dynamic</b>	显示动态条目
<b>static</b>	显示静态条目
<b>address mac-addr</b>	显示特定 MAC 地址的条目
<b>interface interface-id</b>	显示特定物理接口或聚合接口上的所有条目
<b>vlan vlan-id</b>	显示特定 VLAN 中的所有条目. 范围为 1 - 4094

### 命令模式

特权模式

### 默认

无

### 使用说明

无

### 举例说明

以下例子说明了使用 `show mac address-table hardware` 命令查看条目输出:

```
Switch # show mac address-table hardware
          Mac Address Table
-----
(*) - Security Entry
Vlan    Mac Address      Type      Ports
----    -
1       0000.0000.0001   static    eth-0-2
1       0000.0001.0003   static(*)  eth-0-1
1       0000.0001.0002   static(*)  eth-0-1
2       26fc.72e5.0100   dynamic(*) eth-0-9
1       0100.0000.0001   static    eth-0-2
                               eth-0-1
```

## 相关命令

mac-address-table

### 2.3.8 show mac address-table count

使用特权命令 `show mac address-table count` 显示所有 MAC 的条目总数。

## 命令语法

```
show mac address-table count
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

以下例子说明了使用 `show mac address-table count` 命令查看条目总数：

```
Switch# show mac address-table count
Dynamic Address Count      :    1  (Security: 0)
Static Address Count       :    1  (Security: 0)
Total Mac Addresses       :    2  (Security: 0)
```

## 相关命令

show mac address-table

### 2.3.9 show mac address-table add-fdb-fail

使用特权命令 `show mac address-table add-fdb-fail` 显示因为 Hash 冲突而无法加入的静态 FDB。

## 命令语法

```
show mac address-table add-fdb-fail
```

## 命令模式

特权模式

## 默认

无

## 使用说明

有大量 FDB 的情况下添加静态 FDB 有极小的概率出现 Hash 冲突而无法配置到硬件的情况，使用这条命令可以查看因为冲突而添加失败的 FDB。

## 举例说明

以下例子说明了使用 `show mac address-table add-fdb-fail` 命令查看添加失败的条目：

```
Switch# show mac address-table add-fdb-fail
```

## 相关命令

`show mac address-table`

## 2.3.10 show mac-filter address-table

使用特权命令 `show mac-filter address-table` 显示所有 mac-filter 的条目总数。

## 命令语法

`show mac-filter address-table`

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

以下例子说明了使用命令 `show mac-filter address-table` 查看所有 mac-filter 的条目总数：

```
Switch# show mac-filter address-table
```

```
MAC Filter Address Table
-----
Current count      : 1
Max count          : 128
Left count         : 127
Filter address list :
-----
```

```
0000.000a.000a
```

## 相关命令

```
show mac address-table
```

### 2.3.11 show resource mac-filter

使用该命令显示系统中 mac-filter 占用的硬件资源统计信息。

## 命令语法

```
show resource mac-filter
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面的例子显示了使用命令 show resource mac-filter 的输出结果：

```
Switch# show resource mac-filter
```

```
MAC-FILTER
Resource                               Used          Capability
=====
Blackhole MAC Addresses                 0              128
```

## 相关命令

```
show resource static-fdb
```

### 2.3.12 show resource static-fdb

使用该命令显示系统中静态 FDB 占用的硬件资源统计信息。

## 命令语法

```
show resource static-fdb
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面的例子显示了使用命令 `show resource static-fdb` 的输出结果：

```
Switch# show resource static-fdb
```

```
STATIC-FDB
Resource                               Used           Capability
=====
Static FDB                             0              1024
```

## 相关命令

```
show resource mac-filter
```

## 2.4 VLAN 命令

### 2.4.1 vlan database

使用该命令进入 VLAN 配置模式。

## 命令语法

```
vlan database
```

## 命令模式

全局配置模式

## 默认

无

## 用法

当要创建或删除一个 VLAN 时，必须首先使用该命令进入 VLAN 配置模式。使用 `exit` 命令退出 VLAN 配置模式。

## 举例

- 以下例子说明了进入 VLAN 配置模式：

```
Switch(config)# vlan database
```



```
Switch(config-vlan)#
```

- 以下例子说明了退出 VLAN 配置模式：

```
Switch(config-vlan)# exit
Switch(config)#
```

## 相关命令

exit

## 2.4.2 vlan

使用该命令配置 VLAN 数据结构中的 VLAN 特性。使用 no 命令删除一个 VLAN。

## 命令语法

```
vlan vlan (name name) (state (enable |disable))
```

```
no vlan vlan
```

vlan	<1-4094> vlan 号
name name	特定 VLAN 的名称，不超过 31 个字符
enable	设定 VLAN 有效可操作，默认值为 enable
disable	设定 VLAN 不可操作

## 命令模式

VLAN 配置模式

## 默认

VLAN 1 是默认的 VLAN，不可删除。所有接口默认都添加到 VLAN1 中。

## 用法

无

## 举例

- 以下例子说明了创建 VLAN 11 并且命名为“vlan11”：

```
Switch(config-vlan)# vlan 11 name vlan11 state enable
```

- 以下例子说明了移除 VLAN 11：

```
Switch(config-vlan)# no vlan 11
```

## 相关命令

**vlan** VLAN\_LIST  
 show vlan *vlan*  
 show vlan all

### 2.4.3 vlan port

使用该命令把 port 加入 VLAN。使用 no 命令将 port 从 VLAN 中取出。

## 命令语法

**vlan** *vlan* **port slot** *slotid* **port** *portid*  
**no** **vlan** *vlan* **port slot** *slotid* **port** *portid*

<b>vlan</b>	<1-4094> vlan 号
<b>slot</b> <i>slotid</i>	端口所在的槽位号
<b>port</b> <i>portid</i>	端口所在的端口号

## 命令模式

VLAN 配置模式

## 默认

无

## 用法

无

## 举例

- 以下例子说明了把 VLAN 11 加入 eth-0-4:  
 Switch(config-vlan)# vlan 11 port slot 0 port 4

## 相关命令

**vlan** VLAN\_LIST

### 2.4.4 vlan VLAN\_LIST

使用该命令添加一个范围内的 VLAN 序列到 VLAN 数据结构中。

## 命令语法

```
vlan VLAN_LIST
no vlan VLAN_LIST
```

VLAN_LIST	VLAN 序列以 ‘-’ 和 ‘,’ 符号相连接，如 “1-10,15,20,30-40”
-----------	---

## 命令模式

VLAN 配置模式

## 默认

VLAN 1 是默认的 VLAN，不可删除。所有接口默认都添加到 VLAN1 中。

## 用法

VLAN 序列以 ‘-’ 和 ‘,’ 符号相连接，VLAN 的值的范围在 1-4094 之间，并且 VLAN 序列的值需要符合升序的原则。

## 举例

- 以下例子说明了添加 VLAN 序列 “100,200,300-400”：  
Switch(config-vlan)# vlan 100,200,300-400
- 以下例子说明了移除 VLAN 序列 “100,200,300-400”：  
Switch(config-vlan)# no vlan 100,200,300-400

## 相关命令

```
vlan <1-4094>
show vlan vlan
show vlan all
```

### 2.4.5 show vlan

使用该命令显示特定 VLAN 的信息。

## 命令语法

```
show vlan vlan
```

vlan	<1-4094> vlan id
------	------------------

## 命令模式

特权模式

## 默认

无

## 用法

该命令用来显示特定 VLAN 的相关属性信息，包括：名称、状态、stp id、DSCP 和接口信息。

## 举例

以下例子说明了显示 VLAN 11 的相关信息：

```
Switch# show vlan 11
```

## 相关命令

```
show vlan all
```

## 2.4.6 show vlan all

使用该命令显示所有 VLAN 的信息。

## 命令语法

```
show vlan all
```

## 命令模式

特权模式

## 默认

无

## 用法

该命令用来显示所有 VLAN 的相关属性信息，包括：名称、状态、stp id、DSCP 和接口信息。

## 举例

以下例子说明了显示所有 VLAN 的信息：

```
Switch# show vlan all
```

## 相关命令

`show vlan vlan`

### 2.4.7 show vlan brief

使用该命令显示所有设备 VLAN 的简要信息。

## 命令语法

`show vlan brief`

## 命令模式

特权模式

## 默认

无

## 用法

该命令用来显示所有设备 VLAN 的简要信息，包括静态和动态信息。

## 举例

使用该命令显示所有设备 VLAN 的简要信息：

```
Switch# show vlan brief
```

## 相关命令

`show vlan vlan`

### 2.4.8 show interface switchport

使用该命令显示特定交换接口或所有交换接口的 vlan 配置信息。

## 命令语法

`show interface switchport {interface IFNAME}`

IFNAME	接口名称
--------	------

## 命令模式

特权模式

## 默认

无

## 用法

该命令用来显示一个或所有 VLAN 的二层配置信息。

## 举例

以下例子说明了显示特定交换接口或所有交换接口的 `vlan` 配置信息：

```
Switch# show interface switchport interface eth-0-1
```

## 相关命令

`switchport mode access`

`switchport mode trunk`

## 2.4.9 switchport hybrid allowed

使用该命令允许或禁止来自特定 VLAN 的报文通过 `hybrid` 接口。

## 命令语法

```
switchport hybrid allowed vlan (add | all | none | remove) vlan_id
```

add	允许来自特定 VLAN 的报文通过 hybrid 接口
all	允许来自所有 VLAN 的报文通过 hybrid 接口
none	允许来自不带 VLAN 的报文通过 hybrid 接口
remove	禁止来自特定 VLAN 的报文通过 hybrid 接口
vlan	VLAN 序列使用 ‘-’ 和 ‘,’ 符号连接，如：“1-10,15,20,30-40”

## 命令模式

接口配置模式

## 默认

无

## 用法

该命令用来允许或禁止来自特定 VLAN 的报文通过 hybrid 接口。

## 举例

- 以下例子说明了允许来自 VLAN 11 的报文通过 hybrid 接口：  
Switch(config-if)# switchport hybrid allowed vlan add 11
- 以下例子说明了禁止来自 VLAN 12 的报文通过 hybrid 接口：  
Switch(config-if)# switchport hybrid allowed vlan remove 12

## 相关命令

switchport trunk allowed

### 2.4.10 switchport hybrid native vlan

使用该命令设置能够发送和接收没有 tag 报文的本地 VLAN。使用 no 命令恢复本地 VLAN 到默认值。

## 命令语法

switchport hybrid native vlan *vlan*

no switchport hybrid native vlan

vlan	已存在的 VLAN ID，范围：2-4094
------	------------------------

## 命令模式

接口配置模式

## 默认

vlan 1

## 用法

该命令用来设置能够发送和接收没有 tag 报文的本地 VLAN。

## 举例

- 以下例子说明了在接口上设置 VLAN 10 为本地 VLAN：  
Switch(config-if)# switchport hybrid native vlan 10
- 以下例子说明了在接口上恢复本地 VLAN 到默认值：  
Switch(config-if)# no switchport hybrid native vlan

## 相关命令

switchport trunk allowed

### 2.4.11 switchport access vlan

使用该命令添加一个 access 接口 到特定的 VLAN 中。可以使用 no 命令恢复 access 接口到默认的 VLAN1 中。

## 命令语法

switchport access vlan *vlan*

no switchport access vlan

vlan	范围为： 2-4094
------	-------------

## 命令模式

接口配置模式

## 默认

所有的接口默认添加到 vlan 1 中

## 用法

在使用该命令前需要使用 switchport mode access 命令将接口设置成 access 接口类型。

## 举例

- 以下命令说明了将接口添加到 vlan 11 中：  
Switch(config-if)# switchport access vlan 11
- 以下命令说明了将接口恢复到默认的 vlan 1 中：  
Switch(config-if)# no switchport access vlan

## 相关命令

switchport mode access

### 2.4.12 switchport mode hybrid

使用该命令设置接口成为 hybrid 类型。



## 命令语法

```
switchport mode hybrid
```

## 命令模式

接口配置模式

## 默认

无

## 用法

hybrid 模式用来连接到终端设备，如：PC。当接口模式更改时，该接口上学习到的动态 MAC 位址和配置的静态位址都将被清空。

## 举例

以下例子说明了设置接口成为 hybrid 类型：

```
Switch(config-if)# switchport mode hybrid
```

## 相关命令

```
switchport mode trunk
```

## 2.4.13 switchport mode access

使用该命令设置接口成为 access 类型。

## 命令语法

```
switchport mode access
```

## 命令模式

接口配置模式

## 默认

无

## 用法

access 模式用来连接到终端设备，如：PC。当接口模式更改时，该接口上学习到的动态 MAC 位址和配置的静态位址都将被清空。

## 举例

以下例子说明了设置接口成为 access 类型：

```
Switch(config-if)# switchport mode access
```

## 相关命令

```
switchport mode trunk
```

### 2.4.14 switchport mode trunk

使用该命令设置接口成为 trunk 类型。使用 `switchport mode access` 命令恢复接口到默认的模式。

## 命令语法

```
switchport mode trunk
```

## 命令模式

接口配置模式

## 默认

无

## 用法

trunk 模式可以用来连接其它交换设备，也可以连接主机设备。当接口模式更改时，该接口上学习到的动态 MAC 位址和配置的静态位址都将被清空。

## 举例

以下例子说明了设置接口成为 trunk 类型：

```
Switch(config-if)# switchport mode trunk
```

## 相关命令

```
switchport mode access
```

### 2.4.15 switchport trunk allowed

使用该命令允许来自特定 VLAN 的报文在 trunk 类型的接口上传送，使用 `no` 命令取消该命令设置。

## 命令语法

```
switchport trunk allowed vlan (add vlan | remove vlan| all | none)
```

```
no switchport trunk
```

vlan	VLAN 序列使用 ‘-’ 和 ‘,’ 符号连接, 如: “1-10,15,20,30-40”
add	允许来自特定 VLAN 的报文在 trunk 类型的界面上发送
remove vlan	禁止来自特定 VLAN 的报文在 trunk 类型的界面上发送
all	允许来自所有 VLAN 的报文在 trunk 类型的接口上发送
none	禁止来自所有 VLAN 的报文在 trunk 类型的接口上发送

## 命令模式

接口配置模式

## 默认

无

## 用法

该命令用来允许来自特定 VLAN 的报文在 trunk 类型的界面上发送。

## 举例

- 以下例子说明了允许来自 VLAN11,12 的报文在 trunk 类型的界面上发送:  
Switch(config-if)# switchport trunk allowed vlan add 11,12
- 以下例子说明了禁止来自 VLAN11,12 的报文在 trunk 类型的界面上发送:  
Switch(config-if)# switchport trunk allowed vlan remove 11,12
- 以下例子说明了允许来自所有 VLAN 的报文在 trunk 类型的接口上发送:  
Switch(config-if)# switchport trunk allowed vlan all
- 以下例子说明了禁止来自所有 VLAN 的报文在 trunk 类型的接口上发送:  
Switch(config-if)# switchport trunk allowed vlan none

## 相关命令

switchport access allowed

### 2.4.16 switchport trunk native

使用该命令设置能够发送和接收没有 tag 报文的本地 VLAN。使用 no 命令恢复本地 VLAN 到默认值。

## 命令语法

switchport trunk native vlan *vlan*

no switchport trunk native vlan

vlan	已存在的 VLAN ID，范围：2-4094
------	------------------------

## 命令模式

接口配置模式

## 默认

vlan 1

## 用法

该命令用来设置能够发送和接收没有 tag 报文的本地 VLAN。

## 举例

- 以下例子说明了在接口上设置 VLAN 10 为本地 VLAN：

```
Switch(config-if)# switchport trunk native vlan 10
```

- 以下例子说明了在接口上恢复本地 VLAN 到默认值：

```
Switch(config-if)# no switchport trunk native vlan
```

## 相关命令

switchport trunk allowed

### 2.4.17 vlan bridge disable

使用该命令可以关闭特定 vlan 上的桥功能，使该 vlan 丢弃所有通过的二层报文。

## 命令语法

vlan *vlan* bridge disable

no vlan *vlan* bridge disable

vlan	Vlan 标识，取值范围<1-4094>
------	----------------------

## 命令模式

VLAN 配置模式

## 默认

打开 vlan 上的桥功能

## 使用说明

无

## 举例说明

- 以下示例展示了如何关闭 VLAN 2 上的桥功能：

```
Switch(config-vlan)# vlan 2 bridge disable
```

- 以下示例展示了如何打开 VLAN 2 上的桥功能：

```
Switch(config-vlan)# no vlan 2 bridge disable
```

## 相关命令

无

## 2.4.18 vlan statistics enable

使用该命令可以使能基于 vlan 的报文统计。

## 命令语法

```
vlan vlan statistics enable
```

```
no vlan vlan statistics enable
```

vlan	Vlan 标识，取值范围<1-4094>
------	----------------------

## 命令模式

VLAN 配置模式

## 默认

关闭

## 使用说明

无

## 举例说明

- 以下示例展示了如何使能 VLAN 2 上的统计功能：

```
Switch(config-vlan)# vlan 2 statistics enable
```

## 相关命令

```
vlan statistics interval
```

```
clear vlan statistics
```

```
show vlan vlan statistics
```

## 2.4.19 vlan statistics interval

使用该命令可以配置 vlan 统计的采样间隔时间。

### 命令语法

```
vlan statistics interval VALUE
```

```
no vlan statistics interval
```

VALUE	采样间隔时间，取值范围<5-600>，单位：秒
-------	-------------------------

### 命令模式

VLAN 配置模式

### 默认

10 秒

### 使用说明

无

### 举例说明

- 以下示例展示了如何配置 vlan 统计间隔时间：  
Switch(config-vlan)# vlan statistics interval 20

### 相关命令

```
vlan statistics enable
```

```
clear vlan statistics
```

```
show vlan vlan statistics
```

## 2.4.20 clear vlan statistics

使用该命令可以清空统计信息。

### 命令语法

```
clear vlan vlan statistics
```

<i>vlan</i>	Vlan 标识，取值范围<1-4094>
-------------	----------------------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

- 以下示例展示了如何清空 `vlan2` 的统计信息：

```
Switch# clear vlan 2 statistics
```

## 相关命令

`vlan statistics enable`

`vlan statistics interval`

`show vlan vlan statistics`

## 2.4.21 show vlan statistics

使用该命令可以显示统计信息。

## 命令语法

```
show vlan vlan statistics
```

<i>vlan</i>	Vlan 标识，取值范围<1-4094>
-------------	----------------------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

- 以下示例展示了如何显示 `vlan2` 的统计信息：

```
Switch# show vlan 2 statistics
Switch# show vlan 2 statistics
VLAN: 2
-----
Item                               Packets
-----
Inbound:                           3654365
Outbound:                           3654365
-----
```

## 相关命令

```
vlan statistics enable
vlan statistics interval
clear vlan statistics
```

## 2.5 VOICE VLAN 命令

### 2.5.1 voice vlan

使用该命令指定某个 VLAN 做为 VOICE VLAN。

## 命令语法

```
voice vlan vlan_id
no voice vlan
```

<i>vlan_id</i>	vlan id, 范围为 2~4094
----------------	---------------------

## 命令模式

全局配置模式

## 默认

未启用

## 用法

该命令用于全局启用 VOICE VLAN。

## 举例

将 VLAN 指定为 VOICE VLAN:



```
Switch(config)# voice vlan 2
```

## 相关命令

无

### 2.5.2 voice vlan security enable

使用该命令启用 VOICE VLAN 的安全模式。

## 命令语法

```
voice vlan security enable  
no voice vlan security enable
```

## 命令模式

全局配置模式

## 默认

默认启用

## 用法

启用安全模式后，VOICE VLAN 中没有匹配 OUI 的所有报文都会被丢弃。

## 举例

启用 VOICE VLAN:

```
Switch(config)# voice vlan security enable
```

## 相关命令

```
show voice vlan state
```

### 2.5.3 voice vlan set cos to

使用该命令设置通过 VOICE VLAN 报文的 COS。

## 命令语法

```
voice vlan set cos to <0-7>  
no voice vlan set cos
```

## 命令模式

全局配置模式

## 默认

默认为 5

## 用法

该命令用于设置通过 VOICE VLAN 报文的 COS。

## 举例

将报文的 COS 修改为 7:

```
Switch(config)# voice vlan set cos to 7
```

## 相关命令

```
show voice vlan state
```

## 2.5.4 voice vlan mac-address

使用该命令为 VOICE VLAN 添加 OUI。

## 命令语法

```
voice vlan mac-address MAC MASK description LINE
```

```
no voice vlan mac-address MAC
```

MAC	要加到 mac 地址表的 mac 地址（单播或者组播）
MASK	源 mac 掩码
LINE	OUI 说明信息

## 命令模式

全局配置模式

## 默认

在系统中有五条默认 OUI:

```
0003-6b00-0000 Cisco phone
```

```
000f-e200-0000 H3C Aolynk phone
```

```
00d0-1e00-0000 Pingtel phone
```

```
00e0-7500-0000 Polycom phone
```

```
00e0-bb00-0000 3Com phone
```

## 用法

该命令为系统添加新的 OUI。只有匹配 OUI 的报文才会被认为是语音报文。

## 举例

如何为系统添加一条新的 OUI:

```
Switch(config)# voice vlan mac-address 0034.3400.0000 FFFF.FF00.0000 description test
```

## 相关命令

```
show voice vlan state
```

### 2.5.5 voice vlan enable

使用该命令在端口上启用 VOICE VLAN。

## 命令语法

```
voice vlan enable
```

```
no voice vlan enable
```

## 命令模式

端口模式

## 默认

默认不启用

## 用法

该命令用于在端口上启用 VOICE VLAN。

## 举例

在端口上启用 VOICE VLAN 功能:

```
Switch(config-if)# voice vlan enable
```

## 相关命令

```
show voice vlan state
```

### 2.5.6 show voice vlan state

使用该命令显示当前 VOICE VLAN 的配置。

## 命令语法

```
show voice vlan state
```

## 命令模式

特权模式

## 默认

无

## 用法

该命令用于显示当前 VOICE VLAN 的配置。

## 举例

显示当前系统的 VOICE VLAN 配置：

```
Switch# show voice vlan state
```

## 相关命令

```
voice vlan enable
```

## 2.6 VLAN Classification 命令

### 2.6.1 vlan classifier activate

使用该命令将 VLAN 分类规则组应用到一个端口，使用 `no` 命令删除。

## 命令语法

```
vlan classifier activate group-id based ( ip | mac | protocol )
```

```
no vlan classifier activate
```

group-id	VLAN 分类规则组标识，取值范围 0-31，仅有 31 可用于按协议类型分类
ip	基于 IP 类型分类
mac	基于 MAC 类型分类
protocol	基于协议类型分类

## 命令模式

端口配置模式

## 默认

无

## 使用说明

一个端口上只能应用一个 VLAN 分类规则组。

一个分类规则组可以应用于多个端口。

该命令应用 VLAN 分类规则组到一个端口，端口会根据分类规则将报文转发到不同的 VLAN。

为创建规则，参考命令 `vlan classifier rule`。

为创建分类规则，参考命令 `vlan classifier group`。

## 举例说明

- 以下示例展示如何应用 VLAN 分类规则组 1 到端口上：

```
Switch(config-if)# vlan classifier activate 1 based ip
```

- 以下示例展示如何移除 VLAN 分类规则组 1 在端口上的应用：

```
Switch(config-if)# no vlan classifier activate
```

## 相关命令

`vlan classifier group`

`vlan classifier rule`

### 2.6.2 vlan classifier group

使用该命令添加或删除分类规则到 VLAN 分类规则组。使用 `no` 命令删除分类规则组。

## 命令语法

`vlan classifier group group ( add | delete ) rule rule`

`no vlan classifier group group`

<code>group</code>	VLAN 分类规则组标识，取值范围 0-31，仅有 31 可用于按协议类型分类
<code>add</code>	添加规则到 VLAN 分类规则组
<code>delete</code>	删除规则到 VLAN 分类规则组

rule	规则的标识
------	-------

## 命令模式

全局配置模式

## 默认

无

## 使用说明

为创建规则，参考命令 `vlan classifier rule`。

为应用 VLAN 分类规则组到一个端口，参考命令 `vlan classifier activate`。

添加一条规则到一个 VLAN 分类规则组时，如果 VLAN 分类规则组已应用到一个端口，这条规则将立即起作用。

从一个 VLAN 分类规则组删除一条规则时，如果 VLAN 分类规则组已应用到一个端口，这条规则将立即不再起作用。

当最后一条规则从 VLAN 分类规则组删除时，VLAN 分类规则组将被删除。

## 举例说明

- 以下示例将展示如何将规则 1 添加到 VLAN 分类规则组：

```
Switch(config)# vlan classifier group 1 add rule 1
```

- 以下示例将展示如何将规则 1 从 VLAN 分类规则组中删除：

```
Switch(config)# vlan classifier group 1 delete rule 1
```

- 以下示例将展示如何删除 VLAN 分类规则组 1：

```
Switch(config)# no vlan classifier group 1
```

## 相关命令

`vlan classifier activate`

`vlan classifier rule`

### 2.6.3 vlan classifier rule

使用该命令创建 VLAN 分类规则，使用 `no` 命令可以移除分类规则。

## 命令语法

```
vlan classifier rule rule ( ip ipv4_address | mac mac_address | protocol (arp | ip | mpls | mpls-  
mcast | pppoe | rarp) ) vlan vlan-id
```

```
no vlan classifier rule rule
```

rule	分类规则的标识，取值范围 0-4095
ip ipv4_address	报文的源 ipv4 地址
mac mac_address	报文的源 mac 地址
protocol	指定报文的协议类型
arp	ARP 协议类型
ip	IP 协议类型
mpls	MPLS 协议类型
mpls-mcast	MPLS 组播协议类型
pppoe	PPPOE 协议类型
rarp	RARP 协议类型
vlan-id	VLAN 标识，范围 1-4094

## 命令模式

全局配置模式

## 默认

无

## 使用说明

当绑定到端口上后，分类规则才会起作用。

当报文匹配到分类规则后，分类规则会将报文在新分配的 vlan 中转发，并将新的 vlan id 添加到报文中。

添加分类规则到 VLAN 分类规则组，参见命令 `vlan classifier group`。

应用分类规则组到一个端口，参见命令 `vlan classifier activate`。

## 举例说明

- 以下示例将展示如何创建分类规则 1，将 ipv4 报文转发到 vlan11 中：

```
Switch(config)# vlan classifier rule 1 protocol ip vlan 11
```

- 以下示例展示如何删除分类规则 1：

```
Switch(config)# no vlan classifier rule 1
```

## 相关命令

vlan classifier group  
vlan classifier activate

### 2.6.4 show vlan classifier group

使用该命令显示 VLAN 分类规则组的信息。

## 命令语法

```
show vlan classifier group group
```

group	VLAN 分类规则组标识, 取值范围 0-31
-------	-------------------------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

以下示例展示如何显示分类规则组 1 的相关信息:

```
Switch# show vlan classifier group 1
```

## 相关命令

show vlan classifier interface  
show vlan classifier rule

### 2.6.5 show vlan classifier interface

使用该命令显示 VLAN 分类规则组应用在哪些端口上及相关信息。

## 命令语法

```
show vlan classifier interface group group
```



group	VLAN 分类规则组标识, 取值范围 0-31
-------	-------------------------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

以下示例展示分类规则组 1 应用在哪些端口上:

```
Switch# show vlan classifier interface group 1
```

## 相关命令

show vlan classifier group

show vlan classifier rule

## 2.6.6 show vlan classifier rule

使用该命令显示分类规则的信息。

## 命令语法

```
show vlan classifier rule ( rule )
```

rule	分类规则的标识, 取值范围 0~4095
------	----------------------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

- 以下示例展示如何显示所有分类规则的相关信息：

```
Switch# show vlan classifier rule
```

- 以下示例展示如何显示分类规则 1 的相关信息：

```
Switch# show vlan classifier rule 1
```

## 相关命令

```
show vlan classifier group
```

```
show vlan classifier interface
```

## 2.6.7 show resource vlan-classification

使用该命令显示系统中 VLAN 分类规则占用的硬件资源统计信息。

## 命令语法

```
show resource vlan-classification
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面的例子显示了使用命令 `show resource vlan-classification` 的输出结果：

```
Switch# show resource vlan-classification
VLAN-CLASS
Resource                               Used          Capability
=====
MAC Based VLAN Classification           0             512
IPv4 Based VLAN Classification          0             512
```

## 相关命令

无

## 2.7 VLAN Mapping 命令

### 2.7.1 ethernet evc

使用该命令添加或删除 EVC 表。

#### 命令语法

```
ethernet evc WORD
```

```
no ethernet evc WORD
```

WORD	EVC 名称
------	--------

#### 命令模式

全局配置模式

#### 默认

无

#### 使用说明

无

#### 举例说明

以下示例展示如何创建 EVC 表 *evc\_table*：

```
Switch(config)# ethernet evc evc_table  
Switch(config-evc)# dot1q mapped-vlan 10
```

#### 相关命令

```
show ethernet evc NAME
```

### 2.7.2 dot1q mapped-vlan

使用该命令添加 EVC 条目到 EVC 表。

#### 命令语法

```
dot1q mapped-vlan VLAN_ID
```

```
no dot1q mapped-vlan
```

VLAN_ID	VLAN 标识, 范围<1 - 4094>
IFNMAE	指定转发接口

## 命令模式

EVC 配置模式

## 默认

无

## 使用说明

无

## 举例说明

添加 EVC 对应 VLAN 为 100:

```
Switch(config)# ethernet evc evc_table
Switch(config-etc)# dot1q mapped-vlan 100
```

## 相关命令

show ethernet evc *NAME*

## 2.7.3 dot1q mapped-double-vlan

使用该命令添加带有两层 VLAN 的 EVC 条目到 EVC 表。

## 命令语法

dot1q mapped-double-vlan *inner-vlan outer-vlan*

no dot1q mapped-double-vlan

inner-vlan	映像的内层 VLAN ID, 范围 1-4094
outer-vlan	映像的外层 VLAN ID, 范围 1-4094

## 命令模式

EVC 配置模式

## 默认

无

## 使用说明

该命令仅用于 **untagged** 的报文

## 举例说明

添加映射的 EVC 条目，内层 vlan 为 100，外层 vlan 为 10:

```
Switch(config)# ethernet evc evc_table  
Switch(config-enc)# dot1q mapped-double-vlan 100 10
```

## 相关命令

show ethernet evc *NAME*

## 2.7.4 vlan mapping table

使用该命令添加或删除 VLAN 映射表。

## 命令语法

vlan mapping table *WORD*

no vlan mapping table *WORD*

WORD	VLAN 映射表的名称
------	-------------

## 命令模式

全局配置模式

## 默认

无

## 使用说明

无

## 举例说明

创建 VLAN 映射表 VMT。

```
Switch(config)# vlan mapping table VMT  
Switch(config-vlan-mapping)#
```

## 相关命令

show vlan mapping table *WORD*

### 2.7.5 raw vlan group

使用该命令创建一个 raw VLAN 组。

## 命令语法

raw vlan group *GROUP\_ID* vlan *VLAN\_LIST*

no raw vlan group *GROUP\_ID*

GROUP_ID	组的编号，范围为 1- 64。
VLAN_LIST	VLAN 的一个集合，格式可以为 10-20

## 命令模式

全局配置模式

## 默认

无

## 使用说明

无

## 举例说明

创建 raw VLAN 组 1，VLAN 范围是 10-20:

```
Switch(config)# raw vlan group 1 vlan 10-20
```

## 相关命令

show vlan mapping table *WORD*

### 2.7.6 raw-vlan

使用该命令添加 VLAN 映射表条目到 VLAN 映像表。

## 命令语法

raw-vlan (*VLAN\_ID* / out-of-range | untagged | group *GROUP\_ID*) evc *WORD*

no raw-vlan (*VLAN\_ID* / out-of-range | untagged| group )

**raw-vlan** *INNER\_VLAN* *OUTER\_VLAN* **egress-vlan** (*untagged* | *MAPPED\_VLAN*)

no raw-vlan *INNER\_VLAN* *OUTER\_VLAN* egress-vlan

VLAN_ID	收到报文的源 vlan，范围为 1- 4094。格式可以为 1,2,3 或 1-20
out-of-range	没有特殊指定的 vlans
untagged	不带 vlan tag 的报文
<b>Group</b> GROUP_ID	Raw VLAN 组，使用组会比直接使用 vlan 范围更省资源。
WORD	EVC 名称
INNER_VLAN	Inner vlan id, 取值范围 1 到 4094
OUTER_VLAN	Outer vlan id, 取值范围 1 到 4094
MAPPED_VLAN	Mapped vlan id, 取值范围 1 到 4094

## 命令模式

VLAN mapping 配置模式

## 默认

无

## 使用说明

无

## 举例说明

添加 VLAN 映像条目，源 VLAN ID 范围是 10-20，映像到 evc\_table:

```
Switch(config)# vlan mapping table VMT
Switch(config-vlan-mapping)# raw-vlan 10-20 evc evc_table
```

## 相关命令

show vlan mapping table *WORD*

## 2.7.7 dot1q ethertype

使用该命令设置端口的 ethertype。

## 命令语法

dot1q ethertype *VALUE*

VALUE	指定发送报文的 VLAN tag 的 ethertype。格式可以为 16 进制，默认为 0x8100
-------	---

## 命令模式

端口配置模式

## 默认

无

## 使用说明

无

## 举例说明

修改端口 1 的 ethertype，使其出去报文 VLAN tag 的 ethertype 为 0x9100:

```
Switch (config-if)# dot1q ethertype 9100
```

## 相关命令

无

## 2.7.8 show vlan mapping table

使用该命令显示 VLAN 映像表。

## 命令语法

```
show vlan mapping table (WORD |)
```

WORD	VLAN 映射表的名称
------	-------------

## 命令模式

特权模式

## 默认

无



## 使用说明

无

## 举例说明

以下用例展示如何显示 vlan 映像表:

```
Switch# show vlan mapping table
Table Name      EVC Name      Mapped VLAN  Forward Interface  Raw VLAN
=====
VMT             evc_table     100          n/a                10-20
VMT_double     evc_double    10(100)     n/a                untagged
VMT_forward    evc_forward   20          eth-0-9            30
```

## 相关命令

show vlan mapping table applied-interface

### 2.7.9 show vlan mapping table applied-interface

使用该命令显示 VLAN 映像表应用在哪些端口上。

## 命令语法

show vlan mapping table applied-interface

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

以下示例展示如何显示 vlan 映像表应用在哪些端口上:

```
Switch# show vlan mapping table applied-interface
Table Name      Interface Name  Type
=====
VMT             eth-0-1        802.1Q-Tunnel
```

## 相关命令

show vlan mapping table *WORD*

## 2.7.10 switchport mode

使用该命令配置端口模式。

### 命令语法

```
switchport mode ( access | trunk | dot1q-tunnel )
```

```
no switchport dot1q-tunnel
```

access	配置端口模式为 access 类型
trunk	配置端口模式为 trunk 类型
dot1q-tunnel	配置端口模式为 dot1q-tunnel 类型

### 命令模式

端口配置模式

### 默认

无

### 使用说明

无

### 举例说明

以下示例显示如何配置端口为 dot1q-tunnel 端口：

```
Switch(config-if)# switchport mode dot1q-tunnel
```

### 相关命令

```
show interface switchport
```

## 2.7.11 switchport dot1q-tunnel type

使用该命令配置 dot1q-tunnel 的类型。

### 命令语法

```
switchport dot1q-tunnel type ( basic | selective )
```

basic	Dot1q-tunnel 基本类型，对进入的报文统一映射到一个 VLAN
-------	--------------------------------------

selective	Dot1q-tunnel 选择类型，对进入的报文根据 vlan 映射到对应的 VLAN
-----------	---

## 命令模式

端口配置模式

## 默认

Basic type

## 使用说明

无

## 举例说明

以下示例展示了如何配置接口 dot1q-tunnel 类型为选择类型：

```
Switch(config-if)# switchport dot1q-tunnel type selective
```

## 相关命令

show interface switchport

## 2.7.12 switchport dot1q-tunnel native

使用该命令配置 dot1q-tunnel 端口的默认 VLAN。

## 命令语法

```
switchport dot1q-tunnel native (vlan | inner-vlan) VLAN_ID
```

```
no switchport dot1q-tunnel native vlan
```

vlan	被添加的 VLAN
inner-vlan	Untagged inner VLAN
VLAN_ID	Vlan Id, 范围 1~4094

## 命令模式

端口配置模式

## 默认

无

## 使用说明

无

## 举例说明

配置 eth-0-1 为 dot1q-tunnel 并配置端口的默认 VLAN 为 10:

```
Switch(config)# vlan database
Switch(config-vlan)# vlan 100
Switch(config-vlan)# exit
Switch(config)# interface eth-0-23
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# switchport dot1q-tunnel native vlan 100
```

## 相关命令

无

### 2.7.13 switchport dot1q-tunnel allow vlan

使用该命令配置 dot1q-tunnel 端口允许 VLAN 通过。

## 命令语法

```
switchport dot1q-tunnel allow vlan (all | none | add VLAN_ID | remove VLAN_ID)
```

<b>all</b>	允许系统中配置的所有 VLAN 通过
<b>none</b>	不允许任何 VLAN 通过
<b>add VLAN_ID</b>	添加一个 VLAN 通过，范围<1-4094>
<b>remove VLAN_ID</b>	从运行通过列表中删除一个 VLAN，范围为<1-4094>

## 命令模式

端口配置模式

## 默认

无

## 使用说明

无

## 举例说明

以下示例展示了如何在 dot1q-tunnel 端口上允许 VLAN 100 通过:

```
Switch(config-if)# switchport dot1q-tunnel allowed vlan add 100
```

## 相关命令

```
show vlan brief
```

## 2.7.14 switchport dot1q-tunnel vlan mapping table

使用该命令将 VLAN 映射表应用在可选的 dot1q tunnel 端口上。

## 命令语法

```
switchport dot1q-tunnel vlan mapping table WORD
```

```
no switchport dot1q-tunnel vlan mapping table
```

WORD	VLAN 映射表的名称
------	-------------

## 命令模式

端口配置模式

## 默认

无

## 使用说明

需要将 dot1q-tunnel 端口的类型配置为 selective, 才可以将 VLAN mapping 表绑定到该接口上。

## 举例说明

以下用例展示如何配置在端口上应用 VLAN 映射表 mp:

```
Switch(config-if)# switchport dot1q-tunnel vlan mapping table mp
```

## 相关命令

```
show interface switchport
```

## 2.7.15 switchport dot1q-tunnel vlan mapping miss-forward

使用该命令将未匹配 vlan 映射表的报文在端口上做普通转发。

### 命令语法

```
switchport dot1q-tunnel vlan mapping miss-forward  
no switchport dot1q-tunnel vlan mapping miss-forward
```

### 命令模式

端口配置模式

### 默认

无

### 使用说明

需要将 dot1q-tunnel 端口的类型配置为 selective，才可以使用该命令。

### 举例说明

以下用例展示如何将未匹配 vlan 映射表的报文在端口上做普通转发：

```
Switch(config-if)# switchport dot1q-tunnel vlan mapping miss-forward
```

### 相关命令

## 2.7.16 switchport trunk vlan-translation

使用该命令开启 VLAN 转换功能，使用 no 命令关闭该功能。

### 命令语法

```
switchport trunk vlan-translation  
no switchport trunk vlan-translation
```

### 命令模式

端口配置模式

### 默认

无

### 使用说明

只有 trunk 口上可以开启 VLAN 转换功能。

## 举例说明

以下示例展示如何配置 trunk 口和如何在 trunk 口上使能 vlan 转化功能：

```
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk vlan-translation
```

## 相关命令

```
show interface switchport
```

## 2.7.17 switchport trunk vlan-translation mapping table

使用该命令将 vlan 映射表应用到启用 VLAN 转换功能的端口上。

## 命令语法

```
switchport trunk vlan-translation mapping table WORD
no switchport trunk vlan-translation mapping table
```

WORD	VLAN mapping table name
------	-------------------------

## 命令模式

端口配置模式

## 默认

无

## 使用说明

无

## 举例说明

以下示例展示如何将 VLAN 映射表应用到启用 VLAN 转换功能的端口上：

```
Switch(config-if)# switchport trunk vlan-translation vlan mapping table map_table
```

## 相关命令

```
show interface switchport
```

## 2.7.18 switchport trunk vlan-translation miss-forward

使用该命令将未匹配 vlan 映射表的报文在端口上做普通转发。

## 命令语法

```
switchport trunk vlan-translation mapping miss-forward  
no switchport trunk vlan-translation mapping miss-forward
```

## 命令模式

端口配置模式

## 默认

无

## 使用说明

无

## 举例说明

以下示例展示如何配置将未匹配 `vlan` 映射表的报文在端口上做普通转发：

```
Switch(config-if)# switchport trunk vlan-translation mapping miss-forward
```

## 相关命令

### 2.7.19 vlan dot1q tag native

使用该命令配置带默认 VLAN 的报文从端口出去时带上 VLAN，使用 `no` 命令可删除配置。

## 命令语法

```
vlan dot1q tag native  
no vlan dot1q tag native
```

## 命令模式

端口配置模式

## 默认

无

## 使用说明

无



## 举例说明

以下示例展示了配置带默认 VLAN 的报文从端口出去时带上 VLAN:

```
Switch(config-if)# vlan dot1q tag native
```

## 相关命令

无

## 2.7.20 show resource vlan-mapping

使用该命令显示系统中 VLAN 映像表占用的硬件资源统计信息。

## 命令语法

```
show resource vlan-mapping
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面的例子显示了使用命令 `show resource vlan-mapping` 的输出结果:

```
Switch# show resource vlan-mapping
VLAN-MAPPING
Resource                               Used           Capability
=====
Applied VLAN Mapping Entry             0              1024
```

## 相关命令

无

## 2.8 Link Aggregation 命令

### 2.8.1 channel-group

使用该命令来将端口加入某一动态聚合组。使用该命令的 `no` 形式将端口移出该动态聚合组。

## 命令语法

`channel-group channel-group-number mode (active | passive)`

`no channel-group`

<code>channel-group-number</code>	聚合组 ID, 范围 <1-31>
<code>active</code>	在端口上使能动态聚合组
<code>passive</code>	在端口上去使能动态聚合组

## 命令模式

端口配置模式

## 默认

无

## 使用说明

无

## 举例说明

- 下面的例子显示了如何将端口加入聚合组 1:

```
Switch(config-if)# channel-group 1 mode active
```

- 下面的例子显示了如何将端口从聚合组 1 里移出:

```
Switch(config-if)# no channel-group
```

## 相关命令

无

## 2.8.2 static-channel-group

使用该命令将端口加入静态聚合组。使用该命令的 `no` 形式将端口移出该静态聚合组。

## 命令语法

`static-channel-group static-channel-group-number`

`no static-channel-group`

<code>static-channel-group-number</code>	聚合组 ID, 范围 <1-31>
--	-------------------

## 命令模式

端口配置模式

## 默认

无

## 使用说明

无

## 举例说明

- 下面的例子显示了如何将端口加入聚合组 1:

```
Switch(config-if)# static-channel-group 1
```

- 下面的例子显示了如何将端口从聚合组 1 里移出:

```
Switch(config-if)# no static-channel-group
```

## 相关命令

无

### 2.8.3 lacp port-priority

使用该命令用来配置端口的 LACP 协议优先级，使用该命令的 no 形式恢复端口优先级默认值。

## 命令语法

```
lacp port-priority priority
```

priority	优先级，范围是 1~65535
----------	-----------------

## 命令模式

端口配置模式

## 默认

32768

## 使用说明

无

## 举例说明

- 下面的例子显示了如何将端口的 LACP 优先级设置为 100:

```
Switch(config-if)# lacp port-priority 100
```

- 下面的例子显示了如何将端口的优先级恢复默认值:

```
Switch(config-if)# no lacp port-priority
```

## 相关命令

无

## 2.8.4 lacp timeout

使用该命令来设置端口的 LACP 超时时间。使用该命令的 no 形式恢复默认值。

## 命令语法

```
lacp timeout (short | long)
```

short	设置 LACP 超时时间为长超时
long	设置 LACP 超时时间为短超时

## 命令模式

端口配置模式

## 默认

Long

## 使用说明

无

## 举例说明

- 下面的例子显示了如何将端口的 LACP 超时时间设置为短模式:

```
Switch(config-if)# lacp timeout short
```

- 下面的例子显示了如何将端口的 LACP 超时时间恢复为默认值:

```
Switch(config-if)# no lacp timeout
```

## 相关命令

无

### 2.8.5 lacp system-priority

使用该命令用来配置系统的 LACP 协议优先级，使用该命令的 **no** 形式恢复系统优先级默认值。

## 命令语法

`lacp system-priority priority`

priority	优先级，范围是 1~65535
----------	-----------------

## 命令模式

全局配置模式

## 默认

32768

## 使用说明

无

## 举例说明

- 下面的例子显示了如何将系统的 LACP 优先级设置为 100:

```
Switch(config)# lacp system-priority 100
```

- 下面的例子显示了如何将系统的优先级恢复默认值:

```
Switch(config)# no lacp system-priority
```

## 相关命令

无

### 2.8.6 lacp system-mac

使用该命令用来配置系统的 LACP 协议 MAC 地址。

使用该命令的 **no** 形式取消该配置。

## 命令语法

`lacp system-mac mac-address`

`no lacp system-mac`

mac-address	MAC 地址，格式为 HHHH.HHHH.HHHH
-------------	---------------------------

## 命令模式

全局配置模式

## 默认

系统默认不配置 LACP MAC 地址。

## 使用说明

无

## 举例说明

配置系统的 LACP MAC 地址为 4321.1234.3421:

```
Switch(config)# lacp system-mac 4321.1234.3421
```

取值配置系统的 MAC 地址:

```
Switch(config)# no lacp system-mac
```

## 2.8.7 lacp device-id

使用该命令用来配置系统的 LACP 协议的设备 ID。

使用该命令的 **no** 形式恢复系统默认值。

## 命令语法

**lacp device-id** *id*

**no lacp device-id**

id	设备 ID 值,范围为 0~15
----	------------------

## 命令模式

全局配置模式

## 默认

0

## 使用说明

当多台设备的 LACP 系统的 MAC 地址配置相同时，可以配置 device-id 来区分不同设备的端口。

## 举例说明

将系统的 LACP device-id 设置为 15:

```
Switch(config)# lacp device-id 15
```

将系统的 device-id 恢复默认值:

```
Switch(config)# no lacp device-id
```

## 2.8.8 lacp max-bundle

使用该命令来配置成员端口聚合成功的最大个数。

使用该命令的 **no** 形式来关闭该功能。

## 命令语法

**lacp max-bundle** *number*

**no lacp max-bundle**

number	成员端口聚合成功的最大个数，取值范围为 0~32
--------	--------------------------

## 命令模式

接口配置模式

## 默认

关闭

## 使用说明

该命令只能在聚合端口下配置。

## 举例说明

开启 max-bundle 功能:

```
Switch(config-if)# lacp max-bundle 3
```

关闭端口 max-bundle 功能:

```
Switch(config-if)# no lacp max-bundle
```

## 2.8.9 port-channel load-balance hash-field-select

使用该命令设置 LACP 的 hash 字段选择，使用该命令的 no 形式恢复默认值。

## 命令语法

**port-channel load-balance hash-field-select** {ipda | ipsa | macda | macsa | sourceport | destport | ip-protocol | vxlan-vni | nvgre-vid | inner-ipda | inner-ipsa | inner-ip-protocol | inner-macda | inner-macsa | inner-sourceport | inner-destport }

## no port-channel load-balance hash-field-select

macda	根据目地 MAC 进行负载均衡
macsa	根据源 MAC 进行负载均衡
ipda	根据目的 IP 进行负载均衡
ipsa	根据源 IP 进行负载均衡
srcport	根据源端口进行负载均衡
dstport	根据目的端口进行负载均衡
ip-protocol	根据 ip 协议进行负载均衡
nvgre-vsidi	根据 Nvgre 的 Vsid 进行负载均衡
vxlani-vni	根据 Vxlan 的 Vsid 进行负载均衡
inner-destport	根据内层报文的端口进行负载均衡
inner-ip-protocol	根据内层报文的 ip 协议进行负载均衡
inner-ipda	根据内层报文的 IP 进行负载均衡
inner-ipsa	根据内层报文的源 IP 进行负载均衡
inner-macda	根据内层报文的目地 MAC 进行负载均衡
inner-macsa	根据内层报文的源 MAC 进行负载均衡
inner-sourceport	根据内层报文的源端口进行负载均衡

## 命令模式

全局配置模式

## 默认

macda macsa ipda ipsa

## 使用说明

系统默认 IP hash，即根据报文的源和目的 IP 位址做 hash 来决定报文应该从 LACP 的哪一个成员端口出去。您还可以选择根据目的 MAC 来做 hash，根据源 MAC 来做 hash，根据源和目的来做 hash；或者根据目的 IP 来做 hash；或者根据源 IP 来做 hash。

## 举例说明

下面的例子显示了如何配置 LACP 的负载均衡模式：



```
Switch(config)# port-channel load-balance hash-field-select macsa
```

## 相关命令

无

### 2.8.10 port-channel load-balance hash-arithmetic

使用该命令设置 LACP 的 hash 算法，使用该命令的 no 形式恢复默认值。

## 命令语法

```
port-channel load-balance hash-arithmetic (xor|crc)
```

```
no port-channel load-balance hash-arithmetic
```

xor	用异或算法计算 hash 值
crc	使用循环冗余校验算法计算 hash 值

## 命令模式

全局配置模式

## 默认

xor

## 使用说明

无

## 举例说明

下面的例子显示了如何配置 LACP 的 hash 算法：

```
Switch(config)# port-channel load-balance hash-arithmetic crc
```

## 相关命令

无

### 2.8.11 port-channel *channel-group-number* load-balance-mode dynamic

使用该命令使能动态负载均衡。

## 命令语法

```
port-channel channel-group-number load-balance-mode dynamic
```

```
no port-channel channel-group-number
```

channel-group-number	需要使能动态负载均衡的聚合组 ID，范围是 1-31
----------------------	----------------------------

## 命令模式

全局配置模式

## 默认

无

## 使用说明

系统默认不为聚合组使能动态负载均衡，使能/去使能动态负载均衡模式前，聚合组必须没有被创建。

## 举例说明

下面的例子显示了如何使能 agg1 上的动态负载均衡：

```
Switch(config)# port-channel 1 load-balance-mode dynamic
```

## 相关命令

无

## 2.8.12 port-channel *channel-group-number* load-balance-mode round-robin

使用该命令使能 round-robin 负载均衡。

## 命令语法

```
port-channel channel-group-number load-balance-mode round-robin
```

```
no port-channel channel-group-number
```

channel-group-number	需要使能 round-robin 负载均衡的聚合组 ID，范围是 1-31
----------------------	---------------------------------------

## 命令模式

全局配置模式

## 默认

无

## 使用说明

系统默认不为聚合组使能 `round-robin` 负载均衡，使能/去使能 `round-robin` 负载均衡模式前，聚合组必须没有被创建。

## 举例说明

下面的例子显示了如何使能 `agg1` 上的 `round-robin` 负载均衡：

```
Switch(config)# port-channel 1 load-balance-mode round-robin
```

## 相关命令

无

### 2.8.13 `port-channel channel-group-number self-healing`

使用该命令使能 `self-healing`。

## 命令语法

```
port-channel channel-group-number self-healing
```

```
no port-channel channel-group-number
```

<code>channel-group-number</code>	需要使能 <code>self-healing</code> 聚合组 ID，范围是 1-31
-----------------------------------	--

## 命令模式

全局配置模式

## 默认

无

## 使用说明

系统默认不为聚合组使能 `self-healing`，使能/去使能 `self-healing` 模式前，聚合组必须没有被创建。

## 举例说明

下面的例子显示了如何使能 `agg1` 上的 `self-healing` 功能：

```
Switch(config)# port-channel 1 self-healing
```

## 相关命令

无

## 2.8.14 show channel-group summary

使用该命令来显示所有的聚合组或者某个指定的聚合组。

### 命令语法

**show channel-group** (*channel-group-number* |) **summary**

channel-group-number	聚合组 ID, 范围是 1~31
----------------------	------------------

### 命令模式

特权模式

### 默认

无

### 使用说明

无

### 举例说明

下面的例子显示了如何显示所有的聚合组信息：

```
Switch1# show channel-group summary
port-channel load-balance hash-arithmetic: xor
port-channel load-balance hash-field-select:
    srcport
Flags:  s - suspend                T - standby
        D - down/admin down      B - in Bundle
        R - Layer3                S - Layer2
        w - wait                  U - in use
Mode:   SLB - static load balance
        DLB - dynamic load balance
        SHLB - self-healing load balance
        RR  - round robin load balance
Aggregator Name  Mode      Protocol  Ports
-----+-----+-----+-----
agg1 (SU)                DLB      Static    eth-0-1 (B)
```

下面的例子显示了如何显示某个指定聚合组的信息：

```
Switch1# show channel-group 1 summary

port-channel load-balance hash-arithmetic: xor
port-channel load-balance hash-field-select:
    srcport
```

```

Flags:  s - suspend                T - standby
        D - down/admin down       B - in Bundle
        R - Layer3                S - Layer2
        w - wait                  U - in use
Mode:   SLB - static load balance
        DLB - dynamic load balance
        SHLB - self-healing load balance
        RR  - round robin load balance
Aggregator Name Mode      Protocol  Ports
-----+-----+-----+-----
agg1 (SU)          DLB      Static    eth-0-1 (B)

```

## 相关命令

无

## 2.8.15 show channel-group detail

使用该命令显示所有的聚合组或某个指定聚合组的详细信息。

## 命令语法

**show channel-group** (*channel-group-number* |) **detail**

channel-group-number	聚合组 ID，范围是 1~31
----------------------	-----------------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面的例子显示如何显示某个指定聚合组的详细信息：

```

Switch# show channel-group 10 detail
      Channel-group listing:
      -----
Group: 10
-----

```

**Group state = L2**

```
Ports: 1   Maxports = 48
Number of ports in bundle: 1 Max Channel-groups = 31
Standby port = NULL
Protocol:  LACP
```

```
Ports in the group:
-----
```

**Port: eth-0-10**

```
-----
Port state      = Up In-Bndl
Channel number = 10          Protocol = LACP          Channel-group = agg10
Port index     = 10          Mode = Active
Flags:  S - Device is sending Slow LACPDUs  F - Device is sending fast LACPDUs
        A - Device is in active mode        P - Device is in passive mode
Local information:
Port      Flags  State  LACP port  Admin  Oper  Port  Port
eth-0-10 SA    bndl   32768     10     10    0xa   0x3d
Partner's information:
Port      Flags  Priority  Dev ID  Oper  Port  Port
eth-0-10 SA    32768    fed3.7914.b000  10    0xa   0x1d
```

**相关命令**

无

**2.8.16 show lacp internal**

使用该命令来显示 LACP 的内部信息。

**命令语法**

**show lacp** (*channel-group-number*) **internal**

channel-group-number	聚合组 ID，范围是 1~31
----------------------	-----------------

**命令模式**

特权模式

**默认**

无

## 使用说明

无

## 举例说明

- 下面的例子显示了所有聚合组的内部信息：

```
Switch# show lacp internal
Flags: S - Device is requesting Slow LACPDUs
       F - Device is requesting Fast LACPDUs
       A - Device is in Active mode           P - Device is in Passive mode
```

### Channel group 1

Port	Flags	State	LACP port Priority	Admin key	Oper Key	Port Number	Port State
eth-0-11	FA	bndl	32768	1	1	0x5a	0x3f
eth-0-12	FA	bndl	32768	1	1	0x5b	0x3f

### Channel group 30

Port	Flags	State	LACP port Priority	Admin key	Oper Key	Port Number	Port State
eth-0-9	FA	bndl	32768	50	50	0x58	0x3f
eth-0-10	FA	bndl	32768	50	50	0x59	0x3f

- 下面的例子显示了指定聚合组的内部信息：

```
Switch# show lacp 1 internal
Flags: S - Device is requesting Slow LACPDUs
       F - Device is requesting Fast LACPDUs
       A - Device is in Active mode           P - Device is in Passive mode
```

### Channel group 1

Port	Flags	State	LACP port Priority	Admin key	Oper Key	Port Number	Port State
eth-0-11	FA	bndl	32768	1	1	0x5a	0x3f
eth-0-12	FA	bndl	32768	1	1	0x5b	0x3f

## 相关命令

无

### 2.8.17 show lacp internal detail

使用该命令显示 LACP 的详细内部信息。

## 命令语法

**show lacp** (*channel-group-number*) **internal detail**

channel-group-number	聚合组 ID，范围是 1~31
----------------------	-----------------

## 命令模式

特权模式

## 默认

无

## 举例说明

无

## 举例

下面的例子显示了所有聚合组的详细内部信息：

```
Switch# show lacp internal detail
Flags: S - Device is requesting Slow LACPDUs
       F - Device is requesting Fast LACPDUs
       A - Device is in Active mode           P - Device is in Passive mode

Channel group 1 neighbors
Actor's information:
      Actor                Actor      Actor
Port  System ID           Port Number  Flags
eth-0-11  32768,ca9c.e21d.a301  0x56        FA
      LACP Actor          Actor      Actor
      Port Priority       Oper Key   Port State
      32768              1         0x3f
      Port State Flags Decode:
      Activity:  Timeout:  Aggregation:  Synchronization:
      Active     Short     Yes          Yes
      Collecting: Distributing: Defaulted:  Expired:
      Yes        Yes          No           No
      Actor                Actor      Actor
Port  System ID           Port Number  Flags
eth-0-12  32768,ca9c.e21d.a301  0x57        FA
      LACP Actor          Actor      Actor
      Port Priority       Oper Key   Port State
      32768              1         0x3f
      Port State Flags Decode:
      Activity:  Timeout:  Aggregation:  Synchronization:
      Active     Short     Yes          Yes
      Collecting: Distributing: Defaulted:  Expired:
      Yes        Yes          No           No

Channel group 30 neighbors
Actor's information:
      Actor                Actor      Actor
Port  System ID           Port Number  Flags
eth-0-9  32768,ca9c.e21d.a301  0x54        FA
      LACP Actor          Actor      Actor
      Port Priority       Oper Key   Port State
```



```

32768          199          0x3f
Port State Flags Decode:
Activity:   Timeout:   Aggregation:   Synchronization:
Active     Short      Yes           Yes
Collecting: Distributing: Defaulted:   Expired:
Yes        Yes          No            No
Actor
Port System ID          Port Number  Flags
eth-0-10 32768,ca9c.e21d.a301  0x55        FA
LACP Actor Actor          Actor
Port Priority Oper Key      Port State
32768      199          0x3f
Port State Flags Decode:
Activity:   Timeout:   Aggregation:   Synchronization:
Active     Short      Yes           Yes
Collecting: Distributing: Defaulted:   Expired:
Yes        Yes          No            No

```

- 下面的例子显示了某个指定聚合组的详细内部信息：

```

Switch# show lacp 1 internal detail
Flags: S - Device is requesting Slow LACPDU
      F - Device is requesting Fast LACPDU
      A - Device is in Active mode      P - Device is in Passive mode
Channel group 1 neighbors
Actor's information:
Actor Actor Actor
Port System ID          Port Number  Flags
eth-0-11 32768,ca9c.e21d.a301  0x56        FA
LACP Actor Actor          Actor
Port Priority Oper Key      Port State
32768      1            0x3f
Port State Flags Decode:
Activity:   Timeout:   Aggregation:   Synchronization:
Active     Short      Yes           Yes
Collecting: Distributing: Defaulted:   Expired:
Yes        Yes          No            No
Actor Actor Actor
Port System ID          Port Number  Flags
eth-0-12 32768,ca9c.e21d.a301  0x57        FA
LACP Actor Actor          Actor
Port Priority Oper Key      Port State
32768      1            0x3f
Port State Flags Decode:
Activity:   Timeout:   Aggregation:   Synchronization:
Active     Short      Yes           Yes
Collecting: Distributing: Defaulted:   Expired:
Yes        Yes          No            No

```

## 相关命令

无

### 2.8.18 show lacp neighbor

使用该命令显示所有聚合组或某个指定聚合组的邻居信息。

## 命令语法

**show lacp** (*channel-group-number* |) **neighbor**

channel-group-number	聚合组 ID，范围是 1~31
----------------------	-----------------

## 命令模式

特权模式

## 默认

无

## 用法

无

## 举例说明

- 下面的例子显示了所有聚合组的邻居信息：

```
Switch# show lacp neighbor
Flags: S - Device is requesting Slow LACPDUs
       F - Device is requesting Fast LACPDUs
       A - Device is in Active mode           P - Device is in Passive mode
```

#### Channel group 1 neighbors

```
Partner's information:
      LACP port
Port  Flags Priority Dev ID      Admin Oper  Port  Port
      key   Key   Number  State
eth-0-11 FA   32768 ca9c.e21d.a301  0    1    0x56  0x3f
eth-0-12 FA   32768 ca9c.e21d.a301  0    1    0x57  0x3f
```

#### Channel group 30 neighbors

```
Partner's information:
      LACP port
Port  Flags Priority Dev ID      Admin Oper  Port  Port
      key   Key   Number  State
eth-0-9  FA   32768 ca9c.e21d.a301  0    99   0x54  0x3f
eth-0-10 FA   32768 ca9c.e21d.a301  0    99   0x55  0x3f
```

- 下面的例子显示了某个指定聚合组的邻居信息：

```
Switch# show lacp 1 neighbor
Flags: S - Device is requesting Slow LACPDUs
       F - Device is requesting Fast LACPDUs
       A - Device is in Active mode           P - Device is in Passive mode
```

#### Channel group 1 neighbors

```
Partner's information:
```

Port	Flags	LACP port		Admin key	Oper Key	Port Number	Port State
		Priority	Dev ID				
eth-0-11	FA	32768	ca9c.e21d.a301	0	1	0x56	0x3f
eth-0-12	FA	32768	ca9c.e21d.a301	0	1	0x57	0x3f

## 相关命令

无

## 2.8.19 show lacp neighbor detail

使用该命令显示所有聚合组或某个指定聚合组的详细邻居信息。

## 命令语法

**show lacp** (*channel-group-number*) **neighbor detail**

channel-group-number	聚合组 ID，范围是 1~31
----------------------	-----------------

## 命令模式

特权模式

## 默认

无

## 用法

无

## 举例说明

- 下面的例子显示了所有聚合组的详细邻居信息：

```
Switch# show lacp neighbor detail
Flags: S - Device is requesting Slow LACPDU's
       F - Device is requesting Fast LACPDU's
       A - Device is in Active mode           P - Device is in Passive mode
Channel group 1 neighbors
Partner's information:
      Partner                Partner                Partner
Port   System ID            Port Number        Flags
eth-0-11 32768,ca9c.e21d.a301  0x56              FA
      LACP Partner          Partner            Partner
      Port Priority         Oper Key          Port State
      32768                 1                0x3f
      Port State Flags Decode:
      Activity:  Timeout:  Aggregation:  Synchronization:
```

```

Active      Short      Yes        Yes
Collecting: Distributing: Defaulted: Expired:
Yes         Yes        No         No
Partner
Port        System ID          Port Number      Flags
eth-0-12   32768,ca9c.e21d.a301  0x57            FA
LACP Partner      Partner          Partner
Port Priority      Oper Key         Port State
32768              1                0x3f
Port State Flags Decode:
Activity:  Timeout:  Aggregation:  Synchronization:
Active    Short    Yes           Yes
Collecting: Distributing: Defaulted: Expired:
Yes       Yes     No            No
    
```

**Channel group 30 neighbors**

```

Partner's information:
Partner      Partner      Partner
Port        System ID          Port Number      Flags
eth-0-9     32768,ca9c.e21d.a301  0x54            FA
LACP Partner      Partner          Partner
Port Priority      Oper Key         Port State
32768              199              0x3f
Port State Flags Decode:
Activity:  Timeout:  Aggregation:  Synchronization:
Active    Short    Yes           Yes
Collecting: Distributing: Defaulted: Expired:
Yes       Yes     No            No
Partner
Port        System ID          Port Number      Flags
eth-0-10   32768,ca9c.e21d.a301  0x55            FA
LACP Partner      Partner          Partner
Port Priority      Oper Key         Port State
32768              199              0x3f
Port State Flags Decode:
Activity:  Timeout:  Aggregation:  Synchronization:
Active    Short    Yes           Yes
Collecting: Distributing: Defaulted: Expired:
Yes       Yes     No            No
    
```

- 下面的例子显示了某个指定聚合组的详细邻居信息:

```

Switch# show lacp 1 neighbor detail
Flags: S - Device is requesting Slow LACPDU's
       F - Device is requesting Fast LACPDU's
       A - Device is in Active mode           P - Device is in Passive mode

Channel group 1 neighbors
Partner's information:
Partner      Partner      Partner
Port        System ID          Port Number      Flags
eth-0-11   32768,ca9c.e21d.a301  0x56            FA
LACP Partner      Partner          Partner
Port Priority      Oper Key         Port State
32768              1                0x3f
Port State Flags Decode:
Activity:  Timeout:  Aggregation:  Synchronization:
    
```

```

Active          Short      Yes          Yes
Collecting:    Distributing:  Defaulted:   Expired:
Yes            Yes          No            No
Partner
Port           System ID          Port Number    Flags
eth-0-12      32768,ca9c.e21d.a301  0x57          FA
LACP Partner          Partner        Partner
Port Priority          Oper Key       Port State
32768                  1              0x3f
Port State Flags Decode:
Activity:   Timeout:   Aggregation:   Synchronization:
Active     Short      Yes            Yes
Collecting: Distributing: Defaulted:   Expired:
Yes        Yes        No            No

```

## 相关命令

无

## 2.8.20 show channel-group port

使用该命令来显示指定端口的链路聚合信息。

## 命令语法

```
show channel-group port (ifname)
```

```
show channel-group channel-group-number port
```

<code>ifname</code>	端口名称
<code>channel-group-number</code>	聚合组 ID，范围是 1~31

## 命令模式

特权模式

## 默认

无

## 用法

无

## 举例说明

- 下面的例子显示了所有端口上的链路聚合信息：

```

Switch# show channel-group port
          Channel-group listing:
          -----

Group: 1

-----

          Ports in the group:
          -----

Port: eth-0-11

-----

Port state      = Up In-Bndl
Channel number = 1          Protocol = LACP          Channel-group = agg1
Port index     = 90        Mode = Active
Flags:  S - Device is sending Slow LACPDUs  F - Device is sending fast LACPDUs
        A - Device is in active mode        P - Device is in passive mode
Local information:

Port      Flags  State      LACP port  Admin  Oper  Port      Port
eth-0-11 FA    bndl      32768      1      1     0x5a      0x3f
Partner's information:

          LACP port          Admin  Oper  Port      Port
Port      Flags  Priority  Dev ID          key   Key   Number    State
eth-0-11 FA    32768    ca9c.e21d.a301  0     1     0x56      0x3f

Port: eth-0-12

-----

Port state      = Up In-Bndl
Channel number = 1          Protocol = LACP          Channel-group = agg1
Port index     = 91        Mode = Active
Flags:  S - Device is sending Slow LACPDUs  F - Device is sending fast LACPDUs
        A - Device is in active mode        P - Device is in passive mode
Local information:

Port      Flags  State      LACP port  Admin  Oper  Port      Port
eth-0-12 FA    bndl      32768      1      1     0x5b      0x3f
Partner's information:

          LACP port          Admin  Oper  Port      Port
Port      Flags  Priority  Dev ID          key   Key   Number    State
eth-0-12 FA    32768    ca9c.e21d.a301  0     1     0x57      0x3f

Group: 30

-----

          Ports in the group:
          -----

Port: eth-0-9

-----

Port state      = Up In-Bndl
Channel number = 30        Protocol = LACP          Channel-group = agg30
Port index     = 88        Mode = Active
Flags:  S - Device is sending Slow LACPDUs  F - Device is sending fast LACPDUs
        A - Device is in active mode        P - Device is in passive mode
Local information:

```

```

Port      Flags  State      LACP port      Admin  Oper  Port      Port
eth-0-9   FA     bndl      32768          50    50    0x58     0x3f
Partner's information:
          LACP port      Admin  Oper  Port      Port
Port      Flags  Priority  Dev ID      key   Key   Number   State
eth-0-9   FA     32768    ca9c.e21d.a301  0    99   0x54     0x3f
Port: eth-0-10
-----
Port state      = Up In-Bndl
Channel number = 30          Protocol = LACP          Channel-group = agg30
Port index     = 89          Mode = Active
Flags: S - Device is sending Slow LACPDUs  F - Device is sending fast LACPDUs
      A - Device is in active mode          P - Device is in passive mode
Local information:
          LACP port      Admin  Oper  Port      Port
Port      Flags  State      Priority      Key   Key   Number   State
eth-0-10  FA     bndl      32768          50    50    0x59     0x3f
Partner's information:
          LACP port      Admin  Oper  Port      Port
Port      Flags  Priority  Dev ID      key   Key   Number   State
eth-0-10  FA     32768    ca9c.e21d.a301  0    99   0x55     0x3f

```

- 下面的例子显示了指定聚合组的所有端口信息：

```

Switch# show channel-group 1 port
      Ports in the group:
      -----

```

#### Port: eth-0-11

```

-----
Port state      = Up In-Bndl
Channel number = 1          Protocol = LACP          Channel-group = agg1
Port index     = 90          Mode = Active
Flags: S - Device is sending Slow LACPDUs  F - Device is sending fast LACPDUs
      A - Device is in active mode          P - Device is in passive mode
Local information:
          LACP port      Admin  Oper  Port      Port
Port      Flags  State      Priority      Key   Key   Number   State
eth-0-11  FA     bndl      32768          1     1     0x5a     0x3f
Partner's information:
          LACP port      Admin  Oper  Port      Port
Port      Flags  Priority  Dev ID      key   Key   Number   State
eth-0-11  FA     32768    ca9c.e21d.a301  0     1     0x56     0x3f

```

#### Port: eth-0-12

```

-----
Port state      = Up In-Bndl
Channel number = 1          Protocol = LACP          Channel-group = agg1
Port index     = 91          Mode = Active
Flags: S - Device is sending Slow LACPDUs  F - Device is sending fast LACPDUs
      A - Device is in active mode          P - Device is in passive mode
Local information:
          LACP port      Admin  Oper  Port      Port
Port      Flags  State      Priority      Key   Key   Number   State
eth-0-12  FA     bndl      32768          1     1     0x5b     0x3f

```

```

Partner's information:
          LACP port
Port      Flags  Priority  Dev ID      Admin  Oper  Port      Port
eth-0-12  FA    32768   ca9c.e21d.a301  0     1     0x57     0x3f

```

- 下面的例子显示了指定端口的链路聚合信息：

```

Switch# show channel-group port eth-0-11
Port: eth-0-11
-----
Port state      = Up In-Bndl
Channel number = 30          Protocol = LACP          Channel-group = agg30
Port index     = 90          Mode = Active
Flags: S - Device is sending Slow LACPDUs  F - Device is sending fast LACPDUs
      A - Device is in active mode          P - Device is in passive mode
Local information:
          LACP port
Port      Flags  State  Priority  Admin  Oper  Port      Port
eth-0-11  FA    bndl   32768    50     50    0x5a     0x3f
Partner's information:
          LACP port
Port      Flags  Priority  Dev ID      Admin  Oper  Port      Port
eth-0-11  FA    32768   381c.9f94.2501  0     90    0x56     0x3f

```

## 相关命令

无

## 2.8.21 show lacp counters

使用该命令显示所有聚合组或某个指定聚合组的报文统计信息。

## 命令语法

**show lacp** [*channel-group-number*] **counters**

channel-group-number	聚合组 ID，范围是 1~31
----------------------	-----------------

## 命令模式

特权模式

## 默认

无

## 使用说明

无



## 举例说明

- 下面的例子显示了所有聚合组的成员端口上的报文统计信息。

```
Switch# show lacp counters
Traffic statistics
Port                               LACPDUs          Pckt err
                                   Sent    Recv    Sent    Recv
-----
Channel-group agg1

eth-0-11                            231     226     0       0
eth-0-12                            224     219     0       0

Traffic statistics

Port                               LACPDUs          Pckt err
                                   Sent    Recv    Sent    Recv
-----
Channel-group agg30

eth-0-9                             29      25     0       0
eth-0-10                            24      18     0       0
```

- 下面的例子显示了指定聚合组的成员端口上的报文统计信息：

```
Switch# show lacp 1 counters
Traffic statistics
Port                               LACPDUs          Pckt err
                                   Sent    Recv    Sent    Recv
-----
Channel-group agg1

eth-0-11                            256     251     0       0
eth-0-12                            249     244     0       0
```

## 相关命令

无

### 2.8.22 show lacp sys-id

使用该命令显示设备的系统 ID 信息，包括 LACP 协议优先级和系统 MAC 地址。

## 命令语法

```
show lacp sys-id
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面的例子显示了系统 ID 信息：

```
Switch# show lacp sys-id
System ID: 32768,4600.0987.6c01
```

## 相关命令

无

## 2.8.23 clear lacp counters

使用该命令来清除所有聚合组的统计信息或某个指定聚合组的统计信息。

## 命令语法

**clear lacp** (*channel-group-number*) **counters**

channel-group-number	聚合组 ID，范围<1-31>
----------------------	-----------------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

- 下面的例子显示了如何清除所有聚合组的统计信息：

```
Switch# clear lacp counters
```

- 下面的例子显示了如何清除某个指定聚合组的统计信息：

```
Switch# clear lacp 10 counters
```

## 相关命令

无

### 2.8.24 lacp force-up

接口使能 LACP force-up 功能。

## 命令语法

**lacp force-up**

**no lacp force-up**

## 命令模式

端口配置模式

## 默认

无

## 使用说明

使用本命令前，接口上需配置动态链路聚合。

## 举例说明

接口使能 LACP force-up 功能：

```
Switch(config)# interface eth-0-1
```

```
Switch(config-if)# channel group 1 mode active
```

```
Switch(config-if)# lacp force-up
```

## 2.9 MSTP 命令

### 2.9.1 spanning-tree enable

使用该命令全局启用 STP 功能，使用 no 命令关闭该功能。

## 命令语法

**spanning-tree enable**

**no spanning-tree enable**

## 命令模式

全局配置模式

## 默认

默认关闭 STP

## 使用说明

无

## 举例说明

以下示例展示如何全局开启和关闭 STP 功能：

```
Switch# configure terminal
Switch(config)# spanning-tree enable
Switch# configure terminal
Switch(config)# no spanning-tree enable
```

## 相关命令

show spanning-tree

## 2.9.2 spanning-tree priority

使用该命令配置 STP 的优先权，使用 no 命令将 STP 的优先权恢复成默认值。

## 命令语法

spanning-tree priority *priority*

no spanning-tree priority

priority	优先权的值，取值范围 0~61440
----------	--------------------

## 命令模式

全局配置模式

## 默认

优先权的默认值 32678 (或十六进制 0x8000)。

## 使用说明

优先权的值必须是 4096 的倍数

## 举例说明

以下示例展示了如何配置优先权值和将优先权值恢复成默认值：

```
Switch# configure terminal
Switch(config)# spanning-tree priority 4096
Switch# configure terminal
Switch(config)# no spanning-tree priority
```

## 相关命令

```
show spanning-stree
```

### 2.9.3 spanning-tree instance priority

使用该命令配置 MST 用例的优先权值，使用 `no` 命令将该优先权值恢复成默认值。

## 命令语法

```
spanning-tree instance instance-id priority priority
```

```
no spanning-tree instance instance-id priority
```

instance-id	用例号，取值范围 1-4094
priority	用例的优先权值，取值范围 0~61440

## 命令模式

全局配置模式

## 默认

每个用例优先权值默认为 32768。

## 使用说明

在该用例中，优先权值小的交换机会成为根桥。优先权值必须是 4096 的倍数。

## 举例说明

```
Switch# configure terminal
Switch(config)# spanning-tree instance 1 priority 0
```

## 相关命令

```
show spanning-stree
```

### 2.9.4 spanning-tree forward-time

使用该命令配置 `forward-time`，这是根桥上每个端口从监听状态转化为学习状态或从学习状态转化为转发状态的时间间隔。使用 `no` 命令将该时间间隔恢复成默认值。

## 命令语法

`spanning-tree forward-time seconds`

`no spanning-tree forward-time`

seconds	时间间隔，时长范围为 4~30
---------	-----------------

## 命令模式

全局配置模式

## 默认

默认值是 15 秒。

## 使用说明

不建议时间间隔设在 7 秒钟以下。

## 举例说明

```
Switch# configure terminal
Switch(config)# spanning-tree forward-time 16
Switch(config)# no spanning-tree forward-time
```

## 相关命令

`show spanning-tree`

## 2.9.5 spanning-tree hello-time

使用该命令配置 `hello-time`，这是根桥定期发送 BPDU 报文的时间间隔。

## 命令语法

`spanning-tree hello-time seconds`

`no spanning-tree hello-time`

seconds	根桥定期发送 BPDU 报文的时间间隔，范围为 1~10
---------	------------------------------

## 命令模式

全局配置模式

## 默认

默认值为 2 秒

## 使用说明

允许配置的时间范围为 1-10 秒。

## 举例说明

以下示例展示了如何配置 `hello-time`：

```
Switch# configure terminal
Switch(config)# spanning-tree hello-time 5
Switch(config)# no spanning-tree hello-time
```

## 相关命令

`show spanning-tree`

## 2.9.6 spanning-tree max-age

使用该命令配置最大的超时时间，使用 `no` 命令将最大超时时间恢复成默认值。

## 命令语法

```
spanning-tree max-age seconds
no spanning-tree max-age
```

<code>seconds</code>	最大超时时间长度，取值范围是 6~40
----------------------	---------------------

## 命令模式

全局配置模式

## 默认

默认值为 20 秒。

## 使用说明

最大超时时间是一个消息被认为是有效的的时间。这防止了报文环回。这个时间应大于两倍的 `hello time` 加 1，小于两倍的 `forward time` 减 1。可配的时间范围是 6-40。

## 举例说明

以下示例展示了如何配置最大超时时间和将这个时间恢复成默认值：

```
Switch# configure terminal
Switch(config)# spanning-tree max-age 12
Switch(config)# no spanning-tree max-age
```

## 相关命令

```
show spanning-tree
```

## 2.9.7 spanning-tree max-hops

使用该命令配置 BPDU 报文所允许的最大跳数。这个参数被所有的用例使用。使用 `no` 命令可以恢复成默认值。

## 命令语法

```
spanning-tree max-hops number
```

```
no spanning-tree max-hops
```

number	最大跳数，取值范围 1 到 40
--------	------------------

## 命令模式

全局配置模式

## 默认

最大跳数默认值为 20

## 使用说明

指定最大跳数是为了防止 BPDU 报文在网络中环回。当交换机收到的报文超过最大跳数，将丢弃 BPDU 报文。

## 举例说明

以下示例展示了如何配置最大跳数及如何将最大跳数恢复默认值：

```
Switch# configure terminal
Switch(config)# spanning-tree max-hops 25
Switch(config)# no spanning-tree max-hops
```

## 相关命令

```
show spanning-tree
```



## 2.9.8 spanning-tree transmit-holdcount

使用该命令配置 1 秒内允许发出的最大 BPDU 数目。使用 `no` 命令将允许发出的最大 BPDU 数目恢复为默认值。

### 命令语法

```
spanning-tree transmit-holdcount number
```

```
no spanning-tree transmit-holdcount
```

number	允许发出的最大 BPDU 数目，范围是 1~10
--------	--------------------------

### 命令模式

全局配置模式

### 默认

默认值为 3

### 使用说明

无

### 举例说明

以下命令展示如何配置 1 秒内允许发出的最大 BPDU 数目：

```
Switch# configure terminal
Switch(config)# spanning-tree transmit-holdcount 5
Switch(config)# no spanning-tree transmit-holdcount
```

### 相关命令

```
show spanning-tree
```

## 2.9.9 spanning-tree edgeport bpdu-guard

使用该命令可以开启 `bpdu-guard` 功能，使用 `no` 命令可关闭该功能。

### 命令语法

```
spanning-tree edgeport bpdu-guard
```

```
no spanning-tree edgeport bpdu-guard
```

### 命令模式

全局配置模式

## 默认

关闭

## 使用说明

当 `bpdu-guard` 功能打开时，如果接收到 BPDU 报文，则端口会 `shutdown`。用户可以通过 `no shutdown` 重新打开端口或配置 `errdisable` 定时器到时重新打开端口。

可以用命令 `show spanning-tree` 来查看 `bpdu-guard` 的配置。

## 举例说明

```
Switch# configure terminal
Switch(config)# spanning-tree edgeport bpdu-guard
```

## 相关命令

`show spanning-tree interface`

## 2.9.10 spanning-tree edgeport bpdu-filter

使用该命令配置边缘端口过滤掉 BPDU 报文。

## 命令语法

```
spanning-tree edgeport bpdu-filter
no spanning-tree edgeport bpdu-filter
```

## 命令模式

全局配置模式

## 默认

关闭

## 使用说明

配置了 `bpdu-filter` 的端口不会接收和发送 BPDU 报文。

使用 `show spanning tree` 命令可以查看 `bpdu-filter` 的配置。

## 举例说明

```
Switch# configure terminal
Switch(config)# spanning-tree edgeport bpdu-filter enable
Switch(config)# no spanning-tree edgeport bpdu-filter
```

## 相关命令

`Show spanning-tree interface`

## 2.9.11 spanning-tree port

使用该命令可以在端口上启用 STP 功能，使用 no 命令可以关闭该功能。

### 命令语法

spanning-tree port (enable | disable)

enable	在端口上启用 STP 功能
disable	在端口上关闭 STP 功能

### 命令模式

端口配置模式

### 默认

默认启用该功能。

### 使用说明

无

### 举例说明

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# spanning-tree port enable
Switch(config-if)# spanning-tree port disable
```

### 相关命令

show spanning-tree interface

## 2.9.12 spanning-tree port-priority

使用该命令可以配置 STP 端口优先权值。如果其它条件一致，端口优先权值较小的一侧会成为根桥。

### 命令语法

spanning-tree port-priority *priority*

no spanning-tree port-priority

priority	端口优先权值，取值范围 0 到 240
----------	---------------------

## 命令模式

端口配置模式

## 默认

默认值为 128

## 使用说明

无

## 举例说明

以下示例展示了如何在端口上配置优先权值：

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# spanning-tree port-priority 240
```

## 相关命令

show spanning-tree interface

## 2.9.13 spanning-tree pathcost-standard

使用该命令可以配置 STP path cost 的协议标准，使用 no 命令恢复默认值。

## 命令语法

spanning-tree pathcost-standard (dot1d-1998 | dot1t)

no spanning-tree pathcost-standard

dot1d-1998	IEEE 802.1D-1998 标准
dot1t	IEEE 802.1T 标准

## 命令模式

全局配置模式

## 默认

默认的协议标准是 IEEE 802.1T

## 使用说明

如果协议标准改变了，每个端口上的 cost 将重置和重新计算。

## 举例说明

以下示例展示了如何配置 pathcost 协议标准:

```
Switch# configure terminal
Switch(config)# spanning-tree pathcost-standard dot1d-1998

Cost of every port has been reset and auto-calculation is available
```

## 相关命令

```
show spanning-tree
```

### 2.9.14 spanning-tree path-cost

使用该命令配置 STP 的 path cost, 使用 no 命令将恢复默认值。如果其它条件都一样, path cost 较小的一侧将成为根桥。

## 命令语法

```
spanning-tree path-cost number
no spanning-tree path-cost
```

number	cost 值, dot1t 取值范围是 1-200000000, dot1d-1998 取值范围是 1-65535
--------	---

## 命令模式

端口配置模式

## 默认

默认的 path cost 是根据端口的速率决定的

## 使用说明

无

## 举例说明

以下示例展示了如何配置 STP path-cost:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# spanning-tree path-cost 123
Switch(config-if)# no spanning-tree path-cost
```

## 相关命令

show spanning-tree interface

### 2.9.15 spanning-tree link-type

使用该命令配置 STP 的 link-type，使用 no 命令恢复默认配置。

## 命令语法

spanning-tree link-type (auto | point-to-point | shared)

no spanning-tree link-type

auto	自动检测和配置 link type
point-to-point	配置 link type 为 point to point link
shared	配置 link type 为 shared

## 命令模式

端口配置模式

## 默认

link type 默认为 auto

## 使用说明

无

## 举例说明

以下示例展示了如何配置 link type:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# spanning-tree link-type shared
```

## 相关命令

show spanning-tree brief

### 2.9.16 spanning-tree edgeport

使用该命令配置端口为边缘端口，使用 no 命令恢复端口为非边缘端口。

## 命令语法

```
spanning-tree edgeport  
no spanning-tree edgeport
```

## 命令模式

端口配置模式

## 默认

端口不是边缘端口

## 使用说明

无

## 举例说明

以下示例展示如何配置边缘端口和如何去配置：

```
Switch# configure terminal  
Switch(config)# interface eth-0-1  
Switch(config-if)# spanning-tree edgeport  
Switch(config-if)# no spanning-tree edgeport
```

## 相关命令

```
show spanning-tree interface
```

## 2.9.17 spanning-tree edgeport bpdu-guard

使用该命令配置在边缘端口上启用或关闭 BPDU Guard，使用 no 命令将该特性恢复为默认值。

## 命令语法

```
spanning-tree edgeport bpdu-guard (enable | disable | default)  
no spanning-tree edgeport bpdu-guard
```

enable	启用 edgeport bpdu-guard 功能
disable	关闭 edgeport bpdu-guard 功能
default	默认值

## 命令模式

端口配置模式

## 默认

默认关闭 BPDU Guard

## 使用说明

使用 `show spanning-tree` 可以查看 BPDU Guard 功能。

## 举例说明

以下命令展示如何配置边缘端口和在边缘端口上启用 `bpdu guard` 功能：

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# spanning-tree edgeport
Switch(config-if)# spanning-tree edgeport bpdu-guard enable
```

## 相关命令

无

## 2.9.18 spanning-tree edgeport bpdu-filter

使用该命令在边缘端口上启用 BPDU filter 功能，使用 `no` 命令将该特性恢复默认值。

## 命令语法

`spanning-tree edgeport bpdu-filter (enable | disable | default)`

`no spanning-tree edgeport bpdu-filter`

enable	启用 edgeport bpdu-filter 功能
disable	关闭 edgeport bpdu-filter 功能
default	默认值

## 命令模式

端口配置模式

## 默认

无



## 使用说明

使用 `show spanning tree` 命令显示 BPDU filter 的配置。

如果 `bpdu-guard` 和 `bpdu-filter` 一起配置，则 `bpdu-filter` 起作用。

## 举例说明

以下命令展示如何在边缘端口上启用和关闭 `bpdu-filter` 功能：

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# spanning-tree edgeport
Switch(config-if)# spanning-tree edgeport bpdu-filter
Switch(config-if)# no spanning-tree edgeport bpdu-filter
```

## 相关命令

Show spanning-tree interface

### 2.9.19 spanning-tree guard root

使用该命令开启 Root Guard 功能，使用 `no` 命令关闭这个功能。当打开这个功能后，交换机将不会接收高优先级的 BPDU 报文。

## 命令语法

```
spanning-tree guard root
no spanning-tree guard root
```

## 命令模式

端口配置模式

## 默认

默认关闭 Root guard

## 使用说明

当配置该功能后，如果在端口上收到高优先级的 BPDU，如果运行 STP 协议就会转入监听状态，如果运行 RSTP 和 MSTP 就会转入阻塞状态。

## 举例说明

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# spanning-tree guard root
Switch(config-if)# no spanning-tree guard root
```

## 相关命令

无

### 2.9.20 spanning-tree guard loop

使用该命令开启 `loop guard` 功能。当打开这个功能后，交换机能够防止在网络中形成数据转发环路的形成。使用 `no` 命令关闭这个功能。

## 命令语法

```
spanning-tree guard loop
```

```
no spanning-tree guard loop
```

## 命令模式

端口配置模式

## 默认

默认关闭 `loop guard`

## 使用说明

`loop guard` 功能需要在非指定端口上启用。

当非指定端口上启用了 `loop guard` 功能，并且在 `max_age` 时间内没有收到 BPDU 报文，该端口将会进入 `loop-inconsistent` 阻塞状态，而不是监听-学习-转发一系列的状态转换。一旦端口进入 `loop-inconsistent` 状态，该端口将不能转发业务数据。

## 举例说明

以下命令展示了如何启用和关闭 `guard loop` 功能：

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# spanning-tree guard loop
Switch(config-if)# no spanning-tree guard loop
```

## 相关命令

```
spanning-tree guard root
```

### 2.9.21 spanning-tree force-version

使用该命令指定 STP 的版本，使用 `no` 命令将 STP 的版本恢复默认值。对于 STP 协议，版本号必须小于 2；对于 RSTP 协议，版本号范围是 0-2；对于 MSTP 协议，版本号是 0-3。

## 命令语法

spanning-tree force-version *number*

no spanning-tree force-version

number	版本号 (取值范围 0 为 STP, 1 为 Not supported, 2 为 RSTP, 3 为 MSTP)
--------	---

## 命令模式

端口配置模式

## 默认

STP 默认值为 0, RSTP 默认值为 2, MSTP 默认值为 3

## 使用说明

无

## 举例说明

使用以下命令指定和恢复 STP 的版本:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# spanning-tree force-version 1
Switch(config-if)# no spanning-tree force-version
```

## 相关命令

无

## 2.9.22 spanning-tree restricted-tcn

使用该命令限制 TCN 消息的转发, 使用 no 命令关闭这种限制。

## 命令语法

spanning-tree restricted-tcn

no spanning-tree restricted-tcn

## 命令模式

端口配置模式

## 默认

默认行为关闭这种限制

## 使用说明

无

## 举例说明

以下示例展示如何配置限制 TCN 消息转发及如何关闭这种限制：

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# spanning-tree restricted-tcn
Switch(config-if)# no spanning-tree restricted-tcn
```

## 相关命令

无

## 2.9.23 spanning-tree restricted-role

使用该命令限制端口被选为根端口，使用 `no` 命令关闭这种限制。

## 命令语法

```
spanning-tree restricted-role
no spanning-tree restricted-role
```

## 命令模式

端口配置模式

## 默认

默认不限制端口被选为根端口

## 使用说明

无

## 举例说明

以下示例展示了如何限制端口成为根端口或如何关闭这种限制：

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# spanning-tree restricted-role
Switch(config-if)# no spanning-tree restricted-role
```

## 相关命令

无

### 2.9.24 spanning-tree tc-protection

使用该命令启用 TC 消息的保护，使用 `no` 命令关闭这种限制。当启用 TC 保护时，在每个 `hello-time` 间隔内，处理的 TC 消息数目不大于系统的 TC 保护上限。

## 命令语法

```
spanning-tree tc-protection  
no spanning-tree tc-protection
```

## 命令模式

全局配置模式

## 默认

默认行为为关闭这种限制

## 使用说明

无

## 举例说明

以下示例展示如何配置限制 TC 消息保护及如何关闭这种限制：

```
Switch# configure terminal  
Switch(config)# spanning-tree tc-protection  
Switch(config)# no spanning-tree tc-protection
```

## 相关命令

无

### 2.9.25 spanning-tree tc-protection threshold

使用该命令配置 TC 消息保护的上限值，使用 `no` 命令将上限值恢复为 1。当启用 TC 保护时，在每个 `hello-time` 间隔内，处理的 TC 消息数目不大于系统的 TC 保护上限。

## 命令语法

```
spanning-tree tc-protection threshold number  
no spanning-tree tc-protection threshold
```

number	TC 消息保护的上限值，取值范围是 1-255，默认值为 1
--------	--------------------------------

## 命令模式

全局配置模式

## 默认

默认 TC 消息保护的上限值为 1

## 使用说明

无

## 举例说明

以下示例展示如何配置限制 TC 消息保护上限：

```
Switch# configure terminal
Switch(config)# spanning-tree tc-protection threshold 255
```

## 相关命令

无

## 2.9.26 spanning-tree mode

使用该命令配置 STP 模式或 RSTP 模式或 MSTP 模式。

## 命令语法

spanning-tree mode (stp|rstp|mstp)

## 命令模式

全局配置模式

## 默认

默认模式是 STP 模式

## 用法

无

## 举例说明

```
Switch# configure terminal
Switch(config)# spanning-tree mode mstp
```

## 相关命令

无

### 2.9.27 spanning-tree instance priority

使用该命令配置某个用例的端口优先权值，使用 `no` 命令将优先权值恢复成默认值。

## 命令语法

```
spanning-tree instance instance-id port-priority priority
```

```
no spanning-tree instance instance-id port-priority
```

instance-id	用例号
priority	配置端口优先权值，取值范围 0~240

## 命令模式

端口配置模式

## 默认

默认值为 128。

## 使用说明

MSTP 协议使用该优先权值作为一个标准来判断端口是否作为某个用例的根端口。优先权值较小的优先。如果优先权值一样，还会比较端口号。可以配值为 0-240，优先权值必须是 16 的倍数。

## 举例说明

以下示例展示了如何配置 `eth-0-1` 上用例 3 的优先权值为 112：

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# spanning-tree instance 3 port-priority 112
Switch(config-if)# no spanning-tree instance 3 port-priority
```

## 相关命令

无

### 2.9.28 spanning-tree instance path-cost

使用该命令配置端口上 `path-cost`，使用 `no` 命令将该 `path-cost` 恢复成默认值。

## 命令语法

`spanning-tree instance instance-id path-cost cost`

`no spanning-tree instance instance-id path-cost`

instance-id	用例号
cost	如果协议类型是 dot1t, cost 取值范围 1~200000000; 如果协议类型是 dot1d-1998, cost 取值范围是 1~65535

## 命令模式

端口配置模式

## 默认

默认值根据端口速率确定

## 使用说明

必须首先配置用例, 然后才能配置某个端口上的 `path-cost`。

## 举例说明

以下示例展示了如何配置用例和相关的 `path-cost` 值:

```
Switch# configure terminal
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# instance 3 vlan 3
Switch(config-mst)# exit
Switch(config)# interface eth-0-1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 3
Switch(config-if)# spanning-tree instance 3 path-cost 1000
Switch(config-mst)# exit
Switch(config)# interface eth-0-1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 3
Switch(config-if)# spanning-tree instance 3 path-cost 1000
```

## 相关命令

无

### 2.9.29 spanning-tree instance restricted-tcn

使用该命令限制某个用例中 TCN 的广播, 使用 `no` 命令关闭这种限制。



## 命令语法

```
spanning-tree instance instance-id restricted-tcn  
no spanning-tree instance instance-id restricted-tcn
```

instance-id	用例号
-------------	-----

## 命令模式

端口配置模式

## 默认

默认不限制用例中 TCN 的广播

## 使用说明

无

## 举例说明

以下示例展示了如何在用例 2 中限制端口 eth-0-1 转发 TCN 报文：

```
Switch# configure terminal  
Switch(config)# interface eth-0-1  
Switch(config-if)# spanning-tree instance 2 restricted-tcn
```

## 相关命令

无

### 2.9.30 spanning-tree instance restricted-role

使用该命令限制在用例中某个端口不能成为根端口，使用 no 命令关闭这种限制。

## 命令语法

```
spanning-tree instance instance-id restricted-role  
no spanning-tree instance instance-id restricted-role
```

instance-id	用例号
-------------	-----

## 命令模式

端口配置模式

## 默认

默认行为不做任何限制。

## 使用说明

无

## 举例说明

以下示例展示了如何在用例 2 中限制端口 eth-0-1 的角色：

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# spanning-tree instance 2 restricted-role
```

## 相关命令

无

## 2.9.31 spanning-tree mst configuration

使用该命令进入 Mst 配置模式。

## 命令语法

```
spanning-tree mst configuraiton
```

## 命令模式

全局配置模式

## 默认

无

## 使用说明

无

## 举例说明

以下示例展示如何进入 mst 配置模式：

```
Switch# configure terminal
Switch(config)# spanning-tree Mst configuration
Switch(config-mst)# instance 1 vlan 2
```

## 相关命令

无

### 2.9.32 instance

使用该命令创建 MSTP 用例，并将 VLAN 关联到 MST 用例。

## 命令语法

**instance** instance-id **vlan** vlan-id

**no instance** instance-id **vlan** vlan-id

instance-id	用例标识，最多支持 64 个用例
vlan-id	VLAN ID，取值范围 1-4094

## 命令模式

MST 配置模式

## 默认

无

## 使用说明

当将 VLANs 映射到 MST 用例，这些 VLANs 应该已经配置，否则配置不会生效；当这些 VLANs 删除时，对应的 MST 用例将删除。

## 举例说明

以下示例展示了如何将用例 1 关联到 vlan 10:

```
Switch# configure terminal
Switch(config)# vlan database
Switch(config-vlan)# vlan 10
Switch(config-vlan)# exit
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# instance 1 vlan 10
```

## 相关命令

无

### 2.9.33 region

使用该命令创建 MSTP 域。

## 命令语法

*region name*  
*no region name*

name	指定 MSTP 域名，字符串长度最大为 32 个字节，区分大小写。
------	-----------------------------------

## 命令模式

MST 配置模式

## 默认

默认域名为空字符串

## 使用说明

无

## 举例说明

以下示例展示了如何将域名配成 Switch:

```
Switch# configure terminal
Switch(config)# vlan database
Switch(config-vlan)# vlan 10
Switch(config-vlan)# exit
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# region Switch
```

## 相关命令

无

### 2.9.34 revision

使用该命令创建一个 MSTP 版本号。

## 命令语法

*revision number*  
*no revision number*

number	版本号，取值范围是 0~65535
--------	-------------------

## 命令模式

MST 配置模式

## 默认

默认值为 0

## 使用说明

无

## 举例说明

以下示例展示了如何配置版本号：

```
Switch# configure terminal
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# revision 1
```

## 相关命令

无

## 2.9.35 clear spanning-tree detected protocols

使用该命令清除端口是否接收到 RSTP/MSTP 报文，再重新检测一次。

## 命令语法

clear spanning-tree detected protocols (interface *interface-id* | )

<b>interface interface-id</b>	端口名
-------------------------------	-----

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

以下示例展示了如何清除端口上是否接收到 RSTP/MSTP 状态，重新接收：

```
Switch# clear spanning-tree detected protocols interface eth-0-1
```

## 相关命令

无

## 2.9.36 clear spanning-tree disabled-port

使用该命令打开所有端口上 STP 功能。

## 命令语法

```
clear spanning-tree disabled-port
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

以下示例展示了如何打开所有端口上 STP 功能：

```
Switch# clear spanning-tree disabled-port
```

## 相关命令

无

## 2.9.37 show spanning-tree

使用该命令显示 STP 的详细信息，这个命令只显示 UP 端口的状态。

## 命令语法

```
show spanning-tree
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

以下示例展示了如何显示 STP 详细信息：

```
Switch# show spanning-tree
  Bridge up - Spanning Tree Enabled
Mode - Multiple spanning tree protocol
Path Cost Standard - dot1t
CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge Priority 32768
Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
Tx Hold Count 6
CIST Root Id 80008afa58e9cb00
CIST Reg Root Id 80008afa58e9cb00
CIST Bridge Id 80008afa58e9cb00
Edgeport bpdu-filter disabled
Edgeport bpdu-guard disabled
eth-0-1: Port 1 - Id 8001 - Role Designated - State Forwarding
eth-0-1: Designated External Path Cost 0 -Internal Path Cost 0
eth-0-1: Configured Path Cost 20000 - Add type Explicit ref count 1
eth-0-1: Designated Port Id 8001 - CIST Priority 128
eth-0-1: CIST Root 80008afa58e9cb00
eth-0-1: Regional Root 80008afa58e9cb00
eth-0-1: Designated Bridge 80008afa58e9cb00
eth-0-1: Message Age 0 - Max Age 20
eth-0-1: CIST Hello Time 2 - Forward Delay 15
eth-0-1: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
eth-0-1: Forward-transitions 2
eth-0-1: BPDU sent 373 - BPDU received 0
eth-0-1: Version Multiple spanning tree protocol - Received None - Send MSTP
eth-0-1: No edgeport configured - Current edgeport off
eth-0-1: Edgeport bpdu-guard Default - Current edgeport bpdu-guard off
eth-0-1: Edgeport bpdu-filter Default - Current edgeport bpdu-filter off
eth-0-1: No root guard configured - Current root guard off
eth-0-1: No loop guard configured - Current loop guard off
eth-0-1: Configured Link Type auto - Current point-to-point
```

## 相关命令

无

### 2.9.38 show spanning-tree interface

使用该命令显示指定端口上 STP 的详细信息。

## 命令语法

show spanning-tree interface *interface-id* (brief|)

interface-id	端口名
brief	生成树简要信息

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

以下示例展示了如何显示端口 **eth-0-1** 上 STP 的详细信息：

```
Switch# show spanning-tree interface eth-0-1
Bridge up - Spanning Tree Enabled
Mode - Multiple spanning tree protocol
Path Cost Standard - dot1t
CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge Priority 32768
Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
Tx Hold Count 6
CIST Root Id 80008afa58e9cb00
CIST Reg Root Id 80008afa58e9cb00
CIST Bridge Id 80008afa58e9cb00
Edgeport bpdu-filter disabled
Edgeport bpdu-guard disabled
eth-0-1: Port 1 - Id 8001 - Role Designated - State Forwarding
eth-0-1: Designated External Path Cost 0 -Internal Path Cost 0
eth-0-1: Configured Path Cost 20000 - Add type Explicit ref count 1
eth-0-1: Designated Port Id 8001 - CIST Priority 128
eth-0-1: CIST Root 80008afa58e9cb00
eth-0-1: Regional Root 80008afa58e9cb00
eth-0-1: Designated Bridge 80008afa58e9cb00
eth-0-1: Message Age 0 - Max Age 20
eth-0-1: CIST Hello Time 2 - Forward Delay 15
eth-0-1: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
eth-0-1: Forward-transitions 2
eth-0-1: BPDU sent 352 - BPDU received 0
eth-0-1: Version Multiple spanning tree protocol - Received None - Send MSTP
```



```

eth-0-1: No edgeport configured - Current edgeport off
eth-0-1: Edgeport bpdu-guard Default - Current edgeport bpdu-guard off
eth-0-1: Edgeport bpdu-filter Default - Current edgeport bpdu-filter off
eth-0-1: No root guard configured - Current root guard off
eth-0-1: No loop guard configured - Current loop guard off
eth-0-1: Configured Link Type auto - Current point-to-point

```

## 相关命令

无

### 2.9.39 show spanning-tree brief

以下命令用于显示 STP 的简略信息。

## 命令语法

```
show spanning-tree brief
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

以下示例展示了如何显示 STP 的简略信息：

```

Switch# show spanning-tree brief
Multiple spanning tree protocol Enabled
Root ID      Priority    32768 (0x8000)
              Address    8afa.58e9.cb00
              Hello Time 2 sec    Max Age 20 sec Forward Delay 15 sec
Bridge ID    Priority    32768 (0x8000)
              Address    8afa.58e9.cb00
              Hello Time 2 sec    Max Age 20 sec Forward Delay 15 sec
              Aging Time 300 sec

Interface    Role          State          Cost          Priority.Number  Type
-----
eth-0-1      Designated   Forwarding     20000          128.1            P2p
eth-0-2      Designated   Forwarding     20000          128.2            P2p

```

## 相关命令

无

## 2.9.40 show spanning-tree disabled-port

使用该命令显示关闭 STP 功能的接口。

### 命令语法

```
show spanning-tree disabled-port
```

### 命令模式

特权模式

### 默认

无

### 使用说明

无

### 举例说明

以下示例展示了如何显示关闭 STP 协议的接口：

```
Switch# show spanning-tree disabled-port
Interface
-----
eth-0-1
```

### 相关命令

无

## 2.9.41 show spanning-tree mst

使用该命令显示 MSTP 的相关信息。

### 命令语法

```
show spanning-tree mst
```

### 命令模式

特权模式

### 默认

无

## 使用说明

无

## 举例说明

以下用例展示了如何显示了如何显示 MSTP 相关信息：

```
Switch#show spanning-tree mst
Bridge up - Spanning Tree Enabled
Mode - Multiple spanning tree protocol
Path Cost Standard - dot1t
CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge Priority 32768
Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
Tx Hold Count 6
CIST Root Id 80008afa58e9cb00
CIST Reg Root Id 80008afa58e9cb00
CIST Bridge Id 80008afa58e9cb00
Edgeport bpdu-filter disabled
Edgeport bpdu-guard disabled

Instance Interface VLAN

0 :                               1, 3
1 :      eth-0-2                   2
```

## 相关命令

无

### 2.9.42 show spanning-tree mst config

使用该命令显示 MST 的配置信息。

## 命令语法

```
show spanning-tree mst config
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

以下用例展示了如何显示 MST 的配置信息：

```
Switch#show spanning-tree mst config
MSTP Configuration Information:
-----
Format Id      : 0
Name           : switch
Revision Level : 0
Digest         : 0x3AB68794D602FDF43B21C0B37AC3BCA8
Instances configured 1
-----

Instance Vlans mapped
-----
0          1, 3
1          2
-----
```

## 相关命令

无

## 2.9.43 show spanning-tree mst detail

使用该命令显示 MSTP 的详细信息。

## 命令语法

```
show spanning-tree mst detail (interface interface-id | )
```

<b>interface interface-id</b>	端口名
-------------------------------	-----

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

以下示例展示了如何显示 MSTP 的详细信息：

```
Switch#show spanning-tree mst detail interface eth-0-1
Bridge up - Spanning Tree Enabled
```

```

Mode - Multiple spanning tree protocol
Path Cost Standard - dot1t
CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge Priority 32768
Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
Tx Hold Count 6
CIST Root Id 80008afa58e9cb00
CIST Reg Root Id 80008afa58e9cb00
CIST Bridge Id 80008afa58e9cb00
Edgeport bpdu-filter disabled
Edgeport bpdu-guard disabled
eth-0-1: Port 1 - Id 8001 - Role Designated - State Forwarding
eth-0-1: Designated External Path Cost 0 -Internal Path Cost 0
eth-0-1: Configured Path Cost 20000 - Add type Explicit ref count 1
eth-0-1: Designated Port Id 8001 - CIST Priority 128
eth-0-1: CIST Root 80008afa58e9cb00
eth-0-1: Regional Root 80008afa58e9cb00
eth-0-1: Designated Bridge 80008afa58e9cb00
eth-0-1: Message Age 0 - Max Age 20
eth-0-1: CIST Hello Time 2 - Forward Delay 15
eth-0-1: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
eth-0-1: Forward-transitions 2
eth-0-1: BPDU sent 247 - BPDU received 0
eth-0-1: Version Multiple spanning tree protocol - Received None - Send MSTP
eth-0-1: No edgeport configured - Current edgeport off
    
```

### 相关命令

无

## 2.9.44 show spanning-tree mst instance

使用该命令显示一个特定用例的 MSTP 信息。

### 命令语法

show spanning-tree mst instance *instance-id* (interface *interface-id* |)

instance-id	用例号
<b>interface</b> interface-id	端口名

### 命令模式

特权模式

### 默认

无

## 使用说明

无

## 举例说明

以下示例展示了如何显示用例 2 中 MSTP 的相关信息：

```
Switch#show spanning-tree mst instance 2
MSTI Root Path Cost 0 - MSTI Root Port 0
MSTI Root Id 8002e083bce89601
MSTI Bridge Id 8002e083bce89601
MSTI Bridge Priority 32768
eth-0-48: Port 48 - Id 8030 - Role Disabled - State Discarding
eth-0-48: Designated Internal Path Cost 0 - Designated Port Id 0
eth-0-48: Configured Internal Path Cost 20000
eth-0-48: Configured CST External Path cost 20000
eth-0-48: CST Priority 128 - MSTI Priority 128
eth-0-48: Designated Root 0000000000000000
eth-0-48: Designated Bridge 0000000000000000
eth-0-48: Message Age 0 - Max Age 0
eth-0-48: Hello Time 2 - Forward Delay 15
eth-0-48: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0

eth-0-1: Port 1 - Id 8001 - Role Disabled - State Discarding
eth-0-1: Designated Internal Path Cost 0 - Designated Port Id 0
eth-0-1: Configured Internal Path Cost 20000
eth-0-1: Configured CST External Path cost 20000
eth-0-1: CST Priority 128 - MSTI Priority 128
eth-0-1: Designated Root 0000e083bce89601
eth-0-1: Designated Bridge 0000e083bce89601
eth-0-1: Message Age 0 - Max Age 0
eth-0-1: Hello Time 2 - Forward Delay 15
eth-0-1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
```

## 相关命令

无

### 2.9.45 show spanning-tree mst interface

使用该命令显示某个特定端口上 MSTP 的详细信息。

## 命令语法

```
show spanning-tree mst interface interface-id
```

interface-id	端口名
--------------	-----

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

以下示例展示了如下显示端口 `eth-0-1` 上 MSTP 的详细配置：

```
Switch# show spanning-tree mst interface eth-0-1
Bridge up - Spanning Tree Enabled
Mode - Multiple spanning tree protocol
Path Cost Standard - dot1t
CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge Priority 32768
Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
Tx Hold Count 6
CIST Root Id 8000be8c722f7f00
CIST Reg Root Id 8000be8c722f7f00
CIST Bridge Id 8000be8c722f7f00
Edgeport bpdu-filter disabled
Edgeport bpdu-guard disabled
Loop guard configured disabled

Instance Interface VLAN

0 :                1, 4-100
1 :      eth-0-1    2
2 :      eth-0-1    3
```

## 相关命令

无

### 2.9.46 show spanning-tree mst brief

使用该命令显示 MSTP 的简略信息。

## 命令语法

```
show spanning-tree mst brief (interface interface-id | instance instance-id )
```

<b>interface interface-id</b>	端口名
-------------------------------	-----

<b>instance instance-id</b>	用例号
-----------------------------	-----

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

以下示例展示了如何显示 MSTP 的简略配置信息：

```
Switch#show spanning-tree mst brief
##### MST0: Vlans: 1
Multiple spanning tree protocol Enabled
Root ID      Priority    32768 (0x8000)
              Address    e083.bce8.9601
              Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID    Priority    32768 (0x8000)
              Address    e083.bce8.9601
              Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
              Aging Time 300 sec
Interface    Role          State          Cost          Priority.Number  Type
-----
##### MST2: Vlans: 2
Root ID      Priority    32770 (0x8002)
              Address    e083.bce8.9601
Bridge ID    Priority    32770 (0x8002)
              Address    e083.bce8.9601
Interface    Role          State          Int-Cost      Priority.Number  Type
-----
eth-0-48     Disabled     Discarding     20000         128.48          P2p
eth-0-1      Disabled     Discarding     20000         128.1           P2p
##### MST15: Vlans: 15
Root ID      Priority    32783 (0x800f)
              Address    e083.bce8.9601
Bridge ID    Priority    32783 (0x800f)
              Address    e083.bce8.9601
Interface    Role          State          Int-Cost      Priority.Number  Type
-----
eth-0-48     Disabled     Discarding     20000         128.48          P2p
eth-0-1      Disabled     Discarding     20000         128.1           P2p
```



## 相关命令

无

### 2.9.47 spanning-tree instance forward

使用该命令可配置某端口上 STP 用例的状态为固定转发态。

## 命令语法

```
spanning-tree instance instance-id forward
```

```
no spanning-tree instance instance-id forward
```

instance-id	实例号
-------------	-----

## 命令模式

端口配置模式

## 默认

无

## 使用说明

无

## 举例说明

以下示例展示了如何在端口 eth-0-1 上设置实例 1 的状态为固定转发态：

```
Switch# configure terminal
Switch(config)# spanning-tree mode mstp
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# instance 1 vlan 2
Switch(config)# interface eth-0-1
Switch(config-if)# spanning-tree instance 1 forward
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no spanning-tree instance 1 forward
```

## 相关命令

无

## 2.10 Flow control 命令

### 2.10.1 flowcontrol send

使用此命令在端口上使能发送 flowcontrol 的功能。

#### 命令语法

```
flowcontrol send ( on | off )
```

on	启用 flowcontrol 发送功能
off	关闭 flowcontrol 发送功能

#### 命令模式

接口配置模式

#### 默认

不启用

#### 使用说明

该功能只在物理口有效。

#### 举例说明

下面的例子表明如何在端口上启用发送 flowcontrol 的功能：

```
Switch(config-if)# flowcontrol send on
```

#### 相关命令

```
flowcontrol receive on
```

### 2.10.2 flowcontrol receive

使用此命令在端口上使能接收 flowcontrol 的功能。

#### 命令语法

```
flowcontrol receive ( on | off )
```

on	启用 flowcontrol 接收功能
----	---------------------

off	关闭 flowcontrol 接收功能
-----	---------------------

## 命令模式

接口配置模式

## 默认

不启用

## 使用说明

该功能只在物理口有效。

## 举例说明

下面的例子表明如何在端口上启用接收 flowcontrol 的功能：

```
Switch(config-if)# flowcontrol receive on
```

## 相关命令

flowcontrol send on

## 2.10.3 show flowcontrol

使用此命令查看 flowcontrol 的具体信息。

## 命令语法

```
show flowcontrol (INTERFACE|)
```

INTERFACE	端口名（可选）
-----------	---------

## 命令模式

特权模式

## 默认

无

## 使用说明

使用这个命令查看每个端口的 flowcontrol 能力和 pause 帧的信息。

## 举例说明

下面的例子表明如何查看 flowcontrol 的信息：

```
Switch# show flowcontrol
```

## 相关命令

无

## 2.11 Priority-based flow control 命令

### 2.11.1 priority-based flowcontrol enable

使用此命令在端口上使能 priority-based flowcontrol 的功能。

## 命令语法

```
priority-flow-control mode (on | auto)  
no priority-flow-control
```

## 命令模式

接口配置模式

## 默认

不启用

## 使用说明

该功能只在物理口有效，默认在 priority 3 上使能 priority-based flowcontrol 的功能。

## 举例说明

下面的例子表明如何在端口上强制启用 priority-based flowcontrol 的功能（不与对端协商）：

```
Switch(config-if)# priority-flow-control mode on
```

下面的例子表明如何在端口上启用 priority-based flowcontrol 的功能（需要与对端协商）：

```
Switch(config-if)# priority-flow-control mode auto
```

## 相关命令

```
priority-flow-control enable priority  
lldp tlv 8021-org-specific dcbx
```

## 2.11.2 priority-flow-control enable priority

使用此命令在端口上的哪个 priority 上使能 priority-based flowcontrol 的功能。

### 命令语法:

```
priority-flow-control enable priority {0|1|2|3|4|5|6|7}
no priority-flow-control enable priority {0|1|2|3|4|5|6|7}
```

### 命令模式

接口配置模式

### 默认

不启用

### 使用说明

该功能只在物理口有效。

### 举例说明

下面的例子表明如何在端口上的哪些 priorities 上使能 priority-based flowcontrol 的功能:

```
Switch(config-if)# priority-flow-control enable priority 1 3 4 7
```

### 相关命令

```
priority-flow-control mode (on | auto)
lldp tlv 8021-org-specific dcbx
```

## 2.11.3 show priority-flow-control

使用此命令查看 priority-based flowcontrol 的状态信息。

### 命令语法:

```
show priority-flow-control (INTERFACE | )
```

INTERFACE	端口名 (可选)
-----------	----------

### 命令模式

特权模式

### 默认

无

## 使用说明

使用这个命令查看每个端口上 priority-based flowcontrol 状态信息。

## 举例说明

下面的例子表明如何查看 priority-based flowcontrol 的状态信息：

```
Switch# show priority-flow-control
Port          PFC-enable          PFC-enable on priority
              admin    oper              admin    oper
-----
eth-0-1       off     off              off     off
eth-0-2       off     off              off     off
eth-0-3       off     off              off     off
eth-0-4       off     off              off     off
```

## 相关命令

无

### 2.11.4 show priority-flow-control statistics

使用此命令查看 priority-based flowcontrol 的统计信息。

## 命令语法:

```
show priority-flow-control statistics (INTERFACE |)
```

INTERFACE	端口名（可选）
-----------	---------

## 命令模式

特权模式

## 默认

无

## 使用说明

使用这个命令查看每个端口上 priority-based flowcontrol 统计信息。

## 举例说明

下面的例子表明如何查看 priority-based flowcontrol 的统计信息：

```
Switch# show priority-flow-control statistics
Port          RxPause          TxPause
-----
eth-0-1       0                 0
eth-0-2       0                 0
```

eth-0-3	0	0
eth-0-4	0	0

## 相关命令

无

## 2.12 Layer 2 Protocols Tunneling 命令

### 2.12.1 l2protocol enable

使用该命令开启二层协议报文透传功能，使用对应的 **no** 命令关闭该功能。

## 命令语法

```
l2protocol enable
no l2protocol enable
```

## 命令模式

全局配置模式

## 默认

无

## 使用说明

使用该命令开启二层协议报文透传功能。

## 举例说明

```
全局开启二层协议报文透传功能：
Switch(config)# l2protocol enable
```

## 相关命令

```
show l2protocol
```

### 2.12.2 l2protocol tunnel-dmac

使用该命令配置给二层协议报文添加的二层头的目的 MAC 位址，使用 **no** 命令将该 MAC 地址恢复为默认值。

## 命令语法

```
l2protocol tunnel-dmac MAC
```

```
no l2protocol tunnel-dmac
```

MAC	为二层协议报文添加的二层头的目的 MAC，取值范围 <b>0100.0CCD.CDD0-D2 or 010F.E200.0003</b>
-----	---

## 命令模式

全局配置模式

## 默认

无

## 使用说明

使用该命令配置给二层协议报文添加二层头的目的 MAC 位址，默认值为 0100.0CCD.CDD0。

## 举例说明

使用以下配置给二层协议报文添加的二层头目的 MAC 位址指定为 010F.E200.0003:

```
Switch(config)# l2protocol tunnel-dmac 010F.E200.0003
```

## 相关命令

```
show l2protocol
```

### 2.12.3 l2protocol mac 1

使用该命令配置可透传的二层协议报文地址。

## 命令语法

```
l2protocol mac 1 MAC mask MASK
```

```
no l2protocol mac 1
```

MAC	取值范围 0180.C200.0000 ~ 0180.C2FF.FFFF 0180.C200.0000~0180.C200.003F 这段 MAC 已经被系统的其他功能使用，因此无法起透传。
MASK	取值范围 FFFF.FF00.0000-FFFF.FFFF.FFFF



## 命令模式

全局配置模式

## 默认

无

## 使用说明

使用该命令配置可透传的二层协议报文地址。

## 举例说明

使用以下命令配置可透传的二层协议报文地址：

```
Switch (config)# l2protocol mac 1 0180.c222.0000 mask ffff.ffff.0000
```

## 相关命令

`l2protocol full-mac`

### 2.12.4 l2protocol mac <2-6>

使用该命令配置可透传的二层协议报文地址。

## 命令语法

`l2protocol mac MAC_NUM MAC`

`no l2protocol mac MAC_NUM`

MAC_NUM	两个地址段不应互相交迭
MAC	取值范围 0180.C200.0000 ~ 0180.C2FF.FFFF

## 命令模式

全局配置模式

## 默认

无

## 使用说明

使用该命令配置可透传的二层协议报文地址。

## 举例说明

使用以下命令配置可透传的二层协议报文地址：

```
Switch (config)# l2protocol mac 3 0180.c200.0000
```

## 相关命令

l2protocol full-mac

### 2.12.5 l2protocol

使用该命令配置进入该端口的二层协议报文是丢弃，正常处理还是透传。

## 命令语法

```
l2protocol (stp|slow-proto|dot1x|cfm|mac MAC_NUM | full-mac)(discard|peer|tunnel) (evc WORD |)
```

```
no l2protocol (stp|slow-proto|dot1x|cfm|mac MAC_NUM | full-mac)
```

stp	<b>MAC: 0180.c200.0000</b>
slow-proto	MAC: 0180.c200.0002, ethertype: 0x8809
dot1x	MAC: 0180.c200.0003, ethertype: 0x888e
cfm	ethertype: 0x8902
mac MAC_NUM	全局配置的以 0180.c2XX.XXXX 开头的二层协议报文地址段
discard	丢弃
peer	将二层协议报文正常处理
tunnel	从上联口出去时，给二层协议报文添加新的二层头，其中 mac da 为配置的 tunnel-dmac，vlan 为 evc 对应的 svlan；从其它 tunnel 端口出去时，不改变二层协议报文
full-mac	任意可配的二层报文地址段
WORD	EVC 名称

## 命令模式

端口配置模式

## 默认

无

## 使用说明

使用该命令配置进入该端口的二层协议报文是丢弃，正常处理还是透传。默认是送给对应协议模块正常处理。

## 举例说明

使用以下命令配置进入该端口的 STP 报文丢弃：

```
Switch (config-if)# l2protocol stp discard
```

使用以下命令配置进入该端口的慢协议报文透传：

```
Switch (config-if)# l2protocol slow-proto tunnel evc evc1
```

## 相关命令

无

## 2.12.6 l2protocol uplink enable

使用该命令配置二层协议报文透传时的上联口。

## 命令语法

```
l2protocol uplink enable
```

```
no l2protocol uplink enable
```

## 命令模式

端口配置模式

## 默认

无

## 使用说明

使用该命令配置二层协议报文透传时的上联口。从配置为 **tunnel** 的端口进来的二层报文，从上联口出去时会添加目的 **mac** 为 **tunnel dmac** 的二层头；从上联口进来的添加新二层头的报文，从 **tunnel** 端口出去时，会将二层头去掉。

## 举例说明

使用以下命令配置该端口在二层协议报文透传时为上联口：

```
Switch(config-if)# l2protocol uplink enable
```

## 相关命令

无

## 2.12.7 show l2protocol

使用该命令显示二层协议报文透传功能的配置。

### 命令语法

show l2protocol (interface *IFNAME* | tunnel-dmac )

interface <i>IFNAM</i>	界面名
tunnel-dmac	2层 tunnel 目的 MAC 位址

### 命令模式

特权模式

### 默认

无

### 使用说明

使用该命令显示二层协议报文透传功能的配置。

### 举例说明

以下命令显示了 eth-0-1 口二层协议报文透传功能的相关配置：

```
Switch # show l2protocol interface eth-0-1
Interface  PDU Address      MASK                Status  EVC
=====  =====  =====  =====  =====
eth-0-1    stp        ffff.ffff.ffff    Peer    N/A
eth-0-1    slow-proto ffff.ffff.ffff    Peer    N/A
eth-0-1    dot1x     ffff.ffff.ffff    Peer    N/A
```

以下命令显示了 2 层 tunnel 目的 MAC 位址为 0100.0ccd.cdd0 的透传功能的相关配置：

```
Switch # show l2protocol tunnel-dmac
Layer2 protocols tunnel destination MAC address is 0100.0ccd.cdd0
```

### 相关命令

无

## 2.12.8 l2protocol cos

使用该命令配置新加二层头的 vlan tag 中的 Priority。

## 命令语法

```
l2protocol cos cos_value
```

```
no l2protocol cos
```

cos_value	vlan tag priority, <0-7>
-----------	--------------------------

## 命令模式

全局配置模式

## 默认

无

## 使用说明

使用该命令配置新加二层头的 vlan tag 中的 Priority，默认值为 0。

## 举例说明

使用以下命令配置新加二层头的 vlan tag 中的 Priority 为 7：

```
Switch(config)# l2protocol cos 7
```

## 相关命令

无

## 2.12.9 l2protocol full-mac

使用该命令配置可透传的二层协议报文地址。支持任意 MAC 地址。

## 命令语法

```
l2protocol full-mac MAC
```

```
no l2protocol full-mac
```

MAC	取值范围 0000.0000.0000 ~ FFFF.FFFF.FFFF
-----	--------------------------------------

## 命令模式

全局配置模式

## 默认

无

## 使用说明

当配置的 MAC 地址和 stp, slow-proto, dot1x 或 mac <1-4>地址重叠时, tunnel 选择的优先级为: stp > slow-proto > dot1x > full-mac > mac<1-4>。

当配置的 full-mac 地址和 l2protocol tunnel-dmac 地址重叠时, 重叠的 full-mac 地址无法 tunnel。

## 举例说明

使用以下命令配置可透传的二层协议报文地址:

```
Switch (config)# l2protocol full-mac 0100.0CCC.CCCC
```

## 相关命令

l2protocol mac

# 2.13 Storm Control 命令

## 2.13.1 storm-control

使用此命令在二层端口上配置风暴控制。

使用关键词 no 恢复设置为默认值。

## 命令语法

```
storm-control (broadcast | multicast | unicast) (level LEVEL| pps PPS)
```

```
no storm-control (broadcast | multicast | unicast)
```

<b>broadcast</b>	接口上启用广播控制
<b>multicast</b>	接口上启用组播控制
<b>unicast</b>	接口上启用未知单播控制
<b>level LEVEL</b>	设置报文占可用带宽的最大百分比, 范围<0.00-100.00>
<b>pps PPS</b>	设置每秒钟发送报文的最大数量, 范围<0-1000000000>

## 命令模式

端口配置模式

## 默认

关闭

## 使用说明

只能在二层端口上配置。

## 举例说明

设置广播报文占可用带宽的最大百分比为 30%:

```
Switch(config-if)# storm-control broadcast level 30
```

恢复端口默认设置:

```
Switch(config-if)# no storm-control broadcast
```

## 相关命令

```
show storm-control
```

## 2.13.2 show storm-control

使用此命令显示风暴控制的配置信息。

## 命令语法

```
show storm-control (interface INTERFACE )
```

<b>interface</b> INTERFACE	端口名（可选）
----------------------------	---------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

- 显示所有端口的风暴控制设置:

```
Switch# show storm-control
```

- 显示端口 **eth-0-1** 风暴控制设置:

```
Switch# show storm-control interface eth-0-1
```

## 相关命令

storm-control

### 2.13.3 ipg storm-control enable

使用此命令全局指定风暴控制是否计算帧间隙。

使用关键词 **no** 恢复此设置为默认值。

## 命令语法

```
ipg storm-control enable
```

```
no ipg storm-control enable
```

## 命令模式

全局配置模式

## 默认

关闭

## 使用说明

该命令只可以在全局配置模式中配置。

## 举例说明

配置风暴控制计算帧间隙:

```
Switch(config)# ipg storm-control enable
```

配置风暴控制计算帧间隙:

```
Switch(config)# no ipg storm-control enable
```

## 相关命令

无

## 2.14 Loopback Detection 命令

### 2.14.1 Loopback-detect enable

使用此命令在端口上使能 **loopback detection** 功能。



## 命令语法

**loopback-detect enable**  
**no loopback-detect enable**

## 命令模式

接口配置模式

## 默认

不启用

## 使用说明

使用该命令开启端口 loopback detection 功能。

## 举例说明

使能端口 eth-0-1 上的 loopback detection 功能：

```
DUT1(config)# interface eth-0-1
DUT1(config-if)# loopback-detect enable
```

## 相关命令

**show loopback-detect**

## 2.14.2 loopback-detect packet-interval

设置 loopback detection 报文的发送间隔，该配置对所有端口生效。默认的发送间隔为 5 秒。

## 命令语法

**loopback-detect packet-interval <1-300>**  
**no loopback-detect packet-interval**

**<1-300>** 以秒为单位，默认发送间隔为 5 秒。

## 命令模式

全局配置模式

## 默认

5 秒

## 使用说明

使用该命令设置 loopback detection 报文的发送间隔，配置后，对所有端口生效。

## 举例说明

设置 loopback detection 报文的发送间隔为 10 秒：

```
Switch(config)# loopback-detect packet-interval 10
```

## 相关命令

**show loopback-detect**

### 2.14.3 loopback-detect action

配置 loopback detection 的处理动作，可配置发送告警、关闭接口等处理动作。

## 命令语法

**loopback-detect action** {shutdown | trap }

**no loopback-detect action**

**shutdown**     检测到环回后，关闭接口。

**Trap**             检测到环回后，发送告警。

## 命令模式

接口配置模式

## 默认

Trap: 发送告警

## 使用说明

使用该命令设置 loopback detection 的处理动作，只有当 loopback detection 使能时，才能配置。

## 举例说明

配置接口 eth-0-1 的环回处理行为，当环回触发时，关闭接口：

```
Switch(config)#interface eth-0-1
Switch (config-if)# loopback-detect action shutdown
```

## 相关命令

**show loopback-detect**

**Loopback-detect enable**

## 2.14.4 loopback-detect packet vlan

配置对指定一个或多个指定 VLAN 进行环回检测。

### 命令语法

```
loopback-detect packet vlan <1-4094>
```

```
no loopback-detect packet vlan vlan-id
```

<1-4094> VLAN ID, 最多可指定 8 个.

### 命令模式

接口配置模式

### 默认

无指定 VLAN

### 使用说明

接口开启 Loopback Detection 功能后, 系统默认发送的为 Untag 检测报文, 即不对任何指定 VLAN 进行环回检测。当接口是以 Tagged 方式加入 VLAN, 接口发出去 Untag 检测报文在链路上会被丢弃, 接口将收不到环回回来的报文, 因此需要配置对指定的 VLAN 进行环回检测。

配置对指定 VLAN 的 Loopback Detection 功能, 接口会定时发送 1 份 Untagged 检测报文和多份带指定 VLAN Tag 的检测报文, 一个接口最多可发送 8 份带指定 VLAN Tag 的检测报文。

### 举例说明

在接口 eth-0-1 下, 配置对 VLAN 30 进行 loopback detection 检测:

```
Switch(config)#interface eth-0-1
Switch (config-if)# loopback-detect packet vlan 30
```

### 相关命令

```
show running-config
```

## 2.14.5 show loopback-detect

使用此命令查看 loopback detection 的配置信息和接口状态。

### 命令语法

```
show loopback-detect {interface interface-name | packet-interval}
```

**interface** *interface-name* (可选) 显示接口上的状态和配置信息.

**packet-interval** (可选) 显示 loopback detection 报文发送间隔时间.

## 命令模式

特权模式

## 默认

无

## 使用说明

可以查看 loopback detection 的配置信息，以及使能了 loopback detection 的接口状态。

## 举例说明

查看 loopback detection 配置信息，及使能了 loopback detection 的接口状态：

```
DUT1# show loopback-detect
Loopback detection packet interval(second): 5
Loopback detection recovery time(second): 15
Interface      Action      Status
eth-0-1        trap        NORMAL
eth-0-4        trap        NORMAL
eth-0-5        trap        NORMAL
eth-0-6        trap        NORMAL
```

## 相关命令

**loopback-detect action**

**loopback-detect enable**

## 2.15 MLAG 命令

### 2.15.1 mlag configuration

使用此命令来创建 mlag 模式，并进入 mlag 配置模式。

## 命令语法

```
mlag configuration
no mlag configuration
```

## 默认

无

## 命令模式

全局配置模式

## 使用说明

使用此命令来创建 **mlag** 模式，并进入 **mlag** 配置模式。使用 **exit** 命令可以退出该模式，同时并不影响该模式。使用 **no** 命令删除该模式，该模式下的所有配置均会同时被删除。

## 举例说明

```
DUT1(config)# mlag configuration
DUT1(config-mlag)# exit
```

## 相关命令

```
show mlag
```

### 2.15.2 peer-address

此命令用来指定 **mlag** 邻居的 **ipv4** 地址。

## 命令语法

```
peer-address ipv4_addr
no peer-address
```

<i>ipv4_addr</i>	MLAG 邻居的 <b>ipv4</b> 地址
------------------	-------------------------

## 默认

无

## 命令模式

MLAG 配置模式

## 使用说明

此命令用来指定 **mlag** 邻居的 **ipv4** 地址，根据此地址进行邻居的建立。

## 举例说明

```
DUT1(config-mlag)# peer-address 12.1.1.2
DUT1(config-mlag)#
```

## 相关命令

```
show mlag peer
```

## 2.15.3 peer-link

此命令用来指定连接 **mlag** 邻居所用的接口。

### 命令语法

```
peer-link IFNAME
```

```
no peer-link
```

IFNAME	连接 peer-link 所用的接口
--------	--------------------

注意: 只能设置成普通物理口或者聚合口

### 默认

无

### 命令模式

MLAG 配置模式

### 使用说明

此命令用来指定连接 **mlag** 邻居所使用的接口。要形成 **mlag** 邻居，需要有两台互联的设备，中间用来连接彼此的接口，称作 **peer-link**。**Peer-link** 上既承载了协议报文，也承载了数据报文。

### 举例说明

```
DUT1(config-mlag)# peer-link eth-0-9
DUT1(config-mlag)#
```

### 相关命令

```
show mlag
```

## 2.15.4 timers mlag

此命令用来指定 **keepalive** 发送间隔和 **holdtime** 时间。

### 命令语法

```
timers mlag keepalive holdtime
```

```
no timers mlag
```

keepalive	keepalive 间隔，数值范围从 1 到 65535 秒
holdtime	holdtime 间隔，数值范围从 1 到 65535 秒

注意: holdtime 时间不能小于 4 倍的 keepalive 间隔。

## 默认

keepalive 间隔默认 60 秒，holdtime 时间默认 240 秒。

## 命令模式

MLAG 配置模式

## 使用说明

此命令指定了 keepalive 间隔和 holdtime 时间。此设置将在下一次邻居建立时生效。在本地配置的 keepalive 和通过 open 报文里携带的远端 holdtime 的四分之一中，系统会选择较小数值的那个来进行计算。

## 举例说明

```
DUT1(config-mlag)# timers mlag 10 100
DUT1(config-mlag)#
```

## 相关命令

show mlag peer

## 2.15.5 reload-delay

此命令用来指定在 mlag 邻居设备重启之后，除 peer-link 之外的其他端口处于 error disable 的时间。

## 命令语法

reload-delay *period*

no reload-delay

period	端口处于 error disable 的时间。范围从 0 到 86400 秒
--------	--

注意：数值 0 代表不让端口处于 error disable 状态。

## 默认

300 秒。

## 命令模式

MLAG 配置模式

## 使用说明

当 MLAG 邻居重启时，除了 peer link 之外的其他端口会在 error disable 状态下保持一段时间。在这段时间里，可以让拓扑达到稳定的状态，比如 mlag 邻居状态机可以在这段时间里进行建立。此命令就是用来设置这个时间值的。

## 举例说明

```
DUT1(config-mlag)# reload-delay 100
DUT1(config-mlag)#
```

## 相关命令

```
show mlag
```

### 2.15.6 sync-orphan

此命令用来使能 mlag 邻居同步 orphan 端口上的 MAC 表项。

## 命令语法

```
sync-orphan
no sync-orphan
```

## 默认

使能

## 命令模式

MLAG 配置模式

## 使用说明

如果该命令没有配置，mlag 设备只会同步 mlag 组内的 MAC 表项。

## 举例说明

```
DUT1(config-mlag)# sync-orphan
DUT1(config-mlag)#
```

## 相关命令

```
show mlag
```

### 2.15.7 mlag

此命令用来在聚合口上指定 MLAG ID。

## 命令语法

```
mlag MLAGID
no mlag
```

MLAGID	MLAG ID 值。取值范围从 1 到 55
--------	------------------------



## 默认

无

## 命令模式

接口模式

## 使用说明

此命令用来在聚合口上指定 MLAG ID。每个聚合口只能指定一个 MLAG ID，每个 MLAG ID 只能同时被一个聚合口使用。

## 举例说明

```
DUT1(config)# interface agg1
DUT1(config-if)# mlag 1
```

## 相关命令

show mlag interface

## 2.15.8 clear mlag count

此命令用来清除 mlag 计数信息。

## 命令语法

```
clear mlag count
```

## 默认

无

## 命令模式

特权模式

## 使用说明

使用此命令用来清除 mlag 计数信息，可以使用 show mlag peer 来查看相关计数。

## 举例说明

```
DUT1# clear mlag count
DUT1# show mlag peer
MLAG neighbor is 12.1.1.2, MLAG version 1
MLAG state = Established, up for 00:00:39
Last read 00:00:15, hold time is 240, keepalive interval is 60 seconds
Received 0 messages,Sent 0 messages
Open      : received 0, sent 0
KAlive    : received 0, sent 0
```

```
Fdb sync : received 0, sent 0
Failover : received 0, sent 0
Conf      : received 0, sent 0
Syspri    : received 0, sent 0
Peer fdb  : received 0, sent 0
STP Total: received 0, sent 0
  Global  : received 0, sent 0
  Packet  : received 0, sent 0
  Instance: received 0, sent 0
  State   : received 0, sent 0
Connections established 1; dropped 0
Local host: 12.1.1.1, Local port: 61000
Foreign host: 12.1.1.2, Foreign port: 37335
remote_sysid: 0ecb.3030.1100
```

## 相关命令

```
show mlag peer
```

## 2.15.9 show mlag

此命令用来显示 mlag 的相关的配置信息。

## 命令语法

```
show mlag
```

## 默认

无

## 命令模式

特权模式

## 使用说明

使用此命令来显示 mlag 的相关配置信息。

## 举例说明

```
DUT1# show mlag
MLAG configuration:
-----
role          : Master
local_sysid   : 001e.080a.6fca
remote_sysid  : 0000.0000.0000
mlag_sysid    : 001e.080a.6fca
local_syspri  : 32768
remote_syspri : 0
mlag_syspri  : 32768
peer-link     : -
peer conf     : No
```

```
reload-delay : 300
```

## 相关命令

mlag configuration

### 2.15.10 show mlag peer

此命令用来显示 mlag 邻居信息。

## 命令语法

```
show mlag peer
```

## 默认

无

## 命令模式

特权模式

## 使用说明

使用此命令来显示 mlag 邻居信息。

## 举例说明

```
DUT1# show mlag peer
MLAG neighbor is 12.1.1.2, MLAG version 1
MLAG state = Established, up for 4d02h14m
Last read 00:00:29, hold time is 240, keepalive interval is 60 seconds
Received 6835 messages, Sent 7185 messages
Open      : received 1, sent 2
KAlive    : received 6831, sent 6830
Fdb sync  : received 0, sent 0
Failover  : received 0, sent 87
Conf      : received 1, sent 1
STP Total: received 2, sent 265
  Global  : received 2, sent 3
  Packet  : received 0, sent 0
  Instance: received 0, sent 0
  State   : received 0, sent 262
Connections established 1; dropped 0
Local host: 12.1.1.1, Local port: 61000
Foreign host: 12.1.1.2, Foreign port: 34283
remote_sysid: 5e26.6a03.d400
```

## 相关命令

peer-address

## 2.15.11 show mlag interface

此命令用来显示 mlag 接口信息。

### 命令语法

```
show mlag interface
```

### 默认

无

### 命令模式

特权模式

### 使用说明

使用此命令来显示 mlag 接口信息。

### 举例说明

```
DUT1# show mlag interface
mlagid  local-if  local-state  remote-state
1        agg1    up          up
2        agg2    up          up
```

### 相关命令

**mlag** MLAGID

## 2.16 PoE 命令

### 2.16.1 power inline enable

打开全局 PoE 供电功能。

### 命令语法

```
power inline enable
no power inline enable
```

### 命令模式

全局配置模式

## 默认

全局供电状态打开

## 使用说明

全局关闭后，不论端口的供电状态是打开还是关闭，均不会对外供电。

## 举例说明

在全局启用 PoE:

```
Switch(config)# power inline enable
```

## 2.16.2 power inline enable

打开端口 PoE 供电功能。

## 命令语法

```
power inline enable [ auto | static ]
```

```
no power inline enable
```

## 命令模式

端口配置模式

## 默认

端口供电状态打开

## 使用说明

使用时：自动检测。处于该状态时，PSE 自动检测 PD，并自动进行分类，然后根据分类进行供电。当 PSE 检测到有 PD 连接时，如果此时有足够的剩余功率，则给该 PD 指定的输出功率，并更新 LED 的指示；如果没有足够的功率，则由功率分配机制决定是否供电。当在该状态正常供电过程中，PD 有额外申请功率并超过最高设定阈值，则断开对该 PD 的供电，并更新 LED 的指示。当正常断开 PD 与 PSE 的连接时，则 PSE 停止对外供电，并更新 LED 的指示。

关闭时：禁止供电。关闭 PSE 供电功能，无论是否有 PD 连接都不对其进行供电。此时端口为普通以太网的数据端口，不影响数据的转发。

## 举例说明

在端口模式下启用 PoE:

```
Switch (config)# interface eth-0-1
```

```
Switch(config-if)# power inline enable
```

### 2.16.3 power inline legacy

设定是否对非 IEEE 标准 PD 进行供电。

#### 命令语法

```
power inline legacy enable  
no power inline legacy enable
```

#### 命令模式

端口配置模式

#### 默认

不对非 IEEE 标准 PD 供电

#### 使用说明

打开该功能时，交换机可以兼容非 IEEE 标准的 PD，并对其进行正常供电。

#### 举例说明

在接口下启用 legacy:

```
Switch (config-if)# power inline legacy enable
```

### 2.16.4 power inline max

设定 PoE 电源的全局最大输出功率。

#### 命令语法

```
power inline max max-wattage  
no power inline max
```

max-wattage	最大功率值。单位为 W，粒度为 1W，全局可设置范围为 37~180W。
-------------	--------------------------------------

## 命令模式

全局配置模式

## 默认

全局最大输出功率为 180W。no 命令将恢复到缺省配置。

## 使用说明

设定 PoE 电源的全局最大输出功率，以保证电源供电安全，也可用于有效控制。

## 举例说明

在全局设置功率为 100W：

```
Switch (config)# power inline max 100
```

## 2.16.5 power inline port max

设置 PoE 电源的端口最大输出功率。

## 命令语法

**power inline port max** *max-wattage*

**no power inline port max**

max-wattage	最大功率值。单位为 mW，端口可设置范围为 1~15400mW。
-------------	----------------------------------

## 命令模式

端口配置模式

## 默认

端口最大输出功率为 15400mW。no 命令将恢复到缺省配置。

## 使用说明

与全局最大功率的配合下，有效控制各个端口的输出功率。

## 举例说明

设置 PoE 电源的端口最大输出功率为 1000mW：

```
Switch (config-if)# power inline port max 1000
```

## 2.16.6 power inline policy

打开/关闭功率优先级管理策略模式。

### 命令语法

**power inline policy enable**

**no power inline policy enable**

### 命令模式

全局配置模式

### 默认

功率优先级管理策略模式默认开启。

### 使用说明

使能命令使用优先级策略，**no** 命令恢复先到先得策略。当打开优先级策略时，可对端口的优先级进行单独配置。

在优先级模式下，当 PSE 剩余功率不足时，将自动关闭低优先级的端口，保证高优先级端口的正常供电，而与 PD 接入的时间无关。若端口的优先级相同，则序号小的端口的优先级较高。

在先到先得模式下，当 PSE 剩余功率不足时，不能对新接入的 PD 进行供电。

### 举例说明

全局开启功率优先级策略模式：

```
Switch (config)# power inline policy enable
```

## 2.16.7 power inline priority

设置端口供电优先级。

### 命令语法

**power inline priority { critical | high | low }**

### 命令模式

端口配置模式



## 默认

端口优先级为 low。

## 使用说明

在 **power inline policy enable** 状态下生效，在剩余功率不足以对新接入的 PD 供电时，对高优先级的端口优先供电。

## 举例说明

在端口模式下设置供电优先级：

```
Switch (config-if)# power inline priority high
```

## 2.16.8 power inline high-inrush

使能/关闭上电瞬间高冲击电流。

## 命令语法

```
power inline high-inrush enable  
no power inline high-inrush enable
```

## 命令模式

端口配置模式

## 默认

使能上电瞬间高冲击电流

## 使用说明

不规范的PD上电瞬间会产生高冲击电流，导致设备启动自我保护，而将PD断电。在这种情况下，若一定要给此PD供电，需要允许上电瞬间的高冲击电流。关闭设备的自我保护功能，允许上电瞬间的高冲击电流，可能会对设备器件造成损害。

## 举例说明

在端口模式下使能上电瞬间高冲击电流：

```
Switch (config-if)# power inline high-inrush enable
```

## 2.16.9 power inline admin disable time-range

设置下电时间段。

### 命令语法

**power inline admin disable time-range** *name*

**no power inline admin disable time-range** *name*

name	时间字段
------	------

### 命令模式

端口配置模式

### 默认

取消设置下电时间段

### 使用说明

*name* 为时间字段，需要预先配置。

### 举例说明

在端口模式下设置下电时间段：

```
Switch (config-if)# power inline admin disable time-range word
```

## 2.16.10 power inline pd-description

设置供电端口描述。

### 命令语法

**power inline pd-description** *name*

**no power inline pd-description**

name	PD 描述名称，为任意字符，取值范围为 0~32
------	--------------------------

### 命令模式

端口配置模式

**默认**

无

**使用说明**

无

**举例说明**

在端口设置供电描述信息：

Switch(config-if)# power inline pd-description inspur

## 2.17 PoE 检测和调试命令

### 2.17.1 show power inline

显示全局PoE设置与状态。

**命令语法****show power inline****命令模式**

特权模式

**默认**

无

**使用说明**

各显示字段含义如下表：

字段	描述
Power Inline Status	全局功能开关状态
Power Available	全局可用功率上限值
Power Used	全局功率已使用值
Power Remaining	全局剩余可用功率
Min Voltage	全局欠压阈值
Max Voltage	全局过压阈值
Police	功率优先策略开关状态
Legacy	检测非标准 PD 开关状态

Disconnect	断开 PD 的方式
HW Version	PoE 模块硬件版本号
SW Version	PoE 模块软件版本号
Mode	供电模式 signal: 信号线供电 (Alternative A) spare: 空闲线 供电 (Alternative B)

## 举例说明

在用户特权模式下查看 PoE 状态：

```
Switch # show power inline
```

```
Module Available Used Remaining
      (Watts) (Watts) (Watts)
```

```
-----
1      300.0    0.0   300.0
```

```
Interface Admin Oper Power Priority Class Max Pd-description
          (Watts)
```

```
-----
eth-0-1 Auto Off 0.0 Low 0 90.0
eth-0-2 Auto Off 0.0 Low 0 90.0
eth-0-3 Auto Off 0.0 Low 0 90.0
eth-0-4 Auto Off 0.0 Low 0 90.0
eth-0-5 Auto Off 0.0 Low 0 90.0
eth-0-6 Auto Off 0.0 Low 0 90.0
eth-0-7 Auto Off 0.0 Low 0 90.0
eth-0-8 Auto Off 0.0 Low 0 90.0
eth-0-9 Auto Off 0.0 Low 0 30.1
eth-0-10 Auto Off 0.0 Low 0 30.1
eth-0-11 Auto Off 0.0 Low 0 30.1
eth-0-12 Auto Off 0.0 Low 0 30.1
eth-0-13 Auto Off 0.0 Low 0 30.1
eth-0-14 Auto Off 0.0 Low 0 30.1
eth-0-15 Auto Off 0.0 Low 0 30.1
eth-0-16 Auto Off 0.0 Low 0 30.1
eth-0-17 Auto Off 0.0 Low 0 30.1
```

eth-0-18	Auto	Off	0.0	Low	0	30.1
eth-0-19	Auto	Off	0.0	Low	0	30.1
eth-0-20	Auto	Off	0.0	Low	0	30.1
eth-0-21	Auto	Off	0.0	Low	0	30.1
eth-0-22	Auto	Off	0.0	Low	0	30.1
eth-0-23	Auto	Off	0.0	Low	0	30.1
eth-0-24	Auto	Off	0.0	Low	0	30.1

## 2.17.2 show power inline

显示端口PoE的配置与状态。

### 命令语法

**show power inline** *port-number*

port-number	物理接口，取值范围为eth-<0-0>-<1-28>
-------------	----------------------------

### 命令模式

特权模式

### 默认

无

### 使用说明

各显示字段含义如下表：

字段	描述
Interface	以太网端口号
Status	供电状态
	enable: 使能
	disable: 关闭供电功能
Oper	工作状态
	on: PD 连接并正常受电
	off: PD 未连接
	faulty: PD 检测错误
	deny: 可用功率不够或 PD 申请功率过大
Power	端口当前使用的功率
Max	端口最大分配的功率
Current	端口当前的电流

Volt	端口当前的电压
Priority	供电优先级
	critical: 极高优先级
	high: 高优先级
	low: 低优先级
Class	分类 用途 PD 输入功率(W)
	0 缺省 0.44~12.95
	1 可选 0.44~3.84
	2 可选 3.84~6.49
	3 可选 6.49~12.95
	4 为未来用途预留

## 举例说明

在用户特权模式下查看配置与状态：

```
Switch # show power inline eth-0-2
```

```
Interface Admin Oper Power Priority Class Max Pd-description
              (Watts)
```

```
-----
eth-0-2 Auto Off 0.0 Low 0 90.0
```

## 2.17.3 show environment

获取供电模块温度。

## 命令语法

```
show environment
```

## 命令模式

特权模式

## 默认

无

## 使用说明

获取温度

## 举例说明

显示模块温度：

```
Switch# show environment
```

```
Fan Tray :1 Status:PRESENT
```

FanIndex	Status	SpeedRate	Mode
----------	--------	-----------	------

1-1	OK	50%	Auto
-----	----	-----	------

-----

Power status:

Index	Status	Power	Type	Alert
-------	--------	-------	------	-------

1	ABSENT	-	-	-
---	--------	---	---	---

2	PRESENT	OK	AC	NO
---	---------	----	----	----

-----

Sensor status (Degree Centigrade):

Index	Temperature	Lower_alarm	Upper_alarm	Critical_limit	Position
-------	-------------	-------------	-------------	----------------	----------

1	53	-10	80	100	SWITCH_CHIP
---	----	-----	----	-----	-------------

2	54	-10	80	100	SWITCH_CHIP
---	----	-----	----	-----	-------------

-----

Poe Module status:

Index	Status	Temperature
-------	--------	-------------

1	NORMAL	37
---	--------	----

# 3 设备管理命令行参考

## 3.1 STM 命令 `stm prefer`

### 3.1.1 `stm prefer`

STM 是系统表项管理的简称，您可以使用 `STM prefer` 命令来合理配置交换机的表项资源，以便最大程度地支持您的应用程序正在使用的功能。您可以选择 STM 模版来使系统支持最大的单播 MAC 条目数；或者最大程度的支持（QoS）以及访问控制条目数（ACE）。使用这个命令的 `no` 形式返回到默认配置文件。

#### 命令语法

`stm prefer PROFILE`

`no stm prefer`

PROFILE	<p>Profile 模式，可以是 default, ipv6, layer2 以及 layer3。</p> <ul style="list-style-type: none"> <li>● <b>default:</b> 默认模版，保持系统所有特性均衡</li> <li>● <b>ipv6:</b> 适用于单播，可最大限度的支持 ipv6 的单播路由</li> <li>● <b>layer2:</b> 适合2层网络用户，可最大限度的支持单播MAC条目</li> <li>● <b>layer3:</b> 适合用户三层网络，一般用于路由器或者网络中间的汇聚层</li> </ul>
---------	--

#### 命令模式

全局配置模式

#### 默认

Default 模版，此配置文件平衡所有功能。

#### 使用说明

当你改变配置后，必须重启交换机配置才能生效。



## 举例说明

下面的例子描述了如何使系统最大程度的支持路由功能。

```
Switch(config)# stm prefer layer3
Switch(config)# exit
Switch# reload
```

## 相关命令

**show stm prefer**

### 3.1.2 show stm prefer

该命令显示特定模版的系统资源分配信息。如果该命令后不带参数，则显示当前正在使用的系统配置信息以及重启之后准备使用的系统资源分配情况。

## 命令语法

**show stm prefer** *PROFILE*

PROFILE	<p>Profile 模式，可以是 <b>default</b>，<b>ipv6</b>，<b>layer2</b> 以及 <b>layer3</b>。</p> <ul style="list-style-type: none"> <li>● <b>default</b>: 默认模版，保持系统所有特性均衡</li> <li>● <b>ipv6</b>: 适用于单播，可最大限度的支持 <b>ipv6</b> 的单播路由</li> <li>● <b>layer2</b>: 适合2层网络用户，可最大限度的支持单播MAC条目</li> <li>● <b>layer3</b>: 适合用户三层网络，一般用于路由器或者网络中间的汇聚层</li> </ul>
---------	---

## 命令模式

特权模式

## 默认

无

## 使用说明

当您改变配置但是没有重启交换机，那么显示的是当前正在使用的系统资源信息。重启交换机之后，配置才会真正生效。

## 举例说明

下面的例子显示了改变配置但没有重启交换之前的系统资源分配状况：

```
Switch# show stm prefer
```

```
Current profile is :default
  number of vlan instance           : 1/4094
  number of unicast & multicast mac address : 0/65536
  number of backhole mac address    : 0/128
  number of max applied vlan mapping : 0/1024
  number of mac based vlan class    : 0/512
  number of ipv4 based vlan class    : 0/512
  number of dot1x mac based         : 0/2048
  number of unicast ipv4 host routes : 0/4096
  number of unicast ipv4 indirect routes : 0/8192
  number of unicast ipv4 ecmp groups : 0/256
  number of unicast ipv4 policy based routes : 0/16
  number of unicast ip tunnel peers : 0/8
  number of multicast ipv4 routes   : 0/1023
  number of multicast ipv4 routes member : 0/1024
  number of ipv4 source guard entries : 0/1024
  number of ipv4 acl/qos flow entries : 0/511
  number of link aggregation (static & lacp) : 0/55
  number of ipfix cache             : 0/16384
```

## 相关命令

**stm prefer**

## 3.2 日志管理命令

### 3.2.1 clear logging buffer

使用此命令清除日志缓冲区中的记录。

#### 命令语法

**clear logging buffer**

#### 命令模式

特权模式

#### 默认

无

#### 使用说明

清除日志缓存中的日志。

#### 举例说明

清除日志缓冲区中的日志：

```
Switch# clear logging buffer
```

## 相关命令

**show logging buffer**

### 3.2.2 logging alarm-trap

在日志服务器收到大量日志时，使用此命令设置日志服务器是否发送报警日志以及发送报警日志消息的级别。

## 命令语法

**logging alarm-trap (enable | disable | level (high | lower | middle | minor))**

**no logging alarm-trap level**

enable	设置把报警日志通过 trap 消息发送出去
disable	取消把报警日志通过 trap 消息发送出去
level high	设置把 high 报警日志通过 trap 消息发送出去
level lower	设置把 lower（包括 lower 以上）报警日志通过 trap 消息发送出去
level middle	设置把 middle（包括 middle 以上）报警日志通过 trap 消息发送出去
level minor	设置把 minor（包括 minor 以上）报警日志通过 trap 消息发送出去

## 命令模式

全局配置模式

## 默认

关闭

## 使用说明

该命令用于提示用户，日志服务器接收了大量的日志信息。

## 举例说明

设置把报警日志通过 trap 消息发送出去：

```
Switch(config)# logging alarm-trap enable
Switch(config)# logging alarm-trap level high
```

## 相关命令

**logging alarm-trap level middle**

### 3.2.3 logging file

使用此命令设置是否把日志信息写入到日志文件中。

## 命令语法

**logging file (enable | disable)**

enable	把日志信息写入到日志文件中
disable	取消日志信息写入到日志文件中

## 命令模式

全局配置模式

## 默认

缺省系统将会把日志信息写入到日志文件中。

## 使用说明

一旦启用,日志将当前产生的日志每 10 分钟一次写入到 flash/log 文件中。

## 举例说明

把日志信息写入到日志文件中:

```
Switch(config)# logging file enable
```

## 相关命令

**show logging**

### 3.2.4 logging level file

使用此命令设置可被记入到日志文件的日志消息的阈值; 高于等于此阈值的日志都将被记入到日志文件。

## 命令语法

**logging level file (alert | critical | debug | emergency | error | information | notice | warning | severity-level)**

**no logging level file**

0   emergency	系统无法使用
1   alert	需要立即行动
2   critical	决定调整
3   error	错误调整
4   warning	警告调整
5   notice	正常且适当调整
6   information	信息性消息
7   debug	调试消息
severity-level	安全等级，范围 0-7

## 命令模式

全局配置模式

## 默认

默认等级为 warning

## 使用说明

使用此命令设置可以被记入到日志文件的日志消息的阈值，高于等于此阈值的日志消息会被记录到日志文件，而低于此阈值的不会被记入文件。

如果指定 debug，则所有日志消息都将被记入日志文件中。

## 举例说明

设置等级 3 的告警日志文件：

```
Switch(config)# logging level file 3
```

## 相关命令

**logging level module**

### 3.2.5 logging buffer

使用此命令设置系统临时缓冲区保存的 log 数量。no 命令恢复默认值。

## 命令语法

**logging buffer** *buffersize*

**no logging buffer**

buffersize	< 10-1000 >数量范围
------------	-----------------

**命令模式**

全局配置模式

**默认**

500

**使用说明**

该功能指定 **show logging buffer** 能显示的最多 log 条目。

**举例说明**

设置对系统保存 1000 条日志：

```
Switch(config)# logging buffer 1000
```

**相关命令****show logging buffer**

### 3.2.6 logging level module

使用此命令设置发往终端和记入到 **buffer**（日志缓冲区）的日志消息的阈值；高于等于此阈值的日志都将被显示在终端上（**terminal**），并被记入到 **buffer**（日志缓冲区）。

**命令语法**

**logging level module** (**alert** | **critical** | **debug** | **emergency** | **error** | **information** | **notice** | **warning** | *severity-level*)

**no logging level module**

0   emergency	系统无法使用
1   alert	需要立即行动
2   critical	决定调整
3   error	错误调整
4   warning	警告调整

5   notice	正常且适当调整
6   information	信息性消息
7   debug	调试消息
severity-level	安全等级，范围 0-7

## 命令模式

全局配置模式

## 默认

默认等级 debug

## 使用说明

使用此命令设置发往终端和记入到 **buffer**（日志缓冲区）的日志消息的阈值，高于等于此阈值的日志消息会被显示到终端并写入到日志缓冲区，而低于此阈值的不会被显示在终端，也不会被写入到日志缓冲区。

如果指定 **debug**，则所有日志消息都将被显示在终端并被进入日志缓冲区。

## 举例说明

设置所有日志消息都显示在终端（**terminal**）上：

```
Switch(config)# logging level module debug
```

## 相关命令

**logging level file**

### 3.2.7 logging merge

使用此命令设置对系统日志进行合并，以减少日志数量。

## 命令语法

**logging merge (enable | disable | fifo-size size | timeout seconds)**

**no logging merge (fifo-size | timeout)**

enable	设置对系统日志进行合并
disable	设置不对系统日志进行合并
fifo-size size	设置后台日志合并缓冲区的大小；以条目为单位，缺省为 1024

	条
<code>timeout seconds</code>	指定时间段；在此时间段内出现的相同的日志会被合并为一条；缺省为 10 秒

## 命令模式

全局配置模式

## 默认

启用

## 使用说明

启用了此功能以后，交换机会把在指定时间段内出现的相同的日志合并为一条；而在此时间段内，交换机会把收到的日志放在后台的指定大小的临时缓冲区中。可以使用 `timeout` 参数指定此时间段的大小；可以使用 `fifo-size` 参数指定后台临时缓冲区的大小。

## 举例说明

设置对系统日志进行合并：

```
Switch(config)# logging merge enable
```

## 相关命令

**logging merge timeout 30**

### 3.2.8 logging sync

使用此命令将内存缓冲区中的日志写到 flash 中的 syslog 文件中。

## 命令语法

**logging sync**

## 命令模式

特权模式

## 默认

无



## 使用说明

启用 logging merge 功能后 log 不会马上显示到终端或者 logging buffer 中，使用这条命令是将 log 马上显示到终端或者 logging buffer 中去，并将内存缓冲区中的日志写到 flash 中的 syslog 文件中。

## 举例说明

启用同步缓冲区日志：

```
Switch# logging sync
```

## 相关命令

**logging merge enable**

### 3.2.9 logging operate

使用此命令设置是否发送操作日志。

## 命令语法

**logging operate (enable | disable)**

enable	设置发送操作日志
disable	设置不发送操作日志

## 命令模式

全局配置模式

## 默认

禁用

## 使用说明

如果启用了日志记录操作，所有的 CLI 中配置模式或更高将被保存到记录器的缓冲区。

## 举例说明

设置发送操作日志：

```
Switch(config)# logging operate enable
```

## 相关命令

**logging server**

### 3.2.10 logging server

使用此命令设置是否使用远程日志服务器。

## 命令语法

**logging server (enable | disable)**

enable	启用
disable	禁用

## 命令模式

全局配置模式

## 默认

禁用

## 使用说明

此命令用于发送到远程服务器上的记录器。

## 举例说明

启用远程日志服务器：

```
Switch(config)# logging server enable
```

## 相关命令

**logging server severity**

### 3.2.11 logging server address

使用此命令设置日志服务器的 IP 地址；交换机可以把日志信息发往此服务器。

## 命令语法

**logging server address (mgmt-if | ) (ipv4-address | ipv6-address) (source-interface IFNAME|source-ip A.B.C.D)**

**no logging server address (mgmt-if | ) (ipv4-address | ipv6-address)**

mgmt-if	管理口
ipv4-address	表示日志服务器的 IPv4 地址
ipv6-address	表示的日志服务器的 IPv6 地址
IFNAME	指定源接口名称
A.B.C.D	指定源 IP 地址

## 命令模式

全局配置模式

## 默认

无

## 使用说明

为了使交换机能正确的把系统日志信息发往日志服务器，请确保此服务器在正常工作状态。如果指定源接口或者源 IP 地址，将会使用对应的 IP 地作为发出报文的源 IP 地址。

## 举例说明

设置日志服务器为 209.165.202.169:

```
Switch(config)# logging server address 209.165.202.169
```

## 相关命令

**logging server**

### 3.2.12 logging server facility

使用此命令来配置在服务器上的日志守护进程。

## 命令语法

**logging server facility** *facility-type*

**no logging server facility**

facility-type	工具类型
---------------	------

## 命令模式

全局配置模式

## 默认

Local4

## 使用说明

下表显示了进程编号与进程的对应关系。

进程名	进程名编号	描述
auth	4	Authorization system
authpriv	10	Authorization priv system
cron	9	Cron facility
daemon	3	System daemon
ftp	11	FTP sytem
kern	0	Kernel
local0-7	16-23	Reserved for locally defined messages
lpr	6	Line printer system
mail	2	Mail system
news	7	USENET news
syslog	5	System log
user	1	User
uucp	8	UNIX-to-UNIX

## 举例说明

配置在服务器上的日志守护进程为 local3:

```
Switch(config)# logging server facility local3
```

## 相关命令

**logging server**

### 3.2.13 logging server severity

设置发往远程日志服务器的日志信息的阈值；高于或等于此阈值的日志都将被发往日志服务器。

## 命令语法

**logging server severity** (alert | critical | debug | emergency | error | information | notice | warning | *severity-level*)

**no logging server severity**

0   emergency	系统无法使用
1   alert	需要立即行动
2   critical	决定调整
3   error	错误调整
4   warning	警告调整
5   notice	正常且适当调整
6   information	信息性消息
7   debug	调试消息
severity-level	安全等级，范围 0-7

## 命令模式

全局配置模式

## 默认

默认等级为 information

## 使用说明

如果设置阈值为 debug，则所有日志消息都将被发往日志服务器。

## 举例说明

设置发往日志服务器的日志信息的重要程度是 debug 等级：

```
Switch(config)# logging server severity 3
```

## 相关命令

**logging level module**

**logging level file**

## 3.2.14 logging timestamp

使用此命令设置日志信息的时间戳格式。

### 命令语法

**logging timestamp (bsd | date | iso | none | rfc3164 | rfc3339)**

**no logging timestamp**

bsd	BSD 时间格式
date	使用 date 命令时显示的时间格式
iso	ISO 时间格式
none	日志信息不打时间戳
rfc3164	RFC 3164 时间格式
rfc3339	RFC 3339 时间格式

### 命令模式

全局配置模式

### 默认

BSD 时间格式

### 使用说明

此命令是用来指定记录消息所带的时间戳。

### 举例说明

设置时间戳格式为 iso 模式：

```
Switch(config)# logging timestamp iso
```

### 相关命令

**show logging**

## 3.2.15 show logging

使用此命令查看系统关于日志管理的设置。

## 命令语法

**show logging**

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

显示系统的登录配置信息：

```
Switch# show logging
Current logging configuration:
=====
logging buffer 500
logging timestamp date
logging file enable
logging level file warning
logging level module debug
logging server disable
logging server severity warning
logging server facility local7
logging alarm-trap enable
logging alarm-trap level middle
logging merge disable
logging merge fifo-size 1024
logging merge timeout 10
logging operate disable
```

## 相关命令

**logging level**

### 3.2.16 show logging buffer

显示系统的日志配置信息。

## 命令语法

**show logging buffer** (*number* | **statistics**)

number	显示存储在日志缓冲区的信息，后面所跟参数为条目
--------	-------------------------

statistics	显示存储在日志缓冲区信息的数量
------------	-----------------

## 命令模式

特权模式

## 默认

无

## 使用说明

显示在交换机日志缓冲区中的所有日志信息。

## 举例说明

显示在交换机日志缓冲区中的所有日志信息数量：

```
Switch# show logging buffer statistics
Logging buffer statistics:
=====
Total processed 153 entries
Total dropped 0 entries
Current have 153 entries
The latest message is:
Aug  6 16:06:44 Switch3 IMISH-6: ready to service
The oldest message is:
Aug  6 13:38:38 Switch LOGGING-5: logging starting up; version='\2.0rc4\'
```

## 相关命令

**show logging**

## 3.3 Mirror 命令

### 3.3.1 monitor session destination interface

使用“monitor session destination interface”命令配置镜像目的端口。

在原命令之前加上关键字“no”删除该配置。

## 命令语法

```
monitor session session destination interface interface
no monitor session session destination
```



session	镜像会话编号，有效范围 1-3
destination interface <i>interface</i>	镜像目的端口

## 命令模式

全局配置模式

## 默认

无

## 使用说明

镜像目的端口只能是物理端口，vlan 端口或者聚合端口都不行。

同一个镜像会话只能有一个镜像目的，不能同时配置本地镜像目的端口和远程镜像目的 vlan。

(关于远程镜像，详见 3.3.8 monitor session destination remote 这一章节。)

## 举例说明

- 配置 eth-0-1 为镜像会话 1 的目的端口：  
Switch(config)# monitor session 1 destination interface eth-0-1
- 删除该配置：  
Switch(config)# no monitor session 1 destination

## 相关命令

**monitor session *session-id* source interface**

**monitor session *session-id* source vlan**

**show monitor**

### 3.3.2 monitor session destination cpu

使用“monitor session destination cpu”命令配置镜像目的为 cpu。

在原命令之前加上关键字“no”删除该配置。

## 命令语法

**monitor session *session* destination cpu**

**no monitor session *session* destination**

session	镜像会话编号，有效范围 1-3
---------	-----------------

<code>destination cpu</code>	镜像目的端口
------------------------------	--------

## 命令模式

全局配置模式

## 默认

无

## 使用说明

镜像目的支持配置 `cpu`。

同一个镜像会话只能有一个镜像目的，不能同时配置本地镜像目的端口和远程镜像目的 `vlan`。

(关于远程镜像，详见 3.3.8 `monitor session destination remote` 这一章节。)

## 举例说明

- 配置 `cpu` 为镜像会话 1 的目的：  
Switch(config)# `monitor session 1 destination cpu`
- 删除该配置：  
Switch(config)# `no monitor session 1 destination`

## 相关命令

**`monitor session session-id source interface`**

**`monitor session session-id source vlan`**

**`show monitor`**

### 3.3.3 `monitor session destination group`

使用“`monitor session destination group`”命令创建镜像目的端口组，并进入镜像目的端口组模式。

在原命令之前加上关键字“`no`”删除该配置。

## 命令语法

**`monitor session session destination group groupid`**

**`no monitor session session destination`**

<code>session</code>	镜像会话编号，有效范围 1-3
----------------------	-----------------

<code>destination group <i>groupid</i></code>	镜像目的端口组编号，有效范围 1-32
---	---------------------

## 命令模式

全局配置模式

## 默认

无

## 使用说明

只有一个镜像会话可以配置为镜像目的端口组，一个目的端口组可以配置多个镜像目的端口。

同一个镜像会话只能有一个镜像目的组，不能同时配置本地镜像目的端口和远程镜像目的 `vlan`。

(关于远程镜像，详见 3.3.8 `monitor session destination remote` 这一章节。)

## 举例说明

- 配置创建镜像会话 1 的目的端口组 1：  
`Switch(config)# monitor session 1 destination group 1`
- 删除该配置：  
`Switch(config)# no monitor session 1 destination`

## 相关命令

**`monitor session session-id source interface`**

**`member`**

**`show monitor`**

### 3.3.4 member

使用“`member`”命令配置镜像目的组的目的端口。

在原命令之前加上关键字“`no`”删除该配置。

## 命令语法

**`member interface`**

**`member interface`**

<b><code>member interface</code></b>	镜像目的端口组成员端口
--------------------------------------	-------------

## 命令模式

镜像目的端口组配置模式

## 默认

无

## 使用说明

镜像目的端口只能是物理端口，vlan 端口或者聚合端口都不行。

同一个镜像会话只能有一个镜像目的组，不能同时配置本地镜像目的端口组和远程镜像目的 vlan。

(关于远程镜像，详见 3.3.8 monitor session destination remote 这一章节。)

## 举例说明

- 配置 eth-0-1 为镜像会话目的端口组 1 的目的端口成员：  
Switch(config-monitor-d-group)# member interface eth-0-1
- 删除该配置：  
Switch(config-monitor-d-group)# member interface eth-0-1

## 相关命令

**monitor session *session-id* source interface**

**monitor session *session-id* destination group *groupid***

**show monitor**

### 3.3.5 monitor session source interface

使用“monitor session source interface”命令，配置镜像源端口。

在原命令前加上关键字“no”删除该配置。

## 命令语法

**monitor session *session* source interface *interface* (both | tx | rx)**

**no monitor session *session* source interface *interface* (both | tx | rx)**

session	镜像会话编号，有效范围 1-3
destination interface <i>interface</i>	指定镜像源端口
both	镜像源端口上收到和发送的报文流量

rx	镜像源端口上收到的报文流量
tx	镜像源端口上发送的报文流量

## 命令模式

全局配置模式

## 默认

无

## 使用说明

镜像源端口可以是物理端口，也可以是聚合端口。

如果不特别指明方向（双向、接收、发送），那么默认值是双向。

## 举例说明

- 配置 eth-0-11 为镜像会话 1 的源端口：  
Switch(config)# monitor session 1 source interface eth-0-11
- 删除该配置：  
Switch(config)# no monitor session 1 source interface eth-0-11

## 相关命令

**monitor session *session-id* destination**

**show monitor**

### 3.3.6 monitor session source vlan

使用“monitor session source vlan”命令，配置镜像源 vlan。

在原命令前加上关键字“no”删除该配置。

## 命令语法

**monitor session *session* source vlan *vlan* (both | tx | rx)**

**no monitor session *session* source vlan *vlan* (both | tx | rx)**

session	镜像会话编号，有效范围 1-3
vlan	镜像源 vlan，有效范围 1-4094
both	镜像源 vlan 上收到和发送的报文流量

rx	镜像源 vlan 上收到的报文流量
tx	镜像源 vlan 上发送的报文流量

## 命令模式

全局配置模式

## 默认

无

## 使用说明

如果不特别指明方向（双向、接收、发送），那么默认值是双向。

配置镜像源 vlan 之前，必须先在“vlan database”模式下创建 vlan，且在全局创建 vlan Interface。

## 举例说明

创建 vlan 和 vlan Interface:

```
Switch (config)# vlan database
```

```
Switch (config-vlan)# vlan 2
```

```
Switch (config-vlan)# exit
```

```
Switch(config)#interface vlan2
```

```
Switch(config-if)#exit
```

配置 vlan 2 为镜像会话 1 的源 vlan:

```
Switch(config)# monitor session 1 source vlan 2 both
```

配置 vlan 2 为镜像会话 1 的源 vlan，观察接收方向的报文:

```
Switch(config)# monitor session 1 source vlan 2 rx
```

配置 vlan 2 为镜像会话 1 的源 vlan，观察发送方向的报文:

```
Switch(config)# monitor session 1 source vlan 2 tx
```

删除配置镜像:

```
Switch(config)#no monitor session 1 source vlan 2 both
```

删除 vlan 2:

```
Switch(config)#no interface vlan2
```

```
Switch (config)# vlan database
```

```
Switch (config-vlan)# no vlan 2
```

Switch (config-vlan)# exit

## 相关命令

**monitor session destination**

**show monitor**

**vlan database**

**vlan** *vlan*

**interface vlan** *vlan*

### 3.3.7 monitor session source cpu

使用“monitor session source cpu”命令，配置镜像源 cpu。

在原命令前加上关键字“no”删除该配置。

## 命令语法

**monitor session** *session* **source cpu** (**both** | **tx** | **rx**)

**no monitor session** *session* **source cpu** (**both** | **tx** | **rx**)

session	镜像会话编号，有效值为 1，只支持配置 session 1 上
cpu	镜像源 cpu
both	镜像源 cpu 上收到和发送的报文流量
rx	镜像源 cpu 上收到的报文流量
tx	镜像源 cpu 上发送的报文流量

## 命令模式

全局配置模式

## 默认

无

## 使用说明

如果不特别指明方向（双向、接收、发送），那么默认值是双向。

镜像源 cpu 只支持配在 session 1 上，其他 session 不可以配置。

## 举例说明

配置 cpu 为镜像会话 1 的源：

```
Switch(config)# monitor session 1 source cpu both
```

配置 cpu 为镜像会话 1 的源，观察接收方向的报文：

```
Switch(config)# monitor session 1 source cpu rx
```

配置 cpu 为镜像会话 1 的源，观察发送方向的报文：

```
Switch(config)# monitor session 1 source cpu tx
```

删除配置镜像：

```
Switch(config)#no monitor session 1 source cpu both
```

## 相关命令

**monitor session destination**

**show monitor**

### 3.3.8 monitor session destination remote

使用“monitor session destination remote”命令配置远程端口镜像的目的 vlan 和出端口。

在原命令前加上关键字“no”删除该配置。

## 命令语法

**monitor session *session* destination remote vlan *vlan* interface *interface***

**no monitor session *session* destination remote vlan**

session	镜像会话编号，有效范围 1-3
vlan	远程端口镜像的目的 vlan，有效范围 2-4094
interface	镜像报文的出端口

## 命令模式

全局配置模式

## 默认

无



## 使用说明

在配置远程端口镜像目的 vlan 之前，必须先在 “vlan database”中配置该 vlan。

出端口只能是物理端口。

为了防止出端口中出现泛洪的报文，影响观察结果，可以将默认 vlan 移出该端口。(详见 vlan 命令手册中的 “**switchport trunk allowed vlan remove 1**” 章节)

## 举例说明

创建 vlan2:

```
Switch (config)# vlan database
```

```
Switch (config-vlan)# vlan 2
```

```
Switch (config-vlan)# exit
```

指定 vlan 2 为镜像会话 1 的远程目的 vlan，eth-0-1 为出端口:

```
Switch(config)# monitor session 1 destination remote vlan 2 interface eth-0-1
```

删除远程镜像目的配置:

```
Switch(config)# no monitor session 1 destination remote vlan
```

删除 vlan:

```
Switch (config)# vlan database
```

```
Switch (config-vlan)# no vlan 2
```

```
Switch (config-vlan)# exit
```

## 相关命令

**monitor session session-id source interface**

**monitor session session-id source vlan**

**vlan database**

**vlan vlan**

### 3.3.9 monitor mac escape

使用 “monitor mac escape” 命令配置远程镜像的 mac 地址例外功能。配置了 mac 地址例外表项以后，报文的地址匹配到表项的时候就不会被远程镜像复制（不包括 ERSPAN）。

在原命令前加上关键字 “no” 删除 mac 地址例外表项。

## 命令语法

**monitor mac escape MAC MASK**

**no monitor mac escape (MAC MASK |)**

MAC	mac 地址，格式为 HHHH. HHHH. HHHH
MASK	mac 地址掩码，格式为 HHHH. HHHH. HHHH

## 命令模式

全局配置模式

## 默认

无

## 使用说明

Mac 地址例外表项只对远程镜像有效，不影响本地镜像。

配置了 mac 地址例外表项以后，报文的目的地地址匹配到表项的时候就不会被远程镜像复制。

全局最多支持两个表项。删除的时候如果不指定 mac 地址和 mac 掩码，将会删除所有表项。

## 举例说明

- 配置 mac 地址 00cc.1122.3344，掩码 ffff.ffff.0000 的表项：  
Switch(config)# monitor mac escape 00cc.1122.3344 ffff.ffff.0000
- 删除该表项：  
Switch(config)# no monitor mac escape 00cc.1122.3344 ffff.ffff.0000

## 相关命令

**monitor session *session-id* destination remote**

### 3.3.10 show monitor

使用“show monitor”命令，显示镜像相关配置。

## 命令语法

**show monitor (session *session*)**

session	镜像会话编号，有效范围 1~3
---------	-----------------

## 命令模式

特权模式

## 默认

无

## 使用说明

如果不指定镜像会话号，所有表项都会被显示。

## 举例说明

显示命令的输出结果：

```
DUT1# show monitor
```

```
Session 1
-----
Status          : Valid
Type            : Local Session
Source Ports    :
  Receive Only  :
  Transmit Only :
  Both          : eth-0-2 eth-0-3
Source VLANs    :
  Receive Only  :
  Transmit Only :
  Both          :
Destination Port : eth-0-1
```

```
DUT1# show monitor
```

```
Session 1
-----
Status          : Valid
Type            : Cpu Session
Source Ports    :
  Receive Only  : eth-0-1
  Transmit Only :
  Both          :
Source VLANs    :
  Receive Only  :
  Transmit Only :
  Both          :
Destination Port : cpu
DUT1#
```

## 相关命令

**monitor session *session-id* source interface**

**monitor session *session-id* source vlan**

**monitor session *session-id* source cpu**

**monitor session *session-id* destination interface**

**monitor session *session-id* destination remote**

**monitor session *session-id* destination cpu**

### 3.3.11 show monitor mac escape

使用“show monitor mac escape”显示 mac 地址例外的表项。

#### 命令语法

**show monitor mac escape**

#### 命令模式

特权模式

#### 默认

无

#### 使用说明

该命令可以显示出 mac 地址例外的表项个数和表项内容。

#### 举例说明

显示命令的输出结果：

```
Switch # show monitor mac escape
```

```
-----  
monitor rspan mac escape database  
-----  
count    : 1  
-----  
Mac      : 00:cc:11:22:33:44  
Mask     : ff:ff:ff:ff:00:00  
-----
```

#### 相关命令

**monitor mac escape *MAC MASK***

### 3.3.12 monitor destination forwarding enable

使用该命令，配置镜像目的端口可支持报文正常转发。

在原命令前加上关键字“no”删除该配置。

#### 命令语法

**monitor destination forwarding enable**

**no monitor destination forwarding enable**

## 命令模式

全局配置模式

## 默认

无

## 使用说明

如果有任何镜像目的端口已配，不可以改变本特性。

## 举例说明

- 配置目的端口支持转发：  
Switch(config)# monitor destination forwarding enable

## 相关命令

**monitor session *session-id* destination****show monitor**

### 3.3.13 monitor cpu set packet buffer

使用该命令，配置 mirror cpu 的报文存储空间大小，默认值最大为 1000 个包  
在原命令前加上关键字“no”删除该配置。

## 命令语法

monitor cpu set packet buffer &lt;1-1000&gt;

**no** monitor cpu set packet buffer

## 命令模式

全局配置模式

## 默认

默认值为 1000

## 使用说明

&lt;1-1000&gt;为报文 mirror 上 cpu 存储报文的个数，默认值为 1000

## 举例说明

- 配置 mirror cpu 的报文内存存储空间：

```
Switch(config)# monitor cpu set packet buffer 50
```

## 相关命令

```
show monitor cpu packet buffer size
```

### 3.3.14 monitor cpu capture strategy

使用该命令，配置 mirror cpu 的抓包策略，默认值情况为 replace，即当内存 buffer 满之后，用新报文替换旧报文。

## 命令语法

```
monitor cpu capture strategy replace
```

```
monitor cpu capture strategy drop
```

## 命令模式

配置模式

## 默认

默认是 replace 模式

## 使用说明

replace 模式：当 mirror cpu 内存 buffer 满之后，新来的报文会替换最旧的报文

drop 模式：当 mirror cpu 内存 buffer 满之后，丢弃新来的报文。

## 举例说明

- 配置 mirror cpu 抓包策略为 replace:  
Switch(config)# monitor cpu capture strategy replace
- 配置 mirror cpu 抓包策略为 drop:  
Switch(config)# monitor cpu capture strategy drop

## 相关命令

```
show monitor cpu capture strategy
```

### 3.3.15 show monitor cpu packet

使用该命令，显示 mirror cpu 的内存中存储的报文。

## 命令语法

```
show monitor cpu packet (all|<1-1000>)
```

## 命令模式

特权模式

## 默认

0

## 使用说明

参数 all 是显示所有 mirror cpu 的报文，packetid 是显示第 i 个报文的内容

## 举例说明

- 显示所有 mirror cpu 的报文

```
show monitor cpu packet all
```

## 相关命令

```
monitor session session destination cpu
```

### 3.3.16 clear monitor cpu packet all

使用该命令，清除 mirror cpu 的内存中存储的报文。

## 命令语法

```
clear monitor cpu packet all
```

## 命令模式

特权模式

## 默认

0

## 使用说明

清除 mirror cpu 内存 buffer 里面所有的报文

## 举例说明

- 清除 mirror cpu 内存 buffer 里面所有的报文

```
clear monitor cpu packet all
```

## 相关命令

```
show monitor cpu packet (all|<1-1000>)
```

### 3.3.17 show monitor cpu packet buffer-size

使用该命令，显示 mirror cpu 当前申请的内存空间大小

#### 命令语法

```
show monitor cpu packet buffer-size
```

#### 命令模式

特权模式

#### 默认

0

#### 使用说明

显示 mirror cpu 当前申请的内存空间大小，该大小为最大存储报文个数

#### 举例说明

- 显示 mirror cpu 当前申请的内存空间大小

```
show monitor cpu packet buffer-size
```

#### 相关命令

```
monitor cpu set packet buffer <1-1000>
```

### 3.3.18 show monitor cpu capture strategy

使用该命令，显示 mirror cpu 当前抓包策略

#### 命令语法

```
show monitor cpu capture strategy
```

#### 命令模式

特权模式

#### 默认

0

#### 使用说明

显示 mirror cpu 当前的抓包策略，replace 或者 drop



## 举例说明

- 显示 mirror cpu 当前抓包策略

```
show monitor cpu capture strategy
```

## 相关命令

```
monitor cpu capture strategy (replace|drop)
```

### 3.3.19 cpu-traffic-limit reason mirror-to-cpu

使用该命令，配置 mirror 报文上 cpu 的速率和优先级

## 命令语法

```
cpu-traffic-limit reason mirror-to-cpu rate <0-1000000>
```

```
cpu-traffic-limit reason mirror-to-cpu class <0-3>
```

```
no cpu-traffic-limit reason mirror-to-cpu rate
```

```
no cpu-traffic-limit reason mirror-to-cpu class
```

## 命令模式

配置模式

## 默认

```
rate 256
```

```
class 0
```

## 使用说明

配置 mirror 报文上 cpu 的速率和优先级

## 举例说明

- 配置 mirror 上 cpu 报文的速率为 512，优先级为 2

```
cpu-traffic-limit reason mirror-to-cpu rate 512
```

```
cpu-traffic-limit reason mirror-to-cpu class 2
```

## 相关命令

```
show cpu limit-traffic
```

## 3.4 设备管理命令

### 3.4.1 temperature

使用此命令配置系统温度阈值。

#### 命令语法

**temperature** *low high critical*

**no temperature**

low	低温温度范围为<0-50>
high	高温温度范围为<50-85>
critical	高危温度范围为<55-90>

#### 命令模式

全局配置模式

#### 默认

默认阈值是低温 5，高温 75，高危温度 90。

#### 使用说明

温度单位为摄氏度。

高危温度必须高于高温温度至少 5 度。

高温温度必须高于低温温度至少 5 度。

#### 举例说明

这个例子显示怎样配置温度阈值：

```
Switch# configure terminal
Switch(config)# temperature 5 70 90
```

#### 相关命令

**show environment**

### 3.4.2 show environment

使用此命令显示硬件环境信息。

## 命令语法

**show environment (slot id | )**

id	堆叠情况下的 member 号，非堆叠情况下不支持 slot id
----	-----------------------------------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

这个例子说明怎样显示硬件环境信息。

```
Switch# show environment
Fan tray status:
Index      Status
1          PRESENT
FanIndex   Status  SpeedRate  Mode
1-1       OK      30%        Auto
1-2       OK      30%        Auto
1-3       OK      30%        Auto
-----
Power status:
Index      Status   Power    Type    Alert
1          PRESENT OK        AC      NO
2          ABSENT  -         -       -
-----
Sensor status (Degree Centigrade):
Index Temperature  Lower_alarm  Upper_alarm  Critical_limit
1          64            5            75           90
```

## 相关命令

**temperature**

### 3.4.3 boot system

使用此命令指定交换机启动时加载的系统 image。

## 命令语法

**boot system (file-name | tftp: mgmt-if ip-address file-name)**

file-name	这个文件将会在系统启动时被加载
ip-address	tftp 服务器的 IP 地址
file-name	这个文件将会在系统启动时被加载
tftp: mgmt-if	使用管理口

## 命令模式

全局配置模式

## 默认

无

## 使用说明

无

## 举例说明

下面这个例子简要的说明 `boot system file_name` 命令。

```
Switch# boot system tftp: mgmt-if 10.10.29.160 uImage.r
```

## 相关命令

无

### 3.4.4 show transceiver

使用此命令显示光模块收发器信息。

## 命令语法

**show transceiver** (*detail* |)

detail	显示包括 DDM 信息在内的详细信息
--------	--------------------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

这个例子说明怎样显示光模块收发器的信息：

```
Switch# show transceiver detail
Port eth-1-2 transceiver info:
Transceiver Type: 10G Base-SR
Transceiver Vendor Name : OEM
Transceiver PN          : SFP-10GB-SR
Transceiver S/N         : 201033PST1077C
Transceiver Output Wavelength: 850 nm
Supported Link Type and Length:
    Link Length for 50/125um multi-mode fiber: 80 m
    Link Length for 62.5/125um multi-mode fiber: 30 m
-----
Transceiver is internally calibrated.
mA: milliamperes, dBm: decibels (milliwatts), NA or N/A: not applicable.
++ : high alarm, + : high warning, - : low warning, -- : low alarm.
The threshold values are calibrated.
-----
          High Alarm   High Warn   Low Warn   Low Alarm
Temperature Threshold Threshold Threshold Threshold
Port (Celsius)      (Celsius)   (Celsius) (Celsius) (Celsius)
-----
eth-1-2  25.92      95.00      90.00     -20.00    -25.00
-----
          High Alarm   High Warn   Low Warn   Low Alarm
          Voltage Threshold Threshold Threshold Threshold
Port (Volts) (Volts) (Volts) (Volts) (Volts)
-----
eth-1-2  3.32      3.80      3.70      2.90      2.80
-----
          High Alarm   High Warn   Low Warn   Low Alarm
          Current Threshold Threshold Threshold Threshold
Port (milliamperes) (mA) (mA) (mA) (mA)
-----
eth-1-2  6.41      20.00     18.00     1.00      0.50
-----
          High Alarm   High Warn   Low Warn   Low Alarm
          Optical Transmit Power Threshold Threshold Threshold Threshold
Port (dBm) (dBm) (dBm) (dBm) (dBm)
```

```

-----
-----
eth-1-2    -2.41      2.01      1.00      -6.99      -7.96
-----
-----
          Optical      High Alarm   High Warn   Low Warn   Low Alarm
          Receive Power  Threshold   Threshold   Threshold   Threshold
Port      (dBm)           (dBm)       (dBm)       (dBm)       (dBm)
-----
-----
eth-1-2    -12        -          1.00      0.00      -19.00     -20.00
-----
-----

```

## 相关命令

无

### 3.4.5 update bootrom

使用此命令更新 bootrom image。

## 命令语法

**update bootrom** (*flash* | *udisk*)

flash	源文件目录
udisk	源文件目录

## 命令模式

全局配置模式

## 默认

无

## 使用说明

无

## 举例说明

这个例子说明如何更新 bootrom image。

```
Switch(config)# update bootrom flash:/boot/ bootrom.bin
```

## 相关命令

无

### 3.4.6 update epld

使用此命令更新 epld。

## 命令语法

**update epld** (*flash* | *udisk*)

flash	源文件目录
udisk	源文件目录

## 命令模式

全局配置模式

## 默认

无

## 使用说明

无

## 举例说明

这个例子说明如何更新 epld。

```
Switch(config)# update epld flash:/boot/ vme_v1.0
```

## 相关命令

无

### 3.4.7 Show reboot-info

用此命令显示 reboot info

## 命令语法

**show reboot-info**

## 命令模式

特权模式

## 默认

无

## 使用说明

重启类型	说明
POWER	断电重启
MANUAL	系统下手动 reboot/reload 重启
HIGH-TMPR	高温异常重启
BHMDOG	BHM 看门狗重启，用于监控系统各个功能模块
LCMDOG	LCM 看门狗重启，用于监控 LC
SCHEDULE	定时重启
SNMP-RELOAD	SNMP 重启
HALFAIL	HAGT 与 HSRV 通讯异常重启，需要 stack 功能开启
ABNORMAL	系统非正常方式重启，包括 shell 下的 reboot
CTCINTR	按键重启
LCATTACH	LC 匹配异常重启
OTHER	其他重启

## 举例说明

这个例子说明如何显示 reboot info

```
Switch# show reboot-info
Times      Reboot Type      Reboot Time
1          MANUAL           2016/09/08 15:14:41
2          MANUAL           2016/09/08 14:23:31
3          MANUAL           2000/01/01 00:00:01
4          HIGH-TMPR        2000/01/01 01:01:40
5          MANUAL           2000/01/01 00:08:17
6          ABNORMAL         1959/11/25 17:44:24
7          MANUAL           1959/11/26 14:51:37
8          MANUAL           1959/11/28 09:04:35
9          MANUAL           2016/09/12 09:44:53
10         MANUAL           2000/01/01 00:00:01
```

## 相关命令

无



## 3.5 Bootrom 命令

### 3.5.1 version

使用此命令显示 Bootrom 版本信息。

#### 命令语法

**version**

#### 命令模式

Bootrom CLI

#### 默认

无

#### 使用说明

无

#### 举例说明

这个例子用来说明怎样显示 Bootrom 版本。

```
bootrom:> version
Bootrom 3.0.0 (Development build) (Build time: Apr 13 2011 - 15:31:37)
```

#### 相关命令

无

### 3.5.2 setenv

使用此命令设置 Bootrom 环境变量。

#### 命令语法

**setenv** ( **ipaddr** | **serverip** *IPaddress* | **bootcmd** *boot arguments* )

<code>serverip IPaddress</code>	本地或者 tftp 服务器的 IP 地址
<code>boot arguments</code>	从 flash 或者从 tftp 服务器加载 image 重启

## 命令模式

Bootrom CLI

## 默认

无

## 使用说明

无

## 举例说明

- 这个例子用来说明怎样设置设备 IP 地址作为环境变量。  

```
bootrom:> setenv ipaddr 10.10.29.48
```
- 这个例子用来说明怎样设置 TFTP 服务器 IP 地址作为环境变量。  

```
bootrom:> setenv serverip 10.10.29.160
```
- 这个例子用来说明怎样设置 boot 命令作为环境变量。  

```
bootrom:> setenv bootcmd boot_flash  
bootrom:> setenv bootcmd boot_flash OS-ma-v3.0.1.it.r.bin
```

## 相关命令

无

### 3.5.3 saveenv

使用此命令永久保存 Bootrom 环境变量。

## 命令语法

**saveenv**

## 命令模式

Bootrom CLI

## 默认

无

## 使用说明

无

## 举例说明

这个例子用来说明怎样永久保存 Bootrom 环境变量。

```
bootrom:> saveenv
Saving Environment to EEPROM
```

## 相关命令

**printenv**

### 3.5.4 printenv

使用此命令永久保存 Bootrom 环境变量。

## 命令语法

**printenv**

## 命令模式

Bootrom CLI

## 默认

无

## 使用说明

无

## 举例说明

这个例子用来说明怎样显示 Bootrom 环境变量。

```
bootrom:> printenv
stderr=serial
ipaddr=10.10.29.48
serverip=10.10.29.160
.
Environment size: 818/2044 bytes
```

## 相关命令

**setenv**

### 3.5.5 reset

使用此命令完成 CPU 的复位。

## 命令语法

**reset**

## 命令模式

Bootrom CLI

## 默认

无

## 使用说明

无

## 举例说明

这个例子用来说明怎样在 Bootrom 下将 CPU 复位。

```
bootrom:> reset
```

## 相关命令

**saveenv**

## 3.5.6 ping

使用此命令发送 ICMP ECHO\_REQUEST 到网络主机。

## 命令语法

**ping** *IPaddress*

IPaddress	远端 IPaddress
-----------	--------------

## 命令模式

Bootrom CLI

## 默认

无

## 使用说明

无

## 举例说明

这个例子用来说明怎样在 Bootrom 下使用 ping 命令：

```
bootrom:> ping 10.10.29.160
Interface 0 has 2 ports (GMII)
Using octeth0 device
octeth0: Up 100 Mbps Full duplex (port 0)
host 10.10.29.160 is alive
```

## 相关命令

**saveenv**

### 3.5.7 ls

使用此命令列出一个目录下的文件(默认为 /)。

## 命令语法

**ls**

## 命令模式

Bootrom CLI

## 默认

无

## 使用说明

无

## 举例说明

这个例子用来说明怎样怎样列出一个目录中的文件(默认为 /)。

```
bootrom:> ls
Scanning JFFS2 FS: . done
drwxr-xr-x      0 Thu Jan 01 00:00:04 1970 log
drwxr-xr-x      0 Thu Jan 01 00:00:04 1970 boot
drwxr-xr-x      0 Thu Jan 01 00:00:04 1970 conf
-rw-----    144 Thu Jan 13 19:51:01 2000 dhcpsnooping
```

## 相关命令

无

### 3.5.8 boot\_tftp

使用此命令指定 TFTP 服务器中的 image 启动系统。

## 命令语法

**boot\_tftp** *image name*

image name	tftp 服务器上 Image 名字
------------	--------------------

## 命令模式

Bootrom CLI

## 默认

无

## 使用说明

无

## 举例说明

这个例子用来说明怎样通过 TFTP 服务器 boot 系统：

```
bootrom:> boot_tftp OS-ma-v3.0.1.it.r.bin
```

## 相关命令

无

### 3.5.9 boot\_tftp\_nopass

使用此命令指定 TFTP 服务器中默认配置的系统 image 启动系统。

## 命令语法

**boot\_tftp\_nopass** *image name*

image name	tftp 服务器上 Image 名字
------------	--------------------

## 命令模式

Bootrom CLI

## 默认

无

## 使用说明

无

## 举例说明

这个例子用来说明怎样通过 TFTP 服务器 boot 系统。

```
bootrom:> boot_tftp_nopass OS-ma-v3.0.1.it.r.bin
```

## 相关命令

无

### 3.5.10 boot\_flash

使用此命令指定 flash 中系统 image 或默认的 image 来启动系统。

## 命令语法

**boot\_flash** *image name*

image nam	在 flash 上的 Image 名字
-----------	---------------------

## 命令模式

Bootrom CLI

## 默认

无

## 使用说明

无

## 举例说明

这个例子用来说明怎样 boot 系统通过 flash 中指定的系统 image。

```
bootrom:> boot_flash
```

## 相关命令

无

### 3.5.11 boot\_flash\_nopass

使用此命令能指定 flash 中系统 image 或默认 image 启动系统。

#### 命令语法

**boot\_flash\_nopass** *image name*

image nam	在 flash 上的 Image 名字
-----------	---------------------

#### 命令模式

Bootrom CLI

#### 默认

无

#### 使用说明

无

#### 举例说明

这个例子用来说明通过 flash 中指定的 image 启动系统。

```
bootrom:> boot_flash_nopass /boot/OS-ma-v3.0.1.it.r.bin
Do you want to revert to the default config file ? [Y|N|E]:Y
```

#### 相关命令

无

### 3.5.12 upgrade\_uboot

使用此命令通过 TFTP 服务器更新 Bootrom 的 image。

#### 命令语法

**upgrade\_uboot** *image name*

image name	TFTP 服务器 Image 名字
------------	-------------------



## 命令模式

Bootrom CLI

## 默认

无

## 使用说明

无

## 举例说明

这个例子用来说明怎样通过 TFTP 服务器更新 U-boot 的 image。

```
bootrom:> upgrade_uboot u-boot.bin
```

## 相关命令

无

## 3.6 Bootup Diagnostic 命令

### 3.6.1 diagnostic bootup level

使用这个命令可以配置交换机下次启动的启动诊断等级。

## 命令语法

**diagnostic bootup level (minimal | complete)**

**no diagnostic bootup level**

minimal	最小 bootup level 测试
complete	完全 bootup level 测试

## 命令模式

全局配置模式

## 默认

无

## 使用说明

无

## 举例说明

这个样例用来显示如何配置启动诊断等级：

```
Switch# configure terminal
Switch(config)# diagnostic bootup level minimal
```

## 相关命令

无

### 3.6.2 show diagnostic bootup level

使用这个命令可以查看启动诊断等级。

## 命令语法

```
show diagnostic bootup level
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

这个样例用来显示查看启动诊断等级：

```
Switch# show diagnostic bootup level
The current running bootup diag level is complete
The next running bootup diag level is complete
```

## 相关命令

无

### 3.6.3 show diagnostic bootup result

使用这个命令可以查看系统启动后，启动诊断的诊断结果。

## 命令语法

**show diagnostic bootup result (slot id | )**

**show diagnostic bootup result detail (slot id | )**

id	堆叠情况下的 member 号
----	-----------------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

这个样例用来显示查看启动诊断的诊断结果：

```
Switch# show diagnostic bootup result detail
#####
Item Name                Attribute Result Time(usec)
1    EPLD TEST            C          Pass    57
2    EEPROM0 TEST        C          Pass   101262
3    PHY TEST             C          Pass   1161
4    FAN TEST             C          Pass   4668
5    SENSOR TEST         C          Pass   5472
6    PSU TEST            C          Pass   1370
7    L2 UCAST FUNC TEST  C          Pass  40126
```

## 相关命令

无

## 3.7 Bootstrap 命令

### 3.7.1 bootstrap

使用此命令配置 bootstrap 功能；使用 disable 关键字，取消某项设置。

## 命令语法

**bootstrap (enable | disable )**

enable	启动 bootstrap 初始化配置功能
disable	关闭 bootstrap 初始化配置功能

## 命令模式

全局配置模式

## 默认

bootstrap 初始化配置功能关闭。

## 使用说明

bootstrap 是一种设备启动时自动完成初始化配置的功能。设备在启动时如果没有 startup-config 文件，或者 bootstrap 功能被启用，则开始启动 bootstrap 工作流程。

## 举例说明

启用 bootstrap 功能：

```
Switch(config)# bootstrap enable
```

关闭 smartconfig 功能：

```
Switch(config)# bootstrap disable
```

## 相关命令

**ip address dhcp**

### 3.7.2 show smart-config config

使用此命令显示 smartconfig 的配置信息。

## 命令语法

**show smart-config config**

## 命令模式

特权模式

## 默认

无

## 使用说明

此命令显示当前 smartconfig 的配置。

## 举例说明

查看 smartconfig 功能当前的配置：

```
Switch# show smart-config config
Smart-Config config:
  initial-switch-deployment: on
  hostname-prefix: on
  Send log message to console: on
```

## 相关命令

**ip address dhcp**

**smart-config**

# 4 网络管理命令行参考

## 4.1 网络诊断命令

### 4.1.1 ping

使用该命令来检测到一个网络内的某个主机的可达性以及统计信息。一般会有几种结果，如：目标不可达；网段不可达；主机不可达；端口不可达；超时。该命令可以在公网内或 VRF 内使用。

#### 命令语法

ping (ip | mgmt-if) *WORD*

**ping** (vrf *WORD* | ) [-a *WORD*] -si *IFNAME*|-m *INTERVAL* |-c *COUNT*|-s *DATASIZE* |-f|-tos *TOS*|-h *TTL*|-t *TIMEOUT*] *WORD*

ping (mgmt-if |) ipv6 *WORD* (interface *IFNAME* |)

-a <i>WORD</i>	指定源 IP 地址，默认为出端口的 IP 地址
-si <i>IFNAME</i>	指定 ping 报文的源端口
ip	普通 IPv4 网络
vrf <i>WORD</i>	VRF 网络
mgmt-if	管理口
<i>WORD</i>	要检测的主机地址,支持 IPv4 和 IPv6 地址
ipv6	普通 IPv6 网络
interface	指定出接口 LinkLocal 地址
<i>IFNAME</i>	接口名
-m <i>INTERVAL</i>	指定报文发送间隔，单位是毫秒，范围是 10~10000
-c <i>COUNT</i>	指定发送报文数量，范围是 1~4294967295
-s <i>DATASIZE</i>	指定发送报文的数据部分长度，单位是字节，范围是 20~9600
-f	指定发送的报文不分片

-tos TOS	指定报文中 tos 值，范围是 0~255
-h TTL	指定报文中 ttl 值，范围是 1~255
-t TIMEOUT	指定请求报文的超时时间，单位是毫秒，范围是 0~65535，当前只支持 1000 的整数倍

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面的例子显示了如何在管理口上检测一个主机的可达性。

```
Switch# ping mgmt-if 10.10.29.247
PING 10.10.29.247 (10.10.29.247) 56(84) bytes of data.
64 bytes from 10.10.29.247: icmp_seq=1 ttl=64 time=0.194 ms
64 bytes from 10.10.29.247: icmp_seq=2 ttl=64 time=0.131 ms
64 bytes from 10.10.29.247: icmp_seq=3 ttl=64 time=0.134 ms
64 bytes from 10.10.29.247: icmp_seq=4 ttl=64 time=0.121 ms
64 bytes from 10.10.29.247: icmp_seq=5 ttl=64 time=0.135 ms
--- 10.10.29.247 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3996ms
rtt min/avg/max/mdev = 0.121/0.143/0.194/0.025 ms
```

## 相关命令

traceroute

### 4.1.2 traceroute

该命令用来查看 IPv4 报文从当前设备传到目的设备所经过的路径。

当用户使用 ping 命令测试发现网络出现故障后，可以用 **traceroute** 命令分析出现故障的网络节点。

## 命令语法

```
traceroute (ip|ipv6|vrf WORD |mgmt-if) WORD
```

-a	指定源 IP 地址，默认为出端口的 IP 地址
-si	指定 traceroute 报文的源端口
ip	普通 IPv4 网络
ipv6	普通 IPv6 网络
vrf WORD	VRF 网络
mgmt-if	管理口
WORD	要检测的主机地址

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面的例子显示了如何查看到 1.1.1.2 这个主机所经过的路径：

```
Switch# traceroute 1.1.1.2
traceroute to 1.1.1.2 (1.1.1.2), 30 hops max, 38 byte packets
 1  1.1.1.2 (1.1.1.2)  108.129 ms  99.313 ms  94.720 ms
```

## 相关命令

ping

## 4.2 NTP 命令

### 4.2.1 ntp ace

使用此命令创建对 NTP 服务器/对端设备的访问控制规则（ACE）。使用关键字 **no** 删除访问控制规则。

## 命令语法

```
ntp ace (address | hostname) (mask A.B.C.D) (version | kod | ignore | noquery | nomodify | notrap | noserve | nopeer | notrust | limited | none)
```



no ntp ace (*address | hostname*) (mask *A.B.C.D*) (version | kod | ignore | noquery | nomodify | notrap | noserve | nopeer | notrust | limited | none)

address	NTP 服务器/对端设备的 IP 地址
hostname	NTP 服务器/对端设备的名称
mask A.B.C.D	地址掩码
version	忽略不匹配版本号的服务器
kod	如果拒绝访问，发送 kiss-of-death 报文
ignore	忽略所有报文
noquery	忽略 NTP 6 和 7 模式的报文
nomodify	忽略 NTP 6 和 7 模式中试图改变服务器状态的报文
notrap	忽略 trap 报文
noserve	忽略 NTP 6 和 7 以外的报文
nopeer	不作为 NTP 对端使用
notrust	不信任的服务器，不作为同步源
limited	限制同一网络中 client 的数量
none	无限制

## 命令模式

全局配置模式

## 默认

无

## 使用说明

使用此命令创建对 NTP 服务器/对端设备的访问控制规则（ACE）。

## 举例说明

下面是创建一个 1.1.1.1 的访问控制规则的例子：

```
Switch# configure terminal
Switch(config)# ntp ace 1.1.1.1 version
```

## 相关命令

show ntp

### 4.2.2 ntp authentication

通过使用 `ntp authentication enable` 命令，使能 NTP 鉴权功能。

通过使用 `ntp authentication disable` 命令，去使能 NTP 鉴权功能。

## 命令语法

ntp authentication (enable | disable)

enable	使能 NTP 鉴权
disable	去使能 NTP 鉴权

## 命令模式

全局配置模式

## 默认

无

## 使用说明

当 NTP 鉴权功能使能时，设备会使用信任的 key 加密与 NTP server 同步时间。更多的信息可参考 `ntp trustedkey` 命令行。

## 举例说明

下面举例使能 NTP 鉴权功能：

```
Switch# configure terminal
Switch(config)# ntp authentication enable
```

## 相关命令

show ntp

### 4.2.3 ntp broadcast client

在端口模式下使用 `ntp broadcast client` 命令，使得该端口监听 NTP 广播报文。使用关键字 `no` 关闭该功能。

## 命令语法

```
ntp broadcast client
no ntp broadcast client
```

## 命令模式

端口配置模式

## 默认

无

## 使用说明

在 interface 模式下使用此命令，使得系统监听此 interface 上的 NTP 广播报文。

## 举例说明

举例说明，在 interface eth-0-1 上配置 ntp broadcast client，使能 NTP 广播报文监听。

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ntp broadcast client
```

## 相关命令

ntp broadcastdelay

### 4.2.4 ntp broadcastdelay

使用 ntp broadcastdelay 命令，配置设备与 NTP 广播服务器之间的传输延时。使用关键字 no 关闭该功能。

## 命令语法

```
ntp broadcastdelay delay
no ntp broadcastdelay
```

delay	NTP 广播延时时长，配置范围为 1-10000ms。
-------	-----------------------------

## 命令模式

全局配置模式

## 默认

关闭

## 使用说明

无

## 举例说明

下面举例，将 NTP 广播延时时长配置成 2000ms:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config)# ntp broadcastdelay 2000
```

## 相关命令

ntp broadcast client

### 4.2.5 ntp disable

使用 ntp disable 命令，在特定的端口上禁止接受 NTP 报文。

## 命令语法

```
ntp disable
no ntp disable
```

## 命令模式

端口配置模式

## 默认

缺省所有接口都接受 NTP 报文

## 使用说明

无

## 举例说明

下面举例，在端口 eth-0-1 上禁止 NTP 报文接受:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ntp disable
```

## 相关命令

无

### 4.2.6 ntp key

使用 ntp key 配置 NTP 鉴权 key。

## 命令语法

**ntp key** keyid value

no ntp key *keyid*

keyid	鉴权 key 序号，范围是 1~64000
value	鉴权 key 值

## 命令模式

全局配置模式

## 默认

无

## 使用说明

使用此命令配置一个 NTP 可以有效值。

## 举例说明

下面举例，在 NTP key 123 中配置 key 值 321。

```
Switch# configure terminal
Switch(config)# ntp key 123 321
```

## 相关命令

show ntp

### 4.2.7 ntp interface reload

使用 ntp interface reload 命令，在端口下重新加载 NTP 配置。

## 命令语法

ntp interface reload

## 命令模式

全局配置模式

## 默认

无

## 使用说明

使用此命令在所有端口下重新加载 NTP 配置。

## 举例说明

下面举例重新加载所有端口下的 NTP 配置。

```
Switch# configure terminal
Switch(config)# ntp interface reload
```

## 相关命令

show ntp

## 4.2.8 ntp max-distance

使用 ntp max-distance，配置 NTP 最大同步距离的阈值。ntp max-distance 命令主要应用于 NTP 客户端，在客户端，NTP 会计算到各个 NTP 服务器的同步距离并且会和使用 ntp max-distance 命令配置的距离阈值相比较，如果同步距离超过了配置的阈值，客户端将不会同步该服务器的时钟。

## 命令语法

```
ntp max-distance <1-16>
```

```
no ntp max-distance <1-16>
```

<1-16>	指定 NTP 最大同步距离的阈值。缺省情况下，NTP 的最大同步距离阈值是 10 秒。
--------	---

## 命令模式

全局配置模式

## 默认

无

## 使用说明

无

## 举例说明

下面举例，配置最大同步距离 16。

```
DUT1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DUT1(config)# ntp max-distance 16
```

## 相关命令

无

### 4.2.9 ntp peer

使用 `ntp peer` 命令，配置设备同步 NTP 的对端。使用关键字 `no` 关闭该功能。

## 命令语法

**ntp peer** ( *hostname* | *address* ) { **key** *key-id* | **prefer** | **version number** } { *source-interface* *IFNAME* | *source-ip* *A.B.C.D* }

**no ntp peer** ( *hostname* | *address* )

<code>hostname</code>	对端名字
<code>address</code>	对端 IP 地址
<b>key</b> <i>key-id</i>	(可选)定义鉴权 key 值，范围是 1~64000
<b>prefer</b>	(可选)该 NTP 对端作为首选同步对端
<b>version number</b>	(可选)NTP 版本(1~3)
<i>IFNAME</i>	指定源接口名称
<i>A.B.C.D</i>	指定源 IP 地址

## 命令模式

全局配置模式

## 默认

无

## 使用说明

使用此命令，配置 NTP 对端，并且可以指定版本号等信息。如果指定源接口或者源 IP 地址，将会使用对应的 IP 地址作为发出报文的源 IP 地址。

## 举例说明

下面举例，配置 NTP 对端为 192.168.22.33，版本号为 2。

```
Switch# configure terminal
Switch(config)# ntp peer 192.168.22.33 version 2
```

## 相关命令

```
show ntp
```

### 4.2.10 ntp refclock

使用 ntp refclock 命令，为 NTP 配置外部时钟源。使用关键字 no 关闭该功能。

## 命令语法

```
ntp refclock stratum number
```

```
no ntp refclock
```

number	(可选) 配置 NTP 层次，数值从 1 到 15
--------	---------------------------

## 命令模式

全局配置模式

## 默认

关闭

## 使用说明

无

## 举例说明

下面举例配置 NTP 外部时钟源，NTP 层次为 1 层。

```
Switch# configure terminal
Switch(config)# ntp refclock stratum 1
```



## 相关命令

show ntp

### 4.2.11 ntp server

使用 ntp server 命令，配置设备同步 NTP 服务器。使用关键字 no 关闭该功能。

## 命令语法

**ntp server** ( *hostname* | *address* ) { **key** *key-id* | **prefer** | **version** *number* } { **source-interface** *IFNAME* | **source-ip** *A.B.C.D* }

**no ntp server** ( *hostname* | *address* )

hostname	对端名字
address	对端 IP 地址。
<b>key</b> <i>key-id</i>	(可选) 定义鉴权 key 值，范围是 1~64000
<b>prefer</b>	(可选) 该 NTP 对端作为首选同步对端
<b>version</b> <i>number</i>	(可选) NTP 版本(1~3)
<b>IFNAME</b>	指定源接口名称
<b>A.B.C.D</b>	指定源 IP 地址

## 命令模式

全局配置模式

## 默认

关闭

## 使用说明

使用该命令，配置设备同步 NTP 服务器。如果指定源接口或者源 IP 地址，将会使用对应的 IP 地址作为发出报文的源 IP 地址。

## 举例说明

下面举例，配置 NTP 服务器 172.16.22.44，版本号 2。

```
Switch# configure terminal
Switch(config)# ntp server 172.16.22.44 version 2
```

## 相关命令

show ntp

### 4.2.12 ntp trustedkey

使用 ntp trustedkey ，配置 NTP 信任的鉴权 key。使用关键字 no 关闭该功能。

## 命令语法

ntp trustedkey *key-id*

no ntp trustedkey *key-id*

key-id	KEY ID。范围是 1~64000
--------	--------------------

## 命令模式

全局配置模式

## 默认

无

## 使用说明

使用 ntp trustedkey ，配置 NTP 信任的鉴权 key。

## 举例说明

下面举例，配置鉴权 key 42，并设置成信任 key。

```
Switch# configure terminal
Switch(config)# ntp authentication enable
Switch(config)# ntp key 42 aNiceKey
Switch(config)# ntp trustedkey 42
```

## 相关命令

show ntp

ntp key

### 4.2.13 show ntp

通过 show ntp 命令，显示 NTP 配置。

## 命令语法

```
show ntp
```

## 命令模式

特权模式

## 默认

无

## 使用说明

通过 show ntp 命令，显示 NTP 配置。

## 举例说明

下面是显示 NTP 配置的例子：

```
Switch# show ntp
Current NTP configuration:
=====
NTP access control list:
Unicast peer:
  1.1.1.1
Unicast server:
  2.2.2.2
Broadcast client: enabled
Authentication: enabled
Local reference clock:
  enabled, stratum 10
```

## 相关命令

```
ntp server
```

```
ntp peer
```

### 4.2.14 show ntp ace

通过 show ntp ace 命令，显示 NTP 的 ace 配置信息。

## 命令语法

```
show ntp ace
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面的例子是通过 show 命令显示当前的访问控制规则配置：

```
Switch# show ntp ace
address maskcountflags
=====
0.0.0.0 0.0.0.0 55188noquery, nomodify, notrap
6.6.6.6 255.255.255.255 73 none
127.0.0.1255.255.255.2551259 none
```

## 相关命令

ntp ace

### 4.2.15 show ntp associations

通过 show ntp associations 命令，显示 NTP 邻居的状态。

## 命令语法

```
show ntp associations
```

## 命令模式

特权模式

## 默认

无

## 使用说明

详细的显示信息说明，可参见 NTP 定义（RFC1305）。

## 举例说明

下面举例显示 NTP 邻居状态：

```
Switch# show ntp associations
Current NTP associations:
  remoterefid st when poll reachdelayoffset disp
=====
*6.6.6.6 127.127.1.0 6 161 256 3770.778-0.087 119.400
```

\* synchronized, + candidate, # selected, x falsetick, . excess, - outlyer

## 相关命令

show ntp status

### 4.2.16 show ntp key

通过 show ntp key 命令，显示 NTP key。

## 命令语法

show ntp key

## 命令模式

特权模式

## 默认

无

## 使用说明

使用此命令显示 NTP key。

## 举例说明

下面举例，显示配置的 NTP key:

```
Switch# show ntp key
Current NTP key configuration:
=====
1 abcd
64000 KKKK
```

## 相关命令

ntp key

### 4.2.17 show ntp status

使用 show ntp status 命令，显示 NTP 状态。

## 命令语法

show ntp status

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面举例，显示当前 NTP 状态。

```
Switch# show ntp status
Current NTP status:
=====
clock is synchronized
stratum: 11
reference clock: 127.127.1.0
frequency:0.000 ppm
precision:2**15
reference time: d116c946.4dc2f6a7 ( 1:24:22.303 UTC Tue Mar 1 2011)
root delay: 0.000 ms
root dispersion: 449.207 ms
peer dispersion: 662.059 ms
clock offset:0.000 ms
stability:0.000 ppm
```

## 相关命令

show ntp associations

### 4.2.18 show ntp statistics

使用 show ntp statistics 命令，显示 NTP 统计值。

## 命令语法

```
show ntp statistics
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面是使用 `show ntp statistics` 命令获取统计值的例子：

```
Switch# show ntp statistics
Current NTP I/O statistics:
=====
time since reset: 175834
receive buffers: 10
free receive buffers: 9
used receive buffers: 0
low water refills:1
dropped packets: 0
ignored packets: 0
received packets: 32
packets sent: 31
packets not sent: 0
interrupts handled:32
received by int: 32
```

## 相关命令

`show ntp associations`

### 4.2.19 clear ntp statistics

使用 `clear ntp statistics` 命令，清除 NTP 统计值。

## 命令语法

`clear ntp statistics`

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面是使用 `clear ntp statistics` 命令清除统计值的例子：

```
Switch# clear ntp statistics
```

## 相关命令

`show ntp statistics`

## 4.3 Phy Loopback 命令

### 4.3.1 loopback phy

使用此命令设置接口的 phy-level loopback 模式。使用关键字 `no` 关闭该功能。

#### 命令语法

**loopback phy (internal *IFPHYSICAL* | external)**

<b>internal</b> <i>IFPHYSICAL</i>	芯片内部转发到当前接口的报文不做任何修改地转发到指定接口
<b>external</b>	当前接口从网络上收到的报文不做任何修改地转发回网络

#### 命令模式

端口配置模式

#### 默认

无

#### 使用说明

一个接口只能配置一种 loopback 模式，新的配置会覆盖掉原有配置。

#### 举例说明

下面例子中，从其他端口内部转发到接口 `eth-0-1` 的报文改为从 `eth-0-2` 出去。

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# loopback phy internal eth-0-2
```

#### 相关命令

`no loopback`

### 4.3.2 loopback port

使用此命令设置接口的 port-level loopback 模式。

#### 命令语法

**loopback port (mac-address swap|)**



<b>mac-address swap</b>	源 MAC 和目的 MAC 互换，并更新 FCS
-------------------------	--------------------------

## 命令模式

端口配置模式

## 默认

无

## 使用说明

一个接口只能配置一种 loopback 模式，新的配置会覆盖掉原有配置。

此模式下从网络上收到的报文会转发回网络，swap 字段指定是否进行源 MAC 和目的 MAC 互换。

## 举例说明

下面例子中，接口被设置为 port level loopback 模式。

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# loopback port
```

## 相关命令

no loopback

### 4.3.3 no loopback

使用此命令取消接口的 phy level 或 port level loopback 模式。

## 命令语法

no loopback

## 命令模式

端口配置模式

## 默认

无

## 使用说明

该命令用于取消接口的 loopback 配置。

## 举例说明

下面例子中，取消接口的 port level loopback 配置

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# loopback port
Switch(config-if)# no loopback
```

## 相关命令

loopback phy

loopback port

### 4.3.4 show phy loopback

使用此命令显示 phy loopback 的配置信息。

## 命令语法

```
show phy loopback
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子中，显示 phy loopback 的配置信息。

```
Switch# show phy loopback
InterfaceTypeDestIntfSwapMac
-----
eth-0-1port- no
eth-0-2port- yes
eth-0-3external--
eth-0-4internalet-0-5 -
-----
```

## 相关命令

loopback phy

loopback port

## 4.3.5 l2 ping

使用此命令允许用户使用指定包从指定接口 ping 指定的目的 MAC 地址。

### 命令语法

**l2 ping** *HHHH.HHHH.HHHH* **interface** *IFPHYSICAL* (**{vlan** <1-4094> **|interval** <1-65535> **|timeout** <1-65535> **|count** <1-65535> **|size** <64-1518>} |)

<i>HHHH.HHHH.HHHH</i>	目的 MAC
<b>interface</b> <i>IFPHYSICAL</i>	发送 ping 包的源接口
<b>vlan</b> <1-4094>	ping 包中的 vlan id
<b>interval</b> <1-65535>	两次 ping 包之间的时间间隔, 单位: 秒
<b>timeout</b> <1-65535>	等待 ping 包的时间间隔, 单位: 秒
<b>count</b> <1-65535>	ping 的总时间
<b>size</b> <64-1518>	ping 包大小

### 命令模式

特权模式

### 默认

缺省情况下, ping 协议包不带 vlan tag;

缺省的 ping 间隔 200 毫秒;

缺省的 ping 次数为 5 次;

缺省的 ping 包大小为 64。

### 使用说明

“Ctrl + C” 组合键取消 ping 操作。

### 举例说明

下面例子中, 显示了如何 ping 一个指定的目的 MAC 地址。

```
Switch# l2 ping 0000.0000.0001 interface eth-0-1 vlan 101 interval 200 timeout 1000
count 10 size 1500
```

## 相关命令

l2 ping response

### 4.3.6 l2 ping response

使用此命令使能 l2 ping response 功能。使用关键字 no 关闭该功能。

## 命令语法

**l2 ping response enable**

**no l2 ping response enable**

## 命令模式

端口配置模式

## 默认

无

## 使用说明

如果该功能未启用，l2 ping request 包会被丢掉。

## 举例说明

下面例子中，在接口上使能 l2 ping response 功能。

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# l2 ping response enable
```

## 相关命令

l2 ping

show l2ping response

### 4.3.7 show l2ping response

使用此命令显示 l2 ping 的配置信息。

## 命令语法

show l2ping response

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子中，显示 l2 ping 的配置信息。

```
Switch# show l2 ping response
InterfaceL2pingResp
-----
eth-0-7Enable
eth-0-8Enable
-----
```

## 相关命令

l2 ping response

### 4.3.8 show l2ping state

使用此命令显示 l2 ping 当前的状态。

## 命令语法

```
show l2ping state
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子中，显示 l2 ping 当前状态信息。

```
Switch# show l2ping response
L2 ping state.
-----
Total count  Interval  Timeout  VlanId  Packet size  Sequence
100 1515010
```

```
10 packet(s) transmitted, 0 received, 100 % packet loss
```

## 相关命令

无

### 4.3.9 l2 ping stop

使用此命令停止 L2ping 处理。

## 命令语法

```
l2 ping stop
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子中，停止当前 L2 ping 处理。

```
Switch# l2 ping stop
```

## 相关命令

无

### 4.3.10 l2 ping forward enable

使用此命令使能端口 L2ping 报文转发功能，否则不转发 L2ping 报文。

## 命令语法

```
l2 ping forward enable  
no l2 ping forward enable
```

## 命令模式

端口配置模式

## 默认

使能

## 使用说明

无

## 举例说明

下面例子中，使能端口 L2ping 报文转发功能。

```
Switch (config-if)# l2 ping forward enable
```

## 相关命令

无

### 4.3.11 debug l2ping

使用此命令使能 l2 ping 的 debugging 功能。

## 命令语法

```
debug l2ping (all | packet | send | receive | response)
```

```
no debug l2ping (all | packet | send | receive | response)
```

## 命令模式

特权模式

## 默认

关闭

## 使用说明

如果 debugging 开关打开，系统会打印相关信息。

## 举例说明

下面例子中，使能 l2 ping 的 debugging 功能。

```
Switch# debug l2ping all
```

## 相关命令

l2 ping response

### 4.3.12 show debugging l2ping

使用此命令显示 l2 ping 的 debugging 状态。

#### 命令语法

```
show debugging l2ping
```

#### 命令模式

特权模式

#### 默认

无

#### 使用说明

无

#### 举例说明

下面例子中，显示 l2 ping 的 debugging 状态。

```
Switch# show debugging l2ping
L2ping debugging status:
  l2ping packet debugging is on
  l2ping receive debugging is on
  l2ping send debugging is on
  l2ping response debugging is on
```

#### 相关命令

l2 ping response

## 4.4 SNMP 命令

### 4.4.1 snmp-server access

全局配置模式下，使用 snmp-server access 命令配置 MIB 视图的访问控制属性。该命令的 no 格式删除访问控制属性。

#### 命令语法

```
snmp-server access group-name security-model usm (auth | noauth | priv) {context context
(prefix | exact) | read read-view | write write-view | notify notify-view | }
```

```
no snmp-server access group-name security-model usm (auth | noauth | priv) {context context
| }
```



<b>group-name</b>	组名
<b>security-model</b>	组的安全模式
<b>usm</b>	SNMPv3 usm 安全模式
<b>auth</b>	指明对报文进行认证但不加密
<b>noauth</b>	指明对报文既不认证也不加密
<b>priv</b>	指明对报文进行认证和加密
<b>context context</b>	(可选项) 组内视图的 context
<b>prefix</b>	context 只匹配前缀
<b>exact</b>	全部匹配 context
<b>read read-view</b>	(可选项) 配置组的只读视图。该视图允许用户对代理进行读操作
<b>write write-view</b>	(可选项) 配置组的写视图。该视图允许用户对代理进行写操作
<b>notify notify-view</b>	(可选项) 配置组的通告视图。该视图允许代理发送通告给网管工作站

## 命令模式

全局配置模式

## 默认

无访问控制设置

## 使用说明

该命令配置 MIB 视图的访问安全控制属性。

## 举例说明

下例演示如何配置访问安全控制属性：

```
Switch(config)# snmp-server access manage security-model usm auth write _all_ read
_all_
```

## 相关命令

show snmp-server access

## 4.4.2 snmp-server community

全局配置模式下，使用 `snmp-server community` 命令配置一个新的 SNMP 团体。该命令的 `no` 格式删除 SNMP 团体。

### 命令语法

```
snmp-server community string (read-only | read-write) (view view-name |)
```

```
no snmp-server community string
```

<code>string</code>	团体名，为 1~256 个字符的字符串，作用类型密码。空格表示不允许访问
<code>read-only</code>	表明对 MIB 对象进行只读的访问。网管工作站只能执行读操作
<code>read-write</code>	表明对 MIB 对象进行读写的访问。网管工作站可以执行读写操作
<code>view view-name</code>	用来指定网管工作站可以访问的 MIB 对象的范围

### 命令模式

全局配置模式

### 默认

无 SNMP 团体名

### 使用说明

无

### 举例说明

下例演示如何创建一个名为 `newstring` 的团体，该团体对 `mib` 有读写权限。

```
Switch(config)# snmp-server community newstring read-write
```

### 相关命令

`snmp-server enable`

## 4.4.3 snmp-server context

全局配置模式下，使用 `snmp-server context` 命令配置 SNMP context 信息。该命令的 `no` 格式删除该配置。

## 命令语法

```
snmp-server context context-name  
no snmp-server context context-name
```

context-name	SNMP context
--------------	--------------

## 命令模式

全局配置模式

## 默认

无 SNMP context 配置

## 使用说明

无

## 举例说明

下例演示如何创建一个 context:

```
Switch(config)# snmp-server context contextA
```

## 相关命令

```
show snmp-server context
```

### 4.4.4 snmp-server enable

全局配置模式下，使用 `snmp-server enable` 命令使能 SNMP 代理功能。该命令的 `no` 格式关闭 SNMP 功能。

## 命令语法

```
snmp-server enable  
no snmp-server enable
```

## 命令模式

全局配置模式

## 默认

SNMP 默认为关闭

## 使用说明

该命令用来使能或关闭 SNMP 代理功能。

## 举例说明

下例演示如何启用 SNMP 功能:

```
Switch(config)# snmp-server enable
```

## 相关命令

```
show snmp
```

### 4.4.5 snmp-server engineID

全局配置模式下，使用 `snmp-server engineID` 命令设置本地设备的 SNMP 的引擎 ID。该命令的 `no` 格式删除引擎 ID。

## 命令语法

```
snmp-server engineID engineid-string
```

```
no snmp-server engineID
```

<code>engineid-string</code>	引擎 ID 字符串必须偶数个十六进制数,最小为 10 个字符,最大 64 个字符
------------------------------	--

## 命令模式

全局配置模式

## 默认

可通过 `show snmp-server engineID` 命令显示默认引擎 ID

## 使用说明

SNMP 的引擎 ID 唯一标识了设备。它是一个可选配置。关于 SNMP 引擎的更多信息,请参考 RFC2571。

## 举例说明

下例演示如何配置 engineID:

```
Switch(config)# snmp-server engineID 30383038303830383038
```

## 相关命令

```
show snmp-server engineID
```

## 4.4.6 snmp-server group

全局配置模式下，使用 `snmp-server group` 命令配置一个新的 SNMP 组。该命令的 `no` 格式用来删除组。

### 命令语法

```
snmp-server group group-name user user-name security-model usm
```

```
no snmp-server group group-name user user-name security-model usm
```

group-nam	组名
<b>user</b> user-name	组中用户名
security-model	配置组的安全模型
usm	配置基于用户安全模型（USM）的 SNMPv3 安全模型

### 命令模式

全局配置模式

### 默认

无 SNMP 组

### 使用说明

该命令用于创建一个新的 SNMP 组。

### 举例说明

下例演示如何创建一个新的 SNMP 组：

```
Switch(config)# snmp-server group SampleA user User1 security-model usm
```

### 相关命令

```
show snmp-server group
```

## 4.4.7 snmp-server notify

全局配置模式下，使用 `snmp-server notify` 命令配置 SNMP 的通告。该命令的 `no` 格式用来将通告值恢复成默认。

### 命令语法

```
snmp-server notify notify-name tag tag-name (inform | trap | )
```

`no snmp-server notify notify-name`

<code>notify-name</code>	通告名称
<code>tag tag-name</code>	标记名字
<code>inform</code>	设置通告类型为 <code>inform</code>
<code>trap</code>	设置通告类型为 <code>trap</code>

## 命令模式

全局配置模式

## 默认

无 SNMP 通告

## 使用说明

无

## 举例说明

下例演示如何设置通告：

```
Switch(config)# snmp-server notify note tag tt
```

## 相关命令

`show snmp-server notify`

## 4.4.8 snmp-server system-contact

全局配置模式下，使用 `snmp-server system-contact` 命令配置设备管理者联系方式。该命令的 `no` 格式用来删除联系方式。

## 命令语法

`snmp-server system-contact text`

`no snmp-server system-contact`

<code>text</code>	设备管理者联系方式
-------------------	-----------

## 命令模式

全局配置模式

## 默认

无联系方式

## 使用说明

该命令配置设备管理者联系方式。可通过 `configure` 配置文件查看到该联系方式。

## 举例说明

下例演示将联系方式设置为 `admin@example.com`：

```
Switch(config)# snmp-server system-contact admin@example.com
```

## 相关命令

`snmp-server system-location`

### 4.4.9 snmp-server system-location

全局配置模式下，使用 `snmp-server system-location` 命令配置设备放置位置的描述符。该命令的 `no` 格式用来删除该描述符。

## 命令语法

`snmp-server system-location text`

`no snmp-server system-location`

text	设备放置位置的描述符
------	------------

## 命令模式

全局配置模式

## 默认

无位置描述符

## 使用说明

该命令配置放置位置的描述符。可通过 `configure` 配置文件查看到该描述符。

## 举例说明

下例演示将位置描述符设置为 Sample Place:

```
Switch(config)# snmp-server system-location Sample Place
```

## 相关命令

snmp-server system-contact

### 4.4.10 snmp-server target-address

全局配置模式下，使用 snmp-server target-address 命令指定允许接收 SNMP 请求报文的目的主机。该命令的 no 格式用来删除该配置。

## 命令语法

```
snmp-server target-address WORD param WORD ((mgmt-if) ipv4-address | ipv6-address)
({udpport port | timeout number | retries number } |) (taglist LINE |)
```

```
no snmp-server target-address WORD (mgmt-if)
```

WORD	远程目的主机名称
param	地址参数表
WORD	地址参数表名（必须是本地已经配置的地址参数名）
mgmt-if	使用管理口
ipv4-address	IPv4 格式的目的地址
ipv6-address	IPv6 格式的目的地址
community string	团体名
udpport port	(可选项)UDP 端口号，默认值 162
timeout number	超时时间
retries number	重传次数
taglist LINE	标记列表，用于标识发送通告和转发消息到其上的目的地址，可以配置多个值，中间使用空格隔开（最多支持 128 个），最大长度 255 个字符

## 命令模式

全局配置模式



## 默认

无目的主机 IP 配置

## 使用说明

只用于 SNMPv3。

## 举例说明

下例演示将主机 10.0.0.2 设置为信任，允许响应该主机的 SNMP 请求。

```
Switch(config)# snmp-server target-address targ1 param parm1 10.0.0.2 taglist
tmptag
```

## 相关命令

show snmp-server target-address

### 4.4.11 snmp-server trap enable

全局配置模式下，使用 snmp-server trap enable 命令使能相关的 SNMP 通告类型。该命令的 no 格式用来关闭此功能。

## 命令语法

snmp-server trap enable *notification-type*

no snmp-server trap enable *notification-type*

notification-ty	使能或关闭的通告类型。如果使用“all”参数。系统将使能或者关闭使用该命令的所有通告类型
-----------------	--

## 命令模式

全局配置模式

## 默认

关闭此功能

## 使用说明

snmp-server trap enable 和 snmp-server trap target-address 命令是一起使用的。使用该命令允许设备发送指定类型的 trap。

## 举例说明

下例演示如何启用设备的所有 trap 功能:

```
Switch(config)# snmp-server trap enable all
```

## 相关命令

```
snmp-server trap target-address
```

### 4.4.12 snmp-server trap delay

全局配置模式下, 使用 `snmp-server trap delay` 命令延迟 snmp trap 发送。该命令的 `no` 格式用来关闭此功能。

## 命令语法

```
snmp-server trap delay (linkup| linkdown) <1-100>
```

```
no snmp-server trap delay (linkup| linkdown)
```

## 命令模式

全局配置模式

## 默认

关闭此功能

## 使用说明

默认配置下端口 up/down 时会马上出发相关 trap, 配置改命令后端口状态改变后会等待一个延迟后才产生 trap。比如在环网中链路切换后, 由于三层网络不能马上切换, 如果马上发送 trap 的话可能会丢失。该命令的单位是 100ms。

## 举例说明

下例演示如何设置设备链路 up 时的 delay 功能:

```
Switch(config)# snmp-server trap delay linkup 10
```

## 相关命令

```
snmp-server trap target-address
```

### 4.4.13 snmp-server trap target-address

全局配置模式下, 使用该命令配置系统产生的 trap 发送到指定的服务器。该命令的 `no` 格式用来删除。

## 命令语法

**snmp-server trap target-address (mgmt-if | (ipv4-address | ipv6-address) community string (udpport number | )**

**no snmp-server trap target-address (mgmt-if | (ipv4-address | ipv6-address) community string (udpport number | )**

mgmt-if	通过管理口发送
ipv4-address	Trap 接收服务器的 IPv4 地址
ipv6-address	Trap 接收服务器的 IPv6 地址
community string	团体名称
udpport number	Trap 发送的端口号。默认端口号为 162

## 命令模式

全局配置模式

## 默认

无相关配置

## 使用说明

该命令用于指定系统产生的 trap 发送目的地。

## 举例说明

下例演示如何将系统产生的 trap 通过管理口发送到 IP 为 192.168.1.100 的设备：

```
Switch(config)# snmp-server trap target-address mgmt-if 192.168.1.100 community
test udpport 6000
```

## 相关命令

snmp-server trap enable

### 4.4.14 snmp-server inform target-address

全局配置模式下，使用该命令配置系统产生的 inform 发送到指定的服务器。该命令的 no 格式用来删除。

## 命令语法

**snmp-server inform target-address (mgmt-if | (ipv4-address | ipv6-address) community string (udpport number | )**

`no snmp-server inform target-address (mgmt-if | ) (ipv4-address | ipv6-address) community string (udpport number | )`

mgmt-if	通过管理口发送
ipv4-address	Inform 接收服务器的 IPv4 地址
ipv6-address	Inform 接收服务器的 IPv6 地址
community string	团体名称
udpport number	Trap 发送的端口号。默认端口号为 162

## 命令模式

全局配置模式

## 默认

无相关配置

## 使用说明

该命令用于指定系统产生的 Inform 发送目的地。

## 举例说明

下例演示如何将系统产生的 inform 通过管理口发送到 IP 为 192.168.1.100 的设备：

```
Switch(config)# snmp-server inform target-address mgmt-if 192.168.1.100 community test udpport 6000
```

## 相关命令

无

### 4.4.15 snmp-server usm-user

全局配置模式下，使用 `snmp-server usm-user` 命令配置一个用户。该命令的 `no` 格式用来删除此用户。

## 命令语法

**snmp-server usm-user** *username* (*remote engine-id* |) (**authentication** (**md5** | **sha**) (8 |) *auth-passsword* (**privacy** (**aes** | **des**) (8 |) *privpassword* |) |)

`no snmp-server usm-user username`

username	用来连接到代理设备的用户名
remote engine-id	(可选项)用户所属远程设备的 engine-id
authentication	(可选项)配置认证协议
md5	(可选项)配置认证协议为 HMAC-MD5
sha	(可选项)配置认证协议为 HMAC-SHA
auth-passwor	(可选项)配置认证密码
privacy	(可选项)配置安全模型为 SNMPv3 USM
aes	(可选项)配置加密协议为 AES(the Advanced Encryption Standard)
des	(可选项)配置加密协议为 DES(Digital Encryption Standard)
8	(可选项)是否隐藏密码
privpassword	(可选项)指定加密密码

## 命令模式

全局配置模式

## 默认

无配置用户

## 使用说明

要使配置的用户生效，必须要指定远程代理设备的 IP 地址或端口号。

## 举例说明

下例演示如何配置一个用户：

```
Switch(config)# snmp-server usm-user user1 authentication md5 mypassword privacy
des yourpassword
```

## 相关命令

snmp-server engineID

### 4.4.16 snmp-server version

全局配置模式下，使用 `snmp-server version` 命令配置系统支持的 SNMP 的版本号。该命令的 `no` 格式用来恢复版本号为默认值。

## 命令语法

```
snmp-server version (all | v1 | v2c | v3)
```

```
no snmp-server version
```

all	支持所有版本号（v1，v2c 和 v3）
v1	只支持 v1
v2c	只支持 v2c
v3	只支持 v3

## 命令模式

全局配置模式

## 默认

支持所有版本号

## 使用说明

该命令设置交换机支持的 SNMP 版本号。

## 举例说明

下例演示如何使系统支持所有 SNMP 版本：

```
Switch(config)# snmp-server version all
```

## 相关命令

```
show snmp-server version
```

### 4.4.17 snmp-server view

全局配置模式下，使用 `snmp-server view` 命令创建或更新 SNMP 视图。该命令的 `no` 格式用来删除 SNMP 视图。

## 命令语法

```
snmp-server view view-name (included | excluded) sub-tree (mask WORD | )
```

```
no snmp-server view view-name (included | excluded) sub-tree
```

view-name	创建或更新的视图名称
-----------	------------

included	视图包含的 MIB 树节点，即允许访问 MIB 子树的所有节点
excluded	视图不包含的 MIB 树节点，，即禁止访问 MIB 子树的所有节点
sub-tree	MIB 对象子树
mask	MIB 对象子树掩码

## 命令模式

全局配置模式

## 默认

无视图

## 使用说明

该命令创建的 SNMP 视图将作为其他 SNMP 命令的参数被使用。

## 举例说明

下例演示如何创建一个 SNMP 视图：

```
Switch(config)# snmp-server view abc excluded 1.3.6.2
```

## 相关命令

show snmp-server view

### 4.4.18 snmp-server access-group NAME in

全局配置模式下，使用该命令配置 ACL 过滤访问控制。该命令的 no 格式用来删除改配置。

## 命令语法

snmp-server access-group *name* in

name	访问控制列表名称
in	过滤方向

## 命令模式

全局配置模式

## 默认

无访问控制组

## 使用说明

该命令在 SNMP 模块中应用 ACL 功能。

## 举例说明

下例演示如何应用一条 ACL 到 SNMP:

```
Switch(config)# snmp-server access-group abc in
```

## 相关命令

无

### 4.4.19 show snmp

特权模式下，使用 show snmp 命令显示 SNMP 的服务信息。

## 命令语法

```
show snmp
```

## 命令模式

特权模式

## 默认

无

## 使用说明

该命令显示 SNMP 的服务信息（使能或关闭）。

## 举例说明

下例演示如何显示 SNMP 服务:

```
Switch# show snmp  
SNMP services: enable
```

## 相关命令

```
snmp-server enable
```



## 4.4.20 show snmp-server access

特权模式下，使用 `show snmp-server access` 命令显示 SNMP 的访问控制信息。

### 命令语法

```
show snmp-server access (group-name|)
```

group-name	指定组名
------------	------

### 命令模式

特权模式

### 默认

无

### 使用说明

该命令用来显示 `snmp-server access` 命令配置的访问控制信息。

### 举例说明

下例演示如何显示访问控制信息：

```
Switch# show snmp-server access gp1
Group-namemodel
=====
Group name:group1
Context:
Security model: usm
Security level:  priv
Context Match: exact
Read view:_all_
Write view:none
Notify view:none
Storage Type:  permanent
Row status:active
```

### 相关命令

`snmp-server access`

## 4.4.21 show snmp-server community

特权模式下，使用 `show snmp-server community` 命令显示 SNMP 团体信息。

## 命令语法

```
show snmp-server community
```

## 命令模式

特权模式

## 默认

无

## 使用说明

该命令用来显示 `snmp-server community` 命令配置的团体信息。

## 举例说明

下例演示如何显示系统当前的团体信息：

```
Switch# show snmp-server community
Community-AccessCommunity-String Security-name
=====
read-onlypubliccomm1
read-writeprivatecomm2
```

## 相关命令

```
snmp-server community
```

### 4.4.22 show snmp-server context

特权模式下，使用 `show snmp-server context` 命令显示 SNMP context 信息。

## 命令语法

```
show snmp-server context
```

## 命令模式

特权模式

## 默认

无

## 使用说明

该命令用来显示 `snmp-server context` 命令配置的 SNMP context 信息。

## 举例说明

下例演示如何显示 context 信息：

```
Switch# show snmp-server context
samplecontext
```

## 相关命令

snmp-server context

### 4.4.23 show snmp-server engineID

特权模式下，使用 show snmp-server engineID 命令显示 engineID 信息。

## 命令语法

```
show snmp-server engineID
```

## 命令模式

特权模式

## 默认

无

## 使用说明

SNMP 引擎 ID 是 SNMP 实体的唯一标识。

## 举例说明

下例演示如何显示 engineID：

```
Switch# show snmp-server engineID
Engine ID: 00000009020000000c025808
```

## 相关命令

snmp-server engineID

### 4.4.24 show snmp-server group

特权模式下，使用 show snmp-server group 命令显示组信息。包括组名，安全模式，视图，存储类型的等。

## 命令语法

```
show snmp-server group (group-name)
```

group-name	指定组名
------------	------

## 命令模式

特权模式

## 默认

无

## 使用说明

使用 `snmp-server group` 命令配置 SNMP 组。

## 举例说明

下例演示如何显示 SNMP 组：

```
Switch# show snmp-server group
Group-namemodel Security-name
=====
allusma
allusmab
```

## 相关命令

`snmp-server group`

### 4.4.25 show snmp-server notify

特权模式下，使用 `show snmp-server notify` 命令显示 SNMP 通告信息。

## 命令语法

`show snmp-server notify (group-name)`

group-name	指定组名
------------	------

## 命令模式

特权模式

## 默认

无

## 使用说明

该命令用来显示 `snmp-server notify` 命令配置的 SNMP 通告信息。

## 举例说明

下例演示如何显示 SNMP 通告信息：

```
Switch# show snmp-server notify
Notify-name Notify-type
=====
sampletrap
```

## 相关命令

`snmp-server notify`

### 4.4.26 show snmp-server sys-info

特权模式下，使用 `show snmp-server sys-info` 命令显示当前 SNMP 设备的系统信息。

## 命令语法

```
show snmp-server sys-info
```

## 命令模式

特权模式

## 默认

无

## 使用说明

该命令用于显示 `snmp-server system-contact` 和 `snmp-server system-location` 命令设置的信息。

## 举例说明

下例演示如何显示系统信息：

```
Switch# show snmp-server sys-info
Contact:admin@sampldomain.com
Location:Denvor
```

## 相关命令

`snmp-server system-contact`

`snmp-server system-location`

## 4.4.27 show snmp-server trap-receiver

特权模式下，使用 `show snmp-server trap-receiver` 命令显示 SNMP 的 traps 接收主机。

### 命令语法

```
show snmp-server trap-receiver
```

### 命令模式

特权模式

### 默认

无

### 使用说明

该命令用来显示 `snmp-server trap target-address` 命令配置的 trap 接收信息。

### 举例说明

下例演示如何显示 SNMP 的 traps 接收主机：

```
Switch# show snmp-server trap-receiver
Target-ipaddress  udpport  version  pdu-type  community
=====
1.1.1.1234        v2c    informpublic
1.1.1.1234        v2c    trap    public
1.1.1.1234        v1trap public
```

### 相关命令

`snmp-server trap target-address`

## 4.4.28 show snmp-server usm-user

特权模式下，使用 `show snmp-server usm-user` 命令显示 SNMP 的用户信息。

### 命令语法

```
show snmp-server usm-user (username)
```

username	(可选项) 显示指定名字的用户信息
----------	-------------------

### 命令模式

特权模式

## 默认

无

## 使用说明

SNMP 用户必须属于一个组。通过 `snmp-server usm-user` 命令配置用户名。

## 举例说明

下例演示如何显示 SNMP 的用户信息：

```
Switch# show snmp-server usm-user user1
EnginedID:01234567890123456789
User Name:user1
Auth Protocol: md5
priv Protocol: des
Storage Type: nonvolatile
Row status:active
```

## 相关命令

`snmp-server usm-user`

### 4.4.29 show snmp-server version

特权模式下，使用 `show snmp-server version` 命令显示支持的 SNMP 版本。

## 命令语法

```
show snmp-server version
```

## 命令模式

特权模式

## 默认

无

## 使用说明

该命令用来显示系统当前支持的 SNMP 版本信息。

## 举例说明

下例演示如何显示当前支持的 SNMP 版本信息：

```
Switch# show snmp-server version
SNMPv1/SNMPv2c/SNMPv3
```

## 相关命令

snmp-server version

### 4.4.30 show snmp-server view

特权模式下，使用 show snmp-server view 命令显示 SNMP 视图信息。

## 命令语法

show snmp-server view (*view-name*)

view-name	指定视图名称
-----------	--------

## 命令模式

特权模式

## 默认

无

## 使用说明

该命令显示 SNMP 视图配置信息。

## 举例说明

下例演示如何显示 SNMP 所有配置的视图：

```
Switch# show snmp-server view
View-nameView-type Subtree
=====
abcexcluded .1.3.6.2
_all_ included.0
_all_ included.1
_all_ included.2
_none_excluded .0
_none_excluded .1
_none_excluded .2
```

## 相关命令

snmp-server view



## 4.5 SFLOW 命令

### 4.5.1 sflow enable

使用此命令全局使能 sFlow，使用此命令的 **no** 形式关闭 sflow 功能。

#### 命令语法

```
sflow enable  
no sflow enable
```

#### 命令模式

全局配置模式

#### 默认

Sflow 默认全局不使能

#### 使用说明

在进行 sflow 其他配置前必须先使用此命令全局使能 sflow 服务。使用此命令的 **no** 形式，所有 sflow 的配置将会被清空。

#### 举例说明

如下例子显示了如何全局使能 sflow：

```
Switch# configure terminal  
Switch(config)# sflow enable
```

#### 相关命令

```
show sflow
```

### 4.5.2 sflow agent

使用此命令设置 sflow 代理地址。

#### 命令语法

```
sflow agent (ip ipv4-address | ipv6 ipv6-address)  
no sflow agent (ip | ipv6)
```

ipv4-address	代理的 IPv4 地址
ipv6-address	代理的 IPv6 地址

## 命令模式

全局配置模式

## 默认

无

## 使用说明

使用此命令配置 sflow 代理地址。如果没有配置，系统将会使用第一个合法的 router-id 作为代理地址，并且不会再改变。

## 举例说明

如下例子显示如何配置代理地址：

```
Switch# configure terminal
Switch(config)# sflow agent ip 10.0.0.254
```

## 相关命令

show sflow

### 4.5.3 sflow collector

使用此命令设置 sflow 采样报文的收集、分析服务器的 IP 地址，使用此命令的 no 命令清空配置。

## 命令语法

**sflow collector** (ipv4-address | ipv6-address) (<1-65535>|)

**no sflow collector** (ipv4-address | ipv6-address) (<1-65535>|)

ipv4-address	收集服务器的 IPv4 地址
ipv6-address	收集服务器的 IPv6 地址
<1-65535>	收集服务器的接收 UDP 端口号，如果不指定，使用默认值 6343

## 命令模式

全局配置模式

## 默认

默认 UDP 目的端口号 6343

## 使用说明

使用此命令添加一个收集服务器的 IP 地址以及 UDP 端口号，系统最多支持两个收集服务器。使用此命令的 **no** 形式可以删除一个收集服务器。

## 举例说明

如下例子显示如何添加一个收集服务器：

```
Switch# configure terminal
Switch(config)# sflow collector 10.0.0.254 3000
```

## 相关命令

show sflow

### 4.5.4 sflow counter interval

使用此命令配置基于统计的采样间隔。使用此命令的 **no** 形式恢复默认值。

## 命令语法

sflow counter interval *interval\_val*

no sflow counter interval

interval_val	采样间隔，单位：秒，可配范围：1~2000
--------------	-----------------------

## 命令模式

全局配置模式

## 默认

20 秒

## 使用说明

采样间隔越短对系统的影响越大。

## 举例说明

如下例子显示如何配置基于统计的采样的间隔：

```
Switch# configure terminal
```

```
Switch(config)# sflow counter interval 10
```

## 相关命令

```
show sflow
```

### 4.5.5 sflow counter-sampling enable

使用此命令在指定端口上使能基于统计的采样功能。使用此命令的 `no` 形式关闭采样功能。

## 命令语法

```
sflow counter-sampling enable
```

```
no sflow counter-sampling enable
```

## 命令模式

接口配置模式

## 默认

所有的端口基于统计的采样功能默认不使能

## 使用说明

基于统计的采样是指每个采样间隔内，系统会将端口上的统计信息通过 `sflow` 协议报文送往采样收集服务器。

此命令可以配置在非 `linkagg` 成员的物理口上，也可以配置的 `linkagg` 端口上。

## 举例说明

如下例子显示了如何在端口上使能基于统计的采样功能：

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# sflow counter-sampling enable
```

## 相关命令

```
show sflow
```

### 4.5.6 sflow flow-sampling rate

使用此命令配置基于报文的采样的速率。使用此命令的 `no` 形式恢复默认值。

## 命令语法

```
sflow flow-sampling rate rate_val
```

```
no sflow flow-sampling rate
```

rate_val	基于报文采样的速率，必须是 2 的整数幂，可配范围为 1~8192
----------	-----------------------------------

## 命令模式

接口配置模式

## 默认

基于报文的采样速率的默认值是 8192

## 使用说明

这个数值可以简单的理解成多少个报文进入芯片采样一次。数值 1 表示 100%采样。但由于芯片实现上是通过计算概率的方式实现，所以并不一定严格按照这个数字进行采样。系统对报文进行采样时会将报文的前 256 字节封装到 sflow 协议报文中。系统对基于统计和基于报文的采样都是软件实现的，如果采样速率配置的很低，CPU 利用率就会非常高。另外 cpu 流量控制模块将 sflow 采样报文上 cpu 的速率限制为 400kbps，如果用户要求高的采样速率可以修改这个值。

此命令可以配置在非 linkagg 成员的物理口上，也可以配置的 linkagg 端口上。

## 举例说明

如下的例子显示了如何配置基于报文的采样速率：

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# sflow flow-sampling rate 2048
% Warning: sFlow sampling requires high CPU usage, especially with a low rate.
It is suggested not configure a rate less than default value 8192.
```

## 相关命令

show sflow

### 4.5.7 sflow flow-sampling enable

使用此命令在端口上使能基于报文的采样功能。使用此命令的 no 形式关闭采样功能。

## 命令语法

```
sflow flow-sampling enable (input|output|both)
no sflow flow-sampling enable (input|output|both)
```

## 命令模式

接口配置模式

## 默认

基于报文的采样功能在所有的端口上默认都是不使能

## 使用说明

使用此命令使能对进入指定端口的报文进行采样的功能。

此命令可以配置在非 linkagg 成员的物理口上，也可以配置的 linkagg 端口上。

## 举例说明

使用此命令在端口上使能基于报文的采样功能：

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# sflow flow-sampling enable input
```

## 相关命令

show sflow

### 4.5.8 show sflow

使用此命令查看 sflow 的配置信息。

## 命令语法

show sflow

## 命令模式

特权模式

## 默认

此命令无默认值

## 使用说明

此命令可以查看 sflow 详细的配置信息。

## 举例说明

如下例子显示了 sflow 的配置信息：

```
Switch# show sflow
sFlow Version: 5
sFlow Global Information:
  Agent IP address : 0.0.0.0
  Counter Sampling Interval : 20 seconds
  Collector IP : Not configured
```

```
sFlow Port Information:
Flow-SampleFlow-Sample
PortCounter Flow Direction Rate
-----
eth-0-1 Disable Enable Input8192
```

## 相关命令

```
sflow enable
sflow collector
sflow counter interval
sflow counter-sampling enable
sflow flow-sampling rate
sflow flow-sampling enable
```

## 4.6 LLDP 命令

### 4.6.1 lldp enable(全局)

在全局配置模式下，使用 `lldp enable` 命令来启用 LLDP 功能。使用命令相应的 `no` 形式关闭该项功能。

#### 命令语法

```
lldp enable
lldp disable
```

#### 命令模式

全局配置模式

#### 默认

默认情况下此功能未打开。

#### 使用说明

在启用 LLDP 功能前，必需同时在全局和接口上使能 LLDP。

#### 举例说明

```
全局启用 LLDP 功能：
Switch(config)# lldp enable
```

## 相关命令

lldp enable(接口)

### 4.6.2 lldp enable(接口)

在接口模式下使用 `lldp enable` 命令使能 LLDP 功能。使用命令相应的 `no` 形式，在接口上关闭 LLDP 功能。

## 命令语法

lldp enable (txonly|txrx|rxonly)

lldp disable

txonly	使能 LLDP 报文传输
txrx	使能 LLDP 报文传输和发送
rxonly	使能 LLDP 报文发送

## 命令模式

接口配置模式

## 默认

默认情况下此功能打开。

## 使用说明

在启用 LLDP 功能前，必需同时在全局和接口上使能 LLDP。

## 举例说明

接口上启用 LLDP 功能：

```
Switch(config-if)# lldp enable txrx
```

## 相关命令

lldp enable(全局)

### 4.6.3 lldp system-name

在全局配置模式下，使用 `lldp system-name` 命令配置系统名称 TLV 的值。使用命令相应的 `no` 形式，恢复默认配置。



## 命令语法

```
lldp system-name NAME
```

```
no lldp system-name
```

NAME	系统名称，范围为 1 到 64
------	-----------------

## 命令模式

全局配置模式

## 默认

默认情况下，使用系统名称。

## 使用说明

如果该命令没有配置，使用系统名称作为该 TLV 的值。

## 举例说明

配置系统名称 TLV 的值为 switch:

```
Switch(config)# lldp system-name switch
```

## 相关命令

lldp enable(全局)

lldp enable(接口)

### 4.6.4 lldp system-description

在全局模式下，使用 lldp system- description 命令配置系统描述 TLV 的值。使用命令相应的 no 形式，恢复默认配置。

## 命令语法

```
lldp system-description LINE
```

```
no lldp system-description
```

LINE	系统描述，长度范围为 1 到 255，允许空格
------	-------------------------

## 命令模式

全局配置模式

## 默认

默认情况下，使用系统描述。

## 使用说明

如果该命令没有配置，使用系统描述作为该 TLV 的值。

## 举例说明

配置系统描述 TLV 的值为 switch:

```
Switch(config)# lldp system-description switch
```

## 相关命令

lldp enable(全局)

lldp enable(接口)

## 4.6.5 lldp management

在全局模式下，使用 lldp management 命令，配置管理地址 TLV 的值。使用命令相应的 no 形式，恢复默认配置。

## 命令语法

lldp management (ip *ADDRESS*| interface *IFNAME*)

no lldp management (ip| interface)

ADDRESS	IPv4 地址, 例如 1.1.1.1
IFNAME	端口名称, 需要是三层端口

## 命令模式

全局配置模式

## 默认

使用默认管理地址。

## 使用说明

配置的管理地址优先于配置的接口，如果两者都没有配置，系统将会按照环回接口，管理口，其他三层接口，系统 MAC 地址的顺序，使用默认管理地址。同类接口中将使用 IP 地址较小的接口

。

## 举例说明

配置管理地址 TLV 的值：

```
Switch(config)# lldp management ip 192.168.1.2
```

## 相关命令

lldp enable(全局)

lldp enable(接口)

### 4.6.6 lldp msg-tx-hold

在全局模式下，使用 lldp msg-tx-hold 配置 msg-tx-hold 值。使用命令相应的 no 形式，恢复默认配置。

## 命令语法

```
lldp msg-tx-hold NUMBER
```

```
no lldp msg-tx-hold
```

NUMBER	值的范围为 2 到 10
--------	--------------

## 命令模式

全局配置模式

## 默认

默认 msg-tx-hold 值为 4。

## 使用说明

无

## 举例说明

配置 msg-tx-hold 的值：

```
Switch(config)# lldp msg-tx-hold 3
```

## 相关命令

lldp enable(全局)

lldp enable(接口)

### 4.6.7 lldp timer msg-tx-interval

在全局模式下，使用 `lldp timer msg-tx-interval` 命令配置消息传输间隔 `msg-tx-interval`。使用命令相应的 `no` 形式，恢复默认配置。

## 命令语法

```
lldp timer msg-tx-interval NUMBER
```

```
no lldp timer msg-tx-interval
```

NUMBER	值的范围为 5 到 32768
--------	-----------------

## 命令模式

全局配置模式

## 默认

默认 `msg-tx-interval` 值为 30s。

## 使用说明

无

## 举例说明

配置 `msg-tx-interval` 的值：

```
Switch(config)# lldp timer msg-tx-interval 20
```

## 相关命令

lldp enable(global)

lldp enable(interface)

### 4.6.8 lldp timer reinit-delay

在全局模式下，使用 `lldp timer reinitDelay` 命令配置 `reinitDelay`。使用命令相应的 `no` 形式，恢复默认配置。

## 命令语法

lldp timer reinit-delay *NUMBER*

no lldp timer reinit-delay

NUMBER	值的范围为 1 到 10
--------	--------------

## 命令模式

全局配置模式

## 默认

默认 reinitDelay 值为 2s。

## 使用说明

无

## 举例说明

配置 reinitDelay 的值：

```
Switch(config)# lldp timer reinit-delay 1
```

## 相关命令

lldp enable(全局)

lldp enable(接口)

## 4.6.9 lldp timer tx-delay

在全局模式下，使用 lldp timer tx-delay 命令配置传输延迟 tx-delay。使用命令相应的 no 形式，恢复默认配置。

## 命令语法

lldp timer tx-delay *NUMBER*

no lldp timer tx-delay

NUMBER	值的范围从 1 到 8192
--------	----------------

## 命令模式

全局配置模式

## 默认

默认 tx-delay 的值为 2s。

## 使用说明

tx-delay 的值需要遵守公式： $1 \leq \text{tx-delay} \leq ((0.25) * \text{msg-tx-interval})$ 。

## 举例说明

配置 tx-delay 的值。

```
Switch(config)# lldp timer tx-delay 3
```

## 相关命令

lldp enable(全局)

lldp enable(接口)

### 4.6.10 lldp tlv basic

在接口模式下，使用 lldp tlv basic 命令选择基础 TLV。使用命令相应的 no 形式，取消选择。

## 命令语法

```
lldp tlv basic { port-description | system-name | system-description | system-capabilities |  
management-address [all]}
```

```
no lldp tlv basic { port-description | system-name | system-description | system-capabilities |  
management-address [all]}
```

port-description	选择端口描述 Tlv
system-name	选择系统名称 Tlv
system-description	选择系统描述 Tlv
system-capabilities	选择系统能力 Tlv
management-address	选择管理地址 Tlv
all	选择所有基础 tlv

## 命令模式

端口配置模式

## 默认

所有基础 tlv 都已使能。

## 使用说明

无

## 举例说明

在端口配置模式下使用选择系统名称 tlv:

```
Switch(config-if)# lldp tlv basic system-name
```

## 相关命令

lldp enable(global)

lldp enable(interface)

### 4.6.11 lldp tlv 8021-org-specific

在接口模式下，使用 lldp tlv 8021-org-specific 命令选择 IEEE 802.1TLV。使用命令相应的 no 形式，取消选择。

## 命令语法

```
lldp tlv 8021-org-specific {port-vlan | protocol-vlan | vlan-name | protocol-id | link-  
aggregation | dcbx |all}
```

```
no lldp tlv 8021-org-specific {port-vlan | protocol-vlan | vlan-name | protocol-id | link-  
aggregation | dcbx |all}
```

port-vlan	选择 Port Vlan ID Tlv
protocol-vlan	选择 Port and Protocol Vlan ID Tlv
vlan-name	选择 Vlan Name Tlv
protocol-id	选择 Protocol Identity Tlv
link-aggregation	选择 Link Aggregation Tlv
dcbx	选择 DCBX Tlv
all	选择除 Link Aggregation Tlv 的所有 IEEE 802.1 tlv

## 命令模式

端口配置模式

## 默认

除 Link Aggregation Tlv 的所有 IEEE 802.1 tlv 都已使能。

## 使用说明

Link Aggregation Tlv 默认在 IEEE 802.3 tlv 中使能

## 举例说明

在端口配置模式下选择 IEEE802.1 tlv:

```
Switch(config-if)# lldp tlv 8021-org-specific vlan-name
```

## 相关命令

lldp enable(global)

lldp enable(interface)

### 4.6.12 lldp tlv 8021-org-specific vlan-name-value

在接口模式下，使用 lldp tlv 8021-org-specific vlan-name-value 命令配置 VLAN NAME TLV。使用命令相应的 no 形式，取消配置。

## 命令语法

lldp tlv 8021-org-specific vlan-name-value *VALUE*

no lldp tlv 8021-org-specific vlan-name-value

VALUE	VLAN NAME TLV 中包含的 vlan 的 id
-------	------------------------------

## 命令模式

端口配置模式

## 默认

VLAN NAME TLV 携带端口所属的默认 VLAN。

## 使用说明

无



## 举例说明

在端口配置模式下配置 VLAN NAME TLV 中携带的 Vlan id:

```
Switch(config-if)# lldp tlv 8021-org-specific vlan-name-value 2000
```

## 相关命令

```
lldp enable(global)
```

```
lldp enable(interface)
```

### 4.6.13 lldp tlv 8023-org-specific

在接口模式下，使用 `lldp tlv 8023-org-specific` 命令选择 IEEE 802.3TLV。使用命令相应的 `no` 形式，取消选择。

## 命令语法

```
lldp tlv 8023-org-specific {mac-phy-cfg | power | link-aggregation | max-frame-size | all}
```

```
no lldp tlv 8023-org-specific {mac-phy-cfg | power | link-aggregation | max-frame-size | all}
```

mac-phy-cfg	选择 MAC/PHY Configuration/Status TLV
power	选择 Power Via MDI Tlv
link-aggregation	选择 Link Aggregation Tlv
max-frame-size	选择 Maximum Frame Size Tlv
all	选择所有 IEEE 802.3 tlv

## 命令模式

端口配置模式

## 默认

所有 IEEE 802.3 tlv 都已使能。

## 使用说明

Link Aggregation Tlv 默认在 IEEE 802.3 tlv 中使能

## 举例说明

在端口配置模式下选择 IEEE802.3 tlv:

```
Switch(config-if)# lldp tlv 8023-org-specific power
```

## 相关命令

```
lldp enable(global)
lldp enable(interface)
```

### 4.6.14 lldp tlv med

在接口模式下，使用 `lldp tlv med` 命令选择 MED TLV。使用命令相应的 `no` 形式，取消选择。

## 命令语法

```
lldp tlv med {network-policy | ext-power | inventory | all}
no lldp tlv med {network-policy | ext-power | inventory | all}
```

network-policy	选择 Network Policy TLV
ext-power	选择 Extend Power-Via-MDI Tlv
inventory	选择 Inventory Tlv
all	选择除 Location Identification Tlv 的所有 MED tlv

## 命令模式

端口配置模式

## 默认

除 Location Identification Tlv 的所有 MED tlv 都已使能。

## 使用说明

当有 MED 的某一个 tlv 被选择的时候，LLDP-MED Capabilities TLV 会自动被选择；而当没有 MED 的其他 tlv 被选择时，LLDP-MED Capabilities TLV 会自动被取消。

## 举例说明

在端口配置模式下选择 MED tlv:

```
Switch(config-if)# lldp tlv med inventory
```

## 相关命令

```
lldp enable(global)
lldp enable(interface)
```

## 4.6.15 lldp tlv med location-id

在接口模式下，使用 `lldp tlv med location-id` 命令选择并配置 MED Location-id TLV。使用命令相应的 `no` 形式，取消选择。

### 命令语法

**lldp tlv med location-id (ecs-elin VALUE | civic DEV-TYPE CODE**

**CA1-TYPE CA1-VALUE (CA2-TYPE CA2-VALUE (CA3-TYPE CA3-VALUE  
(CA4-TYPE CA4-VALUE (CA5-TYPE CA5-VALUE (CA6-TYPE CA6-VALUE  
(CA7-TYPE CA7-VALUE (CA8-TYPE CA8-VALUE (CA9-TYPE CA9-VALUE  
(CA10-TYPE CA10-VALUE))))))))))**

**no lldp tlv med location-id**

ecs-elin VALUE	ECS ELIN 的地址，类型为电话号码，有效长度为[10-25]
civic DEV-TYPE CODE CA-TYPE CA-VALUE	<b>DEV-TYPE</b> ，设备类型，有效值为-2，0 表示配置设备类型为 DHCP server，1 表示配置设备类型为 Switch，2 表示配置设备类型为 LLDP-MED Endpoint <b>CODE</b> ，国家编码，取值范围请参考 ISO 3166。 <b>CA-TYPE CA-VALUE</b> 地址信息，最多可以有 10 组， <b>CA-TYPE</b> 的范围是 0-255， <b>CA-VALUE</b> 的长度范围是[1-232]

### 命令模式

端口配置模式

### 默认

无

### 使用说明

无。

### 举例说明

在端口配置模式下配置 MED Location-id tlv:

```
Switch(config-if)# lldp tlv med location-id ecs-elin 1234567890
```

## 相关命令

```
lldp enable(global)
lldp enable(interface)
```

### 4.6.16 debug lldp

在特权模式下，使用 `debug lldp` 命令打开 LLDP 的调试显示。使用该命令的 `no` 形式，恢复默认值。

## 命令语法

```
debug lldp ( events | packet | all | tlv-info)
no debug lldp ( events | packet | all | tlv-info)
```

events	LLDP 事件
packet	LLDP 报文信息
all	打开所有 LLDP 调试
tlv-info	打开 TLV 信息调试

## 命令模式

特权模式

## 默认

无

## 使用说明

该命令用于显示属于 DHCPv6 中继的接口信息。

使用“`terminal monitor`”使调试信息打印在 VTY 终端，使用“`show logging buffer`”查看 log 缓存中的信息。

## 举例说明

在特权模式下打开 LLDP 调试：

```
Switch# debug lldp all
```

## 相关命令

```
terminal monitor
```

show logging buffer

## 4.6.17 show lldp local

在特权模式下，使用 show lldp local 命令显示 LLDP 的本地信息。

### 命令语法

show lldp local (config | tlv-info) (interface *IFNAME* )

config	配置信息
tlv-info	本地 LLDP TLV 内容
interface	指定端口
IFNAME	物理端口名称

### 命令模式

特权模式

### 默认

无

### 使用说明

如果没有指定端口名称，将会显示全局的 LLDP 本地信息。

### 举例说明

在特权模式下显示 LLDP 本地信息：

```
Switch# show lldp local config
LLDP global configuration:
=====
LLDP function global enabled : NO
LLDP msgTxHold : 4
LLDP msgTxInterval : 30
LLDP reinitDelay: 2
LLDP txDelay: 2
Switch# show lldp local config interface eth-0-4
LLDP configuration on interface eth-0-4 :
=====
LLDP admin status : Disabled
Basic optional TLV Enabled:
Port Description TLV
System Name TLV
System Description TLV
```

```

System Capabilities TLV
Management Address TLV
IEEE 802.1 TLV Enabled:
Port Vlan ID TLV
Port and Protocol Vlan ID TLV
Vlan Name TLV
Protocol Identity TLV
IEEE 802.3 TLV Enabled:
MAC/PHY Configuration/Status TLV
Power Via MDI TLV
Link Aggregation TLV
Maximum Frame Size TLV
LLDP-MED TLV Enabled:
Med Capabilities TLV
Network Policy TLV
Extended Power-via-MDI TLV
Inventory TLV

```

## 相关命令

```

lldp enable(global)
lldp enable(interface)
lldp tlv basic
lldp tlv med
lldp tlv 8023-org-specific
lldp tlv 8021-org-specific
lldp msg-tx-hold
lldp timer msg-tx-interval
lldp timer reinitDelay
lldp timer tx-delay

```

### 4.6.18 show lldp neighbor

在特权模式下，使用 `show lldp neighbor` 命令显示 LLDP 邻居信息。

## 命令语法

```
show lldp neighbor (interface IFNAME |) (brief |)
```

interface	指定端口
IFNAME	物理端口名称
brief	显示简要信息

## 命令模式

特权模式

## 默认

无

## 使用说明

该命令用于显示 LLDP 邻居信息。

## 举例说明

在特权模式下显示 LLDP 邻居简要信息：

```
Switch# show lldp neighbor interface eth-0-4 brief
Local Port   : eth-0-4
Remote Port  : eth-0-6
Hold Time: 120
Expire Time : 116
System Name : switch
-----
```

## 相关命令

lldp enable(global)

lldp enable(interface)

### 4.6.19 show lldp statistics

在特权模式下，使用 show lldp statistics 命令显示 LLDP 统计信息。

## 命令语法

```
show lldp statistics (interface IFNAME )
```

interface	指定端口
IFNAME	物理端口名称

## 命令模式

特权模式

## 默认

无

## 使用说明

该命令用于显示 LLDP 统计的详情。

## 举例说明

在特权模式下显示 LLDP 统计：

```
Switch# show lldp statistics interface eth-0-4
LLDP statistics information:
=====
LLDP Port statistics for eth-0-4
Frames transmitted: 568
Frames Aged out: 0
Frames Discarded: 0
Frames with Error: 0
Frames Recieved: 364
TLVs discarded: 0
TLVs unrecognized: 0
```

## 相关命令

`clear lldp statistics`

### 4.6.20 clear lldp statistics

在特权模式下，使用 `clear lldp statistics` 命令清除 LLDP 统计信息。

## 命令语法

`clear lldp statistics (interface IFNAME |)`

interface	指定端口
IFNAME	物理端口名称

## 命令模式

特权模式

## 默认

无

## 使用说明

该命令清除 LLDP 统计信息。



## 举例说明

在特权模式下清除 LLDP 统计信息：

```
Switch# clear lldp statistics
```

## 相关命令

### 4.6.21 lldp ignore-pvid-inconsistency

**lldp ignore-pvid-inconsistency** 命令可以用来关闭 LLDP 的 PVID 不一致检查功能。

**no lldp ignore-pvid-inconsistency** 命令可以用来开启 LLDP PVID 不一致检查功能。

## 命令语法

**lldp ignore-pvid-inconsistency**

**no lldp ignore-pvid-inconsistency**

## 命令模式

全局配置模式

## 默认

开启

## 使用说明

一般组网情况下，要求链路两端的 PVID 保持一致。设备会对收到的 LLDP 报文中的 PVID TLV 进行检查，如果发现报文中的 PVID 与本端 PVID 不一致，则认为网络中可能存在错误配置，LLDP 会打印日志信息，提示用户。

但在一些特殊情况下，可以允许链路两端的 PVID 配置不一致。例如为了简化接入交换机的配置，各接入交换机的上行口采用相同的 PVID，而对端汇聚交换机的各接口采用不同的 PVID，从而使各接入交换机的流量进入不同 VLAN。

## 举例说明

关闭 LLDP 的 PVID 不一致检查功能：

```
Switch(config)# lldp ignore-pvid-inconsistency
```

## 4.7 TELEMETRY 命令

### 4.7.1 sensor-group

使用此命令创建 telemetry 采样传感器组，并进入 sensor-group 视图。如果采样组存在则直接进入 sensor-group 视图。

使用 **no** 命令删除创建的采样传感器组。

## 命令语法

**sensor-group** *WORD*

**no sensor-group** *WORD*

WORD	指定采样传感器组名称。字符串形式，区分大小写，由字母、数字或字母和数字的组合组成，字母或数字之间不允许有空格，长度范围是1~64。
------	---

## 命令模式

全局配置模式

## 默认

默认无采样传感器组

## 使用说明

执行 **sensor-group** 命令可以创建一个或多个采样传感器组，包含需要采样的数据对象。采样传感器组创建数量上限为 16 个。

## 举例说明

创建名称为 `sensor1` 的采样传感器组：

```
Switch# configure terminal
Switch(config)# sensor-group sensor1
Switch(config-telemetry-sensor-group)#
```

## 4.7.2 sensor-path

使用此命令为当前采样传感器组创建采样路径。

使用 **no** 命令删除创建的采样路径。

## 命令语法

**sensor-path** *WORD*

**no sensor-path** *WORD*

WORD	指定采样路径名称。字符串形式，区分大小写，长度范围是1~255。支持基于YANG模型的采样路径。
------	--

## 命令模式

Sensor-group 视图

## 默认

默认无采样路径

## 使用说明

成功创建采样传感器组后，可以执行此命令配置采样路径。同一个采样传感器组下配置的路径数量上限为 5 条。当采样路径达到配置上限时，无法再增加新条目。

## 举例说明

为采样传感器组 sensor1 创建采样路径（cpu 使用率）：

```
Switch# configure terminal
Switch(config)# sensor-group sensor1
Switch(config-telemetry-sensor-group)# sensor-path inspur-device:device-
info/performance/cpu-use-rate
```

### 4.7.3 destination-group

使用此命令创建 telemetry 采样数据的上送目标组，并进入 destination-group 视图。如果目标组存在则直接进入 destination-group 视图。

使用 no 命令删除创建的上送目标组。

## 命令语法

**destination-group** *WORD*

**no destination-group** *WORD*

WORD	指定上送目标组名称。字符串形式，区分大小写，由字母、数字或字母和数字的组合组成，字母或数字之间不允许有空格，长度范围是1~64。
------	--

## 命令模式

全局配置视图

## 默认

默认无上送目标组

## 使用说明

执行 **destination-group** 命令可以创建一个或多个采样上送目标组，包含需要上送的目标参数。上送目标组创建数量上限为 16 个。

## 举例说明

创建名称为 dst1 的上送目标组：

```
Switch# configure terminal
Switch(config)# destination-group dst1
Switch(config-telemetry-destination-group)#
```

### 4.7.4 ipv4-address port protocol grpc

使用此命令为当前上送目标组创建目标采集器的协议，其中包括 IP 地址和端口号。

使用 no 命令删除创建的目标采集器条目。

## 命令语法

**ipv4-address ip-address port port-number protocol grpc**

**no ipv4-address ip-address port port-number**

ip-address	指定目标采集器IP地址。点分十进制格式。
port	指定目标采集器端口号。整数形式，取值范围50000~65535。
protocol grpc	指定数据上送协议为GRPC。目前仅支持grpc，且无加密。

## 命令模式

Destination-group 视图

## 默认

默认无目标采集器条目

## 使用说明

成功创建上送目标组后，可以执行此命令配置目标采集器信息条目。同一个上送目标组下配置的采集器数量上限为 5 条。当采集器条目达到配置上限时，无法再增加新条目。

## 举例说明

为上送目标组 dst1 创建目标采集器：

```
Switch# configure terminal
```

```
Switch(config)# destination-group dst1
```

```
Switch(config-telemetry-destination-group)# ipv4-address 10.0.0.1 port 50001 protocol grpc
```

## 4.7.5 subscription

使用此命令创建 **telemetry** 静态订阅，并进入 **subscription** 视图。如果订阅存在则直接进入 **subscription** 视图。订阅用于关联采样传感器组和上送目标组。

使用 **no** 命令删除创建的订阅名称。

### 命令语法

**subscription** *WORD*

**no subscription** *WORD*

<b>WORD</b>	指定订阅名称。字符串形式，区分大小写，由字母、数字或字母和数字的组合组成，字母或数字之间不允许有空格，长度范围是1~64。
-------------	---

### 命令模式

全局配置模式

### 默认

默认无订阅

### 使用说明

执行 **subscription** 命令可以创建一个或多个订阅名称，将采样传感器组和上送目标组关联，完成采样数据上送。订阅创建数量上限为 16 个。

### 举例说明

创建名称为 **subs1** 的订阅，并进入 **subscription** 视图：

```
Switch# configure terminal
```

```
Switch(config)# subscription subs1
```

```
Switch(config-telemetry-subscription)#
```

## 4.7.6 subs-sensor-group sample-interval

使用此命令关联采样传感器组，并可配置该采样传感器组的采样周期。

使用 **no** 命令取消与采样传感器组的关联。

## 命令语法

**subs-sensor-group** *WORD* [ **sample-interval** *interval-value* ]

**no subs-sensor-group** *WORD*

WORD	指定关联采样传感器组名称。取值必须是已经在全局配置视图下创建成功的采样传感器组名称。
interval-value	指定采样时间间隔。整数形式，取值范围是100~1800000，单位：毫秒。目前仅支持配置1000、5000、10000、30000、60000、180000、300000、900000、1800000。缺省值10000ms。

## 命令模式

Subscription 视图

## 默认

默认无关联采样传感器组

## 使用说明

用户成功创建的采样传感器组必须在 Subscription 视图下进行关联才可以完成后续的采样任务。同一订阅下关联的传感器组上限为 5 个。

注意事项：

- 关联的采样传感器组必须是已在全局配置视图下创建成功的采样传感器组，否则会关联失败。
- 如果配置的采样周期小于采样路径的最小采样精度，则设备会按照最小采样精度进行数据上报；如果配置的采样周期大于最小采样精度，则设备按照配置的采样周期进行数据上报。

例如：inspur-device:device-info/performance/cpu-use-rate 采样路径的最小采样精度为 10000，如果执行命令设置的 *sample-interval* 参数的值为 5000，则设备按照 10000ms 的周期进行数据上报，如果设置的值为 60000，则设备按照 60000ms 的周期进行数据上报。

## 举例说明

关联名称为 sensor1 的采样传感器组，配置采样周期为 10000ms：

```
Switch# configure terminal
Switch(config)# subscription subs1
Switch(config-telemetry-subscription)# subs-sensor-group sensor1 sample-interval 10000
```

### 4.7.7 subs-destination-group

使用此命令关联上送目标组。

使用 `no` 命令取消与上送目标组的关联。

## 命令语法

**subs-destination-group** *WORD*

**no subs-destination-group** *WORD*

WORD	指定关联上送目标组名称。取值必须是已经在全局配置视图下创建成功的上送目标组名称。
------	--

## 命令模式

Subscription 视图

## 默认

默认无关联上送目标组

## 使用说明

用户成功创建的上送目标组，必须在 Subscription 视图下进行关联才可以完成后续的上送任务。同一订阅下关联的目标组上限为 5 个。

注意事项：

关联的上送目标组必须是已在全局配置视图下创建成功的上送目标组，否则会关联失败。

## 举例说明

关联名称为 `dst1` 的上送目标组：

```
Switch# configure terminal
Switch(config)# subscription subs1
Switch(config-telemetry-subscription)# subs-destination-group dst1
```

## 4.7.8 telemetry-sample enable

使用此命令全局使能 `telemetry` 采样动作。

使用此命令的 `disable` 形式关闭采样功能。

## 命令语法

**telemetry-sample enable**

**telemetry-sample disable**

## 命令模式

全局配置模式

## 默认

telemetry-sample 默认全局不使能

## 使用说明

在完成 telemetry 所有配置后使用此命令全局使能采样上送功能。修改订阅配置前需先去使能采样上送功能。

## 举例说明

全局使能 telemetry 采样动作：

```
Switch# configure terminal
Switch(config)# telemetry-sample enable
```

## 4.7.9 show telemetry sensor-path

使用此命令查看设备支持的采样路径。

## 命令语法

**show telemetry sensor-path**

## 命令模式

特权模式

## 默认

此命令无默认值

## 使用说明

执行此命令可查看目前设备支持的采样路径、对应采样类型和最小采样精度。

命令输出信息描述：

项目	描述
Type	采样类型(sample、event等)
Min-period(ms)	最小采样精度，单位毫秒
Path	采样路径



## 举例说明

查看设备支持的采样路径：

```
Switch# show telemetry sensor-path
Valid sampling path:
```

Type	Min-period(ms)	Path
sample	10000	inspur-device:device-info/performance/cpu-use-rate
sample	10000	inspur-device:device-info/performance/memory-use-rate

### 4.7.10 show telemetry sensor

使用此命令查看采样传感器组信息。

## 命令语法

```
show telemetry sensor
```

## 命令模式

特权模式

## 默认

此命令无默认值

## 使用说明

执行此命令可以查看采样传感器组的名称、订阅状态、采样路径。

命令输出信息描述：

项目	描述
Total sensor group num	采样传感器组总数
Sensor-name	采样传感器组名称
State	采样传感器组状态 <ul style="list-style-type: none"> <li>● RESOLVED：已被订阅</li> <li>● NA：未被订阅</li> </ul>
Sensor-path	包含的采样路径

## 举例说明

查看所有采样传感器组信息：

```
Switch# show telemetry sensor
Total sensor group num = 2
```

Sensor-name	State	Sensor-path
sensor2	N/A	inspur-device:device-info/performance/memory-use-rate inspur-device:device-info/performance/cpu-use-rate
sensor1	N/A	inspur-device:device-info/performance/cpu-use-rate inspur-device:device-info/performance/memory-use-rate

### 4.7.11 show telemetry destination

使用此命令查看上送目标组信息。

#### 命令语法

**show telemetry destination**

#### 命令模式

特权模式

#### 默认

此命令无默认值

#### 使用说明

执行此命令可以查看上送目标组的名称、订阅状态、包含目标采集器 IP 地址、端口号和支持协议。

命令输出信息描述：

项目	描述
Total destination group num	上送目标组总数
Dest-name	上送目标组名称
State	上送目标组状态 <ul style="list-style-type: none"> <li>● RESOLVED: 已被订阅</li> <li>● NA: 未被订阅</li> </ul>
Dest-addr	目标采集器 IP 地址
Dest-port	目标采集器端口
Protocol	数据通信协议

#### 举例说明

查看所有上送目标组信息：

Switch# show telemetry destination

Total destination group num = 2

Dest-name	State	Dest-addr	Dest-port	Protocol
dest2	N/A	1.1.2.2	50003	GRPC
dest1	N/A	1.1.1.1	50001	GRPC
		2.2.2.2	50002	GRPC

## 4.7.12 show telemetry subscription

使用此命令查看订阅信息。

### 命令语法

**show telemetry subscription**

### 命令模式

特权模式

### 默认

此命令无默认值

### 使用说明

执行此命令可以查看订阅的名称、关联采样传感器组名称和采样周期、关联上送目标组名称。

命令输出信息描述：

项目	描述
Total subscription num	订阅总数
Subscription name	订阅名称
Sensor-groups	关联采样传感器组列表
Sensor-name	采样传感器组名称
Sample-interval	采样传感器组对应的采样周期，单位毫秒
Destination groups	关联上送目标组列表
Dest-name	上送目标组名称
Protocol-Encoding	协议与编码格式，默认 GRPC 协议和 gpbkv 格式

## 举例说明

查看所有订阅信息：

```
Switch# show telemetry subscription
Total subscription num = 1
-----
Subscription name: subs1

[Sensor groups]
Sensor-name   Sample-interval(ms)
-----
sensor1      10000

[Destination groups]
Dest-name     Protocol-Encoding
-----
dest1        GRPC-gpbkv
```

## 4.8 Restconf 配置

### 4.8.1 service restconf enable

使用此命令启动空闲配置。

#### 命令语法

```
service restconf enable
```

#### 命令模式

特权模式

#### 默认

无

#### 使用说明

无

#### 举例说明

在特权模式下，启动空闲配置：

```
Switch# service restconf enable
```

# 5 组播命令行参考

## 5.1 组播路由命令

### 5.1.1 ip multicast-routing

使用此命令启用交换机的多播路由功能。使用关键字 `no` 禁用此功能。

#### 命令语法

```
ip multicast-routing  
no ip multicast-routing
```

#### 命令模式

全局配置模式

#### 默认

开启

#### 使用说明

无

#### 举例说明

启用交换机的多播路由功能。

```
Switch(config)# ip multicast-routing
```

禁用交换机的多播路由功能。

```
Switch(config)# no ip multicast-routing
```

#### 相关命令

无

## 5.1.2 ip multicast route-limit

使用此命令设置组播路由的最大数目。使用关键字 **no** 恢复此项设置为默认值。

### 命令语法

**ip multicast route-limit** *route-number* (*threshold-number*)

**no ip multicast route-limit**

route-number	组播路由的最大数目，范围是 1 到 2048
threshold-number	超过阈值时生成警告消息，这个阈值应小于组播路由的最大数量

### 命令模式

全局模式

### 默认

默认组播路由最大数目为 2048。

默认阈值应为组播路由的最大数量相同。

### 使用说明

无

### 举例说明

设置组播路由的最大数目为 512。

```
Switch(config)# ip multicast route-limit 512
```

设置组播路由的最大数目为默认值。

```
Switch(config)# no ip multicast route-limit
```

### 相关命令

无

## 5.1.3 ip mroute-rpf

此命令用于命令用来配置组播静态路由。使用关键字 **no** 来删除组播静态路由表中的组播静态路由。

### 命令语法

**ip mroute-rpf** source-address/mask-length (**static** | **rip** | **ospf** | ) rpf-nbr-address distance

no ip mroute-rpf *source-address/ mask-length* (static | rip | ospf |)

source-address	组播源地址
mask-length	掩码长度
static	静态路由
rip	RIP 协议
ospf	OSPF 协议
rpf-nbr-address	RPF 邻居的 IP 地址
distance	路由优先级

## 命令模式

全局模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子显示如何设置组播源 10.10.1.1/24 的 RPF 邻居地址是 192.168.1.1。

```
Switch(config)# ip mroute-rpf 10.10.1.1/24 192.168.1.1
```

## 相关命令

show ip mroute-rpf

## 5.1.4 show ip mroute

使用此命令查看多播路由表。

## 命令语法

show ip mroute (sparse|) (count|summary|)

show ip mroute *address* (sparse|) (count|summary|)

show ip mroute route-limit

sparse	查看稀疏模式的多播路由
--------	-------------

count	查看路由和数据包的统计情况
summary	查看多播路由的总体情况
address	源 IP 地址或者组播 IP 地址；查看此地址的路由
route-limit	查看路由数目的最大值

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子显示组播路由表信息。

```
Switch# show ip mroute
IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)
(10.0.1.20, 228.1.1.1), uptime 00:35:46, stat expires 00:02:19
Owner PIM-SM, Flags: TF
  Incoming interface: eth-0-1
  Outgoing interface list:
    eth-0-2 (1)
```

下面例子显示组播路由表总体信息。

```
Switch# show ip mroute summary
IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)
(10.0.1.20, 228.1.1.1), 00:36:59/00:02:46, PIM-SM, Flags: TF
```

## 相关命令

无

### 5.1.5 show ip mvif

使用此命令查看 IP 的多播接口信息。



## 命令语法

```
show ip mvif (IFNAME )
```

IFNAME	接口名称
--------	------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子查看所有多播接口信息。

```
Switch# show ip mvif
Interface Vif   Owner          TTL  Local          Remote
Uptime
      Idx  Module
eth-0-1   0    PIM-SM        1    10.0.1.1      0.0.0.0
00:42:56
eth-0-2   2    PIM-SM        1    10.0.2.1      0.0.0.0
00:42:53
```

## 相关命令

无

### 5.1.6 show ip multicast groups count

此命令用于显示组播组数目。

## 命令语法

```
show ip multicast groups count
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面的例子显示当前的组播组数目。

```
Switch# show ip multicast groups count
multicast group record count: 1
multicast source record count: 0
multicast total record count: 1
multicast max record count: 2048
```

## 相关命令

无

## 5.1.7 show ip mroute-rpf

使用此命令查看多播路由的反向路径查询。

## 命令语法

```
show ip mroute-rpf source-address
```

source-address
----------------

多播源地址
-------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

查看多播源地址为 192.168.1.1 的反向路径查询。

```
Switch# show ip mroute-rpf 192.168.1.1
RPF information for 192.168.1.1
  RPF interface: eth-0-10
  RPF neighbor: 0.0.0.0
  RPF route: 192.168.1.0/24
  RPF type: unicast (connected)
  RPF recursion count: 0
  Doing distance-preferred lookups across tables
  Distance: 0
  Metric: 0
```

## 相关命令

ip mroute-rpf

## 5.1.8 show resource mcast

此命令用于显示组播路由资源使用情况。

## 命令语法

```
show resource mcast
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子显示组播路由资源使用情况。

```
Switch# show resource mcast
MCAST
Resource                               Used      Capability
=====
Mcast Entry                             0         1023
Mcast Normal Member                     0         2046
Mcast Vlan Member                       0         1023
```

## 相关命令

无

## 5.1.9 clear ip mroute

此命令清除组播路由表项。

### 命令语法

**clear ip mroute** (\* | group-address (source-address))

group-address	指定组播组路由
source-address	指定组播源路由
*	所有的组播组信息

### 命令模式

特权模式

### 默认

无

### 使用说明

无

### 举例说明

下面例子显示如何删除所有的组播路由信息。

```
Switch# clear ip mroute *
```

### 相关命令

show ip mroute

## 5.2 IGMP 命令

### 5.2.1 ip igmp access-group

此命令根据访问控制列表对加入组播组的主机或可以加入的组播组进行限制。使用关键字 **no** 取消此种限制。

### 命令语法

ip igmp access-group *list*

```
no ip igmp access-group
```

list	访问控制列表名称
------	----------

## 命令模式

端口配置模式

## 默认

无

## 使用说明

使用 IP 访问控制列表来控制 IGMP 报文的学习。

## 举例说明

在 VLAN1 的端口上根据访问控制列表 acl1 对可加入组播组的主机和可加入的组播组进行限制。

```
Switch(config-if)# interface vlan 1  
Switch(config-if)# ip igmp access-group acl1
```

取消在 VLAN1 的端口上的限制。

```
Switch(config-if)# no ip igmp access-group
```

## 相关命令

```
show ip igmp interface
```

## 5.2.2 ip igmp immediate-leave group-list

此命令根据访问控制列表限制可快速离开的主机和主机可快速离开的组播组。使用关键字 no 取消此种限制。

## 命令语法

```
ip igmp immediate-leave group-list list
```

```
no ip igmp immediate-leave
```

list	访问控制列表名称
------	----------

## 命令模式

端口配置模式

## 默认

无

## 使用说明

假如 ACE' s 的行为是拒绝, 数据包将会被忽略; 此外, ACE' s 的行为如果允许的话, 那么数据包正常转发。

## 举例说明

在 VLAN1 端口上限制可快速离开的主机和主机可快速离开的组播组。

```
Switch(config-if)# interface vlan 1
Switch(config-if)#ip igmp immediate-leave group-list acl1
```

在 VLAN1 端口上取消此种限制。

```
Switch(config-if)#no ip igmp immediate-leave group-list
```

## 相关命令

show ip igmp interface

### 5.2.3 ip igmp last-member-query-count

使用此命令设置当组播组的最后一个成员离开后所发送的特定组查询报文的数量; 如果在发送完所有的成员查询报文后, 仍然没有收到成员报告报文, 则端口会退出此多播组。使用关键字 no 恢复成员查询报文的数量为默认值。

## 命令语法

ip igmp last-member-query-count *count*

no ip igmp last-member-query-count

count	特定组查询报文的数目, 范围是 2 到 7
-------	-----------------------

## 命令模式

端口配置模式

## 默认

2

## 使用说明

无

## 举例说明

设置发送成员查询报文的最大数目为 5。

```
Switch(config-if)# ip igmp last-member-query-count 5
```

恢复发送成员查询报文的数目为默认值。

```
Switch(config-if)# no ip igmp last-member-query-count
```

## 相关命令

```
show ip igmp interface
```

```
ip igmp last-member-query-interval
```

### 5.2.4 ip igmp last-member-query-interval

使用此命令设置当组播组的最后一个成员离开后，发送特定组查询报文的间隔。使用关键字 `no` 恢复此间隔为默认值。

## 命令语法

```
ip igmp last-member-query-interval interval
```

```
no ip igmp last-member-query-interval
```

interval	特定组查询报文的间隔 (毫秒)，范围是 1000 到 25500
----------	----------------------------------

## 命令模式

端口配置模式

## 默认

1000 毫秒

## 使用说明

无

## 举例说明

设置端口发送组成员查询报文的时间间隔是 10000ms。

```
Switch(config-if)# ip igmp last-member-query-interval 10000
```

恢复端口发送组成员查询报文的时间间隔默认值。

```
Switch(config-if)# no ip igmp last-member-query-interval
```

## 相关命令

```
show ip igmp interface
```

```
ip igmp last-member-query-count
```

## 5.2.5 ip igmp limit

使用此命令设置全局或端口上可加入的组播组的最大个数。使用关键字 **no** 恢复此设置为默认值。

## 命令语法

```
ip igmp limit number except list
```

```
no ip igmp limit
```

number	全局或端口上可加入的组播组的最大个数，取值范围<1-2048>
list	组播组在这个访问控制列表中时不做数目限制

## 命令模式

全局模式和端口配置模式

## 默认

2048

## 使用说明

默认情况下，端口可加入的组播组的最大数目是 2048。

在全局配置模式下，设置所有端口可加入的组播组的最大数目。

在端口配置模式下，设置此端口可加入的组播组的最大数目。

## 举例说明

设置所有端口可加入的组播组的最大个数为 1000。

```
Switch(config)# ip igmp limit 1000
```

设置所有端口可加入的组播组的最大个数为默认值。

```
Switch(config)# no ip igmp limit
```



## 相关命令

```
show ip igmp interface
```

### 5.2.6 ip igmp mroute-proxy

使用此命令设置本端口的 IGMP 代理的上行端口。

## 命令语法

```
ip igmp mroute-proxy IFNAME
```

```
no ip igmp mroute-proxy IFNAME
```

IFNAME	端口名称，指定的上行端口
--------	--------------

## 命令模式

端口配置模式

## 默认

无

## 使用说明

一个端口只能设置一个上行代理端口。多次设置时，后面的设置会覆盖前面的设置。

## 举例说明

设置本端口的上行代理端口为 eth-0-1

```
Switch(config-if)# ip igmp mroute-proxy eth-0-1
```

删除本端口的上行代理端口

```
Switch(config-if)# no ip igmp mroute-proxy
```

## 相关命令

```
ip igmp proxy-service
```

### 5.2.7 ip igmp proxy-service

使用此命令启用端口的 IGMP 代理服务。使用关键字 no 关闭此服务。

## 命令语法

```
ip igmp proxy-service
```

```
no ip igmp proxy-service
```

## 命令模式

端口配置模式

## 默认

无

## 使用说明

此命令与 `ip igmp mroute-proxy` 配合使用，用来设定交换机的 IGMP 代理上联口。

## 举例说明

启用此端口的 IGMP 代理服务的上联口。

```
Switch(config-if)# ip igmp proxy-service
```

关闭此端口作为 IGMP 代理服务的上联口。

```
Switch(config-if)# no ip igmp proxy-service
```

## 相关命令

```
ip igmp mroute-proxy
```

## 5.2.8 ip igmp querier-timeout

使用此命令设置 Querier 的超时时间。使用关键字 `no` 恢复此超时时间为默认值。

## 命令语法

```
ip igmp querier-timeout intval
```

```
no ip igmp querier-timeout
```

<code>intval</code>	超时时间，以秒为单位，范围是 60 到 300 秒
---------------------	---------------------------

## 命令模式

端口配置模式

## 默认

255 秒

## 使用说明

无

## 举例说明

设置 Querier 的超时时间为 100 秒。

```
Switch(config-if)# ip igmp querier-timeout 100
```

恢复 Querier 的超时时间为默认值。

```
Switch(config-if) #no ip igmp querier-timeout
```

## 相关命令

ip igmp query-interval

ip igmp query-max-response-time

### 5.2.9 ip igmp query-interval

使用此命令设置端口发送 Querier 查询报文的时间间隔。使用关键字 no 恢复此时间间隔为默认值。

## 命令语法

ip igmp query-interval *intval*

no ip igmp query-interval

intval	端口发送 Querier 查询报文的时间间隔，以秒为单位，范围是 2 到 18000 秒
--------	--

## 命令模式

端口配置模式

## 默认

125 秒

## 使用说明

无

## 举例说明

设置发送 Querier 查询报文的时间间隔为 300 秒。

```
Switch(config-if)# ip igmp query-interval 300
```

恢复此时间间隔为默认值。

```
Switch(config-if)# no ip igmp query-interval
```

## 相关命令

```
ip igmp querier-timeout
```

```
ip igmp query-max-response-time
```

### 5.2.10 ip igmp query-max-response-time

使用此命令设置查询报文的最大响应时间；要求成员在此时间范围内必须响应一个报告消息。使用关键字 **no** 恢复此最大响应时间为默认值。

## 命令语法

```
ip igmp query-max-response-time intval
```

```
no ip query-max-response-time
```

<i>intval</i>	查询报文的最大响应时间，以秒为单位，范围是 1 到 25 秒
---------------	--------------------------------

## 命令模式

端口配置模式

## 默认

10 秒

## 使用说明

无

## 举例说明

设置查询报文的最大响应时间为 20 秒。

```
Switch(config-if)# ip igmp query-max-response-time 20
```

恢复此最大响应时间为默认值。

```
Switch(config-if)# no ip igmp query-max-response-time
```

## 相关命令

```
ip igmp querier-timeout
```

```
ip igmp query-interval
```

## 5.2.11 ip igmp robustness-variable

使用此命令设置 IGMP 查询器的健壮系数。使用关键字 `no` 恢复此项设置为默认值。

### 命令语法

```
ip igmp robustness-variable value
```

```
no ip robustness-variable
```

value	设定 IGMP 报文的健壮程度，范围是 2 到 7
-------	---------------------------

### 命令模式

端口配置模式

### 默认

2

### 使用说明

无

### 举例说明

设置 IGMP 查询器的健壮系数为 6。

```
Switch(config-if)# ip igmp robustness-variable 6
```

恢复此设置到默认值。

```
Switch(config-if)# no ip igmp robustness-variable
```

### 相关命令

```
show ip igmp interface
```

## 5.2.12 ip igmp version

使用此命令设定端口使用的 IGMP 协议的版本。使用关键字 `no` 恢复端口所使用的版本为默认值。

### 命令语法

```
ip igmp version number
```

```
no ip version
```

number	端口所使用的 IGMP 协议版本，范围是 1 到 3
--------	----------------------------

## 命令模式

端口配置模式

## 默认

2

## 使用说明

无

## 举例说明

设定端口使用的 IGMP 协议的版本为 version 1。

```
Switch(config-if)# ip igmp version 1
```

设定端口使用的 IGMP 协议的版本为默认值。

```
Switch(config-if)# no ip igmp version
```

## 相关命令

```
show ip igmp interface
```

## 5.2.13 ip igmp static-group

此命令用来设置或删除端口上的静态组播组。

## 命令语法

```
ip igmp static-group group-address ( source source-address )
```

```
no ip igmp static-group group-address ( source source-address )
```

group-address	组播组地址
<b>source</b> source-address	组播源地址

## 命令模式

端口配置模式

## 默认

无

## 使用说明

无

## 举例说明

下面的例子说明如何在接口上配置静态组播组。

```
Switch # configure terminal
Switch (config)# interface eth-0-1
Switch (config-if)# ip igmp static-group 226.1.2.3
Switch (config-if)# ip igmp static-group 226.1.2.4 source 1.2.3.4
```

下面的例子说明如何删除接口上配置的静态组播组。

```
Switch # configure terminal
Switch (config)# interface eth-0-1
Switch (config-if)# no ip igmp static-group 226.1.2.3
```

## 相关命令

show ip igmp groups

### 5.2.14 ip igmp ssm-map enable

此命令用来使能 IGMP ssm-mapping 功能。使用关键字 no 禁用此功能。

## 命令语法

```
ip igmp ssm-map enable
no ip igmp ssm-map enable
```

## 命令模式

全局模式

## 默认

关闭

## 使用说明

无

## 举例说明

使能 IGMP ssm-mapping 功能。

```
Switch(config)# ip igmp ssm-map enable
```

关闭 IGMP ssm-mapping 功能。

```
Switch(config)# no ip igmp ssm-map enable
```

## 相关命令

无

### 5.2.15 ip igmp ssm-map static

此命令用来设置 IGMP ssm-mapping 的规则。使用关键字 no 禁用此功能。

## 命令语法

```
ip igmp ssm-map static list source-address
```

```
no ip igmp ssm-map static list source-address
```

list	访问控制列表，指定组播组范围
source-address	组播源地址

## 命令模式

全局模式

## 默认

关闭

## 使用说明

无

## 举例说明

设置在 ipacl 中的 group 映射的 source 地址为 192.168.1.1

```
Switch(config)# ip igmp ssm-map static ipacl 192.168.1.1
```

取消在 ipacl 中的 group 的映射的 source 地址为 192.168.1.1

```
Switch(config)# no ip igmp ssm-map static ipacl 192.168.1.1
```

## 相关命令

无

### 5.2.16 clear ip igmp

此命令清除动态学习的组播组信息。

## 命令语法

```
clear ip igmp (* | group group-address |)
```



group-address	指定组播组地址
*	所有的组播组信息

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子显示如何删除所有的组播组信息。

```
Switch# clear ip igmp
Switch# clear ip igmp group *
```

下面例子显示如何删除组播组 228.1.1.1。

```
Switch# clear ip igmp group 228.1.1.1
```

## 相关命令

show ip igmp groups

## 5.2.17 clear ip igmp interface

此命令清除指定端口上动态学习的组播组信息。

## 命令语法

clear ip igmp (group *group-address* | interface ) *IFNAME*

group-address	指定组播组地址
IFNAME	指定接口名称

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子显示如何清除端口 `eth-0-1` 上动态组播组信息。

```
Switch# clear ip igmp group interface eth-0-1
```

## 相关命令

```
show ip igmp groups
```

### 5.2.18 show ip igmp groups

此命令用于显示组播组信息。

## 命令语法

```
show ip igmp groups group-address (detail |)
```

group-address	指定组播组地址
detail	组播组详细信息

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子显示组播组的详细信息。

```
Switch# show ip igmp groups detail
Interface:      eth-0-1
```

```

Group:          227.0.0.1
Uptime:        00:00:33
Group mode:    Exclude (Expires: 00:04:18)
Last reporter: 10.0.1.100
Source list is empty

```

## 相关命令

无

## 5.2.19 show ip igmp groups interface

此命令用于显示端口的 IPv6 组播组信息。

## 命令语法

```
show ip igmp groups IFNAME (group-address | ) (detail |)
```

group-address	指定组播组地址
detail	组播组详细信息
IFNAME	接口名称

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子显示接口 **eth-0-1** 上的组播组信息。

```

Switch# show ip igmp groups eth-0-1
IGMP Connected Group Membership
Group Address   Interface      Uptime   Expires   Last Reporter
227.0.0.1      eth-0-1       00:01:11 00:04:16 10.0.1.100

```

## 相关命令

无

## 5.2.20 show ip igmp groups count

此命令用于显示组播组数目。

### 命令语法

```
show ip igmp groups (IFNAME |) count
```

IFNAME	接口名称
--------	------

### 命令模式

特权模式

### 默认

无

### 使用说明

无

### 举例说明

下面例子显示端口 **eth-0-1** 上的组播组数目。

```
Switch# show ip igmp groups eth-0-1 count
Dynamic multicast groups count: 1
Static multicast groups count: 0
Total multicast groups count: 1
```

### 相关命令

无

## 5.2.21 show ip igmp interface

此命令用于查看组播组端口的信息。

### 命令语法

```
show ip igmp interface (IFNAME |)
```

IFNAME	接口名称
--------	------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

查看端口 eth-0-1 的多播设置信息。

```
Switch# show ip igmp interface eth-0-1
Interface eth-0-1 (Index 1)
  IGMP Enabled, Active, Querier, Version 2 (default)
  Internet address is 10.0.1.1
  IGMP interface limit is 8192
  IGMP interface has 1 group-record states
  IGMP activity: 97 joins, 0 leaves
  IGMP query interval is 125 seconds
  IGMP querier timeout is 255 seconds
  IGMP max query response time is 10 seconds
  Last member query response interval is 1000 milliseconds
  Group Membership interval is 260 seconds
  Last member query count is 2
  Robustness Variable is 2
```

## 相关命令

无

## 5.3 IGMP Snooping 命令

### 5.3.1 ip igmp snooping

使用此命令启用 IGMP Snooping 使用关键字 no 关闭此项功能。

## 命令语法

```
ip igmp snooping (vlan vlan_id |)
no ip igmp snooping (vlan vlan_id |)
```

vlan_id	VLAN id, 范围是 1 到 4094
---------	-----------------------

## 命令模式

全局配置模式

## 默认

使能

## 使用说明

在全局模式下或者 VLAN 模式下启用 Igmp Snooping。

默认，igmp snooping 启用。

## 举例说明

启用 IGMP Snooping 功能。

```
Switch(config)# ip igmp snooping
```

关闭 IGMP Snooping 功能。

```
Switch(config)# no ip igmp snooping
```

## 相关命令

```
show ip igmp snooping
```

### 5.3.2 ip igmp snooping fast-leave

使用此命令启用 IGMP snooping 成员快速离开功能。使用关键字 no 关闭此功能。

## 命令语法

```
ip igmp snooping (vlan vlan_id | ) fast-leave
```

```
no ip igmp snooping (vlan vlan_id | ) fast-leave
```

vlan_id	VLAN id, 范围是 1 到 4094
---------	-----------------------

## 命令模式

全局配置模式

## 默认

关闭

## 使用说明

此命令会覆盖 `immediate-leave` 的设置。

## 举例说明

启用成员快速离开功能。

```
Switch(config)# ip igmp snooping fast-leave
```

关闭成员快速离开功能。

```
Switch(config)# no ip igmp snooping fast-leave
```

## 相关命令

```
show ip igmp snooping global
```

### 5.3.3 ip igmp snooping last-member-query-interval

使用此命令设置当仅存最后一个成员时的查询间隔。使用关键字 `no` 恢复查询间隔为默认值。

## 命令语法

```
ip igmp snooping (vlan vlan_id | ) last-member-query-interval interval
```

```
no ip igmp snooping (vlan vlan_id | ) last-member-query-interval
```

<b>vlan</b> <i>vlan_id</i>	VLAN id, 范围是 1 到 4094
<b>interval</b>	查询间隔, 单位为毫秒, 范围是 1000 到 25500

## 命令模式

全局配置模式

## 默认

1000 毫秒

## 使用说明

无

## 举例说明

设置当仅存最后一个成员时的查询间隔。

```
Switch(config)# ip igmp snooping last-member-query-interval 2000
```

恢复查询间隔为默认值。

```
Switch(config)# no ip igmp snooping last-member-query-interval
```

## 相关命令

```
show ip igmp snooping
```

```
show ip igmp snooping vlan
```

### 5.3.4 ip igmp snooping global source-address

使用此命令设置 IGMP snooping 查询器源地址。

## 命令语法

```
ip igmp snooping global source-address address
```

```
no ip igmp snooping global source-address
```

address	查询器源 IP 地址
---------	------------

## 命令模式

全局配置模式

## 默认

0.0.0.0

## 使用说明

VLAN 上没有配置查询器源地址时使用全局的查询器地址，VLAN 上配置了查询器地址后使用 VLAN 上配置的查询器地址。

## 举例说明

全局模式下配置查询器源 IP 地址 1.3.4.5。

```
Switch(config)# ip igmp snooping global source-address 1.3.4.5
```

恢复全局模式的查询器地址。

```
Switch(config)# no ip igmp snooping global source-address
```

## 相关命令

```
show ip igmp snooping querier
```



### 5.3.5 ip igmp snooping max-member-num

使用此命令设置 IGMP snooping 最大成员数目。使用关键字 `no` 恢复此数目为默认值。

#### 命令语法

```
ip igmp snooping (vlan vlan_id | ) max-member-num number
```

```
no ip igmp snooping (vlan vlan_id | ) max-member-num
```

<b>vlan</b> <i>vlan_id</i>	VLAN id, 范围是 1 到 4094
<b>number</b>	最大成员数目, 范围是 1 到 2048

#### 命令模式

全局配置模式

#### 默认

2048

#### 使用说明

无

#### 举例说明

设置 IGMP snooping 最大成员数目为 1024。

```
Switch(config)# ip igmp snooping max-member-num 1024
```

恢复 IGMP snooping 最大成员数目为默认值。

```
Switch(config)# no ip igmp snooping max-member-num
```

#### 相关命令

```
show ip igmp snooping global
```

```
show ip igmp snooping vlan
```

### 5.3.6 ip igmp snooping query-interval

使用此命令设置成员查询的间隔。使用关键字 `no` 恢复此间隔为默认值。

#### 命令语法

```
ip igmp snooping (vlan vlan_id | ) query-interval interval
```

no ip igmp snooping (vlan *vlan\_id* | ) query-interval

vlan <i>vlan_id</i>	VLAN id, 范围是 1 到 4094
interval	成员查询间隔, 以秒为单位, 范围是 2 到 18000

## 命令模式

全局配置模式

## 默认

125 秒

## 使用说明

查询的间隔时间不能少于 IGMP snooping 查询最大的响应时间。

## 举例说明

设置成员查询间隔为 64 秒。

```
Switch(config)# ip igmp snooping query-interval 64
```

恢复成员查询间隔为默认值。

```
Switch(config)# no ip igmp snooping query-interval
```

## 相关命令

```
show ip igmp snooping querier
```

```
show ip igmp snooping querier vlan
```

### 5.3.7 ip igmp snooping query-max-response-time

使用此命令设置等待查询应答报文的超时时间。使用关键字 no 恢复此超时时间为默认值。

## 命令语法

```
ip igmp snooping (vlan vlan_id | ) query-max-response-time time
```

```
no ip igmp snooping (vlan vlan_id | ) query-max-response-time
```

vlan_id	VLAN id, 范围是 1 到 4094
time	等待查询应答报文的超时时间, 以秒为单位, 范围是 1 到 25

## 命令模式

全局配置模式

## 默认

10 秒

## 使用说明

查询应答时间不能少于 IGMP snooping 查询间隔。

## 举例说明

设置等待查询应答报文的超时时间为 15 秒。

```
Switch(config)# ip igmp snooping query-max-response-time 15
```

恢复此超时时间。

```
Switch(config)# no ip igmp snooping query-max-response-time
```

## 相关命令

```
show ip igmp snooping querier
```

```
show ip igmp snooping querier vlan
```

### 5.3.8 ip igmp snooping report-suppression

使用此命令设置端口对 IGMPv1/v2 的成员报告报文进行抑制。使用关键字 `no` 取消对 IGMPv1/v2 的成员报告报文的抑制。

## 命令语法

```
ip igmp snooping (vlan vlan_id | ) report-suppression
```

```
no ip igmp snooping (vlan vlan_id | ) report-suppression
```

vlan_id	VLAN id, 范围是 1 到 4094
---------	-----------------------

## 命令模式

全局配置模式

## 默认

启用

## 使用说明

IGMP snooping 工作在 v3 模式时，成员报告报文不进行抑制。

## 举例说明

对 IGMPv1/IGMPv2 的成员报告报文进行抑制。

```
Switch(config)# ip igmp snooping report-suppression
```

取消对 IGMPv1/IGMPv2 的成员报告报文的抑制

```
Switch(config)# no ip igmp snooping report-suppression
```

## 相关命令

```
show ip igmp snooping
```

```
show ip igmp snooping vlan
```

### 5.3.9 ip igmp snooping version

使用此命令指定运行的 IGMP 版本。使用关键字 **no** 恢复运行的 IGMP 版本为默认值

## 命令语法

```
ip igmp snooping (vlan vlan_id | ) version version
```

```
no ip igmp snooping (vlan vlan_id | ) version
```

vlan_id	VLAN id, 范围是 1 到 4094
version	IGMP 版本, 范围是 1 到 3

## 命令模式

全局配置模式

## 默认

2

## 使用说明

无

## 举例说明

指定全局 IGMP snooping 运行 IGMPv1 模式下。

```
Switch(config)# ip igmp snooping version 1
```

## 相关命令

```
show ip igmp snooping
```

```
show ip igmp snooping vlan
```

### 5.3.10 ip igmp snooping discard-unknown

使用此命令丢弃未知的组播流量。使用 `no` 命令恢复默认值。

## 命令语法

```
ip igmp snooping (vlan vlan_id | ) discard-unknown
```

```
no ip igmp snooping (vlan vlan_id | ) discard-unknown
```

<b>vlan</b> <i>vlan_id</i>	VLAN id, 范围是 1 到 4094
----------------------------	-----------------------

## 命令模式

全局配置模式

## 默认

未知组播流量在 VLAN 内泛洪。

## 使用说明

无

## 举例说明

在全局模式下配置交换机丢弃未知组播流量

```
Switch(config)# ip igmp snooping discard-unknown
```

## 相关命令

```
show ip igmp snooping
```

```
show ip igmp snooping vlan
```

### 5.3.11 ip igmp snooping querier tcn

使用此命令设置 IGMP snooping 的 TCN 相关参数。

#### 命令语法

```
ip igmp snooping querier tcn (enable|query-count count | query-interval interval| query-max-response-time)
```

```
no ip igmp snooping querier tcn (enable|query-count | query-interval| query-max-response-time)
```

enable	使能 IGMP snooping 查询器 TCN 查询
query-count <i>count</i>	IGMP snooping 查询 TCN 查询次数，范围是 1 到 10
query-interval <i>interval</i>	IGMP snooping 查询 TCN 查询间隔，范围是 1 到 255
query-max-response-time	IGMP snooping 查询 TCN 查询最大响应时间 (sec)，范围是 1 到 10，默认 5 秒

#### 命令模式

全局配置模式

#### 默认

关闭

#### 使用说明

Igmp snooping tcn 查询次数必须配置，默认值为 2，范围取值 1-10。

Igmp snooping tcn 查询间隔必须配置，默认值 10 秒，范围 1-255 秒。

#### 举例说明

设置 IGMP Snooping Tcn 的查询次数为 2 次。

```
Switch(config)# ip igmp snooping querier tcn query-count 2
```

#### 相关命令

```
show ip igmp snooping vlan
```

### 5.3.12 ip igmp snooping vlan access-group

此命令用于设置允许加入的组播组范围。

## 命令语法

```
ip igmp snooping vlan vlan_id access-group acl
```

```
no ip igmp snooping vlan vlan_id access-group
```

vlan_id	VLAN id, 范围是 1 到 4094
acl	访问控制列表名称

## 命令模式

全局配置模式

## 默认

无

## 使用说明

无

## 举例说明

在 VLAN 上设置运行加入的组播组范围是 *acl* 中的组播组范围。

```
Switch(config)# ip igmp snooping vlan 10 access-group acl
```

## 相关命令

```
show ip igmp snooping vlan
```

### 5.3.13 ip igmp vlan mrouter interface

此命令用于静态配置 VLAN 的组播路由端口。

## 命令语法

```
ip igmp snooping vlan vlan_id mrouter interface IFNAME
```

```
no ip igmp snooping vlan vlan_id mrouter interface IFNAME
```

vlan_id	VLAN id, 范围是 1 到 4094
IFNAME	端口名称

## 命令模式

全局配置模式

## 默认

无

## 使用说明

指定的组播路由端口必须属于指定的 VLAN。

## 举例说明

将 eth-0-1 设置成 VLAN10 的组播路由端口。

```
Switch(config)# ip igmp snooping vlan 10 mrouter interface eth-0-1
```

## 相关命令

```
show ip igmp snooping vlan
```

### 5.3.14 ip igmp vlan mrouter-aging-interval

此命令用于设置动态组播路由端口老化的时间间隔。

## 命令语法

```
ip igmp snooping vlan vlan_id mrouter-aging-interval interval
```

```
no ip igmp snooping vlan vlan_id mrouter-aging-interval
```

vlan_id	VLAN id, 范围是 1 到 4094
interval	老化时间间隔, 单位是秒, 范围是 1 到 65535

## 命令模式

全局配置模式

## 默认

255 秒

## 使用说明

无

## 举例说明

设置 VLAN 上的动态组播路由端口老化间隔是 100 秒。

```
Switch(config)# ip igmp snooping vlan 10 mrouter-aging-interval 100
```



## 相关命令

```
show ip igmp snooping vlan
```

### 5.3.15 ip igmp snooping vlan querier

此命令用于在 VLAN 上使能组播查询器功能。

## 命令语法

```
ip igmp snooping vlan vlan_id querier
```

```
no ip igmp snooping vlan vlan_id querier
```

<i>vlan_id</i>	VLAN id, 范围是 1 到 4094
----------------	-----------------------

## 命令模式

全局配置模式

## 默认

关闭

## 使用说明

无

## 举例说明

在 VLAN10 上使能组播查询器功能。

```
Switch(config)# ip igmp snooping vlan 10 querier
```

## 相关命令

```
show ip igmp snooping querier vlan
```

### 5.3.16 ip igmp snooping vlan querier address

此命令用于设置 VLAN 上组播查询器的源地址。

## 命令语法

```
ip igmp snooping vlan vlan_id querier address address
```

```
no ip igmp snooping vlan vlan_id querier address address
```

vlan_id	VLAN id, 范围是 1 到 4094
address	组播查询器源地址

## 命令模式

全局配置模式

## 默认

无

## 使用说明

VLAN 上配置的组播查询器源地址将覆盖全局的组播查询器地址。

## 举例说明

设置 VLAN10 上组播查询器的源地址是 1.1.1.1。

```
Switch(config)# ip igmp snooping vlan 10 querier address 1.1.1.1
```

## 相关命令

```
show ip igmp snooping querier vlan
```

### 5.3.17 ip igmp snooping vlan querier-timeout

此命令用于设置 VLAN 上查询器老化时间。

## 命令语法

```
ip igmp snooping vlan vlan_id querier-timeout interval
```

```
no ip igmp snooping vlan vlan_id querier-timeout
```

vlan_id	VLAN id, 范围是 1 到 4094
interval	查询器老化时间间隔, 单位是秒, 范围是 60 到 300 秒

## 命令模式

全局配置模式

## 默认

255 秒

## 使用说明

无

## 举例说明

设置 VLAN10 查询器老化间隔为 100 秒

```
Switch(config)# ip igmp snooping vlan 10 querier-timeout 100
```

## 相关命令

```
show ip igmp snooping querier vlan
```

### 5.3.18 ip igmp snooping vlan static-group

此命令用于设置 VLAN 的成员端口加入组播组或组播源组。

## 命令语法

```
ip igmp snooping vlan vlan_id static-group group-address (source source-address |) interface IFNAME
```

```
no ip igmp snooping vlan vlan_id static-group group-address (source source-address |) interface IFNAME
```

vlan_id	VLAN id, 范围是 1 到 4094
group-address	组播组地址
source source-address	组播源地址
IFNAME	VLAN 的成员端口名称

## 命令模式

全局配置模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子显示如何将 VLAN10 的成员端口 eth-0-11 加入组播组 238.1.1.1。

```
Switch(config)# ip igmp snooping vlan 10 static-group 238.1.1.1 interface eth-0-11
```

## 相关命令

```
show ip igmp snooping group
```

### 5.3.19 clear ip igmp snooping group

此命令用于删除所有的 IGMP snooping 组信息。

## 命令语法

```
clear ip igmp snooping (group * )
```

## 命令模式

特权模式

## 默认

无

## 使用说明

此命令用来删除动态学习到的组播组信息。

## 举例说明

下面例子显示如何删除所有的组播组信息。

```
Switch# clear ip igmp snooping
```

## 相关命令

无

### 5.3.20 clear ip igmp snooping vlan

此命令用于删除指定 VLAN 上的组播组信息。

## 命令语法

```
clear ip igmp snooping vlan vlan_id
```

vlan_id	VLAN id, 范围是 1 到 4094
---------	-----------------------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子显示如何删除 VLAN10 上的组播组信息

```
Switch# clear ip igmp snooping vlan 10
```

## 相关命令

无

### 5.3.21 show ip igmp snooping global

使用此命令查看所有关于 IGMP Snooping 的全局配置。

## 命令语法

```
show ip igmp snooping global
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

查看所有关于 IGMP Snooping 的全局配置。

```
Switch# show ip igmp snooping global
Global Igmp Snooping Configuration
-----
Igmp Snooping                               :Enabled
Igmp Snooping Fast-Leave                       :Disabled
Igmp Snooping Version                         :2
```

```

Igmp Snooping Robustness Variable      :2
Igmp Snooping Max-Member-Number       :2048
Igmp Snooping Unknown Multicast Behavior :Flood
Igmp Snooping Report-Suppression      :Enabled

```

## 相关命令

无

### 5.3.22 show ip igmp snooping groups

此命令用于显示 IGMP snooping 组播组信息。

## 命令语法

```
show ip igmp snooping groups
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

显示 IGMP snooping 组播组信息。

```

Switch# show ip igmp snooping groups
VLAN   Interface      Group-Address      Uptime      Expires-time
1      eth-0-1        227.0.0.1         00:03:44   00:04:18

```

## 相关命令

无

### 5.3.23 show ip igmp snooping groups vlan

此命令用于指定 VLAN 上的组播组信息。

## 命令语法

```
show ip igmp snooping groups vlan vlan_id (group_address |)
```

vlan_id	VLAN id, 范围是 1 到 4094
---------	-----------------------

group_addres	组播组信息
--------------	-------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子显示 VLAN1 上的组播组信息。

```
Switch# show ip igmp snooping groups vlan 1
IGMP Snooping groups for vlan1
Interface:      eth-0-1
Group:         227.0.0.1
Uptime:        00:05:24
Group mode:    Exclude (Expires: 00:04:20)
Last reporter: 10.0.1.100
Source list is empty
```

## 相关命令

无

### 5.3.24 show ip igmp snooping groups count

此命令用于显示 IGMP snooping 组播组数目。

## 命令语法

```
show ip igmp snooping groups (vlan vlan_id |) count
```

<b>vlan</b> <i>vlan_id</i>	VLAN id, 范围是 1 到 4094
----------------------------	-----------------------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子 VLAN1 上组播组数目。

```
Switch# show ip igmp snooping groups vlan 1 count
Dynamic multicast groups count: 1
Static multicast groups count: 0
Total multicast groups count: 1
```

## 相关命令

无

### 5.3.25 show ip igmp snooping querier

此命令用于显示 IGMP snooping 查询器相关信息。

## 命令语法

```
show ip igmp snooping querier (vlan vlan_id |)
```

<b>vlan</b> <i>vlan_id</i>	VLAN id, 范围是 1 到 4094
----------------------------	-----------------------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子显示 VLAN1 上查询器信息。

```
Switch# show ip igmp snooping querier vlan 1
```



```

Global Igmp Snooping Querier Configuration
-----
Version                               :2
Last-Member-Query-Interval (msec)    :1000
Last-Member-Query-Count              :2
Max-Query-Response-Time (sec)        :10
Query-Interval (sec)                 :125
Global Source-Address                 :0.0.0.0
TCN Query Count                      :2
TCN Query Interval (sec)             :10
TCN Query Max Respose Time (sec)     :5
Vlan 1:  IGMP snooping querier status
-----
Elected querier is : 0.0.0.0
-----
Admin state                           :Disabled
Admin version                          :2
Operational state                     :Non-Querier
Querier operational address            :0.0.0.0
Querier configure address             :N/A
Last-Member-Query-Interval (msec)    :1000
Last-Member-Query-Count              :2
Max-Query-Response-Time (sec)        :10
Query-Interval (sec)                 :125
Querier-Timeout (sec)                :255

```

## 相关命令

无

### 5.3.26 show ip igmp snooping mrouter

此命令用于显示组播路由端口信息。

## 命令语法

```
show ip igmp snooping mrouter (vlan vlan_id |)
```

<b>vlan</b> <i>vlan_id</i>	VLAN id, 范围是 1 到 4094
----------------------------	-----------------------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子显示 VLAN1 上的组播路由端口信息。

```
Switch# show ip igmp snooping mrouter vlan 1
Interface      Mode      Uptime      Expires-time
eth-0-11       static    -           -
```

## 相关命令

无

### 5.3.27 show ip igmp snooping vlan

此命令用于 IGMP snooping 的配置信息。

## 命令语法

```
show ip igmp snooping (vlan vlan_id |)
```

<b>vlan</b> <i>vlan_id</i>	VLAN id, 范围是 1 到 4094
----------------------------	-----------------------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子显示 VLAN1 上 IGMP snooping 的信息。

```
Switch# show ip igmp snooping vlan 1
Global Igmp Snooping Configuration
-----
Igmp Snooping                               :Enabled
Igmp Snooping Fast-Leave                      :Disabled
Igmp Snooping Version                        :2
Igmp Snooping Robustness Variable            :2
Igmp Snooping Max-Member-Number              :2048
Igmp Snooping Unknown Multicast Behavior     :Flood
Igmp Snooping Report-Suppression             :Enabled
Vlan 1
```

```

-----
Igmp Snooping                               :Enabled
Igmp Snooping Fast-Leave                     :Disabled
Igmp Snooping Report-Suppression           :Enabled
Igmp Snooping Version                       :2
Igmp Snooping Robustness Variable          :2
Igmp Snooping Max-Member-Number           :2048
Igmp Snooping Unknown Multicast Behavior   :Flood
Igmp Snooping Group Access-list            :N/A
Igmp Snooping Mrouter Port                 :
Igmp Snooping Mrouter Port Aging Interval(sec) :255

```

## 相关命令

无

### 5.3.28 show resource l2mcast

此命令用于二层组播的资源使用情况。

## 命令语法

```
show resource l2mcast
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子显示二层组播资源使用情况。

```

Switch# show resource l2mcast
L2MCAST
Resource                               Used           Capability
=====
L2 Mcast Entry                          0              2048

```

## 相关命令

无

## 5.4 PIM 命令

### 5.4.1 ip pim accept-register

此命令根据访问控制列表限制 RP 可接受的 PIM 注册报文。使用关键字 **no** 关闭此功能。

#### 命令语法

```
ip pim accept-register list list
```

```
no ip pim accept-register
```

list	访问控制列表
------	--------

#### 命令模式

全局配置模式

#### 默认

无

#### 使用说明

此功能用来防止未经认证的用户注册到交换机；当其用此功能后，如果一个未经认证的主机发送一个 PIM 注册报文给交换机，此交换机会立即发送一个 Stop 报文回去阻止其继续发送报文注册。此命令可以有效的让网络中众多 RP 负载分担，通过 ACL 的设置控制不同的组播组。

#### 举例说明

下面例子讲述了如何根据访问控制列表 **acl1** 限制 RP 可接受的 PIM 注册报文。

```
Switch(config)# ip pim accept-register list acl1
```

#### 相关命令

无

### 5.4.2 ip pim anycast-rp

使用此命令设置任播汇聚路由器地址及其成员。使用关键字 **no** 删除指定成员。

#### 命令语法

```
ip pim anycast-rp anycast_rp_address anycast_member_address
```

```
no ip pim anycast-rp anycast_rp_address (anycast_member_address |)
```

anycast_rp_address	RP 地址
anycast_member_address	组成员地址

## 命令模式

全局配置模式

## 默认

无

## 使用说明

如果要配置，则应该在所有路由器上配置，所有路由器必须使用相同的 RP 地址，当静态配置的 RP 失效时，路由器不可能切换到其它的备用 RP(除非使用 Anycast-RP，在 RP 之间运行)。

## 举例说明

设置任播汇聚路由器地址及其组成员。

```
Switch(config)# ip pim anycast-rp 10.10.10.1 10.10.10.11
Switch(config)# no ip pim anycast-rp 10.10.10.1 10.10.10.11
```

## 相关命令

无

### 5.4.3 ip pim bsr-candidate

使用此命令设置本交换机作为候选的自举交换机，使用关键字 **no** 取消此项设置。

## 命令语法

**ip pim bsr-candidate** IFNAME ( hash-mask (priority))

no ip pim bsr-candidate

IFNAME	端口名称
hash-mask	RP 选举时候 HASH 的掩码长度，范围是 0 到 32
priority	候选 BSR 路由器的优先级，范围是 0 到 255

## 命令模式

全局配置模式

## 默认

无

## 使用说明

无

## 举例说明

设置此交换机作为 BSR，设置端口 eth-0-1 的地址作为 BSR 的地址

```
Switch(config)# ip pim bsr-candidate eth-0-1
```

## 相关命令

ip pim bsr-border

### 5.4.4 ip pim bsr-border

使用此命令设置此交换机作为 PIM 域的边界，BSR 报文不再被转发出去。

## 命令语法

```
ip pim bsr-border  
no ip pim bsr-border
```

## 命令模式

端口配置模式

## 默认

不使能

## 使用说明

无

## 举例说明

设置此交换机作为 PIM 域的边界。

```
Switch(config-if)# ip pim bsr-border
```

## 相关命令

ip pim bsr-candidate

### 5.4.5 ip pim dr-priority

使用此命令设定竞选指定路由器的优先权值，使用关键字 `no` 恢复优先权值为默认值。

## 命令语法

ip pim dr-priority *priority*

no ip pim dr-priority

priority	设定的指定路由器的优先权值，范围是 0 到 4294967294
----------	----------------------------------

## 命令模式

端口配置模式

## 默认

1

## 使用说明

端口的优先权默认为 1，如果一个路由器在它的 Hello 报文中没有宣布它的优先权值，此路由器将被认为具有最大的优先权值，因此将被选举为 DR。如果有不止一个的路由器在它的 HELLO 报文中没有宣布它的优先权值，则具有最高 IP 地址的将被选为 DR。

## 举例说明

设定竞选指定路由器的优先权值是 1000。

```
Switch(config-if)# ip pim dr-priority 1000
```

## 相关命令

无

### 5.4.6 ip pim exclude-genid

使用此命令设置此端口发出的 Hello 报文不包括 GenerationID 选项。使用关键字 `no` 恢复此项设置为默认状态。

## 命令语法

ip pim exclude-genid

```
no ip pim exclude-genid
```

## 命令模式

端口配置模式

## 默认

不使能

## 使用说明

GenerationID 是 PIM 邻居的一个标识 ID，在 PIM Hello 中携带，本端设备会记录对端发送的 hello 报文中携带的 GenerationID，本端设备每次收到对端的 PIM Hello 会去 check 一下这个 ID 是否有变化，如果有变化，则认为邻居状态发生改变，重新走状态机。

## 举例说明

设置 RP 发送的 Hello 报文中无 GenerationID 的报文。

```
Switch(config-if)# ip pim exclude-genid
```

## 相关命令

无

## 5.4.7 ip pim hello-interval

使用此命令设定端口发送 Hello 报文的时间间隔，使用关键字 no 恢复时间间隔为默认值。

## 命令语法

```
ip pim hello-interval interval
```

```
no ip pim hello-interval
```

interval	>发送 Hello 报文的时间间隔，以秒为单位，范围是 1 到 65535
----------	---------------------------------------

## 命令模式

端口配置模式

## 默认

30 秒



## 使用说明

无

## 举例说明

设定发送 Hello 报文的时间间隔是 100 秒。

```
Switch(config-if)# ip pim hello-interval 100
```

## 相关命令

无

### 5.4.8 ip pim ignore-rp-set-priority

设置忽略关于 RP（Rendezvous Router，汇聚路由器）的优先权。使用关键字 **no** 对 RP 优先权不进行忽略。

## 命令语法

```
ip pim ignore-rp-set-priority  
no ip pim ignore-rp-set-priority
```

## 命令模式

全局配置模式

## 默认

默认情况下，对 RP 优先权不进行忽略。

## 使用说明

无

## 举例说明

忽略关于 RP 优先权的设置值。

```
Switch(config)# ip pim ignore-rp-set-priority
```

## 相关命令

无

### 5.4.9 ip pim jp-timer

设置端口发送加入/修剪报文的时间间隔。使用关键字 **no** 恢复此时间间隔为默认值。

## 命令语法

```
ip pim jp-timer timer
```

```
no ip pim jp-timer
```

timer	端口发送加入/修剪报文的时间间隔，以秒为单位，范围是 1 到 65535
-------	--------------------------------------

## 命令模式

全局配置模式

## 默认

60 秒

## 使用说明

无

## 举例说明

设置端口发送加入/修剪报文的时间间隔为 100 秒。

```
Switch(config)# ip pim jp-timer 100
```

## 相关命令

无

### 5.4.10 ip pim neighbor-filter

此命令根据访问控制列表限制与此设备建立邻居关系的节点。使用关键字 **no** 取消此项限制。

## 命令语法

```
ip pim neighbor-filter list
```

```
no ip pim neighbor-filter
```

list	访问控制列表
------	--------

## 命令模式

端口配置模式

## 默认

无

## 使用说明

在 PIM 协议中，节点之间会互相发送 PIM Hello 报文来与对方建立邻居关系；此命令可以根据访问控制列表来限制与此设备建立邻居关系的节点。

## 举例说明

根据访问控制列表 `acl1` 限制与此设备建立邻居关系的节点。

```
Switch(config-if)# ip pim neighbor-filter acl1
```

## 相关命令

无

### 5.4.11 ip pim register-rate-limit

使用此命令设置 DR 发往 RP 的 PIM 注册报文的最大速度。使用关键字 `no` 恢复此项设置为默认值。

## 命令语法

```
ip pim register-rate-limit limit
```

```
no ip pim register-rate-limit
```

limit	DR 发往 RP 的 PIM 注册报文的最大速度，范围是 1 到 65535
-------	--

## 命令模式

全局配置模式

## 默认

默认情况下，对 DR 发往 RP 的 PIM 注册报文的速率不进行限制。如果设定了此项，则超过此速率的 PIM 注册报文在 RP 处会被丢弃。

## 使用说明

无

## 举例说明

设置 DR 发往 RP 的 PIM 注册报文的最大速度为每秒 100 个。

```
Switch(config)# ip pim register-rate-limit 100
```

## 相关命令

```
ip pim register-rp-reachability
```

```
ip pim register-source
```

```
ip pim register-suppression
```

### 5.4.12 ip pim register-source

此命令设置 DR 发往 RP 的注册报文的源 IP 地址，使用关键字 no 恢复注册报文的源 IP 地址为默认值

## 命令语法

```
ip pim register-source IFNAME
```

```
no ip pim register-source
```

IFNAME	接口名称
--------	------

## 命令模式

全局配置模式

## 默认

无

## 使用说明

使用此端口的 IP 地址为注册报文的源 IP 地址，默认情况下，源 IP 地址为 DR 的 interface IP 地址。

## 举例说明

设置注册报文的源 IP 地址为 eth-0-1 端口的 IP 地址。

```
Switch(config)# ip pim register-source eth-0-1
```

## 相关命令

```
ip pim register-rate-limit
```

```
ip pim register-rp-reachability
```

```
ip pim register-suppression
```

### 5.4.13 ip pim register-rp-reachability

此命令设置对 RP（Rendezvous Router，汇聚路由器）可到达性的检测。

#### 命令语法

```
ip pim register-rp-reachability
```

```
no ip pim register-rp-reachability
```

#### 命令模式

全局配置模式

#### 默认

不使能

#### 使用说明

无

#### 举例说明

设置对 RP（Rendezvous Router，汇聚路由器）可到达性的检测。

```
Switch(config)# ip pim register-rp-reachability
```

#### 相关命令

```
ip pim register-rate-limit
```

```
ip pim register-source
```

```
ip pim register-suppression
```

### 5.4.14 ip pim register-suppression

当 RP 给 DR 发送 Stop 报文后，DR 会停止发送 PIM 注册报文一段时间。此命令可以设置 DR 停止发送 PIM 注册报文的时间长短。使用关键字 `no` 恢复此时间段的设置为默认值。

#### 命令语法

```
ip pim register-suppression time
```

```
no ip pim register-suppression
```

time	限制时间的长短，以秒为单位，范围是 11 到 18000
------	------------------------------

## 命令模式

全局配置模式

## 默认

60 秒

## 使用说明

无

## 举例说明

设置当 DR 接受到 Stop 报文后停止发送注册报文的时间间隔为 100 秒。

```
Switch(config)# ip pim register-suppression 100
```

## 相关命令

ip pim register-rate-limit

ip pim register-rp-reachability

ip pim register-source

## 5.4.15 ip pim rp-address

使用此命令为设置静态 RP 地址，使用关键字 no 删除 RP。

## 命令语法

```
ip pim rp-address address ( list | override | )
```

```
no ip pim rp-address address ( list | )
```

address	RP 地址
list	访问控制列表
override	覆盖动态学习的 RP 的映射

## 命令模式

全局配置模式

**默认**

无

**使用说明**

无

**举例说明**

设置 RP 地址为 1.1.1.1。

```
Switch(config)# ip pim rp-address 1.1.1.1
```

**相关命令**

```
ip pim rp-candidate
```

```
ip pim rp-register-kat
```

**5.4.16 ip pim rp-candidate**

使用此命令设置本交换机作为候选的 RP，使用关键字 **no** 取消此设置。

**命令语法**

```
ip pim rp-candidate IFNAME ({priority priority |interval interval |group-list list}|)
```

```
no ip pim rp-candidate (IFNAME |)
```

<i>IFNAME</i>	此端口的 IP 地址会作为候选的 RP 在网络上被广播
<i>priority priority</i>	候选 RP 的优先权，范围是 0 到 255
<i>interval interval</i>	发送宣告报文的时间间隔，单位是秒，范围是 1 到 16383
<i>group-list list</i>	访问控制列表限制可注册到此 RP 的组播组

**命令模式**

全局配置模式

**默认**

无

**使用说明**

无

## 举例说明

设置本交换机的 eth-0-1 端口的 IP 地址为候选的 RP 地址。

```
Switch(config)# ip pim rp-candidate eth-0-1
```

## 相关命令

```
ip pim rp-address
```

### 5.4.17 ip pim rp-register-kat

使用此命令设置 DR 发往 RP 的 PIM 注册报文的存活时间。使用关键字 **no** 恢复此存活时间为默认值。

## 命令语法

```
ip pim rp-register-kat time
```

```
no ip pim rp-register-kat
```

time	DR 发往 RP 的 PIM 注册报文的存活时间，以秒为单位，范围是 1 到 65535
------	--

## 命令模式

全局配置模式

## 默认

185 秒

## 使用说明

DR 发往 RP 的 PIM 注册报文在 RP 上会生成一个(S,G)条目，此条目会在 RP 上存在一段时间，超过此时间后，交换机会删除相应条目；此命令可以设置当 RP 发送 Stop 报文后该条目在 RP 上存活的时间。

## 举例说明

设置 DR 发往 RP 的 PIM 注册报文的存活时间为 100 秒。

```
Switch(config)# ip pim rp-register-kat 100
```

## 相关命令

```
ip pim rp-address
```

```
ip pim rp-candidate
```



## 5.4.18 ip pim spt-switch-threshold infinity

使用此功能设置永远都不切换到最短路径树，使用关键字 `no` 取消此项设置。

### 命令语法

```
ip pim spt-switch-threshold infinity (group-list list|)
```

```
no ip pim spt-switch-threshold infinity (group-list list|)
```

<code>group-list list</code>	组播组地址范围
------------------------------	---------

### 命令模式

全局配置模式

### 默认

默认 DR 收到第一个组播流后立即切换为最短路径树。

### 使用说明

无

### 举例说明

设置永远都不切换到最短路径树。

```
Switch(config)# ip pim spt-switch-threshold infinity
```

### 相关命令

```
show ip pim sparse-mode spt-threshold
```

## 5.4.19 ip pim cisco-register-checksum

使用此功能设置 DR 发送注册报文时使用 CISCO Register Checksum，使用关键字 `no` 取消此项设置。

### 命令语法

```
ip pim cisco-register-checksum (group-list list|)
```

```
no ip pim cisco-register-checksum (group-list list|)
```

<code>group-list list</code>	组播组地址范围
------------------------------	---------

## 命令模式

全局配置模式

## 默认

无

## 使用说明

默认是 RFC 规定的 register checksum，如果配置了访问控制列表，只有通过验证的报文才能以 CISCO Register Checksum 的方式发送。

## 举例说明

设置 DR 发送注册报文时使用 CISCO Register Checksum。

```
Switch(config)# ip pim cisco-register-checksum
```

## 相关命令

无

### 5.4.20 ip pim sparse-mode

使用此命令在此端口启用 PIM-SM 协议，使用关键字 no 在此端口关闭 PIM-SM 协议。

## 命令语法

```
ip pim sparse-mode (passive|)
```

```
no ip pim sparse-mode (passive|)
```

passive	被动模式
---------	------

## 命令模式

端口配置模式

## 默认

不使能

## 使用说明

默认情况下，端口没有启用 PIM-SM 协议；工作在被动模式的端口不会发送 PIM Hello 报文。

## 举例说明

在此端口启用 PIM 协议。

```
Switch(config-if)# ip pim sparse-mode
```

## 相关命令

无

### 5.4.21 ip pim dense-mode

使用此命令在此端口启用 PIM-DM 协议，使用关键字 no 在此端口关闭 PIM-DM 协议。

## 命令语法

```
ip pim dense-mode (passive|)
```

```
no ip pim dense-mode (passive|)
```

passive	被动模式
---------	------

## 命令模式

端口配置模式

## 默认

不使能

## 使用说明

PIM-DM 和 PIM-SM 模式在同一个端口上是互斥的，默认情况下，端口没有启用 PIM-DM 协议；工作在被动模式的端口不会发送 PIM Hello 报文。

## 举例说明

在此端口启用 PIM DM 协议。

```
Switch(config-if)# ip pim dense-mode
```

## 相关命令

无

### 5.4.22 ip pim hello-holdtime

配置pim dense模式下hello-holdtime，即在多长时间没有收到hello报文就认为邻居失效。

## 命令语法

**(ip) pim hello-holdtime <1-65535>**

**no (ip) pim hello-holdtime**

## 命令模式

端口配置模式

## 默认

3.5\*30

## 使用说明

默认情况下，hello-holdtime 是 3.5 倍的 hello-interval 时间。如果配置的 hello-holdtime 小于当前 hello-interval，则配置错误。

Hello-holdtime 会随着 hello-interval 的改变而改变，当 hello-holdtime 没有配置或者配置的 holdtime 小于当前 hello-interval 时候。

## 举例说明

设置端口未收到 Hello 报文的保持时间。

```
Switch(config-if)# ip pim hello-holdtime 123
```

## 相关命令

ip pim hello-interval <1-65535>

### 5.4.23 ip pim propagation-delay

使用此命令PIM-DM的端口的传播延时，使用关键字no取消配置。

## 命令语法

**ip pim propagation-delay *timer***

**no ip pim propagation-delay**

<i>timer</i>	传播延时，范围 100-5000 毫秒
--------------	---------------------

## 命令模式

端口配置模式

## 默认

500 毫秒

## 使用说明

当一个网络上所有的路由器都支持剪枝延迟选项时，PIM-DM 路由器将用接收到的所有的传播延时来修正加入和剪枝的覆盖间隔。

## 举例说明

在此端口配置传播延时。

```
Switch(config-if)# ip pim propagation-delay 400
```

在此端口取消传播延时。

```
Switch(config-if)# no ip pim propagation-delay
```

## 相关命令

无

### 5.4.24 ip pim state-refresh origination-interval

使用此命令PIM-DM源端路由器发送SR消息的间隔时间，使用关键字no取消配置。

## 命令语法

```
ip pim state-refresh origination-interval interval
```

```
no ip pim state-refresh origination-interval
```

<i>interval</i>	SR 消息的间隔，范围 1-100 秒
-----------------	---------------------

## 命令模式

端口配置模式

## 默认

60 秒

## 使用说明

PIM 的 SR 消息是由与组播源直接相连的路由器发送的，此命令可以控制 SR 消息的发送间隔。

## 举例说明

在此端口配置 SR 的消息间隔。

```
Switch(config-if)# ip pim state-refresh origination-interval 50
```

在此端口取消 SR 的消息间隔配置。

```
Switch(config-if)# no ip pim state-refresh origination-interval
```

## 相关命令

无

### 5.4.25 ip pim unicast-bsm

默认情况下，端口会向整个 PIM 域发送 BSM 报文；此命令可以限制交换机只向它的邻居发送 BSM 报文。使用关键字 no 恢复此项设置为默认值。

## 命令语法

```
ip pim unicast-bsm
```

```
no ip pim unicast-bsm
```

## 命令模式

端口配置模式

## 默认

不使能

## 使用说明

每个端口只能创建一条统计。

## 举例说明

设置端口向它的邻居发送单播的 BSM 报文。

```
Switch(config-if)# ip pim unicast-bsm
```

## 相关命令

无

### 5.4.26 ip pim ssm

使用这个命令来使能 PIM-SSM 和指定 SSM 组范围。默认范围是 232.0.0.0~232.255.255.255。使用关键字 no 来关闭 PIM-SSM。

## 命令语法

```
ip pim ssm [default | range list]
```

```
no ip pim ssm
```

default	使用默认的 SSM 组播组范围
range <i>list</i>	使用访问控制列表中的组播组范围作为 SSM 组播组范围

## 命令模式

全局配置模式

## 默认

不使能

## 使用说明

无

## 举例说明

下面的例子用来演示使能 PIM-SSM,并将 SSM 组范围设置为默认范围。

```
Switch(config-if)# ip pim ssm default
```

## 相关命令

无

### 5.4.27 show ip pim sparse-mode bsr-router

使用此命令查看自举路由器信息。

## 命令语法

```
show ip pim sparse-mode bsr-router
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

查看自举路由器信息。

```
Switch# show ip pim sparse-mode bsr-router
PIMv2 bootstrap information
This system is the bootstrap router (BSR)
  BSR address: 12.0.9.2
  Uptime:      00:00:08, BSR Priority: 64, Hash mask length: 10
  Next bootstrap message in 00:00:04
  Role: Candidate BSR
  State: Elected BSR
  Candidate RP: 12.0.9.2(eth-0-9)
    Advertisement interval 60 seconds
    Next C-RP advertisement in 00:00:57
```

## 相关命令

无

### 5.4.28 show ip pim sparse-mode interface

使用此命令查看稀疏模式下的端口信息。

## 命令语法

```
show ip pim sparse-mode interface [detail]
```

detail	查看详细信息
--------	--------

## 命令模式

特权模式



## 默认

无

## 使用说明

无

## 举例说明

查看稀疏模式下的端口信息。

```
Switch# show ip pim sparse-mode interface detail
eth-0-9 (vif 0):
  Address 12.0.9.1, DR 12.0.9.2
  Hello period 30 seconds, Next Hello in 26 seconds
  Triggered Hello period 5 seconds
  Neighbors:
    12.0.9.2
```

## 相关命令

无

### 5.4.29 show ip pim sparse-mode local-member

使用此命令查看稀疏模式下的本地成员信息。

## 命令语法

```
show ip pim sparse-mode local-member (IFNAME | )
```

IFNAME	端口名称
--------	------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

查看稀疏模式下的本地成员信息。

```
Switch# show ip pim sparse-mode local-members
PIM local membership information
eth-0-3:
  (*, 229.1.1.1) : Include
eth-0-9:
  (*, 228.1.1.1) : Include
```

## 相关命令

无

### 5.4.30 show ip pim sparse-mode mroute

使用此命令查看 SM 模式下的多播路由。

## 命令语法

**show ip pim sparse-mode mroute** (*source\_address* | *group\_address* |) (**detail** |)

source_address	多播路由源地址
group_address	多播路由目的地址
detail	详细信息

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

查看稀疏模式下的多播路由。

```
Switch# show ip pim sparse-mode mroute detail
IP Multicast Routing Table
(*,*,RP) Entries: 0
(*,G) Entries: 2
```

```

(S,G) Entries: 0
(S,G,rpt) Entries: 0
FCR Entries: 0
(*, 228.1.1.1) Uptime: 00:09:55
  RP: 0.0.0.0, RPF nbr: None, RPF idx: None
  Upstream:
    State: NOT JOINED, SPT Switch: Enabled, JT: off
  Downstream:
    eth-0-9:
      State: NO INFO, ET: off, PPT: off
      Assert State: NO INFO, AT: off
      Winner: 0.0.0.0, Metric: 4294967295, Pref: 4294967295, RPT bit: on
  Local Olist:
    eth-0-9
(*, 229.1.1.1) Uptime: 00:04:22
  RP: 12.0.9.2, RPF nbr: 12.0.9.2, RPF idx: eth-0-9
  Upstream:
    State: JOINED, SPT Switch: Enabled, JT Expiry: 40 secs
    Macro state: Join Desired,
  Downstream:
    eth-0-3:
      State: NO INFO, ET: off, PPT: off
      Assert State: NO INFO, AT: off
      Winner: 0.0.0.0, Metric: 4294967295, Pref: 4294967295, RPT bit: on
      Macro state: Could Assert, Assert Track
  Local Olist:
    eth-0-3

```

## 相关命令

无

### 5.4.31 show ip pim sparse-mode neighbor

使用此命令查看稀疏模式下的邻居信息。

## 命令语法

```
show ip pim sparse-mode neighbor ((IFNAME (address | )) | detail | )
```

IFNAME	端口名称
address	邻居地址
detail	详细信息

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

查看稀疏模式下的邻居信息

```
Switch# show ip pim sparse-mode neighbor
Neighbor          Interface          Uptime/Expires    Ver  DR
Address
12.0.9.2          eth-0-9            00:18:18 /00:01:20 v2   1 / DR
```

## 相关命令

无

## 5.4.32 show ip pim sparse-mode rp mapping

使用此命令查看多播组与 RP 的对应关系。

## 命令语法

```
show ip pim sparse-mode rp mapping
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

查看多播组与 RP 的对应关系。

```
Switch# show ip pim sparse-mode rp mapping
PIM group-to-RP mappings
Group(s): 224.0.0.0/4
  RP: 12.0.9.2
    Info source: 12.0.9.2, via bootstrap, priority 192
    Uptime: 00:22:56, expires: 00:01:34
```

## 相关命令

无

### 5.4.33 show ip pim sparse-mode rp-hash

使用此命令查看指定多播组的 RP 信息。

## 命令语法

```
show ip pim sparse-mode rp-hash group_address
```

group_address	组播组地址
---------------	-------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

查看多播组 224.0.0.10 的 RP。

```
Switch# show ip pim sparse-mode rp-hash 224.0.0.10
RP: 12.0.9.2
Info source: 12.0.9.2, via bootstrap
```

## 相关命令

无

### 5.4.34 show ip pim sparse-mode spt-threshold

使用此命令查看从共享树切换为最短路径树的阈值。

## 命令语法

```
show ip pim sparse-mode spt-threshold
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

查看从共享树切换为最短路径树的阈值。

```
Switch# show ip pim sparse-mode spt-threshold
PIM sparse-mode immediately switches over to SPT upon receiving the first traffic
```

## 相关命令

无

## 5.4.35 show ip pim dense-mode interface

使用此命令查看从 PIM-DM 的接口信息。

## 命令语法

```
show ip pim dense-mode interface (detail | )
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

查看 PIM-DM 的接口信息。

```
Switch# show ip pim dense-mode interface
Address          Interface VIFIndex Ver/   Nbr
                  Mode     Count
2.2.2.1          eth-0-2   0       v2/D   0
3.3.3.1          eth-0-3   2       v2/D   0
```

## 相关命令

无

### 5.4.36 show ip pim dense-mode mroute

使用此命令查看从 PIM-DM 的组播路由表。

## 命令语法

```
show ip pim dense-mode mroute
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

查看 PIM-DM 的组播路由表。

```
Switch# show ip pim dense-mode mroute
PIM-DM Multicast Routing Table
(2.2.2.2, 225.1.2.3)
  Source directly connected on eth-0-2
  State-Refresh Originator State: Originator
  Upstream IF: eth-0-2
  Upstream State: Forwarding
  Assert State: NoInfo
  Downstream IF List:
  eth-0-3, in 'olist':
    Downstream State: NoInfo
    Assert State: NoInfo
(2.2.2.2, 225.1.2.4)
  Source directly connected on eth-0-2
  State-Refresh Originator State: Originator
  Upstream IF: eth-0-2
  Upstream State: Forwarding
  Assert State: NoInfo
  Downstream IF List:
  eth-0-3, in 'olist':
    Downstream State: NoInfo
    Assert State: NoInfo
```

## 相关命令

无

### 5.4.37 show ip pim dense-mode neighbor

使用此命令查看从 PIM-DM 的邻居。

## 命令语法

```
show ip pim sparse-mode neighbor (detail | )
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

查看 PIM-DM 的邻居。

```
Switch# show ip pim dense-mode neighbor
Neighbor-Address Interface      Uptime/Expires    Ver
4.4.4.4           eth-0-9            03d19h16m/00:01:29 v2
3.3.3.2           agg3               03d19h17m/00:01:37 v2
```

## 相关命令

无

### 5.4.38 show ip pim dense-mode nexthop

使用此命令查看从 PIM-DM 的下一跳信息。

## 命令语法

```
show ip pim sparse-mode nexthop
```

## 命令模式

特权模式



## 默认

无

## 使用说明

无

## 举例说明

查看 PIM-DM 的下一跳信息。

```
Switch# show ip pim dense-mode nexthop
Destination      Nexthop  Nexthop      Nexthop      Metric Pref
                  Num      Addr          Interface
1.1.1.2          0        -            -            -      -
```

## 相关命令

### 5.4.39 ip pim virtual address enable

使用此命令配置 ip pim，bsr 报文中地址是取联动的 vrrp 上虚地址

## 命令语法

```
ip pim virtual address enable
no ip pim virtual address enable
```

## 命令模式

配置模式

## 默认

不使能

## 使用说明

当使能 ip pim 支持 vrrp 的虚地址，需要手动去 disable 和 enable 对应的 vrrp

## 举例说明

配置 ip pim 支持 vrrp 的虚地址

```
DUT1(config)# ip pim virtual address enable
```

## 相关命令

```
no ip pim virtual address enable
show ip pim virtual-address enable
```

## 5.5 MVR 命令

### 5.5.1 mvr

此命令用来使能和去使能 MVR。

#### 命令语法

```
mvr
no mvr
```

#### 命令模式

全局配置模式

#### 默认

不使能

#### 使用说明

在交换机上使能 MVR，在使能 MVR 前，组播路由功能需要关闭。

#### 举例说明

在交换机上使能 MVR。

```
Switch(config)# no ip multicast-routing
Switch(config)# mvr
```

#### 相关命令

无

### 5.5.2 mvr vlan

此命令用来指定 MVR 的源 VLAN。

#### 命令语法

```
mvr vlan vlan vlan_id
no mvr vlan
```

vlan_id	VLAN id, 范围是 1 到 4094
---------	-----------------------

## 命令模式

全局配置模式

## 默认

无

## 使用说明

在指定 MVR 的源 VLAN 前，该 VLAN 的 `vlan interface` 需要先创建起来。

## 举例说明

下面的例子用来说明如何配置 MVR 的源 VLAN。

```
Switch(config)# vlan database
Switch (config-vlan)# vlan 2
Switch (config)# interface vlan 2
Switch (config-if)# exit
Switch(config)# mvr vlan 2
```

## 相关命令

无

### 5.5.3 mvr group

此命令用来设置 MVR 全局 group。

## 命令语法

**mvr group** address (count | )

**no mvr group** address (count | )

address	组播组地址
count	要配置的组播组数目，范围是 1~64

## 命令模式

全局配置模式

## 默认

无

## 使用说明

此命令用来设置 MVR 全局 group。

## 举例说明

下面例子显示如何在端口上创建一条统计

下面的例子说明如何来创建 50 个静态 group, 范围是 238.255.0.1~238.255.0.50。

```
Switch(config)# mvr group 238.255.0.1 50
```

## 相关命令

无

### 5.5.4 mvr source-address

此命令用来设置或删除 MVR 源地址。

## 命令语法

```
mvr source-address address
```

```
no mvr source-address
```

address	MVR 上报组播报文的源地址
---------	----------------

## 命令模式

全局配置模式

## 默认

10.0.0.1

## 使用说明

无

## 举例说明

设置 MVR 源地址为 192.168.11.1

```
Switch(config)# mvr source-address 192.168.11.1
```

## 相关命令

无

## 5.5.5 mvr type

此命令用来设置交换机端口作为 MVR 的源端口或者接收端口。

### 命令语法

```
mvr type (source | receiver vlan vlan_id)
```

```
no mvr type (receiver vlan vlan_id |)
```

source	MVR 源端口
receiver	MVR 接收端口
vlan <i>vlan_id</i>	VLAN id, 范围是 1 到 4094

### 命令模式

端口配置模式

### 默认

无

### 使用说明

在配置某个端口作为 MVR 的源端口或接收端口时，源端口必须在 MVR 源 VLAN 中，接收端口必须不在 MVR 的源 VLAN 中。

### 举例说明

下面的例子将 eth-0-1 配置成 MVR 的源端口，eth-0-2 配置成 VLAN2 中的接收端口。

```
Switch(config)# interface eth-0-1
Switch(config-if)# mvr type source
Switch(config)# interface eth-0-2
Switch(config-if)# mvr type receiver vlan 2
```

### 相关命令

无

## 5.5.6 show mvr

此命令用来显示 MVR 相关的信息。

### 命令语法

```
show mvr
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子显示 MVR 相关的信息。

```
Switch# show mvr
MVR Running: TRUE
MVR Multicast VLAN: 10
MVR Source-address: 1.1.1.1
MVR Max Multicast Groups: 512
MVR Hw Rt Limit: 511
MVR Current Multicast Groups: 0
```

## 相关命令

无

## 5.5.7 show mvr interface

此命令用来显示 MVR 端口相关的信息。

## 命令语法

```
show mvr interface
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子显示 MVR 端口相关的信息。

```
Switch# show mvr interface
Port      Type      VLAN   Status
eth-0-2   source    10     ACTIVE
eth-0-1   receiver  11     ACTIVE
```

## 相关命令

无

### 5.5.8 show mvr group

此命令用来显示从 MVR 接收端口上学习到组播组信息。

## 命令语法

```
show mvr group vlan vlan_id (group_address |)
```

<b>vlan</b> <i>vlan_id</i>	VLAN id, 范围是 1 到 4094
<i>group_address</i>	组播组地址

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子显示如何从 MVR 接收端口上学习到组播组信息。

```
Switch# show mvr groups
VLAN   Interface   Group-Address   Uptime   Expires-time
11     eth-0-1     227.0.0.1       00:25:51 00:04:19
```

## 相关命令

无

### 5.5.9 show mvr group static

此命令用来显示 MVR 全局配置的静态组播组信息。

## 命令语法

```
show mvr group static global
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子显示 MVR 全局配置的静态组播组信息。

```
Switch# show mvr groups static global
MVR Static Global Group:
227.0.0.1
227.0.0.2
227.0.0.3
227.0.0.4
227.0.0.5
227.0.0.6
227.0.0.7
227.0.0.8
227.0.0.9
227.0.0.10
```

## 相关命令

无

### 5.5.10 show resource mvr

此命令用于显示 MVR 的资源使用情况。

## 命令语法

```
show resource mvr
```

## 命令模式

特权模式

## 默认

无



## 使用说明

无

## 举例说明

下面例子显示 MVR 的资源使用情况。

```
Switch# show resource mvr
MVR
Resource                               Used           Capability
=====
MVR Entry                               0              511
MVR Member                              0              1022
```

## 相关命令

无

# 6 安全性命令行参考

## 6.1 端口安全命令

### 6.1.1 clear port-security address-table static

使用此命令清除静态的安全 MAC 地址。

#### 命令语法

**clear port-security address-table static** (**address** *address* | **interface** *interface* | **vlan** *VLAN* |)

<b>address</b> <i>address</i>	根据特定地址清除安全 MAC 地址
<b>interface</b> <i>interface</i>	根据端口清除安全 MAC 地址
<b>vlan</b> <i>vlan</i>	根据 vlan 清除安全 MAC 地址

#### 命令模式

特权模式

#### 默认

无

#### 使用说明

使用此命令清除静态的安全 MAC 地址。

#### 举例说明

以下例子展示如何清除全局的安全 MAC 地址表：

```
Switch# clear port-security address-table static
```

以下例子展示如何清除端口 eth-0-1 上的安全 MAC 地址表：

```
Switch# clear port-security address-table static interface eth-0-1
```

## 相关命令

**show mac address-table**

### 6.1.2 switchport port-security

使用该命令在端口上启用端口安全功能，使用 **no** 命令关闭端口安全功能。

## 命令语法

**switchport port-security**

**no switchport port-security**

## 命令模式

端口配置模式

## 默认

关闭

## 使用说明

当关闭端口安全功能时，所有动态学习的安全 MAC 地址将被清除。静态的 MAC 地址不会被清除但将被置成无效。

## 举例说明

以下示例展示如何在端口上启用端口安全：

```
Switch(config-if)# switchport port-security
```

以下示例展示如何在端口上关闭端口安全：

```
Switch(config-if)# no switchport port-security
```

## 相关命令

**show port-security interface**

### 6.1.3 switchport port-security mac-address

使用该命令添加静态的安全 MAC 地址。

## 命令语法

**switchport port-security mac-address address vlan VLAN**

**no switchport port-security mac-address address vlan VLAN**

address	MAC 地址
VLAN	MAC 地址所关联的 Vlan id

## 命令模式

端口配置模式

## 默认

无

## 使用说明

无

## 举例说明

以下示例展示如何添加静态安全地址：

```
Switch(config-if)# switchport port-security mac-address 0.0.1 vlan 1
```

以下示例展示如何删除静态安全地址：

```
Switch(config-if)# no switchport port-security mac-address 0.0.1 vlan 1
```

## 相关命令

**show mac address-table**

### 6.1.4 switchport port-security maximum

使用该命令配置端口上允许的安全 MAC 地址的最大值，使用 no 命令将该最大值恢复成默认值。

## 命令语法

**switchport port-security maximum** *maximum*

**no switchport port-security maximum**

maximum	端口上允许的最大安全 MAC 的条数，取值范围是 0 到 16384
---------	------------------------------------

## 命令模式

端口配置模式

## 默认

默认值是 1

## 使用说明

如果新配置的最大值小于已存在的安全 MAC 的条数，则不允许修改。

如果端口上的安全 MAC 地址达到最大值，不会有更多的 MAC 地址在端口上学到。

为了保证端口的动态学习 MAC 地址安全，允许端口上的安全 MAC 地址的最大值设置为 0，这样端口就不会学习 MAC 地址，只能允许静态配置安全 MAC 地址。

## 举例说明

以下用例展示如何配置端口上允许的安全 MAC 地址的最大值：

```
Switch(config-if)# switchport port-security maximum 1024
```

以下用例展示如何将最大值改回默认值：

```
Switch(config-if)# no switchport port-security maximum
```

## 相关命令

**switchport port-security violation**

**show port-security maximum mac-num interface *IFNAME***

### 6.1.5 switchport port-security violation

使用该命令配置当违反安全时系统处理行为，使用 no 命令恢复默认值。

## 命令语法

**switchport port-security violation (protect | restrict | errdisable)**

**no switchport port-security violation**

protect	丢弃报文
restrict	丢弃报文且打印日志
errdisable	丢弃报文，打印日志且将端口设成 error-disabled

## 命令模式

端口配置模式

## 默认

丢弃报文

## 使用说明

使用该命令前，先在端口上启用端口安全。

## 举例说明

以下示例展示如何配置当违反端口安全时丢弃报文：

```
Switch(config-if)# switch port-security violation protect
```

## 相关命令

**switchport port-security**

### 6.1.6 switchport port-security sticky

使用该命令配置当端口学习到安全 MAC 地址时自动转变为静态 MAC 地址。

使用 **no** 命令恢复默认值。

## 命令语法

**switchport port-security sticky**

**no switchport port-security sticky**

## 命令模式

端口配置模式

## 默认

关闭

## 使用说明

使用该命令前，应先在端口上启用端口安全功能。

## 举例说明

配置端口开启 sticky 功能：

```
Switch(config-if)# switchport port-security sticky
```

### 6.1.7 switchport port-security sticky mac-address

使用该命令添加静态的安全 MAC 地址。

使用 **no** 命令取消该配置。

## 命令语法

**switchport port-security sticky mac-address** *address* **vlan** *vlan-id*

**no switchport port-security sticky mac-address** *address* **vlan** *vlan-id*

address	MAC 地址
vlan-id	MAC 地址所关联的 VLAN ID

## 命令模式

端口配置模式

## 默认

无

## 使用说明

使用该命令前，先在端口上启用 **port-security sticky** 功能。

## 举例说明

添加一条静态安全 MAC 地址：

```
Switch(config-if)# switchport port-security sticky mac-address 1.0.0.1 vlan 1
```

删除配置的静态安全 MAC 地址：

```
Switch(config-if)# no switchport port-security sticky mac-address 1.0.0.1 vlan 1
```

## 6.1.8 show port-security address-table

使用该命令显示安全 MAC 地址。

## 命令语法

**show port-security address-table** (**dynamic** | **static** |) (**address** *address* | **interface** *interface* | **vlan** *VLAN* |)

<b>dynamic</b>	显示动态学习的安全 MAC 地址条目
<b>static</b>	显示静态配置的安全 MAC 地址条目
<b>address</b> <i>address</i>	显示特定 MAC 地址的条目
<b>interface</b> <i>interface</i>	显示特定端口上的安全 MAC 地址条目
<b>vlan</b> <i>vlan</i>	显示特定 vlan 上的安全 MAC 地址条目

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

以下用例展示如何显示所有安全 MAC 地址条目：

```
Switch# show port-security address-table
          Secure Mac Address Table
-----
Vlan      Mac Address                Type                Ports
-----
1         0001.00ce.ef01            SecureConfigured    eth-0-11
41        001a.a02c.a1dc            SecureConfigured    eth-0-41
```

## 相关命令

无

### 6.1.9 show port-security current mac-num interface

使用该命令显示端口上现有的安全 MAC 地址条数。

## 命令语法

**show port-security current mac-num interface** *interface*

<b>interface</b>	显示特定端口上的安全 MAC 地址条目的数量
------------------	------------------------

## 命令模式

特权模式

## 默认

无



## 使用说明

无

## 举例说明

以下用例展示端口 eth-0-1 上现有的安全 MAC 地址条数：

```
Switch# show port-security current mac-num interface eth-0-1
Current dynamic MAC addresses : 0
Current static MAC addresses  : 0
Current total MAC addresses   : 0
```

## 相关命令

**switchport port-security maximum**

**show port-security maximum mac-num interface *interface***

### 6.1.10 show port-security interface

使用该命令显示指定端口上的端口安全相关信息。

## 命令语法

**show port-security interface *interface***

interface	显示特定端口上的端口安全信息
-----------	----------------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

以下用例展示如何显示端口上的端口安全相关信息：

```
Switch# show port-security interface eth-0-1
Port Security           : disabled
Violation mode          : discard packet silence
Maximum MAC Addresses   : 1
```

```
Total MAC Addresses          : 1
Static configured MAC Addresses : 1
```

## 相关命令

无

### 6.1.11 show port-security maximum mac-num interface

使用该命令显示端口上允许配置的安全 MAC 地址的最大值。

## 命令语法

```
show port-security maximum mac-num interface interface
```

interface	显示特定端口上允许配置的最大安全 MAC 地址
-----------	-------------------------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

以下用例显示了端口 eth-0-1 上允许的安全 MAC 地址的最大值：

```
Switch# show port-security maximum mac-num interface eth-0-1
Maximum dynamic MAC addresses : 1
```

## 相关命令

```
switchport port-security maximum
```

```
show port-security current mac-num interface
```

## 6.2 VLAN 安全命令

### 6.2.1 vlan mac-limit maximum

使用此命令配置指定 vlan 内最大的 fdb 的数目。使用此命令的 no 命令取消限制。

#### 命令格式

**vlan** *VLAN-id* **mac-limit maximum** *maximum*

**no vlan** *VLAN-id* **mac-limit maximum**

VLAN-id	配置的 vlan id, 范围 1 到 4094
maximum	最大数目, 范围 1 到 65535

#### 命令模式

Vlan 配置模式

#### 默认值

所有 vlan 内 fdb 数目不受限。

#### 使用说明

限制 fdb 的 vlan 必须先创建。如果不使用此命令配置 fdb 限制, vlan 内的 fdb 数目不受限。

#### 举例说明

使用此命令配置指定 vlan 的最大 fdb 的数目:

```
Switch# configure terminal
Switch(config)# vlan database
Switch(config-vlan)# vlan 2
Switch(config-vlan)# vlan 2 mac-limit maximum 1000
Switch(config-vlan)# no vlan 2 mac-limit maximum
```

#### 相关命令

**show vlan-security**

### 6.2.2 vlan mac-limit action

使用此命令配置 vlan 内 fdb 数目达到限制时的行为。使用此命令的 no 形式恢复默认值。

## 命令格式

**vlan *VLAN-id* mac-limit action (discard|warn|forward)**

**no vlan *VLAN-id* mac-limit action**

VLAN-id	配置的 vlan id, 范围 1 到 4094
discard	当 vlan 内 fdb 数目达到限制时, 进入此 vlan 的未知源 mac 的报文将会被丢弃, 并且不会进行 fdb 学习
warn	当 vlan 内 fdb 数目达到限制时, 进入此 vlan 的未知源 mac 的报文将会被丢弃, 不会进行 fdb 学习, 而且在 syslog 中打印信息
forward	当 vlan 内 fdb 数目达到限制时, 进入此 vlan 的未知源 mac 的报文将会进行转发, 并且不会进行 fdb 学习

## 命令模式

Vlan 配置模式

## 默认值

默认行为是 forward

## 使用说明

Vlan 必须先创建

## 举例说明

如下例子显示了如何配置 vlan 内 fdb 达到数目限制时的行为:

```
Switch# configure terminal
Switch(config)# vlan database
Switch(config-vlan)# vlan 2
Switch(config-vlan)# vlan 2 mac-limit action warn
```

## 相关命令

**show vlan-security**

### 6.2.3 vlan mac learning

使能此命令使能 vlan 内 fdb 的学习功能。是用此命令的 no 形式关闭 vlan 内 fdb 的学习功能。

## 命令格式

**vlan *VLAN-id* mac learning (enable|disable)**

VLAN-id	配置的 Vlan id, 范围 1 到 4094
---------	--------------------------

## 命令模式

Vlan 配置模式

## 使用说明

Vlan 必须先创建

## 默认值

所有 vlan 的 mac learning 默认使能

## 举例说明

如下例子显示了如何关闭 vlan 内 fdb 的学习功能。

```
Switch# configure terminal
Switch(config)# vlan database
Switch(config-vlan)# vlan 2
Switch(config-vlan)# no vlan 2 mac learning enable
```

## 相关命令

**show vlan-security**

### 6.2.4 show vlan-security

使用此命令查看 vlan 安全的配置。

## 命令格式

**show vlan-security (vlan *vlan-id* )**

<b>vlan <i>vlan-id</i></b>	配置的 vlan id, 范围 1 到 4094
----------------------------	--------------------------

## 命令模式

### 特权模式默认

无

### 无使用说明

使用此命令可以查看所有 vlan 的 mac learning 状态、当前和最大的 fdb 数目、达到最大数目是的行为等信息。

### 举例说明

下面例子显示了如何查看 vlan 安全的信息。

```
Switch# configure terminal
Switch(config)# vlan database
Switch(config-vlan)# vlan 2
Switch(config-vlan)# vlan 2 mac-limit maximum 1000
Switch(config-vlan)# vlan 2 mac-limit action warn
Switch # show vlan-security
Vlan learning-en max-mac-count cur-mac-count action
-----
-
2 Enable 1000 0 Warn
```

### 相关命令

**vlan mac-limit maximum**

**vlan mac-limit action**

**vlan mac learnng**

## 6.3 Time Range 命令

### 6.3.1 time-range

使用此命令定义时间段。

### 命令语法

**time-rang** *TIME-RANGE-NAME*

**no time-rang**

TIME-RANGE-NAME	定义的名字不超过 40 个字符
-----------------	-----------------

## 命令模式

全局配置模式

## 默认

无

## 使用说明

时间范围是用于确定一个时间范围，在此期间内规则是有效的。

## 举例说明

定义名字为 `my-time-range` 的时间段规则。

```
Switch(config)# time-range my-time-range
Switch(config-tm-range)#
```

## 相关命令

**show time-range**

### 6.3.2 absolute

使用此命令定义绝对时间段。

## 命令语法

**absolute (start *HH:MM:SS MONTH <1-31> <2000-2037>*) (end *HH:MM:SS MONTH <1-31> <2000-2037>*)**

start	定义开始的时间
end	定义结束的时间
HH:MM:SS	定义开始的小时,分钟,秒
<i>MONTH &lt;1-31&gt;</i>	定义开始的月份
<i>&lt;2000-2037&gt;</i>	定义开始的年份

## 命令模式

时间段配置模式

## 默认

无

## 使用说明

配置绝对时间范围。

## 举例说明

定义开始时刻为 2008 年 1 月 1 日 11 时 11 分 0 秒，结束时刻为 2009 年 5 月 1 日 0 时 0 分 0 秒的时间段。

```
Switch(config-tm-range)# absolute start 11:11:00 jun 1 2008 end 00:00:00 may 1 2009
```

## 相关命令

**periodic**

### 6.3.3 periodic

定义周期时间段。

## 命令语法

**periodic** *HH:MM WEEKDAY to HH:MM (WEEKDAY )*

**periodic** *HH:MM ( weekdays | weekend | daily ) to HH:MM*

HH:MM	定义小时分钟
WEEKDAY	定义每周的第几天
weekdays	定义一周的周一至周五
weekend	定义周末,周六,周日
daily	定义一周的每一天

## 命令模式

时间段配置模式

## 默认

无

## 使用说明

与绝对时间比较，选择一个合适的类型。

## 举例说明

定义开始时间为周一的 10 时 10 分，结束时间为周三的 11 时 10 分的时间段。



```
Switch(config-tm-range)# periodic 00:00 mon to 18:00 wed
```

定义开始时间为每天的 09 时 00 分，结束时间为每天的 17 时 00 分的时间段。

```
Switch(config-tm-range)# periodic 09:00 daily to 17:00
```

## 相关命令

**absolute**

### 6.3.4 show time-range

使用此命令查看时间访问控制列表。

## 命令语法

**show time-range** (*TIME-RANGE-NAME* [ ])

TIME-RANGE-NAME	时间访问控制列表名称；如果指定了此项，则查看此列表的表项；否则查看所有列表
-----------------	---------------------------------------

## 命令模式

特权模式

## 默认

无

## 使用说明

如果 ACL 没有在端口上被引用,那么不会生效。

## 举例说明

查看所有时间访问控制列表。

```
Switch# show time-range
time-range range1
periodic 00:01 weekdays to 12:01
```

## 相关命令

**time-range**

## 6.4 ACL 命令

### 6.4.1 mac access-list

此命令创建 MAC 访问控制列表并进入访问控制列表配置模式。

使用关键字 **no** 删除指定的 MAC 访问控制列表。

#### 命令语法

**mac access-list** *ACL-NAME*

**no mac access-list** *ACL-NAME*

ACL-NAME	MAC 访问控制列表名称，不超过 40 个字符
----------	-------------------------

#### 命令模式

全局配置模式

#### 默认

无

#### 使用说明

如果访问控制列表名称为一个已经存在的名称，则此命令表示进入 MAC 访问控制列表配置模式；如果访问控制列表名称为新名称，则此命令表示创建此列表并进入 MAC 访问控制列表配置模式；此处创建的访问控制列表配合 **match access-group** 命令使用，具体见相关章节。

#### 举例说明

创建一个名为 `list_mac_1` 的 MAC 访问控制列表并进入配置模式：

```
Switch(config)# mac access-list list_mac_1
Switch(config-mac-acl)#
```

删除一个名为 `list_mac_1` 的 MAC 访问控制列表：

```
Switch(config)# no mac access-list list_mac_1
```

#### 相关命令

**match access-group**

### 6.4.2 sequence-num

使用此命令删除指定的控制规则。

## 命令语法

**no sequence-num** *SEQUENCE-NUM*

SEQUENCE-NUM	序号范围 1~131071
--------------	---------------

## 命令模式

MAC ACL 模式或 IP ACL 模式

## 默认

无

## 使用说明

如果 ACL 所在的 class-map、class-map 所在的 policy-map 已经应用到端口，删除动作立即生效。

## 举例说明

MAC ACL 模式下删除序号为 10 的规则：

```
Switch(config-mac-acl)# no sequence-num 10
```

IP ACL 模式下删除序号为 10 的规则：

```
Switch(config-ip-acl)# no sequence-num 10
```

## 相关命令

**deny**

**deny tcp**

**deny udp**

**deny icmp**

**deny igmp**

**permit**

**permit tcp**

**permit udp**

**permit icmp**

**permit igmp**

### 6.4.3 deny src-mac

使用此命令在 MAC 访问控制列表中添加访问控制规则；此规则拒绝指定源 MAC 地址的报文通过。

#### 命令语法

```
(SEQUENCE-NUM |) deny src-mac (any | MAC MASK | host MAC) ( dest-mac (any | MAC MASK | host MAC) |)(untag-vlan | ( vlan VLAN |) ( cos VALUE |) ( inner-vlan VLAN |) ( inner-cos VALUE |)) ( protocol (arp (arp-op-code) | rarp) | packet-length OPERATOR LENGTH) ( time-range TIME-RANGE-NAME |)
```

SEQUENCE-NUM	此规则在 MAC 访问控制列表中的顺序；如果没有指定此项，则系统会自动给此规则分配顺序号。范围是 1~131071
any	任何主机
MAC MASK	某一类主机
host MAC	某一台主机
dest-mac	目的 MAC 地址
untag-vlan	没有 vlan tag
vlan VLAN	VLAN-ID，范围是 1~4094
cos VALUE	CoS，范围是 0~7
inner-vlan VLAN	内层 VLAN-ID，范围是 1~4094
inner-cos VALUE	内层 CoS，范围是 0~7
protocol	指定 ARP、RARP 或者是指定的 Ether type
arp	ARP 协议
arp-op-code	arp-op-code,范围是 0~65535
rarp	RARP 协议
time-range TIME-RANGE-NAME	应用此选项可以产生基于时间的访问控制列表，详见相关章节
packet-length OPERATOR LENGTH	报文长度，范围是 64~16382，包括 eq (equal to)、lt (less than)、gt (greater than)、和 range

#### 命令模式

MAC ACL 模式

## 默认

无

## 使用说明

如果顺序号为空，交换机会自动给此规则分配顺序号。而分配的顺序号是在现在存在的最大的顺序号的基础上有一个增量；比如现在最大的顺序号是 100，则分配的顺序号就为 110（以 10 为增量）。如果当前存在的最大的顺序号加上 10 之后，超过可配的顺序号最大值，不允许添加空顺序号的规则。指定的 Ether type 在出方向不支持。

## 举例说明

添加规则：拒绝源 MAC 地址为 001A.A02C.A1DF 的报文通过。

```
Switch(config-mac-acl)# 1 deny src-mac host 001A.A02C.A1DF
```

添加规则：拒绝任何报文通过。

```
Switch(config-mac-acl)# 2 deny src-mac any
```

添加规则：拒绝源 MAC 地址为某一范围内的报文通过。

```
Switch(config-mac-acl)# 3 deny src-mac 001A.A02C.A1DF 001A.A02C.0000
```

## 相关命令

**no sequence-num**

### 6.4.4 permit src-mac

使用此命令在 MAC 访问控制列表中添加访问控制规则；此规则允许指定源 MAC 地址的报文通过。

## 命令语法

```
(SEQUENCE-NUM | ) permit src-mac (any | MAC MASK | host MAC) ( dest-mac (any | MAC MASK | host MAC) | ) ( untag-vlan | ( vlan VLAN | ) ) ( cos VLAN | ) ( inner-vlan VLAN | ) ( inner-cos VALUE | ) ) ( protocol (arp (arp-op-code) | rarp) | packet-length OPERATOR LENGTH | ) ( time-range TIME-RANGE-NAME | )
```

SEQUENCE-NUM	此规则在 MAC 访问控制列表中的顺序；如果没有指定此项，则系统会自动给此规则分配顺序号。范围是 1~2147483646
any	任何主机
MAC MASK	某一类主机
host MAC	某一台主机
dest-mac	目的 MAC 地址

untag-vlan	没有 vlan tag
vlan VLAN	VLAN-ID, 范围是 1~4094
cos VALUE	CoS, 范围是 0~7
inner-vlan VLAN	内层 VLAN-ID, 范围是 1~4094
inner-cos VALUE	内层 CoS, 范围是 0~7
protocol	指定 ARP 或者 RARP
arp	ARP 协议
arp-op-code	arp-op-code,范围是 0~65535
rarp	RARP 协议
<b>time-range</b> TIME-RANGE-NAME	应用此选项可以产生基于时间的访问控制列表, 详见相关章节
<b>packet-length</b> OPERATOR LENGTH	报文长度, 范围是 64~16382, 包括 eq (equal to)、lt (less than)、gt (greater than)、和 range

## 命令模式

MAC ACL 模式

## 默认

无

## 使用说明

如果顺序号为空, 交换机会自动给此规则分配顺序号。而分配的顺序号是在现在存在的最大的顺序号的基础上有一个增量; 比如现在最大的顺序号是 100, 则分配的顺序号就为 110 (以 10 为增量)。如果当前存在的最大的顺序号加上 10 之后, 超过可配的顺序号最大值, 不允许添加空顺序号的规则。指定的 Ether type 在出方向不支持。

## 举例说明

添加规则: 允许源 mac 地址为 001A.A02C.A1DF 的报文通过。

```
Switch(config-mac-acl)# 1 permit src-mac host 001A.A02C.A1DF
```

添加规则: 允许任何报文通过。

```
Switch(config-mac-acl)# 2 permit src-mac any
```

添加规则: 允许源 mac 地址为某一范围内的报文通过。

```
Switch(config-mac-acl)# 3 permit src-mac 001A.A02C.A1DF 001A.A02C.0000
```

## 相关命令

**no sequence-num**

### 6.4.5 remark

使用此命令给 MAC 或 IPv4 访问控制列表添加说明。

使用关键字 **no** 删除对访问控制列表的说明。

## 命令语法

**remark** *REMARK*

**no remark**

REMARK	所添加的说明，不超过 100 个字符
--------	--------------------

## 命令模式

MAC ACL 模式或 IP ACL 模式

## 默认

无

## 使用说明

所添加的说明最多可以有 100 个字符，超过的字符会被丢弃，不会被存储。

## 举例说明

为本列表添加说明 “remark of list for mac”:

```
Switch(config-mac-acl)# remark remark of List for mac
```

删除此列表说明:

```
Switch(config-mac-acl)# no remark
```

## 相关命令

**mac access-list**

### 6.4.6 show access-list mac

使用此命令查看 MAC 访问控制列表。

## 命令语法

**show access-list mac** (*ACL-NAME* |)

ACL-NAME	MAC 访问控制列表名称
----------	--------------

## 命令模式

特权模式

## 默认

无

## 使用说明

查看访问控制列表的内容。

## 举例说明

查看 mac 访问控制列表：

```
Switch# show access-list mac
mac access-list list_mac_1
  10 deny src-mac host 0000.0001.0002
  20 permit src-mac any
```

## 相关命令

**mac access-list**

### 6.4.7 ip access-list

此命令创建 IPv4 访问控制列表并进入访问控制列表配置模式。

使用关键字 **no** 删除指定的 IPv4 访问控制列表。

## 命令语法

**ip access-list** *ACL-NAME*

**no ip access-list** *ACL-NAME*

ACL-NAME	IP ACL 名字，不超过 40 个字符
----------	----------------------



## 命令模式

全局配置模式

## 默认

无

## 使用说明

如果访问控制列表名称为一个已经存在的名称，则此命令表示进入 IPv4 访问控制列表配置模式；如果访问控制列表名称为新名称，则此命令表示创建此列表并进入 IPv4 访问控制列表配置模式；此处创建的访问控制列表配合 `match access-group` 命令使用，具体见相关章节。

## 举例说明

- 创建一个名为 `list_ipv4_1` 的 IPv4 访问控制列表并进入配置模式：

```
Switch(config)# ip access-list list_ipv4_1
Switch(config-ip-acl)#
```

- 删除名称为 `list_ipv4_1` 的 IPv4 访问控制列表：

```
Switch(config)# no ip access-list list_ipv4_1
```

## 相关命令

**match access-group**

### 6.4.8 deny

使用此命令拒绝符合规则的 IPv4 报文通过端口。

## 命令语法

**(SEQUENCE-NUM | ) deny (PROTO-NUM | any) (SOURCE SOURCE-MASK | any | host SOURCE) (DESTINATION DESTINATION-MASK | any | host DESTINATION) (ip-precedence PRECEDENCE | dscp DSCP) (non-fragment|first-fragment|non-or-first-fragment|small-fragment|non-first-fragment) (routed-packet |) (options |) (packet-length OPERATOR LENGTH |) (time-range TIME-RANGE-NAME |)**

SEQUENCE-NUM	此规则在 IPv4 访问控制列表中的顺序；如果没有指定此项，则系统会自动给此规则分配顺序号。范围是 1~131071
PROTO-NUM	协议编号，范围是 0~255
any	第一处 any 是指使用任何协议的 IP 报文
SOURCE SOURCE-MASK	地址为某一类的 IPv4 地址的主机和地址掩码

any	第二处 any 是指地址可以为任何地址的主机
host SOURCE	源地址为特定地址的某台主机
DESTINATION DESTINATION-MASK	目的地址为特定地址的某台主机
any	第三处 any 是指目的地址可以为任何地址的主机
host DESTINATION	目的地址为特定地址的某台主机
ip-precedence PRECEDENCE	IP 报文优先级，范围是 0~7
dscp DSCP	DSCP 号，范围是 0~63
non-fragment	报文为 IP 非分片报文
first-fragment	报文为 IP 分片报文且为首片报文
non-or-first-fragment	报文为 IP 非分片报文或者报文为 IP 分片报文且为非首片报文
small-fragment	报文为 IP 小片报文
non-first-fragment	报文为 IP 分片报文且为非首片报文
routed-packet	报文为路由报文
options	报文携带 IP 选项
time-range TIME- RANGE-NAME	应用此选项可以产生基于时间的访问控制列表，详见相关章节
packet-length OPERATOR LENGTH	报文长度，范围是 64~16382，包括 eq (equal to)、lt (less than)、gt (greater than)、和 range

## 命令模式

IP ACL 模式

## 默认

无

## 使用说明

此处创建的访问控制列表不仅限制了报文所使用的协议，而且限制了源地址和目的地址；地址掩码中，为 1 的部分是无关部分，为 0 的部分是要求严格匹配的；使用地址掩码可以指定某一类的 IP 地址；比如 10.10.10.0 0.0.0.255，这个表示地址从 10.10.10.0~10.10.10.255 的地址都符合要求。

如果顺序号为空，交换机会自动给此规则分配顺序号。而分配的顺序号是在现在存在的最大的顺序号的基础上有一个增量；如果现在的最大的顺序号是 100，则分配的顺序号就为 110（以 10 为增量）。

## 举例说明

- 添加规则：拒绝使用任何协议的任何报文通过。  
Switch(config-ip-acl)# 1 deny any any any
- 拒绝报文中源地址为 1.1.1.1，目的地址为任意的 IP 分片报文。  
Switch(config-ip-acl)# 2 deny any host 1.1.1.1 any fragments
- 添加规则：拒绝任何路由报文通过。  
Switch(config-ip-acl)# 3 deny any any any routed-packet

## 相关命令

**no sequence-num**

### 6.4.9 deny tcp

使用此命令拒绝符合规则的 TCP 报文通过端口。

## 命令语法

*(SEQUENCE-NUM |)* **deny tcp** (*SOURCE SOURCE-MASK | any | host SOURCE*) (*src-port OPERATOR PORT |*) (*DESTINATION DESTINATION-MASK | any | host DESTINATION*) (*dst-port OPERATOR PORT |*) (*ip-precedence PRECEDENCE | dscp DSCP |*) (*established | (match-any | match-all FLAG-NAME |)*) (*non-fragment|first-fragment|non-or-first-fragment|small-fragment|non-first-fragment*) (*routed-packet |*) (*options |*) (*packet-length OPERATOR LENGTH |*) (*time-range TIME-RANGE-NAME |*)

SEQUENCE-NUM	此规则在 IPv4 访问控制列表中的顺序；如果没有指定此项，则系统会自动给此规则分配顺序号。范围是 1~131071
SOURCE SOURCE-MASK	地址为某一类的 IPv4 地址的主机和地址掩码
any	第一处 any 是指地址可以为任何地址的主机
host SOURCE	源地址为特定地址的某台主机
src-port OPERATOR PORT	源端口，范围是 0~65535，包括 eq (equal to)、lt (less than)、gt (greater than)、neq (not equal to) 和 range
DESTINATION DESTINATION-MASK	目的地址为特定地址的某台主机
any	第三处 any 是指目的地址可以为任何地址的主机
host DESTINATION	目的地址为特定地址的某台主机

<b>dst-port OPERATOR PORT</b>	目的端口，范围是 0~65535，包括 eq (equal to)、lt (less than)、gt (greater than)、neq (not equal to)和 range
ip-precedence <i>PRECEDENCE</i>	IP 报文优先级，范围是 0~7
dscp <i>DSCP</i>	DSCP 号，范围是 0~63
established	匹配已经建立的连接
match-any	匹配任何 flag-name
match-all <i>FLAG-NAME</i>	匹配 TCP 报文中的 flag 位所有名称，包括 ack、fin、psh、rst、syn 和 urg
non-fragment	报文为 IP 非分片报文
first-fragment	报文为 IP 分片报文且为首片报文
non-or-first-fragment	报文为 IP 非分片报文或者报文为 IP 分片报文且为非首片报文
small-fragment	报文为 IP 小片报文
non-first-fragment	报文为 IP 分片报文且为非首片报文
routed-packet	报文为路由报文
options	报文携带 IP 选项
<b>time-range TIME-RANGE-NAME</b>	应用此选项可以产生基于时间的访问控制列表，详见相关章节
<b>packet-length OPERATOR LENGTH</b>	报文长度，范围是 64~16382，包括 eq (equal to)、lt (less than)、gt (greater than)、和 range

## 命令模式

IP ACL 配置

## 默认

无

## 使用说明

如果指定了四层信息，如 src-port，则 fragments 无效。

## 举例说明

- 添加规则：拒绝任何 TCP 报文。

```
Switch(config-ip-acl)# 1 deny tcp any any
```

- 添加规则：拒绝 TCP 报文中源地址为 1.1.1.1，源端口号为 0~100，目的地址为任意的报文。

```
Switch(config-ip-acl)# 2 deny tcp host 1.1.1.1 src-port range 0 100 any
```

- 添加规则：拒绝任何已建立连接的报文通过。

```
Switch(config-ip-acl)# 3 deny tcp any any established
```

- 添加规则：拒绝源 IP 地址为 10.10.10.0 的发起连接的 TCP 报文通过。

```
Switch(config-ip-acl)# 4 deny tcp 10.10.10.0 0.0.0.0 any match-any ack
```

## 相关命令

**no sequence-num**

### 6.4.10 deny udp

使用此命令拒绝符合规则的 UDP 报文通过端口。

## 命令语法

```
( SEQUENCE-NUM | ) deny udp ( SOURCE SOURCE-MASK | any | host SOURCE ) ( src-port OPERATOR PORT | ) ( DESTINATION DESTINATION-MASK | any | host DESTINATION ) ( dst-port OPERATOR PORT | ) ( ip-precedence PRECEDENCE | dscp DSCP | ) ( non-fragment | first-fragment | non-or-first-fragment | small-fragment | non-first-fragment ) ( routed-packet | ) ( options | ) ( packet-length OPERATOR LENGTH | ) ( time-range TIME-RANGE-NAME | )
```

参数说明请见上文“deny tcp”。

## 命令模式

IP ACL 模式

## 默认

无

## 使用说明

如果指定了四层信息，如 src-port，则 fragments 无效。

## 举例说明

添加规则：拒绝任何 UDP 报文通过。

```
Switch(config-ip-acl)# 1 deny udp any any
```

添加规则：拒绝 UDP 报文中源地址为 1.1.1.1，源端口号为 10，目的地址为任意，目的端口号小于 2000 的报文。

```
Switch(config-ip-acl)# 2 deny udp host 1.1.1.1 src-port eq 10 any dst-port lt 2000
```

## 相关命令

**no sequence-num**

### 6.4.11 deny icmp

使用此命令拒绝符合规则的 ICMP 报文通过端口。

## 命令语法

```
(SEQUENCE-NUM |) deny icmp ( SOURCE SOURCE-MASK | any | host SOURCE )
( DESTINATION DESTINATION-MASK | any | host DESTINATION ) ( icmp-type TYPE-
NUM ( icmp-code CODE-NUM | ) ) ( ip-precedence PRECEDENCE | dscp DSCP | ) ( non-
fragment|first-fragment|non-or-first-fragment|small-fragment|non-first-fragment)
( routed-packet | ) ( options | ) ( packet-length OPERATOR LENGTH | ) ( time-range
TIME-RANGE-NAME | )
```

icmp-type <i>TYPE- NUM</i>	ICMP 报文类型，范围是 0~255
icmp-code <i>CODE- NUM</i>	ICMP 报文代码，范围是 0~255

其他参数说明请见上文“deny”部分描述。

## 命令模式

IP ACL 模式

## 默认

无

## 使用说明

IPv4 访问控制列表配置模式

相关注意事项请见上文“deny tcp”。

## 举例说明

- 添加规则：拒绝使用 ICMP 协议的任何报文通过。  
Switch(config-ip-acl)# 1 deny icmp any any
- 添加规则：拒绝任何报文类型为 3，报文号为 3 的 ICMP 报文通过。  
Switch(config-ip-acl)# 2 deny icmp any any icmp-type 3 icmp-code 3

## 相关命令

**no sequence-num**

## 6.4.12 deny igmp

使用此命令拒绝符合规则的 IGMP 报文通过端口。

### 命令语法

```
(SEQUENCE-NUM |) deny igmp ( SOURCE SOURCE-MASK | any | host SOURCE )
(DESTINATION DESTINATION-MASK | any | host DESTINATION) ( IGMP-TYPE |) ( ip-
precedence PRECEDENCE | dscp DSCP |) (non-fragment|first-fragment|non-or-first-
fragment|small-fragment|non-first-fragment) ( routed-packet |) ( options |) ( packet-
length OPERATOR LENGTH |) ( time-range TIME-RANGE-NAME |)
```

IGMP-TYPE	IGMP 类型、包括 dvmrp、host-query、host-report、mtrace、mtrace-response、pim、precedence、trace、v2-leave、v2-report 和 v3-report
-----------	--

其他参数说明请见上文“deny”部分描述。

### 命令模式

IP ACL 模式

### 默认

无

### 使用说明

用来过滤 IGMP 报文。

### 举例说明

- 添加规则：拒绝任何 IGMP 报文通过。  
Switch(config-ip-acl)# 1 deny igmp any any
- 添加规则：拒绝 IGMP 报文中源地址为 1.1.1.1，目的地址为任意，IGMP 报文类型为 pim 的报文。  
Switch(config-ip-acl)# 2 deny igmp host 1.1.1.1 any pim

### 相关命令

**no sequence-num**

## 6.4.13 deny gre

使用此命令拒绝符合规则的 GRE 报文通过端口。

## 命令语法

(*SEQUENCE-NUM* |) **deny gre** ( *SOURCE SOURCE-MASK* | **any** | **host** *SOURCE* ) ( *DESTINATION DESTINATION-MASK* | **any** | **host** *DESTINATION* ) ( **key** *KEY* **mask** *KEY-MASK* ) ( **ip-precedence** *PRECEDENCE* | **dscp** *DSCP* | ) ( **non-fragment**|**first-fragment**|**non-or-first-fragment**|**small-fragment**|**non-first-fragment**) ( **routed-packet** ) ( **options** ) ( **packet-length** *OPERATOR LENGTH* | ) ( **time-range** *TIME-RANGE-NAME* | )

KEY	GRE 的 KEY，范围 0~4294967295
KEY-MASK	GRE 的 KEY 掩码，范围 0~0xFFFFFFFF

其他参数说明请见上文“deny”部分描述。

## 命令模式

IP ACL 模式

## 默认

无

## 使用说明

过滤类型为 GRE 的报文。

## 举例说明

- 添加规则：拒绝任何 GRE 报文通过。  
Switch(config-ip-acl)# 1 deny gre any any key 0 mask 0
- 添加规则：拒绝 GRE 报文中源地址为 1.1.1.1，目的地址为任意，key 为 10 的报文。  
Switch(config-ip-acl)# 2 deny gre host 1.1.1.1 any key 10 mask 0xffffffff

## 相关命令

**no sequence-num**

### 6.4.14 deny nvgre

使用此命令拒绝符合规则的 NVGRE 报文通过端口。

## 命令语法

(*SEQUENCE-NUM* |) **deny nvgre** ( *SOURCE SOURCE-MASK* | **any** | **host** *SOURCE* ) ( *DESTINATION DESTINATION-MASK* | **any** | **host** *DESTINATION* ) ( **vsid** *VSID* **mask** *VSID-MASK* ) ( **ip-precedence** *PRECEDENCE* | **dscp** *DSCP* | ) ( **non-fragment**|**first-fragment**|**non-**



**or-first-fragment|small-fragment|non-first-fragment|) (routed-packet|) (options|)**  
**(packet-length OPERATOR LENGTH |) (time-range TIME-RANGE-NAME |)**

VSID	NVGRE 的 VSID，范围 0~16777215
VSID-MASK	NVGRE 的 VSID 掩码，范围 0~0xFFFFFFFF

其他参数说明请见上文“deny”部分描述。

## 命令模式

IP ACL 模式

## 默认

无

## 使用说明

过滤类型为 NVGRE 的报文。

## 举例说明

- 添加规则：拒绝任何 NVGRE 报文通过。  

```
Switch(config-ip-acl)# 1 deny nvgre any any vsid 0 mask 0
```
- 添加规则：拒绝 NVGRE 报文中源地址为 1.1.1.1，目的地址为任意，VSID 为 10 的报文。  

```
Switch(config-ip-acl)# 2 deny gre host 1.1.1.1 any vsid 10 mask 0xffffffff
```

## 相关命令

**no sequence-num**

### 6.4.15 permit

使用此命令允许符合规则的 IPv4 报文通过端口。

## 命令语法

**(SEQUENCE-NUM |) permit (PROTO-NUM | any ) ( source SOURCE-MASK | any | host SOURCE ) (destination DESTINATION-MASK | any | host DESTINATION) ( ip-precedence PRECEDENCE | dscp DSCP |) (non-fragment|first-fragment|non-or-first-fragment|small-fragment|non-first-fragment) ( routed-packet |) ( options |) ( packet-length OPERATOR LENGTH |) ( time-range TIME-RANGE-NAME |)**

参数说明请见上文“deny”。

## 命令模式

IP ACL 模式

## 默认

无

## 使用说明

此处创建的访问控制列表不仅可以匹配报文所使用的协议，而且可以匹配源地址和目的地址；地址掩码中，为 1 的部分是无关部分，为 0 的部分是要求严格匹配的；使用地址掩码可以指定某一类的 IP 地址；比如 10.10.10.0 0.0.0.255，这个表示地址从 10.10.10.0~10.10.10.255 的地址都符合要求。

如果序号为空，交换机会自动给此规则分配序号。而分配的序号是在现在存在的最大的序号的基础上有一个增量；如果现在的最大的序号是 100，则分配的序号就为 110（以 10 为增量）。

## 举例说明

- 添加规则：允许使用任何协议的任何报文通过。  
Switch(config-ip-acl)# 10 permit any any any
- 添加规则：允许报文中源地址为 1.1.1.1，目的地址为任意的 IP 分片报文报文。  
Switch(config-ip-acl)# 20 permit tcp host 1.1.1.1 any non-first-fragment
- 添加规则：允许任何路由报文通过。  
Switch(config-ip-acl)# 30 permit any any any routed-packet

## 相关命令

**no sequence-num**

### 6.4.16 permit tcp

使用此命令允许符合规则的 TCP 报文通过端口。

## 命令语法

```
(SEQUENCE-NUM |) permit tcp (source SOURCE-MASK | any | host SOURCE)( src-port OPERATOR PORT |)(DESTINATION DESTINATION-MASK | any | host DESTINATION)
(dst-port OPERATOR PORT |)( ip-precedence PRECEDENCE | dscp DSCP |)
(established | ( match-any | match-all FLAG-NAME | ) | ) ( non-fragment | first-fragment | non-or-first-fragment | small-fragment | non-first-fragment ) ( routed-packet | )
(options | ) ( packet-length OPERATOR LENGTH | ) ( time-range TIME-RANGE-NAME | )
```

参数请见上文“deny tcp”。

## 命令模式

IP ACL 模式

## 默认

无

## 使用说明

如果指定了四层信息，如 `src-port`，则 `fragments` 无效。

## 举例说明

- 添加规则：允许任何 TCP 报文。  
`Switch(config-ip-acl)# 10 permit tcp any any`
- 添加规则：允许 TCP 报文中源地址为 1.1.1.1，源端口号为 0~100，目的地址为任意的报文。  
`Switch(config-ip-acl)# 20 permit tcp host 1.1.1.1 src-port range 0 100 any`
- 添加规则：允许任何已建立连接的报文通过。  
`Switch(config-ip-acl)# 30 permit tcp any any established`
- 添加规则：允许源 IP 地址为 10.10.10.0 的发起连接的 TCP 报文通过。  
`Switch(config-ip-acl)# 4 permit tcp 10.10.10.0 0.0.0.0 any match-any ack`

## 相关命令

**no sequence-num**

### 6.4.17 permit udp

使用此命令允许符合规则的 UDP 报文通过端口。

## 命令语法

```
(SEQUENCE-NUM |) permit udp ( source SOURCE-MASK | any | host SOURCE ) ( src-port OPERATOR PORT | ) ( destination DESTINATION-MASK | any | host DESTINATION ) ( dst-port OPERATOR PORT | ) ( ip-precedence PRECEDENCE | dscp DSCP | ) ( non-fragment | first-fragment | non-or-first-fragment | small-fragment | non-first-fragment ) ( routed-packet | ) ( options | ) ( packet-length OPERATOR LENGTH | ) ( time-range TIME-RANGE-NAME | )
```

参数说明请见上文“deny udp”。

## 命令模式

IP ACL 模式

## 默认

无

## 使用说明

如果指定了四层信息，如 `src-port`，则 `fragments` 无效。

## 举例说明

- 添加规则：允许任何 UDP 报文通过。

```
Switch(config-ip-acl)# 1 permit udp any any
```

- 添加规则：允许 UDP 报文中源地址为 1.1.1.1，源端口号为 10，目的地址为任意，目的端口号小于 2000 的报文。

```
Switch(config-ip-acl)# 2 permit udp host 1.1.1.1 src-port eq 10 any dst-port lt 2000
```

## 相关命令

**no sequence-num**

### 6.4.18 permit icmp

使用此命令允许符合规则的 ICMP 报文通过端口。

## 命令语法

```
(SEQUENCE-NUM |) permit icmp (source SOURCE-MASK | any | host SOURCE)  
(destination DESTINATION-MASK | any | host DESTINATION) (icmp-type TYPE-NUM  
(icmp-code CODE-NUM |)) (ip-precedence PRECEDENCE | dscp DSCP |) (non-fragment|first-fragment|non-or-first-fragment|small-fragment|non-first-fragment)  
(routed-packet |) (options |) (packet-length OPERATOR LENGTH |) (time-range TIME-RANGE-NAME |)
```

参数说明请见上文“deny icmp”。

## 命令模式

IP ACL 模式

## 默认

无

## 使用说明

过滤类型为 ICMP 报文。

## 举例说明

- 添加规则：允许使用 ICMP 协议的任何报文通过。

```
Switch(config-ip-acl)# 1 permit icmp any any
```

- 添加规则：允许任何报文类型为 3，报文号为 3 的 ICMP 报文通过。

```
Switch(config-ip-acl)# 2 permit icmp any any icmp-type 3 icmp-code 3
```

## 相关命令

**deny icmp**

**no sequence-num**

## 6.4.19 permit igmp

使用此命令允许符合规则的 IGMP 报文通过端口。

### 命令语法

```
(SEQUENCE-NUM |) permit igmp ( SOURCE SOURCE-MASK | any | host SOURCE )  
( DESTINATION DESTINATION-MASK | any | host DESTINATION ) ( IGMP-TYPE | ) ( ip-  
precedence PRECEDENCE | dscp DSCP | ) ( non-fragment|first-fragment|non-or-first-  
fragment|small-fragment|non-first-fragment ) ( routed-packet | ) ( options | ) ( packet-  
length OPERATOR LENGTH | ) ( time-range TIME-RANGE-NAME | )
```

其他相关参数请见上文“deny igmp”。

### 命令模式

IP ACL 模式

### 默认

无

### 使用说明

过滤类型为 IGMP 的报文。

### 举例说明

- 添加规则：允许任何 IGMP 报文通过。  
Switch(config-ip-acl)# 1 permit igmp any any
- 添加规则：允许 IGMP 报文中源地址为 1.1.1.1，目的地址为任意，IGMP 报文类型为 pim 的报文。  
Switch(config-ip-acl)# 2 permit igmp host 1.1.1.1 any pim

### 相关命令

**no sequence-num**

## 6.4.20 permit gre

使用此命令允许符合规则的 GRE 报文通过端口。

### 命令语法

```
(SEQUENCE-NUM |) permit gre ( SOURCE SOURCE-MASK | any | host SOURCE )  
( DESTINATION DESTINATION-MASK | any | host DESTINATION ) ( key KEY mask KEY-  
MASK ) ( ip-precedence PRECEDENCE | dscp DSCP | ) ( non-fragment|first-fragment|non-  
or-first-fragment|small-fragment|non-first-fragment ) ( routed-packet ) ( options )  
( packet-length OPERATOR LENGTH | ) ( time-range TIME-RANGE-NAME | )
```

其他相关参数请见上文“deny gre”。

## 命令模式

IP ACL 模式

## 默认

无

## 使用说明

过滤类型为 GRE 的报文。

## 举例说明

- 添加规则：允许任何 GRE 报文通过。  
`Switch(config-ip-acl)# 1 permit gre any any key 0 mask 0`
- 添加规则：允许 GRE 报文中源地址为 1.1.1.1，目的地址为任意，key 为 10 的报文。  
`Switch(config-ip-acl)# 2 permit gre host 1.1.1.1 any key 10 mask 0xffffffff`

## 相关命令

**no sequence-num**

### 6.4.21 permit nvgre

使用此命令允许符合规则的 NVGRE 报文通过端口。

## 命令语法

*(SEQUENCE-NUM | ) permit nvgre ( SOURCE SOURCE-MASK | any | host SOURCE ) ( DESTINATION DESTINATION-MASK | any | host DESTINATION ) (vsid VSID mask VSID-MASK) (ip-precedence PRECEDENCE | dscp DSCP | ) (non-fragment|first-fragment|non-or-first-fragment|small-fragment|non-first-fragment|) (routed-packet|) (options|) (packet-length OPERATOR LENGTH |) (time-range TIME-RANGE-NAME |)*

其他相关参数请见上文“deny nvgre”。

## 命令模式

IP ACL 模式

## 默认

无

## 使用说明

过滤类型为 NVGRE 的报文。

## 举例说明

- 添加规则：允许任何 NVGRE 报文通过。  
Switch(config-ip-acl)# 1 permit nvgre any any vsid 0 mask 0
- 添加规则：允许 NVGRE 报文中源地址为 1.1.1.1，目的地址为任意，VSID 为 10 的报文。  
Switch(config-ip-acl)# 2 permit gre host 1.1.1.1 any vsid 10 mask 0xffffffff

## 相关命令

**no sequence-num**

### 6.4.22 show access-list ip

使用此命令查看 IPv4 访问控制列表。

## 命令语法

**show access-list ip** (*ACL-NAME* |)

ACL-NAME	IP 访问控制列表名称
----------	-------------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

如何显示 IP ACL 的配置信息。

```
Switch# show access-list ip
ip access-list list_ipv4_1
  2 permit tcp host 1.1.1.1 any
  3 deny icmp any any
  12 permit tcp any any
```

## 相关命令

**ip access-list**

## 6.5 Extend ACL 命令

### 6.5.1 ip access-list extend

此命令创建扩展 IPv4 访问控制列表并进入访问控制列表配置模式。

使用关键字 **no** 删除指定的 IPv4 访问控制列表。

## 命令语法

**ip access-list** *ACL-NAME* **extend**

**no ip access-list** *ACL-NAME* **extend**

<b>ACL-NAME</b> <b>extend</b>	扩展 IP ACL 名字
----------------------------------	--------------

## 命令模式

全局配置模式

## 默认

无

## 使用说明

如果访问控制列表名称为一个已经存在的名称，则此命令表示进入扩展 IPv4 访问控制列表配置模式；如果访问控制列表名称为新名称，则此命令表示创建此列表并进入扩展 IPv4 访问控制列表配置模式；此处创建的访问控制列表配合 **match access-group** 命令使用，具体见相关章节。

## 举例说明

- 创建一个名为 **list\_ipv4\_1** 的扩展 IPv4 访问控制列表并进入配置模式：

```
Switch(config)# ip access-list list_ipv4_1 extend  
Switch(config-ex-ip-acl)#
```

- 删除名称为 **list\_ipv4\_1** 的扩展 IPv4 访问控制列表：

```
Switch(config)# no ip access-list list_ipv4_1 extend
```



## 相关命令

**match access-group**

### 6.5.2 sequence-num

使用此命令删除指定的控制规则。

## 命令语法

**no sequence-num** *SEQUENCE-NUM*

SEQUENCE-NUM	顺序号范围是 1~131071
--------------	-----------------

## 命令模式

扩展 IP ACL 配置模式

## 默认

无

## 使用说明

None

## 举例说明

删除顺序号为 10 的规则：

```
Switch(config-ex-ip-acl)# no sequence-num 10
```

## 相关命令

**deny**

**deny tcp**

**deny udp**

**deny icmp**

**deny igmp**

**permit**

**permit tcp**

**permit udp**

**permit icmp**

**permit igmp**  
**deny src-mac**  
**permit src-mac**

### 6.5.3 deny src-mac

使用此命令拒绝符合规则的报文通过端口。

#### 命令语法

*(SEQUENCE-NUM | ) deny src-mac (any | MAC MASK | host MAC) ( dest-mac (any | MAC MASK | host MAC) | ) ( vlan VLAN | ) ( cos VLAN | ) ( inner-vlan VLAN | ) ( inner-cos VALUE | ) (arp-packet ((arp-op-code) (sender-ip (IP MASK|any|host IP))) (target-ip (IP MASK|any|host IP))) | packet-length OPERATOR LENGTH | ) ( time-range TIME-RANGE-NAME | )*

SEQUENCE-NUM	此规则在 IP 访问控制列表中的顺序；如果没有指定此项，则系统会自动给此规则分配顺序号。范围是 1~2147483646
any	任何主机
MAC MASK	某一类主机
host MAC	某一台主机
dest-mac	目的 MAC 地址
vlan VLAN	VLAN-ID，范围是 1~4094
cos VALUE	CoS，范围是 0~7
inner-vlan VLAN	内层 VLAN-ID，范围是 1~4094
inner-cos VALUE	内层 CoS，范围是 0~7
arp	ARP 协议
arp-op-code	arp-op-code，范围是 0~65535
sender-ip	sender-ip
IP MASK	某一类主机
any	任何主机
host IP	某一台主机
target-ip	target-ip
IP MASK	某一类主机
any	任何主机
host IP	某一台主机

<b>time-range</b> TIME-RANGE-NAME	应用此选项可以产生基于时间的访问控制列表，详见相关章节
<b>packet-length</b> OPERATOR LENGTH	报文长度，范围是 64~16382，包括 eq (equal to)、lt (less than)、gt (greater than)、和 range

## 命令模式

扩展 IP ACL 配置模式

## 默认

无

## 使用说明

如果顺序号为空，交换机会自动给此规则分配顺序号。而分配的顺序号是在现在存在的最大的顺序号的基础上有一个增量；如果现在的最大的顺序号是 100，则分配的顺序号就为 110（以 10 为增量）。

## 举例说明

- 添加规则：拒绝源 MAC 地址为 001A.A02C.A1DF 的报文通过。  
Switch(config-ex-ip-acl)# 1 deny src-mac host 001A.A02C.A1DF
- 添加规则：拒绝任何报文通过。  
Switch(config-ex-ip-acl)# 2 deny src-mac any
- 规则：拒绝源 MAC 地址为某一范围内的报文通过。  
Switch(config-ex-ip-acl)# 3 deny src-mac 001A.A02C.A1DF 001A.A02C.0000

## 相关命令

**no sequence-num**

### 6.5.4 permit src-mac

使用此命令允许符合规则的报文通过端口。

## 命令语法

```
(SEQUENCE-NUM |) permit src-mac (any| MAC MASK |host MAC) ( dest-mac (any |MAC MASK | host MAC) |) ( vlan VLAN |) ( cos VALUE |) ( inner-vlan VLAN |) ( inner-cos VALUE |) ( arp-packet ((arp-op-code) (sender-ip (IP MASK|any|host IP))) (target-ip (IP MASK|any|host IP))))| packet-length OPERATOR LENGTH |) ( time-range TIME-RANGE-NAME |)
```

各参数使用说明请参见“deny src-mac”。

## 命令模式

扩展 IP ACL 配置模式

## 默认

无

## 使用说明

如果顺序号为空，交换机会自动给此规则分配顺序号。而分配的顺序号是在现在存在的最大的顺序号的基础上有一个增量；如果现在的最大的顺序号是 100，则分配的顺序号就为 110（以 10 为增量）。

## 举例说明

- 添加规则：允许源 mac 地址为 001A.A02C.A1DF 的报文通过。  
Switch(config-ex-ip-ac)# 1 permit src-mac host 001A.A02C.A1DF
- 添加规则：允许任何报文通过。  
Switch(config-ex-ip-ac)# 2 permit src-mac any
- 添加规则：允许源 mac 地址为某一范围内的报文通过。  
Switch(config-ex-ip-acl)# 3 permit src-mac 001A.A02C.A1DF 001A.A02C.0000

## 相关命令

**no sequence-num**

### 6.5.5 deny

使用此命令拒绝符合规则的 IPv4 报文通过端口。

## 命令语法

*(SEQUENCE-NUM | ) deny (PROTO-NUM | any) (SOURCE SOURCE-MASK | any | host SOURCE) (DESTINATION DESTINATION-MASK | any | host DESTINATION) (ip-precedence PRECEDENCE | dscp DSCP) (non-fragment|first-fragment|non-or-first-fragment|small-fragment|non-first-fragment) (routed-packet |) (options |) (packet-length OPERATOR LENGTH |) (time-range TIME-RANGE-NAME |)*

SEQUENCE-NUM	此规则在 IP 访问控制列表中的顺序；如果没有指定此项，则系统会自动给此规则分配顺序号。范围是 1~131071
PROTO-NUM	协议编号，范围是 0~255
any	第一处 any 是指使用任何协议的 IP 报文
SOURCE SOURCE-MASK	地址为某一类的 IPv4 地址的主机和地址掩码

any	第二处 any 是指地址可以为任何地址的主机
host SOURCE	源地址为特定地址的某台主机
DESTINATION DESTINATION-MASK	目的地址为特定地址的某台主机
any	第三处 any 是指目的地址可以为任何地址的主机
host DESTINATION	目的地址为特定地址的某台主机
ip-precedence PRECEDENCE	IP 报文优先级，范围是 0~7
dscp DSCP	DSCP 号，范围是 0~63
non-fragment	报文为 IP 非分片报文
first-fragment	报文为 IP 分片报文且为首片报文
non-or-first-fragment	报文为 IP 非分片报文或者报文为 IP 分片报文且为非首片报文
small-fragment	报文为 IP 小片报文
non-first-fragment	报文为 IP 分片报文且为非首片报文
routed-packet	报文为路由报文
options	报文携带 IP 选项
time-range TIME- RANGE-NAME	应用此选项可以产生基于时间的访问控制列表，详见相关章节
packet-length OPERATOR LENGTH	报文长度，范围是 64~16382，包括 eq (equal to)、lt (less than)、gt (greater than)、和 range

## 命令模式

扩展 IP ACL 配置模式

## 默认

无

## 使用说明

此处创建的访问控制列表不仅限制了报文所使用的协议，而且限制了源地址和目的地址；地址掩码中，为 1 的部分是无关部分，为 0 的部分是要求严格匹配的；使用地址掩码可以指定某一类的 IP 地址；比如 10.10.10.0 0.0.0.255，这个表示地址从 10.10.10.0~10.10.10.255 的地址都符合要求。

如果顺序号为空，交换机会自动给此规则分配顺序号。而分配的顺序号是在现在存在的最大的顺序号的基础上有一个增量；如果现在的最大的顺序号是 100，则分配的顺序号就为 110（以 10 为增量）。

## 举例说明

- 添加规则：拒绝使用任何协议的任何报文通过。  
Switch(config-ex-ip-acl)# 1 deny any any any
- 拒绝报文中源地址为 1.1.1.1，目的地址为任意的 IP 分片报文。  
Switch(config-ex-ip-acl)# 2 deny any host 1.1.1.1 any non-first-fragment
- 添加规则：拒绝任何路由报文通过。  
Switch(config-ex-ip-acl)# 3 deny any any any routed-packet

## 相关命令

**no sequence-num**

### 6.5.6 deny tcp

使用此命令拒绝符合规则的 TCP 报文通过端口。

## 命令语法

```
(SEQUENCE-NUM |) deny tcp (SOURCE SOURCE-MASK | any | host SOURCE) (src-port OPERATOR PORT |)(DESTINATION DESTINATION-MASK | any | host DESTINATION) (dst-port OPERATOR PORT |) (ip-precedence PRECEDENCE | dscp DSCP |) (established | (match-any | match-all FLAG-NAME |)) (non-fragment|first-fragment|non-or-first-fragment|small-fragment|non-first-fragment) (routed-packet |) (options |) (packet-length OPERATOR LENGTH |) (time-range TIME-RANGE-NAME |)
```

SEQUENCE-NUM	此规则在 IP 访问控制列表中的顺序；如果没有指定此项，则系统会自动给此规则分配顺序号。范围是 1～2147483646
SOURCE SOURCE-MASK	地址为某一类的 IPv4 地址的主机和地址掩码
any	第一处 any 是指地址可以为任何地址的主机
host SOURCE	源地址为特定地址的某台主机
src-port OPERATOR PORT	源端口，范围是 0～65535，包括 eq (equal to)、lt (less than)、gt (greater than)、neq (not equal to)和 range
DESTINATION DESTINATION-MASK	目的地址为特定地址的某台主机
any	第三处 any 是指目的地址可以为任何地址的主机
host DESTINATION	目的地址为特定地址的某台主机

<b>dst-port OPERATOR PORT</b>	目的端口，范围是 0~65535，包括 eq (equal to)、lt (less than)、gt (greater than)、neq (not equal to)和 range
ip-precedence <i>PRECEDENCE</i>	IP 报文优先级，范围是 0~7
dscp <i>DSCP</i>	DSCP 号，范围是 0~63
established	匹配已经建立的连接
match-any	匹配任何 flag-name
match-all <i>FLAG-NAME</i>	匹配 TCP 报文中的 flag 位所有名称，包括 ack、fin、psh、rst、syn 和 urg
non-fragment	报文为 IP 非分片报文
first-fragment	报文为 IP 分片报文且为首片报文
non-or-first-fragment	报文为 IP 非分片报文或者报文为 IP 分片报文且为非首片报文
small-fragment	报文为 IP 小片报文
non-first-fragment	报文为 IP 分片报文且为非首片报文
routed-packet	报文为路由报文
options	报文携带 IP 选项
<b>time-range TIME-RANGE-NAME</b>	应用此选项可以产生基于时间的访问控制列表，详见相关章节
<b>packet-length OPERATOR LENGTH</b>	报文长度，范围是 64~16382，包括 eq (equal to)、lt (less than)、gt (greater than)、和 range

## 命令模式

扩展 IP ACL 配置模式

## 默认

无

## 使用说明

如果指定了四层信息，如 src-port，则 fragments 无效。

其他事项请见上文“deny”。

## 举例说明

- 添加规则：拒绝任何 TCP 报文。

```
Switch(config-ex-ip-acl)# 1 deny tcp any any
```

- 添加规则：拒绝 TCP 报文中源地址为 1.1.1.1，源端口号为 0~100，目的地址为任意的报文。

```
Switch(config-ex-ip-acl)# 2 deny tcp host 1.1.1.1 src-port range 0 100 any
```

- 添加规则：拒绝任何已建立连接的报文通过。

```
Switch(config-ex-ip-acl)# 3 deny tcp any any established
```

- 添加规则：拒绝源 IP 地址为 10.10.10.0 的发起连接的 TCP 报文通过。

```
Switch(config-ex-ip-acl)# 4 deny tcp 10.10.10.0 0.0.0.0 any match-any ack
```

## 相关命令

**no sequence-num**

### 6.5.7 deny udp

使用此命令拒绝符合规则的 UDP 报文通过端口。

## 命令语法

```
(SEQUENCE-NUM |) deny udp (SOURCE SOURCE-MASK | any | host SOURCE) (src-port OPERATOR PORT |)(DESTINATION DESTINATION-MASK | any | host DESTINATION) (dst-port OPERATOR PORT |) (ip-precedence PRECEDENCE | dscp DSCP |) (non-fragment|first-fragment|non-or-first-fragment|small-fragment|non-first-fragment) (routed-packet |) (options |) (packet-length OPERATOR LENGTH |) (time-range TIME-RANGE-NAME |)
```

参数使用说明请见上文“deny tcp”。

## 命令模式

扩展 IP ACL 配置模式

## 默认

无

## 使用说明

如果指定了四层信息，如 src-port，则 fragments 无效。

其他事项请见上文“deny”。

## 举例说明

- 添加规则：拒绝任何 UDP 报文通过。

```
Switch(config-ex-ip-acl)# 1 deny udp any any
```

- 添加规则：拒绝 UDP 报文中源地址为 1.1.1.1，源端口号为 10，目的地址为任意，目的端口号小于 2000 的报文。

```
Switch(config-ex-ip-acl)# 2 deny udp host 1.1.1.1 src-port eq 10 any dst-port lt 2000
```



## 相关命令

**no sequence-num**

### 6.5.8 deny icmp

使用此命令拒绝符合规则的 ICMP 报文通过端口。

## 命令语法

*(SEQUENCE-NUM |)* **deny icmp** (*SOURCE SOURCE-MASK | any | host SOURCE*) (*DESTINATION DESTINATION-MASK | any | host DESTINATION*) (**icmp-type** *TYPE-NUM* (**icmp-code** *CODE-NUM* |)) (**ip-precedence** *PRECEDENCE* | **dscp** *DSCP* |) (**non-fragment**|**first-fragment**|**non-or-first-fragment**|**small-fragment**|**non-first-fragment**) (**routed-packet** |) (**options** |) (**packet-length** *OPERATOR LENGTH* |) (**time-range** *TIME-RANGE-NAME* |)

icmp-type <i>TYPE-NUM</i>	ICMP 报文类型，范围是 0~255
icmp-code <i>CODE-NUM</i>	ICMP 报文代码，范围是 0~255

其他参数说明请见上文“deny”。

## 命令模式

扩展 IP ACL 配置模式

## 默认

无

## 使用说明

None

## 举例说明

- 添加规则：拒绝使用 ICMP 协议的任何报文通过。

```
Switch(config-ex-ip-acl)# 1 deny icmp any any
```

- 添加规则：拒绝任何报文类型为 3，报文号为 3 的 ICMP 报文通过。

```
Switch(config-ex-ip-acl)# 2 deny icmp any any icmp-type 3 icmp-code 3
```

## 相关命令

**no sequence-num**

## 6.5.9 deny igmp

使用此命令拒绝符合规则的 IGMP 报文通过端口。

### 命令语法

```
(SEQUENCE-NUM |) deny igmp ( SOURCE SOURCE-MASK | any | host SOURCE )
( DESTINATION DESTINATION-MASK | any | host DESTINATION ) ( IGMP-TYPE | ) ( ip-
precedence PRECEDENCE | dscp DSCP | ) ( non-fragment|first-fragment|non-or-first-
fragment|small-fragment|non-first-fragment ) ( routed-packet | ) ( options | ) ( packet-
length OPERATOR LENGTH | ) ( time-range TIME-RANGE-NAME | )
```

IGMP-TYPE	IGMP 类型、包括 dvmrp、host-query、host-report、mtrace、mtrace-response、pim、precedence、trace、v2-leave、v2-report 和 v3-report
-----------	--

其他参数说明请见上文“deny”。

### 命令模式

扩展 IP ACL 配置模式

### 默认

无

### 使用说明

None

### 举例说明

- 添加规则：拒绝任何 IGMP 报文通过。

```
Switch(config-ex-ip-acl)# 1 deny igmp any any
```

- 添加规则：拒绝 IGMP 报文中源地址为 1.1.1.1，目的地址为任意，IGMP 报文类型为 pim 的报文。

```
Switch(config-ex-ip-acl)# 2 deny igmp host 1.1.1.1 any pim
```

### 相关命令

**no sequence-num**

## 6.5.10 deny gre

使用此命令拒绝符合规则的 GRE 报文通过端口。

## 命令语法

*(SEQUENCE-NUM |)* **deny gre** (*SOURCE SOURCE-MASK | any | host SOURCE*) (*DESTINATION DESTINATION-MASK | any | host DESTINATION*) (**key** *KEY* **mask** *KEY-MASK*) (**ip-precedence** *PRECEDENCE* | **dscp** *DSCP* |) (**non-fragment|first-fragment|non-or-first-fragment|small-fragment|non-first-fragment**) (**routed-packet**) (**options**) (**packet-length** *OPERATOR LENGTH* |) (**time-range** *TIME-RANGE-NAME* |)

KEY	GRE 的 KEY，范围 0~4294967295
KEY-MASK	GRE 的 KEY 掩码，范围 0~0xFFFFFFFF

其他参数说明请见上文“deny”部分描述。

## 命令模式

扩展 IP ACL 模式

## 默认

无

## 使用说明

过滤类型为 GRE 的报文。

## 举例说明

- 添加规则：拒绝任何 GRE 报文通过。

```
Switch(config-ex-ip-acl)# 1 deny gre any any key 0 mask 0
```

- 添加规则：拒绝 GRE 报文中源地址为 1.1.1.1，目的地址为任意，key 为 10 的报文。

```
Switch(config-ex-ip-acl)# 2 deny gre host 1.1.1.1 any key 10 mask 0xffffffff
```

## 相关命令

**no sequence-num**

### 6.5.11 deny nvgre

使用此命令拒绝符合规则的 NVGRE 报文通过端口。

## 命令语法

*(SEQUENCE-NUM |)* **deny nvgre** (*SOURCE SOURCE-MASK | any | host SOURCE*) (*DESTINATION DESTINATION-MASK | any | host DESTINATION*) (**vsid** *VSID* **mask** *VSID-MASK*) (**ip-precedence** *PRECEDENCE* | **dscp** *DSCP* |) (**non-fragment|first-fragment|non-**

**or-first-fragment|small-fragment|non-first-fragment|) (routed-packet|) (options|)**  
**(packet-length OPERATOR LENGTH |) (time-range TIME-RANGE-NAME |)**

VSID	NVGRE 的 VSID，范围 0~16777215
VSID-MASK	NVGRE 的 VSID 掩码，范围 0~0xFFFFFFFF

其他参数说明请见上文“deny”部分描述。

## 命令模式

扩展 IP ACL 模式

## 默认

无

## 使用说明

过滤类型为 NVGRE 的报文。

## 举例说明

- 添加规则：拒绝任何 NVGRE 报文通过。  

```
Switch(config-ip-acl)# 1 deny nvgre any any vsid 0 mask 0
```
- 添加规则：拒绝 NVGRE 报文中源地址为 1.1.1.1，目的地址为任意，VSID 为 10 的报文。  

```
Switch(config-ip-acl)# 2 deny gre host 1.1.1.1 any vsid 10 mask 0xffffffff
```

## 相关命令

**no sequence-num**

### 6.5.12 permit

使用此命令允许符合规则的 IPv4 报文通过端口。

## 命令语法

**(SEQUENCE-NUM |) permit (PROTO-NUM | any) (source SOURCE-MASK | any | host SOURCE) (destination DESTINATION-MASK | any | host DESTINATION) (ip-precedence PRECEDENCE | dscp DSCP |) (non-fragment|first-fragment|non-or-first-fragment|small-fragment|non-first-fragment) (routed-packet |) (options |) (packet-length OPERATOR LENGTH |) (time-range TIME-RANGE-NAME |)**

参数使用说明请参见“deny”。

## 命令模式

扩展 IP ACL 配置模式

## 默认

无

## 使用说明

此处创建的访问控制列表不仅可以匹配报文所使用的协议，而且可以匹配源地址和目的地址；地址掩码中，为 1 的部分是无关部分，为 0 的部分是要求严格匹配的；使用地址掩码可以指定某一类的 IP 地址；比如 10.10.10.0 0.0.0.255，这个表示地址从 10.10.10.0~10.10.10.255 的地址都符合要求。

如果序号为空，交换机会自动给此规则分配序号。而分配的序号是在现在存在的最大的序号的基础上有一个增量；如果现在的最大的序号是 100，则分配的序号就为 110（以 10 为增量）。

## 举例说明

- 添加规则：允许使用任何协议的任何报文通过。

```
Switch(config-ex-ip-acl)# 10 permit any any any
```

- 添加规则：允许报文中源地址为 1.1.1.1，目的地址为任意的 IP 分片报文。

```
Switch(config-ex-ip-acl)# 20 permit tcp host 1.1.1.1 any non-first-fragments
```

- 添加规则：允许任何路由报文通过。

```
Switch(config-ex-ip-acl)# 30 permit any any any routed-packet
```

## 相关命令

**no sequence-num**

### 6.5.13 permit tcp

使用此命令允许符合规则的 TCP 报文通过端口。

## 命令语法

```
(SEQUENCE-NUM | ) permit tcp (source SOURCE-MASK | any | host SOURCE)( src-port OPERATOR PORT | )( DESTINATION DESTINATION-MASK | any | host DESTINATION )  
( dst-port OPERATOR PORT | )( ip-precedence PRECEDENCE | dscp DSCP | )  
( established | ( match-any | match-all FLAG-NAME | ) | ) ( non-fragment | first-fragment | non-or-first-fragment | small-fragment | non-first-fragment ) ( routed-packet | )  
( options | ) ( packet-length OPERATOR LENGTH | ) ( time-range TIME-RANGE-NAME | )
```

参数使用说明请见上文“deny tcp”。

## 命令模式

扩展 IP ACL 配置模式

## 默认

无

## 使用说明

如果指定了四层信息，如 `src-port`，则 `fragments` 无效。

其他事项请见上文“`permit`”。

## 举例说明

- 添加规则：允许任何 TCP 报文。

```
Switch(config-ex-ip-acl)# 10 permit tcp any any
```

- 添加规则：允许 TCP 报文中源地址为 1.1.1.1，源端口号为 0~100，目的地址为任意的报文。

```
Switch(config-ex-ip-acl)# 20 permit tcp host 1.1.1.1 src-port range 0 100 any
```

- 添加规则：允许任何已建立连接的报文通过。

```
Switch(config-ex-ip-acl)# 30 permit tcp any any established
```

- 添加规则：允许源 IP 地址为 10.10.10.0 的发起连接的 TCP 报文通过。

```
Switch(config-ex-ip-acl)# 4 permit tcp 10.10.10.0 0.0.0.0 any match-any ack
```

## 相关命令

**no sequence-num**

### 6.5.14 permit udp

使用此命令允许符合规则的 UDP 报文通过端口。

## 命令语法

```
(SEQUENCE-NUM | ) permit udp ( source SOURCE-MASK | any | host SOURCE ) ( src-port OPERATOR PORT | ) ( destination DESTINATION-MASK | any | host DESTINATION ) ( dst-port OPERATOR PORT | ) ( ip-precedence PRECEDENCE | dscp DSCP | ) ( non-fragment | first-fragment | non-or-first-fragment | small-fragment | non-first-fragment ) ( routed-packet | ) ( options | ) ( packet-length OPERATOR LENGTH | ) ( time-range TIME-RANGE-NAME | )
```

参数说明请见上文“`deny udp`”。

## 命令模式

扩展 IP ACL 配置模式

## 默认

无

## 使用说明

其他事项请见上文“permit”。

## 举例说明

- 添加规则：允许任何 UDP 报文通过。

```
Switch(config-ex-ip-acl)# 1 permit udp any any
```

- 添加规则：允许 UDP 报文中源地址为 1.1.1.1，源端口号为 10，目的地址为任意，目的端口号小于 2000 的报文。

```
Switch(config-ex-ip-acl)# 2 permit udp host 1.1.1.1 src-port eq 10 any dst-port lt 2000
```

## 相关命令

**no sequence-num**

### 6.5.15 permit icmp

使用此命令允许符合规则的 ICMP 报文通过端口。

## 命令语法

```
(SEQUENCE-NUM | ) permit icmp (source SOURCE-MASK | any | host SOURCE )  
(destination DESTINATION-MASK | any | host DESTINATION ) ( icmp-type TYPE-NUM  
( icmp-code CODE-NUM | ) ) ( ip-precedence PRECEDENCE | dscp DSCP | ) ( non-  
fragment|first-fragment|non-or-first-fragment|small-fragment|non-first-fragment)  
( routed-packet | ) ( options | ) ( packet-length OPERATOR LENGTH | ) ( time-range  
TIME-RANGE-NAME | )
```

参数说明请见上文 “deny icmp”。

## 命令模式

扩展 IP ACL 配置模式

## 默认

无

## 使用说明

过滤类型为 ICMP 报文。

## 举例说明

- 添加规则：允许使用 ICMP 协议的任何报文通过。

```
Switch(config-ex-ip-acl)# 1 permit icmp any any
```

- 添加规则：允许任何报文类型为 3，报文号为 3 的 ICMP 报文通过。

```
Switch(config-ex-ip-acl)# 2 permit icmp any any icmp-type 3 icmp-code 3
```

## 相关命令

None

### 6.5.16 permit igmp

使用此命令允许符合规则的 IGMP 报文通过端口。

## 命令语法

```
(SEQUENCE-NUM |) permit igmp ( SOURCE SOURCE-MASK | any | host SOURCE )  
( DESTINATION DESTINATION-MASK | any | host DESTINATION ) ( IGMP-TYPE | ) ( ip-  
precedence PRECEDENCE | dscp DSCP | ) ( non-fragment|first-fragment|non-or-first-  
fragment|small-fragment|non-first-fragment ) ( routed-packet | ) ( options | ) ( packet-  
length OPERATOR LENGTH | ) ( time-range TIME-RANGE-NAME | )
```

其他相关参数请见上文“deny igmp”。

## 命令模式

扩展 IP ACL 配置模式

## 默认

无

## 使用说明

None

## 举例说明

- 添加规则：允许任何 IGMP 报文通过。

```
Switch(config-ex-ip-acl)# 1 permit igmp any any
```

- 添加规则：允许 IGMP 报文中源地址为 1.1.1.1，目的地址为任意，IGMP 报文类型为 pim 的报文。

```
Switch(config-ex-ip-acl)# 2 permit igmp host 1.1.1.1 any pim
```

## 相关命令

**no sequence-num**

### 6.5.17 permit gre

使用此命令允许符合规则的 GRE 报文通过端口。

## 命令语法

```
(SEQUENCE-NUM |) permit gre ( SOURCE SOURCE-MASK | any | host SOURCE )  
( DESTINATION DESTINATION-MASK | any | host DESTINATION ) ( key KEY mask KEY-  
MASK ) ( ip-precedence PRECEDENCE | dscp DSCP | ) ( non-fragment|first-fragment|non-
```



**or-first-fragment|small-fragment|non-first-fragment|) (routed-packet|) (options|)**  
**(packet-length OPERATOR LENGTH |) (time-range TIME-RANGE-NAME |)**

其他相关参数请见上文“deny gre”。

## 命令模式

扩展 IP ACL 模式

## 默认

无

## 使用说明

过滤类型为 GRE 的报文。

## 举例说明

- 添加规则：允许任何 GRE 报文通过。  

```
Switch(config-ex-ip-acl)# 1 permit gre any any key 0 mask 0
```
- 添加规则：允许 GRE 报文中源地址为 1.1.1.1，目的地址为任意，key 为 10 的报文。  

```
Switch(config-ex-ip-acl)# 2 permit gre host 1.1.1.1 any key 10 mask 0xffffffff
```

## 相关命令

**no sequence-num**

### 6.5.18 permit nvgre

使用此命令允许符合规则的 NVGRE 报文通过端口。

## 命令语法

**(SEQUENCE-NUM |) permit nvgre ( SOURCE SOURCE-MASK | any | host SOURCE )**  
**(DESTINATION DESTINATION-MASK | any | host DESTINATION) (vsid VSID mask VSID-**  
**MASK) (ip-precedence PRECEDENCE | dscp DSCP |) (non-fragment|first-fragment|non-**  
**or-first-fragment|small-fragment|non-first-fragment|) (routed-packet|) (options|)**  
**(packet-length OPERATOR LENGTH |) (time-range TIME-RANGE-NAME |)**

其他相关参数请见上文“deny nvgre”。

## 命令模式

扩展 IP ACL 模式

## 默认

无

## 使用说明

过滤类型为 NVGRE 的报文。

## 举例说明

- 添加规则：允许任何 NVGRE 报文通过。  
Switch(config-ip-acl)# 1 permit nvgre any any vsid 0 mask 0
- 添加规则：允许 NVGRE 报文中源地址为 1.1.1.1，目的地址为任意，VSID 为 10 的报文。  
Switch(config-ip-acl)# 2 permit gre host 1.1.1.1 any vsid 10 mask 0xffffffff

## 相关命令

**no sequence-num**

### 6.5.19 remark

使用此命令给扩展 IPv4 访问控制列表添加说明。

使用关键字 **no** 删除对控制列表的说明。

## 命令语法

**remark** *REMARK*

**no remark**

REMARK	所添加的说明
--------	--------

## 命令模式

扩展 IP ACL 配置模式

## 默认

无

## 使用说明

所添加的说明最多可以有 100 个字符，超过的字符会被丢弃，不会被存储。

## 举例说明

- 为本列表添加说明“remarkoflist1”。  
Switch(config-ex-ip-acl)# remark remard0flist1
- 删除此列表的说明。  
Switch(config-ex-ip-acl)# no remark

## 相关命令

无

## 6.5.20 show access-list ip extend

使用此命令查看扩展 IPv4 访问控制列表。

## 命令语法

**show access-list ip** (*ACL-NAME* **extend** | )

<b>ACL-NAME</b> <b>extend</b>	扩展 IP ACL 名字
----------------------------------	--------------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

如何显示 IP ACL 的配置信息。

```
Switch# show access-list ip
ip access-list ex_ip_list_ipv4_1 extend
  2 permit tcp host 1.1.1.1 any
  3 deny icmp any any
  12 permit tcp any any
```

## 相关命令

**ip access-list extend**

## 6.6 ACLv6 命令

### 6.6.1 ipv6 access-list

此命令创建 IPv6 访问控制列表并进入访问控制列表配置模式。

使用关键字 **no** 删除指定的 IPv6 访问控制列表。

## 命令语法

**ipv6 access-list** *ACL-NAME*

**no ipv6 access-list** *ACL-NAME*

ACL-NAME	IPv6 访问控制列表名称
----------	---------------

## 命令模式

全局配置模式

## 默认

无

## 使用说明

如果访问控制列表名称为一个已经存在的名称，则此命令表示进入 IPv6 访问控制列表配置模式；如果访问控制列表名称为新名称，则此命令表示创建此列表并进入 IPv6 访问控制列表配置模式；此处创建的访问控制列表配合 **match access-group** 命令使用，具体见相关章节。

## 举例说明

创建一个名为 `list_ipv6_1` 的 IPv6 访问控制列表并进入配置模式：

```
Switch(config)# ipv6 access-list list_ipv6_1
Switch(config-ipv6-acl)#
```

删除一个名为 `list_ipv6_1` 的 IPv6 访问控制列表：

```
Switch(config)# no ipv6 access-list list_ipv6_1
```

## 相关命令

**match access-group**

### 6.6.2 sequence-num

使用此命令删除指定的控制规则。

## 命令语法

**no sequence-num** *SEQUENCE-NUM*

SEQUENCE-NUM	序号范围 1~131071
--------------	---------------

## 命令模式

IPv6 ACL 模式

## 默认

无

## 使用说明

如果 ACL 所在的 class-map、class-map 所在的 policy-map 已经应用到端口，删除动作立即生效。

## 举例说明

IPv6 ACL 模式下删除序号为 10 的规则：

```
Switch(config-ipv6-acl)# no sequence-num 10
```

## 相关命令

**deny**

**deny tcp**

**deny udp**

**deny icmp**

**permit**

**permit tcp**

**permit udp**

**permit icmp**

### 6.6.3 remark

使用此命令给 IPv6 访问控制列表添加说明。

使用关键字 no 删除对访问控制列表的说明。

## 命令语法

**remark** *REMARK*

**no remark**

REMARK	所添加的说明
--------	--------

## 命令模式

IPv6 ACL 模式

## 默认

无

## 使用说明

所添加的说明最多可以有 100 个字符，超过的字符会被丢弃，不会被存储。

## 举例说明

为本列表添加说明 “remark of list for ipv6”:

```
Switch(config-ipv6-acl)# remark remark of list for ipv6
```

删除此列表说明:

```
Switch(config-ipv6-acl)# no remark
```

## 相关命令

**ipv6 access-list**

### 6.6.4 deny

使用此命令拒绝符合规则的 IPv6 报文通过端口。

## 命令语法

```
(SEQUENCE-NUM | ) deny (PROTO-NUM | any) (SOURCE-PREFIX | any | host
SOURCE) (DESTINATION-PREFIX | any | host DESTINATION) (routed-packet | )
(packet-length OPERATOR LENGTH | ) (time-range TIME-RANGE-NAME | )
```

SEQUENCE-NUM	此规则在 IPv6 访问控制列表中的顺序；如果没有指定此项，则系统会自动给此规则分配顺序号。范围是 1~131071
PROTO-NUM	协议编号，范围是 0~255
any	第一处 any 是指使用任何协议的 IPv6 报文
SOURCE-PREFIX	源地址为某一类的 IPv6 地址
any	第二处 any 是指地址可以为任何地址的主机

<b>host</b> SOURCE	源地址为特定地址的某台主机
DESTINATION-PREFIX	目的地址为某一类的 IPv6 地址
any	第三处 any 是指目的地址可以为任何地址的主机
<b>host</b> DESTINATION	目的地址为特定地址的某台主机
routed-packet	报文为路由报文
<b>time-range</b> TIME-RANGE-NAME	应用此选项可以产生基于时间的访问控制列表，详见相关章节
<b>packet-length</b> OPERATOR LENGTH	报文长度，范围是 64~16382，包括 eq (equal to)、lt (less than)、gt (greater than)、和 range

## 命令模式

IPv6 ACL 模式

## 默认

无

## 使用说明

如果序号为空，交换机会自动给此规则分配序号。而分配的序号是在现在存在的最大的序号的基础上有一个增量；如果现在的最大的序号是 100，则分配的序号就为 110（以 10 为增量）。

## 举例说明

- 添加规则：拒绝使用任何协议的任何报文通过。

```
Switch(config-ipv6-acl)# 1 deny any any any
```

- 添加规则：拒绝任何路由报文通过。

```
Switch(config-ipv6-acl)# 2 deny any any any routed-packet
```

## 相关命令

**no sequence-num**

### 6.6.5 deny tcp

使用此命令拒绝符合规则的 TCP 报文通过端口。

## 命令语法

```
(SEQUENCE-NUM | ) deny tcp (SOURCE-PREFIX | any | host SOURCE) (src-port OPERATOR PORT | ) (DESTINATION-PREFIX | any | host DESTINATION) (dst-port
```

*OPERATOR PORT* | ) ( **routed-packet** | ) ( **packet-length OPERATOR LENGTH** | ) ( **time-range TIME-RANGE-NAME** | )

SEQUENCE-NUM	此规则在 IPv6 访问控制列表中的顺序；如果没有指定此项，则系统会自动给此规则分配顺序号。范围是 1-131071
SOURCE-PREFIX	源地址为某一类的 IPv6 地址前缀
any	第一处 any 是指地址可以为任何地址的主机
<b>host</b> SOURCE	源地址为特定地址的某台主机
<b>src-port</b> OPERATOR PORT	源端口，范围是 0~65535，包括 eq (equal to)
DESTINATION-PREFIX	目的地址为某一类的 IPv6 地址前缀
any	第三处 any 是指目的地址可以为任何地址的主机
<b>host</b> DESTINATION	目的地址为特定地址的某台主机
<b>dst-port</b> OPERATOR PORT	目的端口，范围是 0~65535，包括 eq (equal to)
routed-packet	报文为路由报文
<b>time-range</b> TIME-RANGE-NAME	应用此选项可以产生基于时间的访问控制列表，详见相关章节
<b>packet-length</b> OPERATOR LENGTH	报文长度，范围是 64~16382，包括 eq (equal to)、lt (less than)、gt (greater than)、和 range

## 命令模式

IPv6 ACL 配置

## 默认

无

## 使用说明

无

## 举例说明

- 添加规则：拒绝任何 TCP 报文。

```
Switch(config-ipv6-acl)# 1 deny tcp any any
```



- 添加规则：拒绝 TCP 报文中源地址为 2001::2020，源端口号为 8080，目的地址为任意的报文。

```
Switch(config-ipv6-acl)# 2 deny tcp host 2001::2020 src-port eq 8080 any
```

## 相关命令

**no sequence-num**

### 6.6.6 deny udp

使用此命令拒绝符合规则的 UDP 报文通过端口。

## 命令语法

```
( SEQUENCE-NUM | ) deny udp ( SOURCE-PREFIX | any | host SOURCE ) ( src-port OPERATOR PORT | ) ( DESTINATION-PREFIX | any | host DESTINATION ) ( dst-port OPERATOR PORT | ) ( routed-packet | ) ( packet-length OPERATOR LENGTH | ) ( time-range TIME-RANGE-NAME | )
```

参数说明请见上文“deny tcp”。

## 命令模式

IPv6 ACL 模式

## 默认

无

## 使用说明

无

## 举例说明

添加规则：拒绝任何 UDP 报文通过。

```
Switch(config-ipv6-acl)# 1 deny udp any any
```

添加规则：拒绝 UDP 报文中源地址为 2001::2020，源端口号为 8080，目的地址为任意。

```
Switch(config-ipv6-acl)# 2 deny udp host 2001::2020 src-port eq 8080 any
```

## 相关命令

**no sequence-num**

### 6.6.7 deny icmp

使用此命令拒绝符合规则的 ICMP 报文通过端口。

## 命令语法

*(SEQUENCE-NUM |)* **deny icmp** (*SOURCE-PREFIX | any | host SOURCE*) (*DESTINATION-PREFIX | any | host DESTINATION*) (**icmp-type** *TYPE-NUM* (**icmp-code** *CODE-NUM* |)) (**routed-packet** |) (**packet-length** *OPERATOR LENGTH* |) (**time-range** *TIME-RANGE-NAME* |)

icmp-type <i>TYPE-NUM</i>	ICMP 报文类型，范围是 0~255
icmp-code <i>CODE-NUM</i>	ICMP 报文代码，范围是 0~255

其他参数说明请见上文“deny”部分描述。

## 命令模式

IPv6 ACL 模式

## 默认

无

## 使用说明

IPv6 访问控制列表配置模式

相关注意事项请见上文“deny tcp”。

## 举例说明

- 添加规则：拒绝使用 ICMP 协议的任何报文通过。  
Switch(config-ipv6-acl)# 1 deny icmp any any
- 添加规则：拒绝任何报文类型为 3，报文号为 3 的 ICMP 报文通过。  
Switch(config-ipv6-acl)# 2 deny icmp any any icmp-type 3 icmp-code 3

## 相关命令

**no sequence-num**

### 6.6.8 deny gre

使用此命令拒绝符合规则的 GRE 报文通过端口。

## 命令语法

*(SEQUENCE-NUM |)* **deny gre** (*SOURCE-PREFIX | any | host SOURCE*) (*DESTINATION-PREFIX | any | host DESTINATION*) (*flow-label FLOW-LABEL-VALUE*) (**key** *KEY* **mask** *KEY-MASK*) (**dscp** *DSCP* |) (**non-fragment**|**first-fragment**|**non-or-first-fragment**|**small-**

**fragment|non-first-fragment|) (routed-packet|) (options|) (packet-length OPERATOR LENGTH |) (time-range TIME-RANGE-NAME |)**

FLOW-LABEL-VALUE	流标签，范围 0~1048575
KEY	GRE 的 KEY，范围 0~4294967295
KEY-MASK	GRE 的 KEY 掩码，范围 0~0xFFFFFFFF

其他参数说明请见上文“deny”部分描述。

## 命令模式

IPv6 ACL 模式

## 默认

无

## 使用说明

过滤类型为 GRE 的报文。

## 举例说明

- 添加规则：拒绝任何 GRE 报文通过。  
Switch(config-ipv6-acl)# 1 deny gre any any key 0 mask 0
- 添加规则：拒绝 GRE 报文中源地址为 2000::1，目的地址为任意，key 为 10 的报文。  
Switch(config-ipv6-acl)# 2 deny gre host 2000::1 any key 10 mask 0xffffffff

## 相关命令

**no sequence-num**

## 6.6.9 deny nvgre

使用此命令拒绝符合规则的 NVGRE 报文通过端口。

## 命令语法

**(SEQUENCE-NUM |) deny nvgre (SOURCE-PREFIX | any | host SOURCE ) (DESTINATION-PREFIX | any | host DESTINATION) (flow-label FLOW-LABEL-VALUE |) (vsid VSID mask VSID-MASK) (dscp DSCP |) (non-fragment|first-fragment|non-or-first-fragment|small-fragment|non-first-fragment|) (routed-packet|) (options|) (packet-length OPERATOR LENGTH |) (time-range TIME-RANGE-NAME |)**

FLOW-LABEL-VALUE	流标签，范围 0~1048575
VSID	NVGRE 的 VSID，范围 0~16777215
VSID-MASK	NVGRE 的 VSID 掩码，范围 0~0xFFFFFFFF

其他参数说明请见上文“deny”部分描述。

## 命令模式

IPv6 ACL 模式

## 默认

无

## 使用说明

过滤类型为 NVGRE 的报文。

## 举例说明

- 添加规则：拒绝任何 NVGRE 报文通过。  
Switch(config-ipv6-acl)# 1 deny nvgre any any vsid 0 mask 0
- 添加规则：拒绝 NVGRE 报文中源地址为 2000::1，目的地址为任意，VSID 为 10 的报文。  
Switch(config-ipv6-acl)# 2 deny gre host 2000::1 any vsid 10 mask 0xffffffff

## 相关命令

**no sequence-num**

### 6.6.10 permit

使用此命令允许符合规则的 IPv6 报文通过端口。

## 命令语法

**(SEQUENCE-NUM | ) permit (PROTO-NUM | any ) (SOURCE-PREFIX | any | host SOURCE ) (DESTINATION-PREFIX | any | host DESTINATION) ( routed-packet | ) ( packet-length OPERATOR LENGTH | ) ( time-range TIME-RANGE-NAME | )**

SEQUENCE-NUM	此规则在 IPv6 访问控制列表中的顺序；如果没有指定此项，则系统会自动给此规则分配顺序号。范围是 1-131071
--------------	--

PROTO-NUM	协议编号，范围是 0~255
any	第一处 any 是指使用任何协议的 IPv6 报文
SOURCE-PREFIX	源地址为某一类的 IPv6 地址
any	第二处 any 是指地址可以为任何地址的主机
host SOURCE	源地址为特定地址的某台主机
DESTINATION-PREFIX	目的地址为某一类的 IPv6 地址
any	第三处 any 是指目的地址可以为任何地址的主机
host DESTINATION	目的地址为特定地址的某台主机
routed-packet	报文为路由报文
time-range TIME-RANGE-NAME	应用此选项可以产生基于时间的访问控制列表，详见相关章节
packet-length OPERATOR LENGTH	报文长度，范围是 64~16382，包括 eq (equal to)、lt (less than)、gt (greater than)、和 range

## 命令模式

IPv6 ACL 模式

## 默认

无

## 使用说明

如果顺序号为空，交换机会自动给此规则分配顺序号。而分配的顺序号是在现在存在的最大的顺序号的基础上有一个增量；如果现在的最大的顺序号是 100，则分配的顺序号就为 110（以 10 为增量）。

## 举例说明

- 添加规则：允许使用任何协议的任何报文通过。

```
Switch(config-ipv6-acl)# 1 permit any any any
```

- 添加规则：允许任何路由报文通过。

```
Switch(config-ipv6-acl)# 2 permit any any any routed-packet
```

## 相关命令

**no sequence-num**

## 6.6.11 permit tcp

使用此命令允许符合规则的 TCP 报文通过端口。

### 命令语法

```
(SEQUENCE-NUM |) permit tcp (SOURCE-PREFIX | any | host SOURCE) ( src-port OPERATOR PORT |) (DESTINATION-PREFIX | any | host DESTINATION) ( dst-port OPERATOR PORT |) ( routed-packet |) ( packet-length OPERATOR LENGTH |) ( time-range TIME-RANGE-NAME |)
```

SEQUENCE-NUM	此规则在 IPv6 访问控制列表中的顺序；如果没有指定此项，则系统会自动给此规则分配顺序号。范围是 1-131071
SOURCE-PREFIX	源地址为某一类的 IPv6 地址前缀
any	第一处 any 是指地址可以为任何地址的主机
host SOURCE	源地址为特定地址的某台主机
src-port OPERATOR PORT	源端口，范围是 0~65535，包括 eq (equal to)
DESTINATION-PREFIX	目的地址为某一类的 IPv6 地址前缀
any	第三处 any 是指目的地址可以为任何地址的主机
host DESTINATION	目的地址为特定地址的某台主机
dst-port OPERATOR PORT	目的端口，范围是 0~65535，包括 eq (equal to)
routed-packet	报文为路由报文
time-range TIME-RANGE-NAME	应用此选项可以产生基于时间的访问控制列表，详见相关章节
packet-length OPERATOR LENGTH	报文长度，范围是 64~16382，包括 eq (equal to)、lt (less than)、gt (greater than)、和 range

### 命令模式

IPv6 ACL 配置

### 默认

无

## 使用说明

无

## 举例说明

- 添加规则：允许任何 TCP 报文。

```
Switch(config-ipv6-acl)# 1 permit tcp any any
```

- 添加规则：允许 TCP 报文中源地址为 2001::2020，源端口号为 8080，目的地址为任意的报文。

```
Switch(config-ipv6-acl)# 2 permit tcp host 2001::2020 src-port eq 8080 any
```

## 相关命令

**no sequence-num**

### 6.6.12 permit udp

使用此命令允许符合规则的 UDP 报文通过端口。

## 命令语法

```
( SEQUENCE-NUM | ) permit udp ( SOURCE-PREFIX | any | host SOURCE ) ( src-port OPERATOR PORT | ) ( DESTINATION-PREFIX | any | host DESTINATION ) ( dst-port OPERATOR PORT | ) ( routed-packet | ) ( packet-length OPERATOR LENGTH | ) ( time-range TIME-RANGE-NAME | )
```

参数说明请见上文“permit tcp”。

## 命令模式

IPv6 ACL 模式

## 默认

无

## 使用说明

无

## 举例说明

添加规则：允许任何 UDP 报文通过。

```
Switch(config-ipv6-acl)# 1 permit udp any any
```

添加规则：允许 UDP 报文中源地址为 2001::2020，源端口号为 8080，目的地址为任意。

```
Switch(config-ipv6-acl)# 2 permit udp host 2001::2020 src-port eq 8080 any
```

## 相关命令

**no sequence-num**

### 6.6.13 permit icmp

使用此命令允许符合规则的 ICMP 报文通过端口。

## 命令语法

*(SEQUENCE-NUM |)* **permit icmp** (*SOURCE-PREFIX | any | host SOURCE*) (*DESTINATION-PREFIX | any | host DESTINATION*) (**icmp-type** *TYPE-NUM* (**icmp-code** *CODE-NUM* |)) (**routed-packet** |) (**packet-length** *OPERATOR LENGTH* |) (**time-range** *TIME-RANGE-NAME* |)

icmp-type <i>TYPE-NUM</i>	ICMP 报文类型，范围是 0~255
icmp-code <i>CODE-NUM</i>	ICMP 报文代码，范围是 0~255

其他参数说明请见上文“permit”部分描述。

## 命令模式

IPv6 ACL 模式

## 默认

无

## 使用说明

IPv6 访问控制列表配置模式

相关注意事项请见上文“permit tcp”。

## 举例说明

- 添加规则：允许使用 ICMP 协议的任何报文通过。

```
Switch(config-ipv6-acl)# 1 permit icmp any any
```

- 添加规则：允许任何报文类型为 3，报文号为 3 的 ICMP 报文通过。

```
Switch(config-ipv6-acl)# 2 permit icmp any any icmp-type 3 icmp-code 3
```

## 相关命令

**no sequence-num**



## 6.6.14 permit gre

使用此命令允许符合规则的 GRE 报文通过端口。

### 命令语法

*(SEQUENCE-NUM | ) permit gre (SOURCE-PREFIX | any | host SOURCE ) (DESTINATION-PREFIX | any | host DESTINATION) (flow-label FLOW-LABEL-VALUE) (key KEY mask KEY-MASK) (dscp DSCP | ) (non-fragment|first-fragment|non-or-first-fragment|small-fragment|non-first-fragment) (routed-packet) (options) (packet-length OPERATOR LENGTH |) (time-range TIME-RANGE-NAME |)*

FLOW-LABEL-VALUE	流标签，范围 0~1048575
KEY	GRE 的 KEY，范围 0~4294967295
KEY-MASK	GRE 的 KEY 掩码，范围 0~0xFFFFFFFF

其他参数说明请见上文“deny gre”。

### 命令模式

IPv6 ACL 模式

### 默认

无

### 使用说明

过滤类型为 GRE 的报文。

### 举例说明

- 添加规则：允许任何 GRE 报文通过。  
Switch(config-ipv6-acl)# 1 permit gre any any key 0 mask 0
- 添加规则：允许 GRE 报文中源地址为 2000::1，目的地址为任意，key 为 10 的报文。  
Switch(config-ipv6-acl)# 2 permit gre host 2000::1 any key 10 mask 0xffffffff

### 相关命令

**no sequence-num**

## 6.6.15 permit nvgre

使用此命令允许符合规则的 NVGRE 报文通过端口。

## 命令语法

*(SEQUENCE-NUM | ) permit nvgre (SOURCE-PREFIX | any | host SOURCE) (DESTINATION-PREFIX | any | host DESTINATION) (flow-label FLOW-LABEL-VALUE |) (vsid VSID mask VSID-MASK) (dscp DSCP |) (non-fragment|first-fragment|non-or-first-fragment|small-fragment|non-first-fragment|) (routed-packet|) (options|) (packet-length OPERATOR LENGTH |) (time-range TIME-RANGE-NAME |)*

FLOW-LABEL-VALUE	流标签，范围 0~1048575
VSID	NVGRE 的 VSID，范围 0~16777215
VSID-MASK	NVGRE 的 VSID 掩码，范围 0~0xFFFFFFFF

其他参数说明请见上文“deny nvgre”。

## 命令模式

IPv6 ACL 模式

## 默认

无

## 使用说明

过滤类型为 NVGRE 的报文。

## 举例说明

- 添加规则：允许任何 NVGRE 报文通过。  
Switch(config-ipv6-acl)# 1 permit nvgre any any vsid 0 mask 0
- 添加规则：允许 NVGRE 报文中源地址为 2000::1，目的地址为任意，VSID 为 10 的报文。  
Switch(config-ipv6-acl)# 2 permit gre host 2000::1 any vsid 10 mask 0xffffffff

## 相关命令

**no sequence-num**

### 6.6.16 show access-list ipv6

使用此命令查看 IPv6 访问控制列表。

## 命令语法

**show access-list ipv6 (ACL-NAME |)**

ACL-NAME	IPv6 访问控制列表名称
----------	---------------

## 命令模式

特权模式

## 默认

无

## 使用说明

查看访问控制列表的内容。

## 举例说明

查看 ipv6 访问控制列表：

```
Switch# show access-list ipv6
ipv6 access-list list_ipv6_1
  10 deny any 2001::/48 any
  20 permit any any any
```

## 相关命令

**ipv6 access-list**

## 6.7 IEEE 802.1x 命令

### 6.7.1 dot1x system-auth-ctrl

使用dot1x system-auth-ctrl命令，全局启用dot1x认证功能。

在原命令之前加上关键字"no"，删除上述配置。

## 命令语法

**dot1x system-auth-ctrl**

**no dot1x system-auth-ctrl**

## 命令模式

全局配置模式

## 默认

关闭 dot1x 认证功能

## 使用说明

无.

## 举例说明

在全局配置模式下启用和关闭dot1x认证功能

```
Switch(config)# dot1x system-auth-ctrl  
Switch(config)# no dot1x system-auth-ctrl
```

## 相关命令

**show dot1x**

**dot1x port-control**

## 6.7.2 dot1x initialize

使用“dot1x initialize”命令，可以强制某一个使能了dot1x认证的端口恢复到初始状态，即“未授权”状态。

## 命令语法

**dot1x initialize interface *interface-NAME***

interface-NAME	指定一个需要恢复初始状态的接口名
----------------	------------------

## 命令模式

特权模式

## 默认

无

## 使用说明

使用这个命令来初始化一个端口上的IEEE 802.1x状态机，这个端口将开始一个全新的认证过程。

使用这条命令之后，指定端口上的认证状态恢复到未授权状态。

## 举例说明

在特权模式下重新开始eth-0-1的dot1x认证。

```
Switch# dot1x initialize interface eth-0-1
```

## 相关命令

**show dot1x**

### 6.7.3 dot1x max-req

使用“dot1x max-req”命令，设置交换机在认证不通过的情况下，向用户发起重新认证请求的最大尝试次数。

在原命令之前加上关键字“no”，恢复默认配置。

## 命令语法

**dot1x max-req***count*

**nodot1x max-req**

<code>dot1x max-req count</code>	交换机向用户发起重新认证请求的最大尝试次数，范围 1-10
--------------------------------------	-------------------------------

## 命令模式

端口配置模式

## 默认

2

## 使用说明

修改这个最大尝试次数，只是为了应对某些特殊情况：例如不可靠的链接、某些客户端和认证服务器的具体行为等。

缺省尝试重认证次数为2次。

## 举例说明

在端口配置模式下，配置交换机向用户发起重新认证请求的最大尝试次数为4次。

```
Switch(config-if)# dot1x dot1x max-req 4
```

## 相关命令

**show dot1x**

## 6.7.4 dot1x port-control

使用“dot1x port-control”命令在端口上启用dot1x认证功能。

在原命令之前加上关键字“no”，删除上述配置。

### 命令语法

**dot1x port-control** ( **auto** | **force-authorized** | **force-unauthorized** | **dir** ( **both** | **in** ) )

**no dot1x port-control**

auto	设置本端口根据认证结果自动设置端口状态
force-authorized	强制本端口的状态为已认证
force-unauthorized	强制本端口的状态为未认证
dir	设置报文控制方向
both	丢弃发送和接受的报文
in	只丢弃接受的报文

### 命令模式

端口配置模式

### 默认

使能 dot1x 认证后，默认只对入方向的报文进行控制。

### 使用说明

全局必须使能dot1x认证功能。（详见“dot1x system-auth-ctrl”命令说明。）

端口默认不使能dot1x认证功能。使能dot1x认证后，默认只对入方向的报文进行控制。

### 举例说明

在端口配置模式下使能dot1x认证功能，根据认证结果自动设置端口状态。

```
Switch(config-if)# dot1x port-control auto
```

### 相关命令

**show dot1x**

## 6.7.5 dot1x protocol-version

使用“dot1x protocol-version”命令设置EAPOL协议报文的版本。

在原命令之前加上关键字“no”，恢复默认配置。

### 命令语法

**dot1x protocol-version** *version*

**no dot1x protocol-version**

<code>protocol-version version</code>	设置 EAPOL 协议报文版本<1-2>. 默认版本为 2
---	-------------------------------

### 命令模式

端口配置模式

### 默认

默认EAPOL协议报文版本为2。

### 使用说明

必须先端口使能dot1x功能，然后才能配置EAPOL协议报文的版本。（详见“dot1x port-control”命令说明）。

### 举例说明

在端口配置模式下配置EAPOL协议报文的版本为1。

```
Switch(config-if)# dot1x protocol-version 1
```

### 相关命令

**show dot1x**

## 6.7.6 dot1x timeout quiet-period

使用“dot1x timeout quiet-period”命令设置端口在验证失败以后的静默时间。

在原命令之前加上关键字“no”，恢复默认配置。

### 命令语法

**dot1x timeout quiet-period** *seconds*

**no dot1x timeout quiet-period**

<code>quiet-period</code> <i>seconds</i>	端口在认证失败后的静默时间；以秒为单位，范围 1-65535
---	--------------------------------

## 命令模式

端口配置模式

## 默认

缺省端口在验证失败后的静默时间为60秒。

## 使用说明

在静默期间，交换机不接受或发起任何身份验证请求。如果你想给用户提供更快的响应时间，输入一个小于默认的数值。

## 举例说明

在端口配置模式下设置端口在认证失败后的静默时间为100秒。

```
Switch(config-if)# dot1x timeout quiet-period 100
```

## 相关命令

**show dot1x**

### 6.7.7 dot1x reauthentication

使用“dot1x reauthentication”命令,在端口启用周期性重新认证功能。

在原命令之前加上关键字“no”，删除上述配置。

## 命令语法

**dot1x reauthentication**

**no dot1x reauthentication**

## 命令模式

端口配置模式

## 默认

缺省端口没有开启周期性重新认证功能。



## 使用说明

当周期性重新认证不使能的时候，重认证的超时时间配置是无效的。

## 举例说明

在端口配置模式下，启用周期性重新认证功能。

```
Switch(config-if)# dot1x reauthentication
```

## 相关命令

**show dot1x**

**dot1x timeout**

## 6.7.8 dot1x re-authenticate

使用“dot1x re-authenticate”命令,使接口重新开始dot1x认证。

## 命令语法

**dot1x re-authenticate interface** *interface-NAME*

<b>interface</b> interface-name	指定一个需要重新开始 dot1x 认证的接口名
---------------------------------	-------------------------

## 命令模式

特权模式

## 默认

无

## 使用说明

使用此命令在指定的端口上发起重新认证，不需要等待周期性重认证时间。

## 举例说明

在eth-0-1端口上进行重新认证。

```
Switch# dot1x re-authenticate interface eth-0-1
```

## 相关命令

**show dot1x**

## 6.7.9 dot1x timeout

使用“dot1x timeout”命令设置端口的dot1x定时器。

在原命令之前加上关键字“no”，恢复dot1x定时器为默认值。

### 命令语法

**dot1x timeout** (re-authperiod *seconds* | server-timeout *seconds* | supp-timeout *seconds* | tx-period *seconds*)

**no dot1x timeout** ( reauth-period | server-timeout | supp-timeout | tx-period)

re-authperiod <i>seconds</i>	设置强制重新认证的超时时间；缺省为 3600 秒，取值范围<60-65535>
server-timeout <i>seconds</i>	设置等待认证服务器回复的超时时间；缺省为 30 秒，取值范围<1-65535>
supp-timeout <i>seconds</i>	设置等待客户端回复的超时时间；缺省为 30 秒，取值范围<1-65535>
tx-period <i>seconds</i>	设置同一 ID 发送连续请求的时间间隔；缺省为 30 秒，取值范围<1-65535>

### 命令模式

端口配置模式

### 默认

重新认证的时间默认为3600秒；

连续请求时间间隔默认为30秒；

客户端超时时间默认为30秒；

服务器超时时间默认为30秒。

### 使用说明

修改这些定时器的时间长度，只是为了应对某些特殊情况：例如不可靠的链接、某些客户端和认证服务器的具体行为等。

重新认证的时间间隔只有在使能了周期性重认证的时候才有效。

### 举例说明

设置周期性重新认证的间隔时间为4000秒。

```
Switch(config-if)# dot1x reauthentication
```

```
Switch(config-if)# dot1x timeout reauth-period 4000
```

## 相关命令

**dot1x reauthentication**

**show dot1x**

### 6.7.10 dot1x guest-vlan

使用“dot1x guest-vlan”命令，配置dot1x guest vlan功能。

在原命令之前加上关键字“no”，删除该配置。

## 命令语法

**dot1x guest-vlan** *VLANid*

**no dot1x guest-vlan**

VLANid	指定一个可用的 vlan 作为 dot1x guest vlan。有效范围是 2-4094
--------	---

## 命令模式

端口配置模式

## 默认

默认情况下系统没有配置guest vlan。

## 使用说明

配置一个guest vlan后，使能了dot1x认证的端口，在客户端通过认证之前都属于该vlan。

Guest vlan功能对三层接口和trunk口无效，只能使用在access接口上。

## 举例说明

配置vlan 5 作为接口eth-0-1上的dot1x guest vlan。

```
Switch(config)#vlan database
Switch(config-vlan)#vlan 5
Switch(config-vlan)#exit
Switch(config)# interface eth-0-1
Switch(config-if)#switchport mode access
Switch(config-if)#dot1x port-control auto
Switch(config-if)#dot1x guest-vlan 5
```

可以在特权模式下使用“show dot1x [interface interface-id]”检查配置。

## 相关命令

**show dot1x** [*interface interface-id*]

### 6.7.11 show dot1x

使用“show dot1x”命令查看802.1x的全局配置信息。

## 命令语法

**show dot1x** ((agnostics | session-statistics | statistics) (all | interface *interface-id*) | all |)

diagnostics	查看指定端口的 802.1x 诊断信息
session-statistics	查看指定端口的 802.1x 会话统计信息
statistics	查看 EAPOL 包的统计信息
all	命令查看 802.1x 的全局配置信息
<b>interface interface-id</b>	指定的接口

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

查看802.1x的全局配置信息。

```
Switch# show dot1x statistics interface eth-0-1
802.1X statistics for interface eth-0-1
  EAPOL Frames Rx: 0 - EAPOL Frames Tx: 323
  EAPOL Start Frames Rx: 0 - EAPOL Logoff Frames Rx: 0
  EAP Rsp/Id Frames Rx: 0 - EAP Response Frames Rx: 0
  EAP Req/Id Frames Tx: 241 - EAP Request Frames Tx: 0
  Invalid EAPOL Frames Rx: 0 - EAP Length Error Frames Rx: 0
  EAPOL Last Frame Version Rx: 0 - EAPOL Last Frame Src: 0000.0000.0000
```

## 相关命令

**dot1x system-auth-ctrl**

**dot1x port-control**

### 6.7.12 debug dot1x

使用此命令可以打开dot1x的模块的调试功能。

在原命令之前加上关键字“no”，关闭调试功能。

## 命令语法

**debug dot1x ( event | timer | packet | all )**

**no debug dot1x ( event | timer | packet | all )**

event	调试 dot1x 事件信息
timer	dot1x 的定时器信息调试信息
packet	dot1x 的数据包信息的调试信息，包括发送和接收
all	上面提到的所有调试信息

## 命令模式

特权模式

## 默认

无

## 使用说明

使用“terminal monitor”打印消息

## 举例说明

使用如下命令，打开dot1x的所有调试信息。

```
Switch# debug dot1x all
```

## 相关命令

**terminal monitor**

**show logging buffer**

## 6.7.13 clear dot1x

使用“clear dot1x”命令来清空dot1x统计数据。

### 命令语法

**clear dot1x (statistics | session-statistics) (all )**

statistics	清空 EAPOL 报文的统计信息
session-statistics	清空 dot1x 客户端会话的统计信息
all	清空所有统计信息

### 命令模式

特权模式

### 默认

无

### 使用说明

使用“clear dot1x”命令来清空dot1x统计数据。

使用“show dot1x”命令可以看到统计数据。

### 举例说明

在特权模式下使用“clear dot1x”命令

```
Switch# clear dot1x statistics
Switch# clear dot1x session-statistics
```

### 相关命令

**dot1x system-auth-ctrl**

**dot1x port-control**

**show dot1x**

## 6.7.14 dot1x re-activate radius-server

使用此命令可以立即激活因认证失败而处于“未激活”状态的Radius服务器。

### 命令语法

**dot1x re-activate radius-server [ host ip-address ] [ auth-port port-number ]**

**dot1x re-activate radius-server [ interface interface-number | all ]**

ip-address	指定 IP 地址
port-number	UDP 端口号
interface-number	为指定的客户端接口，取值范围为 eth-<0-0>-<1-54>
all	激活所有的 Radius 服务器

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

在特权模式下，激活因认证失败而处于“未激活”状态的Radius服务器：

```
Switch # dot1x re-activate radius-server
Switch # dot1x re-activate radius-server host 3.3.3.3 auth-port 1812
Switch # dot1x re-activate radius-server interface eth-0-9
```

## 6.7.15 dot1x mandatory-domain

使用此命令设置端口认证所属的域，若没有配置所属域，则使用默认域。

使用no命令删除配置的域名。

## 命令语法

**dot1x mandatory-domain** *name*

**no dot1x mandatory-domain** *name*

name	配置端口认证指定的域名
------	-------------

## 命令模式

接口配置模式

## 默认

无

## 使用说明

使用domain命令添加了相关域后，用户可以使用**dot1x mandatory-domain**命令配置端口认证所属的域。

## 举例说明

在端口配置模式下，设置端口认证所属的域：

```
Switch(config-if)# dot1x mandatory-domain inspur
```

## 6.7.16 radius scheme

使用此命令可以创建Radius服务器组。

使用**no**命令取消此配置。

## 命令语法

**radius scheme** *group-name*

**no radius scheme** *group-name*

group-name	Radius 服务器组名
------------	--------------

## 命令模式

特权模式

## 默认

无

## 使用说明

多域认证模式下，使用此命令创建Radius服务器组。

## 举例说明

在特权模式下，使用本命令创建Radius服务器组，并通过**authentication server**命令指定Radius服务器组中关联的服务器IP地址：

```
Switch(config)# radius scheme test
```

```
Switch(config-scheme)# authentication server 1.1.1.1
```

## 6.7.17 authentication server

使用此命令指定Radius服务器组关联的服务器IP地址。

使用**no**命令取消此配置。



## 命令语法

**authentication server** *ip-address*

**no authentication server** *ip-address*

ip-address	Radius 服务器组关联的服务器 IP 地址
------------	-------------------------

## 命令模式

特权模式

## 默认

无

## 使用说明

使用**radius scheme**命令创建服务器组后，使用此命令指定Radius 服务器组关联的服务器IP地址。

## 举例说明

指定Radius 服务器组关联的服务器IP地址：

```
Switch(config)# radius scheme test
```

```
Switch(config-scheme)# authentication server 1.1.1.1
```

## 6.7.18 domain

使用此命令创建dot1x认证域。

使用**no**命令取消此配置。

## 命令语法

**domain** *name*

**no domain** *name*

name	认证域域名
------	-------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

在特权模式下，创建dot1x认证域：

```
Switch(config)# domain test
```

## 6.7.19 authentication radius-scheme

使用此命令可以设置dot1x认证域所关联的Radius服务器组。

使用**no**命令取消此配置。

## 命令语法

**authentication radius-scheme** *group-name*

**no authentication radius-scheme**

group-name	Dot1x 认证域所关联的 Radius 服务器组名
------------	----------------------------

## 命令模式

特权模式

## 默认

无

## 使用说明

使用**domain**命令创建认证域后，使用本命令设置dot1x认证域所关联的Radius服务器组。

## 举例说明

在特权模式下，设置dot1x认证域所关联的Radius服务器组。

```
Switch(config)# domain domainname
```

```
Switch(config-domain)# authentication radius-scheme test
```

## 6.7.20 domain default enable

使用此命令设置dot1x认证及SSH认证默认域。

使用**no**命令取消此配置。

## 命令语法

**domain default enable *name***

**no domain default enable**

name	Dot1x 认证默认域名
------	--------------

## 命令模式

特权模式

## 默认

无

## 使用说明

使用**domain**命令创建认证域后，使用此命令设置dot1x认证及SSH登录认证默认域。

## 举例说明

在特权模式下，设置dot1x认证默认域。

```
Switch(config)# domain default enable domainname
```

## 6.7.21 show radius-server-group all

使用此命令显示dot1x的所有Radius服务器组状态。

## 命令语法

**show radius-server-group all**

## 命令模式

特权模式

## 默认

无

## 使用说明

此命令不显示已激活状态和非激活状态下的Radius服务器组状态。

## 举例说明

在特权模式下，显示dot1x的所有Radius服务器组状态：

```
Switch# show radius-server-group all
```

## 6.7.22 dot1x auth-free

使用此命令表明部分设备不支持dot1x，无需进行认证。

### 命令语法

**dot1x auth-free** [ **user mac** *mac-address* | **vlan** *vlan-id* ]

mac-address	无需认证设备的用户 MAC 地址
vlan-id	无需认证设备的 VLAN ID

### 命令模式

特权模式

### 默认

无

### 使用说明

无

### 举例说明

在特权模式下，设备不支持dot1x，无需进行认证：

```
Switch# dot1x auth-free
```

## 6.7.23 clear dot1x statistics

使用此命令来清空 dot1x 统计数据。

### 命令语法

**clear dot1x statistics** [ **interface** *interface-number* ]

interface-number	指定的客户端接口
------------------	----------

### 命令模式

特权模式

### 默认

无

### 使用说明

使用此命令可以清空指定的客户端接口dot1x统计数据。

## 举例说明

在特权模式下，清空dot1x统计数据：

```
Switch# clear dot1x statistics
```

## 6.8 Arp Inspection 命令

### 6.8.1 show ip arp inspection

使用此命令查看 arp inspection 的配置。

#### 命令语法

```
show ip arp inspection
```

#### 命令模式

特权模式

#### 默认

无

#### 使用说明

显示 arp inspection 的配置及其统计。

#### 举例说明

显示 arp inspection 配置。

```
Switch # show ip arp inspection
Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled
Vlan      Configuration    ACL Match      Static ACL
=====
1         enabled          acl
Vlan      ACL Logging      DHCP Logging
=====
1         deny             deny
Vlan      Forwarded        Dropped        DHCP Drops     ACL Drops
=====
1         0                 0              0              0
Vlan      DHCP Permits     ACL Permits     Source MAC Failures
=====
1         0                 0              0
Vlan      Dest MAC Failures IP Validation Failures Invalid Protocol Data
=====
1         0                 0              0
```

## 相关命令

**ip arp inspection vlan**

### 6.8.2 show ip arp inspection interfaces

此命令查看端口是否被设置为可信任端口。

## 命令语法

**show ip arp inspection interfaces** (*IFNAME*)

IFNAME	接口名称
--------	------

## 命令模式

特权模式

## 默认

无

## 使用说明

查看端口是否为可信任端口。

## 举例说明

查看所有端口是否为可信，详细参见如下。

```
Switch # show ip arp inspection interfaces
Interface      Trust State
=====
eth-0-1        untrusted
eth-0-2        untrusted
eth-0-3        untrusted
eth-0-4        untrusted
eth-0-5        untrusted
eth-0-6        untrusted
eth-0-7        untrusted
eth-0-8        untrusted
eth-0-9        untrusted
eth-0-10       untrusted
eth-0-11       untrusted
eth-0-12       untrusted
eth-0-13       untrusted
eth-0-14       untrusted
eth-0-15       untrusted
eth-0-16       untrusted
```

```
eth-0-17      untrusted
eth-0-18      untrusted
eth-0-19      untrusted
eth-0-20      untrusted
eth-0-21      untrusted
eth-0-22      untrusted
eth-0-23      untrusted
eth-0-24      untrusted
eth-0-25      untrusted
eth-0-26      untrusted
eth-0-27      untrusted
eth-0-28      untrusted
eth-0-29      untrusted
eth-0-30      untrusted
eth-0-31      untrusted
eth-0-32      untrusted
eth-0-33      untrusted
eth-0-34      untrusted
eth-0-35      untrusted
eth-0-36      untrusted
eth-0-37      untrusted
eth-0-38      untrusted
eth-0-39      untrusted
eth-0-40      untrusted
eth-0-41      untrusted
eth-0-42      untrusted
eth-0-43      untrusted
eth-0-44      untrusted
eth-0-45      untrusted
eth-0-46      untrusted
eth-0-47      untrusted
eth-0-48      untrusted
```

## 相关命令

**ip arp inspection trust**

### 6.8.3 show ip arp inspection log

此命令查看 ARP Inspection 日志信息。默认 LOG 32 条。

## 命令语法

**show ip arp inspection log** (*NUMber*)

NUMber	指定消息的条目，范围是 1 到 1024
--------	----------------------

## 命令模式

特权模式

## 默认

无

## 使用说明

查看所有 ARP Inspection 记录。

## 举例说明

查看所有 ARP Inspection 日志消息。

```
Switch # show ip arp inspection log
Total Log Buffer Size : 32
Syslog rate : 5 entries per 1 seconds.
No entries in log buffer
```

## 相关命令

**ip arp inspection log-buffer**

### 6.8.4 show ip arp inspection statistics

此命令查看 ARP Inspection 统计信息。包含 MAC 验证失败，IP 验证失败的 ACL 允许和拒绝的，DHCP 允许和拒绝。

## 命令语法

**show ip arp inspection statistics (vlan *VLAN\_id*)**

<b>vlan</b> <i>VLAN_id</i>	VLAN 范围: 1,3-5,7,9-11
----------------------------	-----------------------

## 命令模式

特权模式

## 默认

无

## 使用说明

查看所有 VLAN 的 ARP Inspection 统计信息。

## 举例说明

查看 VLAN 2 的 ARP Inspection 统计信息。



```

Switch # show ip arp inspection statistics vlan 1
Vlan      Forwarded      Dropped      DHCP Drops      ACL Drops
=====
1         0              0            0              0
Vlan      DHCP Permits    ACL Permits    Source MAC Failures
=====
1         0              0            0
Vlan      Dest MAC Failures  IP Validation Failures  Invalid Protocol Data
=====
1         0              0              0

```

## 相关命令

**clear ip arp inspection statistics**

### 6.8.5 show ip arp inspection vlan

此命令查看指定 vlan 上的 ARP Inspection 配置信息。

## 命令语法

**show ip arp inspection vlan** *VLAN\_id*

<b>vlan</b> <i>VLAN_id</i>	VLAN 范围 1, 3-5, 7, 9-11
----------------------------	-------------------------

## 命令模式

特权模式

## 默认

无

## 使用说明

如果没有 VLAN 被指定，那么将无法被显示 VLAN 的 inspection 信息。

## 举例说明

查看此 VLAN 1 的 ARP Inspection 统计信息。

```

Switch # show ip arp inspection vlan 1
Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled
Vlan      Configuration    ACL Match    Static ACL
=====
1         enabled          acl
Vlan      ACL Logging      DHCP Logging

```

```
=====
1          deny          deny
```

## 相关命令

**ip arp inspection vlan**

### 6.8.6 show debugging arp inspection

使用此命令调试 arp inspection 信息。

## 命令语法

**show debugging arp inspection**

## 命令模式

特权模式

## 默认

默认不开启。

## 使用说明

无

## 举例说明

显示交换机的 arp inspection 调试信息。

```
Switch# show debugging arp inspection
arp inspection debugging status:
  packet debugging is on
  error debugging is on
```

## 相关命令

**debug arp inspection**

### 6.8.7 debug arp inspection

使用此命令配置 arp inspection 的调试功能。

## 命令语法

**debug arp inspection (all|packet|events|error)**

all	打开所有的 debug 信息
-----	----------------

packet	ARP 消息
events	ARP 查看事件
error	错误的 dhcp 消息

## 命令模式

特权模式

## 默认

无

## 使用说明

使用此命令配置 arp inspection 的调试功能包含：all, error, events, packet。

## 举例说明

设置交换机打开 arp inspection 的 error 调试功能。

```
Switch # debug ip arp inspection error
```

## 相关命令

**show debugging arp inspection**

## 6.8.8 ip arp inspection filter

此命令为指定 VLAN 添加 ARP 访问控制列表。

使用关键字 no 删除指定 VLAN 上的 ARP 访问控制列表。

## 命令语法

**ip arp inspection filter** *ACL* **vlan** *VLAN\_id* (**static**)

ACL	ARP 访问控制列表
VLAN_id	应用此 arp-acl 到此 vlan-range; 比如 1, 1-3 等
static	如果指定此项, 则不匹配此访问控制列表的报文会被丢掉; 否则, 当报文不匹配此访问控制列表时, 交换机会继续查找 DHCP Snooping 表, 如果匹配, 则转发; 如果不匹配, 则丢弃

## 命令模式

全局配置模式

## 默认

无

## 使用说明

在 vlan 上引用 arp 的访问控制列表。默认情况下 VLAN 上不指定任何的 arp 访问控制列表。

## 举例说明

在 VLAN2 上引用 arp 访问控制列表。

```
Switch(config)# ip arp inspection filter acl vlan 2 static
```

## 相关命令

**arp access-list**

### 6.8.9 ip arp inspection log-buffer entries

此命令设置 ARP Inspection 日志记录的数量。

使用关键字 no 恢复此设置为默认值。

## 命令语法

**ip arp inspection log-buffer entries *NUMBER***

NUMBER	设置可记录到日志缓冲区的 ARP Inspection 日志最大数量，设置范围<10-1024>
--------	--

## 命令模式

全局配置模式

## 默认

无

## 使用说明

缺省可记录到日志缓冲区的 ARP Inspection 日志最大数量为 32。

## 举例说明

设置可记录到日志缓冲区的 ARP Inspection 日志数量为 10。

```
Switch(config)# ip arp inspection log-buffer entries 10
```

## 相关命令

**show ip arp inspection log**

### 6.8.10 ip arp inspection log-buffer logs interval

设置单位周期内可记录到日志缓冲区的 ARP Inspection 日志最大数量。

## 命令语法

**ip arp inspection log-buffer logs** *NUMber interval interval*

NUMber	设置可记录到日志缓冲区的 ARP Inspection 日志最大数量，设置范围<0-1024>
interval	设置记录 Arp Inspection 日志的最大速率；单位为每秒，设置范围<0-86400>

## 命令模式

全局配置模式

## 默认

无

## 使用说明

0 表示所有的 ARP Inspection 日志都不会记录到系统日志；

缺省记录 Arp Inspection 日志的最大速率为每秒 5 个。

## 举例说明

设置可记录到系统日志的 ARP Inspection 日志数量每两秒 2 个。

```
Switch(config)# ip arp inspection log-buffer logs 12 interval 2
```

### 6.8.11 ip arp inspection validate

此命令设置验证 ARP 报文中的指定字段。

使用关键字 **no** 恢复此设置为默认值。

## 命令语法

**[no] ip arp inspection validate (dst-mac|ip|src-mac)**

dst-mac	设置验证目的 MAC 地址
ip	设置验证 IP 地址
src-mac	设置验证源 MAC 地址

## 命令模式

全局配置模式

## 默认

无

## 使用说明

**src-mac:** 检查以太网报头中的源 mac，检查 ARP 请求和响应。一旦启用，如果发现不匹配的源 mac 将被丢弃。

**dst-mac:** 检查以太网报头中的目的 mac，检查 ARP 请求和响应。一旦启用，如果发现不匹配的目的 mac 将被丢弃。

**IP:** 检查以太网报文中的目的 IP 字段是否合法。

缺省 ARP Inspection 不验证 ARP 报文的任何字段。

## 举例说明

设置 ARP Inspection 验证目的 MAC。

```
Switch(config)# ip arp inspection validate dst-mac
```

## 相关命令

**show ip arp inspection**

### 6.8.12 ip arp inspection vlan

此命令在指定 VLAN 上启用 ARP Inspection。

使用关键字 no 在指定 VLAN 上关闭 ARP Inspection。

## 命令语法

**[no] ip arp inspection vlan *VLAN\_id***

VLAN_id	在此 vlan-range 上启用 ARP Inspection; 格式为 1, 1-10
---------	---

## 命令模式

全局配置模式

## 默认

无

## 使用说明

在 VLAN 上启用 arp inspection。

## 举例说明

设置交换机 VLAN2 上启用 arp inspection。

```
Switch(config)# ip arp inspection vlan 2
```

## 相关命令

**show ip arp inspection vlan 2**

## 6.8.13 ip arp inspection vlan WORD logging acl-macth

使用此命令对 arp inspection 的日志进行过滤。

## 命令语法

**[no] ip arp inspection vlan *VLAN\_id* logging acl-macth (matchlog|none)**

VLAN_id	VLAN 范围,例如: 1,3-5,7,9-11
matchlog	将匹配的信息记录日志文件
none	将不匹配的信息记录日志文件

## 命令模式

全局配置模式

## 默认

无

## 使用说明

根据访问控制列表来过滤相应的日志消息。

## 举例说明

设置交换机的 VLAN2 允许 arp 包。

```
Switch(config)# ip arp inspection vlan 2 logging acl-match matchlog
```

## 相关命令

**ip arp inspection vlan**

### 6.8.14 ip arp inspection vlan logging dhcp-bindings (all | none | permit)

使用此命令根据 dhcp 绑定表来过滤日志文件。

## 命令语法

**[no] ip arp inspection vlan *VLAN\_id* logging dhcp-bindings (all|none|permit)**

VLAN_id	VLAN 范围,例如: 1, 3-5, 7, 9-11
all	将匹配的所有信息记录到日志文件
permit	将匹配不通过的信息记录到日志文件
none	将匹配通过的信息记录到日志文件

## 命令模式

全局配置模式

## 默认

无

## 使用说明

根据 dhcp 绑定表来过滤日志报文。



## 举例说明

记录在 VLAN2 上匹配 dhcp 绑定表的所有日志信息。

```
Switch(config)# ip arp inspection vlan 2 logging dhcp-bindings all
```

## 相关命令

**show ip arp inspection vlan**

### 6.8.15 clear ip arp inspection log-buffer

使用此命令清除所有的 arp inspection 日志文件。

## 命令语法

**clear ip arp inspection log-buffer**

## 命令模式

特权模式

## 默认

无

## 使用说明

此命令清除所有的 arp inspection 日志文件。

## 举例说明

设置交换机删除所有的日志文件。

```
Switch# clear ip arp inspection log-buffer
```

## 相关命令

**ip arp inspection log-buffer logs**

### 6.8.16 clear ip arp inspection statistics

使用此命令删除所有的 arp inspection 统计。

## 命令语法

**clear ip arp inspection statistics**

## 命令模式

全局配置模式

## 默认

无

## 使用说明

此命令删除所有的 `arp inspection` 统计。

## 举例说明

删除交换机上所有的 `arp inspection` 统计。

```
Switch(config)# clear ip arp inspection statistics
```

## 相关命令

**show ip arp inspection statistics**

## 6.8.17 ip arp inspection trust

此命令指定本端口为可信端口。

使用关键字 `no` 设置本端口为不可信端口。

## 命令语法

**ip arp inspection trust**

## 命令模式

接口配置模式

## 默认

无

## 使用说明

缺省端口为不可信端口；

如果端口被设置为可信端口，则在启用 ARP Inspection 以后，通过此端口的 ARP 报文不会被验证。

## 举例说明

设置交换机的 `eth-0-2` 端口为非信任端口。

```
untrusted state.
```

```
Switch(config-if)# no ip arp inspection trust
```

## 相关命令

**show ip arp inspection interfaces**

### 6.8.18 arp access-list

使用此命令配置 arp 访问控制列表。

## 命令语法

**arp access-list** *ACL*

ACL	指定 acl 名字,最多 40 个字符
-----	---------------------

## 命令模式

全局配置模式

## 默认

无

## 使用说明

在非 DHCP 环境中，动态 ARP 检测可以通过设置访问控制列表来验证 ARP 报文。

## 举例说明

创建一个 arp 访问控制列表。

```
Switch(config)# arp access-list acl1
```

## 相关命令

**show access-list arp**

### 6.8.19 ip mac

使用此命令配置 arp 的 ace。

## 命令语法

**(deny|permit) (request | response |) ip (address wildcard|any|host address) mac (MAC MASK|any|host MAC) (log |)**

deny	拒绝指定的包
------	--------

permit	允许指定的包
request	arp 请求
response	arp 响应
address	源地址
wildcard	反掩码地址
any	任何源地址
host	主机地址
MAC	主机的源 mac 地址如:HHHH.HHHH.HHHH 格式
MASK	主机的源 mac 地址掩码,如:HHHH.HHHH.HHHH 格式
log	匹配的日志

## 命令模式

ARP-ACL

## 默认

无

## 使用说明

无.

## 举例说明

使用如下命令，配置 ARP ACE。

```
Switch(config-arp-acl)# permit ip host 192.168.1.1 mac any
```

## 相关命令

**show access-list arp**

### 6.8.20 no sequence-num

使用此命令可删除 ARP ACE。

## 命令语法

**no sequence-num** *NUMBER*

NUMber	指定一个序号，取值范围<1-131071>
--------	-----------------------

## 命令模式

ARP-ACL

## 默认

无

## 使用说明

使用此命令删除 ARP 的 ACE 序号。

## 举例说明

适应如下命令，删除一个 ARP ACE。

```
Switch(config-arp-acl)# no sequence-num 10
```

## 相关命令

**show access-list arp**

### 6.8.21 show access-list arp

使用此命令显示 arp 的访问控制列表。

## 命令语法

**show access-list arp (ACL)**

ACL	访问控制列表名字
-----	----------

## 命令模式

特权模式

## 默认

无

## 使用说明

使用此命令显示 arp 的访问控制列表。

## 举例说明

显示 ARP 的访问控制列表。

```
Switch# show access-list arp
arp access-list acl
  10 permit request ip 1.1.1.1 0.255.255.255 mac any
```

## 相关命令

**arp access-list**

# 6.9 DHCP Snooping 命令

## 6.9.1 clear dhcp snooping

在全局配置模式下使用 `clear dhcp snooping` 命令来清除 DHCP 绑定数据库中动态学习条目或 DHCP snooping 统计计数信息。

## 命令语法

**clear dhcp snooping (bindings (learning | manual) (ipv4 *IP-ADDRESS* | mac *MAC-ADDRESS* | vlan *VLAN-ID* | interface *IFNAME* |) | statistics}**

<b>bindings</b>	清除 DHCP snooping 绑定数据库
<b>ipv4 <i>IP-ADDRESS</i></b>	按照 IP 地址清除绑定条目
<b>mac <i>MAC-ADDRESS</i></b>	按照 MAC 地址清除绑定条目
<b>vlan <i>VLAN-ID</i></b>	按照 VLAN 清除绑定条目
<b>interface <i>IFNAME</i></b>	按照端口名称清除绑定条目
<b>statistics</b>	清除 DHCP snooping 统计计数

## 命令模式

全局配置模式

## 默认

无

## 使用说明

该命令用于清除 DHCP snooping 动态绑定条目或计数信息。

## 举例说明

配置清除 DHCP snooping 统计计数：

```
Switch(config)# clear dhcp snooping statistics
```

## 相关命令

**show dhcp snooping binding**

**show dhcp snooping statistics**

## 6.9.2 dhcp snooping

在全局配置模式下使用 `dhcp snooping` 命令配置交换机全局使能 DHCP snooping。使用命令相应的 `no` 形式恢复为默认设置。

## 命令语法

**dhcp snooping**

**no dhcp snooping**

## 命令模式

全局配置模式

## 默认

默认情况下，DHCP snooping 未使能。

## 使用说明

必需在全局使能 DHCP snooping，才可以使 DHCP snooping 的配置生效。

只有在全局配置模式下使用 `dhcp snooping vlan vlan-id` 命令在 VLAN 上使能 snooping，DHCP snooping 才会起作用。

## 举例说明

配置使能 DHCP snooping。

```
Switch(config)# dhcp snooping
```

可以在特权模式下使用 `show dhcp snooping config` 命令验证配置是否启用。

## 相关命令

**dhcp snooping vlan**

**show dhcp snooping config**

## 6.9.3 dhcp snooping binding

在全局配置模式下，使用 `dhcp snooping binding` 命令配置 DHCP snooping 绑定数据库以及向数据库中添加静态绑定条目。

### 命令语法

**dhcp snooping binding mac** *MAC-ADDRESS* **vlan** *VLAN-ID* **ipv4** *IP-ADDRESS* **interface** *IFNAME* **expiry** *SECONDS*

**no dhcp snooping bindings** (**ipv4** *IP-ADDRESS* | **mac** *MAC-ADDRESS* | **vlan** *VLAN-ID* | **interface** *IFNAME* | )

<b>mac</b> <i>MAC-ADDRESS</i>	指定 MAC 地址
<b>vlan</b> <i>VLAN-ID</i>	指定 VLAN 序号。范围为 1 到 4094
<b>ipv4</b> <i>IP-ADDRESS</i>	指定 IP 地址
<b>interface</b> <i>IFNAME</i>	指定添加或删除绑定条目的接口
<b>expiry</b> <i>SECONDS</i>	指定时间间隔(单位为秒)后绑定条目无效。范围为 0 到 86400

### 命令模式

全局配置模式

### 默认

无

### 使用说明

当你在测试或调试交换机时使用该条命令。

在 DHCP snooping 绑定数据库中，每一个数据条目都有一个 IP 地址，一个关联的 MAC 地址，一个租约时间，提供绑定数据的接口，以及该接口属于的 VLAN。

在特权模式下，使用 `show dhcp snooping binding` 命令显示配置的绑定信息。

### 举例说明

为在 VLAN1 的接口 `eth-0-1` 上配置一个 DHCP 绑定，MAC 地址为 `0001.000c.01ef`，IP 地址为 `10.10.1.1`，过期时间为 `1000` 秒。

```
Switch(config)# dhcp snooping binding mac 0001.000c.01ef vlan 1 ipv4 10.10.1.1
interface eth-0-1 expiry 1000
```



## 相关命令

**dhcp snooping**

**show dhcp snooping binding**

## 6.9.4 dhcp snooping database

在全局配置模式下，使用 `dhcp snooping database` 命令位置交换机的 DHCP snooping 绑定数据库代理。使用命令相应的 `no` 形式取消代理，或重置超时时间，或重置保存延期时间。

## 命令语法

**dhcp snooping database auto-save interval *SECONDS***

<b>interval <i>SECONDS</i></b>	指定保存绑定数据库的时间间隔 (单位为秒)。范围为 15 到 1200
--------------------------------	-------------------------------------

## 命令模式

全局配置模式

## 默认

默认时间间隔为 600 秒。

## 使用说明

DHCP snooping 绑定数据库存储在 `flash:/dhcpsnooping` 中。

## 举例说明

配置 DHCP snooping 自动保存数据库时间间隔为 120 秒：

```
Switch(config)# dhcp snooping database auto-save interval 120
```

## 相关命令

**dhcp snooping**

**dhcp snooping binding**

## 6.9.5 dhcp snooping information option

在全局配置模式下使用 `dhcp snooping information option` 命令使能 DHCP 报文中插入 Option82 数据。使用命令相应的 `no` 形式取消 DHCP 插入 Option82 数据。

## 命令语法

**dhcp snooping information option**

**no dhcp snooping information option**

## 命令模式

全局配置模式

## 默认

默认情况下，不插入 DHCP Option82 数据。

## 使用说明

你必须在全局配置模式下使用 `dhcp snooping` 命令全局使能 DHCP snooping，有关 DHCP snooping 的配置才会生效。

当 Option82 功能使能时，交换机收到主机发送的 DHCP 请求报文，会在报文中加入 Option82 选项信息。Option82 选项信息包含交换机的 MAC 地址(远端 ID 选项)，收到 DHCP 报文端口的 ID(电路 ID 选项)，该端口为 vlan 模式端口。交换机转发包含 Option82 选项的 DHCP 请求报文给 DHCP 服务器。

当 DHCP 服务器收到报文，可以使用远端 ID，电路 ID，或分配 IP 地址和执行策略，例如限制 IP 地址的数目可以分配到一个单独的远端 ID 或电路 ID。之后 DHCP 服务器回复带有 Option82 选项的 DHCP 回复报文。

如果 DHCP 请求报文由中继转发给服务器，DHCP 服务器单播 DHCP 回复报文给交换机。当 DHCP 客户端和 DHCP 服务器在同一子网时，DHCP 服务器广播 DHCP 回复报文。交换机检测远端 ID，以及可能存在的电路 ID 来检测 DHCP 报文是否原先就包含 Option82 选项。交换机移除报文的 Option82 选项，转发报文到连接发送 DHCP 请求报文主机的端口。

## 举例说明

配置使能插入 DHCP Option82 选项信息：

```
Switch(config)# dhcp snooping information option
```

你可以在特权模式下使用 `show dhcp snooping config` 命令验证你的配置。

## 相关命令

**show dhcp snooping config**

**show dhcp snooping binding**

### 6.9.6 dhcp snooping information option allow-untrusted

在全局配置模式下使用 `dhcp snooping information option allow-untrusted` 命令配置汇聚交换机接收不信任接口收到的含有 Option82 选项的 DHCP 报文，不信任接口可能连接到一个边缘交换机。使用命令相应的 `no` 形式恢复默认设置。

## 命令语法

```
dhcp snooping information option allow-untrusted  
no dhcp snooping information option allow-untrusted
```

## 命令模式

全局配置模式

## 默认

默认情况下，交换机丢弃不信任接口接收到的含有 Option82 的 DHCP 报文，该不信任接口可能连接到一个边缘交换机。

## 使用说明

你可能想要一个边缘交换机连接的主机在你的边缘网络中 DHCP 报文插入 Option82 选项。你可能也想在一个汇聚交换机上使能 DHCP 安全特性，例如 DHCP snooping，IP 源地址绑定，或动态 ARP 检测。但是，如果在一个汇聚交换机上使能 DHCP snooping，交换机会丢弃从不信任接口收到的含有 Option82 选项的 DHCP 报文，无法学到连接信任接口设备的 DHCP snooping 绑定信息。

如果你想要汇聚交换机启用 DHCP snooping 功能，并能接收从边缘交换机连接主机发来的带有 Option82 选项的 DHCP 报文，使用 `dhcp snooping information option allow-untrusted` 命令配置汇聚交换机。汇聚交换机可以学到从不信任端口收到的 DHCP 报文的绑定系信息。你也可以在汇聚交换机使能 DHCP 安全特性。边缘交换机连接到汇聚交换机的端口必需被配置为信任端口。

## 举例说明

配置接入交换机接收不信任端口收到的从边缘交换机发来的含有 Option82 的 DHCP 报文：

```
Switch(config)# dhcp snooping information option allow-untrusted
```

## 相关命令

```
show dhcp snooping config
```

### 6.9.7 dhcp snooping trust

在端口配置模式下使用 `dhcp snooping trust` 命令配置接口对 DHCP snooping 为信任接口。使用命令相应的 `no` 形式恢复为默认设置。

## 命令语法

```
dhcp snooping trust  
no dhcp snooping trust
```

## 命令模式

端口配置模式

## 默认

默认情况下，为 DHCP snooping 不信任接口。

## 使用说明

配置连接 DHCP 服务器或其他交换机或路由器的接口为信任接口。配置连接 DHCP 客户端的接口为不信任接口。

## 举例说明

配置接口为 DHCP snooping 信任接口：

```
Switch(config-if)# dhcp snooping trust
```

## 相关命令

**show dhcp snooping config**

## 6.9.8 dhcp snooping verify

在全局配置模式下使用 `dhcp snooping verify` 命令配置在不信任端口打开 DHCP 源 MAC 匹配客户端硬件地址的检查功能。使用命令相应的 `no` 形式关闭 MAC 地址检查功能。

## 命令语法

**dhcp snooping verify mac-address**

**no dhcp snooping verify mac-address**

## 命令模式

全局配置模式

## 默认

默认情况下，交换机检查从不信任端口接收到的 DHCP 报文中的源 MAC 地址和客户端硬件地址是否一致。

## 使用说明

在一个服务提供端网络中，当交换机从不信任接口收到 DHCP 客户端发送的 DHCP 报文，会自动对报文的源 MAC 地址和 DHCP 客户端硬件地址进行检查。如果地址一致，交换机转发该报文，否则丢弃该报文。

## 举例说明

配置不对 DHCP 报文 MAC 地址检查:

```
Switch(config)# no dhcp snooping verify mac-address
```

## 相关命令

**show dhcp snooping config**

## 6.9.9 dhcp snooping vlan

在全局配置模式下使用 `dhcp snooping vlan` 命令配置交换机在 VLAN 使能 DHCP snooping。使用命令相应的 `no` 形式恢复为默认设置。

## 命令语法

**dhcp snooping vlan** *VLAN-RANGE*

**no dhcp snooping vlan** *VLAN-RANGE*

<b>vlan</b> <i>VLAN-RANGE</i>	指定使能 DHCP snooping 的 VLAN ID 或 VLAN 的范围。ID 范围为 1 到 4094
-------------------------------	---

## 命令模式

全局配置模式

## 默认

默认情况下 DHCP snooping 在所有 VLAN 都未使能。

## 使用说明

你可以输入 VLAN 序号指定单独一个 VLAN ID，或者输入几个 VLAN 序号使用逗号间隔，或输入一个 VLAN 范围使用连字号间隔，或输入 VLAN 开始 ID 和 VLAN 结束 ID 使用空格间隔。在 VLAN 上使能 DHCP snooping 前，必须先全局使能 DHCP snooping。注意 dhcp snooping 功能和 dhcp server 功能不要在同一个 vlan 上设置。

## 举例说明

在 VLAN10 上配置 DHCP snooping:

```
Switch(config)# dhcp snooping vlan 10
```

## 相关命令

**show dhcp snooping config**

## 6.9.10 dhcp snooping vlan information option format-type circuit-id string

在端口配置模式下使用 `dhcp snooping vlan vlanId information option format-type circuit-id string` 命令配置 Option82 选项中的电路 ID。使用命令相应的 `no` 形式设置为默认电路 ID。

### 命令语法

```
dhcp snooping vlan VLAN-ID information option format-type circuit-id string STRING  
no dhcp snooping vlan VLAN-ID information option format-type circuit-id string
```

<b>vlan</b> <i>VLAN-ID</i>	指定使能 DHCP snooping 的 VLAN ID。范围为 1 到 4094
<b>STRING</b>	ASCII 字符串，范围 1~63

### 命令模式

端口配置模式

### 默认

无

### 使用说明

必需在全局使能 DHCP snooping，才可以使 DHCP snooping 的配置生效。

### 举例说明

在 vlan2 配置 Option82 中的电路 ID 为 vlan2:

```
Switch(config-if)# dhcp snooping vlan 2 information option format-type circuit-id  
string vlan2
```

### 相关命令

无

## 6.9.11 dhcp snooping information option format remote-id

在全局配置模式下使用 `dhcp snooping information option format remote-id` 命令配置 Option82 选项中的远端 ID。使用命令相应的 `no` 形式设置为默认远端 ID。

### 命令语法

```
dhcp snooping information option format remote-id (string NAME | hostname)
```

**no dhcp snooping information option format remote-id**

string <i>NAME</i>	指定远端 ID，使用 1 到 63ASCII 码对应的字符(不可以为空)
hostname	指定交换机的主机名作为远端 ID

**命令模式**

全局配置模式

**默认**

无

**使用说明**

必需在全局使能 DHCP snooping，才可以使 DHCP snooping 的配置生效。

**举例说明**

配置 Option82 的远端 ID 为 hostname:

Switch(config)# dhcp snooping information option format remote-id hostname

**相关命令**

无

**6.9.12 show dhcp snooping binding**

在特权模式下使用 show dhcp snooping binding 命令显示设备 DHCP snooping 绑定数据库和所有接口的配置信息。

**命令语法****show dhcp snooping binding ( (all | manual | learning ) (ipv4 IP-ADDRESS | mac MAC-ADDRESS | vlan VLAN-ID | interface IFNAME | ) | summary)**

all	显示所有绑定条目
manual	显示静态绑定条目
learning	显示动态绑定条目
mac MAC-ADDRESS	指定 MAC 地址

<b>vlan</b> VLAN-ID	指定 VLAN 序号。范围为 1 到 4094
<b>ipv4</b> IP-ADDRESS	指定 IP 地址
<b>interface</b> IFNAME	指定添加或删除绑定条目的接口
<b>summary</b>	显示 DHCP snooping 绑定的概要信息

## 命令模式

特权模式

## 默认

无

## 使用说明

如果使能了 DHCP snooping 功能，即使接口变为断开状态，交换机也不会删除静态配置的绑定条目。

## 举例说明

显示 dhcp snooping 绑定信息：

```
Switch# show dhcp snooping binding all
DHCP snooping binding table:
VLAN MAC Address      Interface  Lease(s)   IP Address
=====
1      0001.0001.0001 eth-0-2    static     1.1.1.1
```

## 相关命令

**dhcp snooping binding**

### 6.9.13 debug dhcp snooping

使用此命令可以打开 dhcp snooping 的模块的调试功能。

在原命令之前加上关键字 “no”，关闭调试功能。

## 命令语法

**debug dhcp snooping ( events | error | packet | dump | all )**

**no debug dhcp snooping ( events | error | packet | dump | all )**

events	调试 dhcp snooping 事件信息
--------	-----------------------



error	调试 dhcp snooping 错误信息
packet	调试 dhcp snooping 的数据包信息
dump	以十六进制调试 dhcp snooping 的数据包信息
all	上面提到的所有调试信息

## 命令模式

特权模式

## 默认

无

## 使用说明

使用“terminal monitor”打印消息

## 举例说明

使用如下命令，打开dhcp snooping的所有调试信息。

```
Switch# debug dhcp snooping all
```

## 相关命令

**terminal monitor**

**show logging buffer**

## 6.9.14 show dhcp snooping config

在特权模式下使用 show dhcp snooping config 命令显示 DHCP snooping 配置。

## 命令语法

**show dhcp snooping config**

## 命令模式

特权模式

## 默认

无

## 使用说明

该命令用于显示 DHCP snooping 配置信息。

## 举例说明

显示 dhcp snooping 配置信息：

```
Switch# show dhcp snooping config
dhcp snooping service: enabled
dhcp snooping switch: enabled
Verification of hwaddr field: enabled
Insertion of relay agent information (option 82): enabled
Relay agent information (option 82) on untrusted port: not allowed
dhcp snooping vlan 1
```

## 相关命令

**dhcp snooping binding**

### 6.9.15 show dhcp snooping statistics

在特权模式下使用 show dhcp snooping statistics 命令显示 DHCP snooping 统计信息。

## 命令语法

**show dhcp snooping statistics**

## 命令模式

特权模式

## 默认

无

## 使用说明

该命令用于显示 DHCP snooping 统计信息。

## 举例说明

显示 dhcp snooping 统计信息：

```
Switch# show dhcp snooping statistics
DHCP snooping statistics:
=====
DHCP packets                11257
BOOTP packets                0
Packets forwarded           10381
Packets invalid              844
Packets MAC address verify failed 354
Packets dropped              516
```

## 相关命令

**clear dhcp snooping statistics**

### 6.9.16 show dhcp snooping trusted-sources

在特权模式下使用 `show dhcp snooping trusted-sources` 命令显示 DHCP snooping 信任端口。

## 命令语法

**show dhcp snooping trusted-sources**

## 命令模式

特权模式

## 默认

无

## 使用说明

该命令用于显示 DHCP snooping 信任端口。

## 举例说明

显示 dhcp snooping 信任端口信息：

```
Switch# show dhcp snooping trusted-sources
List of DHCP snooping trusted interface(s):
=====
eth-0-2
```

## 相关命令

**dhcp snooping trust**

## 6.10 IP Source Guard 命令

### 6.10.1 ip source binding

使用 “ip source binding” 命令配置 IP、MAC、VLAN、接口四者的绑定关系条目。

在原命令前加上关键字 “no” 删除该绑定条目。

## 命令语法

**ip source binding mac** *MAC-ADDRESS* **vlan** *VLAN-ID* **ip** *IP-ADDRESS* **interface** *INTERFACE-ID*

**no ip source binding mac** *MAC-ADDRESS* **vlan** *VLAN-ID* **ip** *IP-ADDRESS* **s interface** *INTERFACE-ID*

MAC-ADDRESS	指定绑定的 MAC
VLAN-ID	指定绑定的 VLAN ID
IP-ADDRESS	指定绑定的 IP
INTERFACE-ID	指定绑定的接口

## 命令模式

全局配置模式

## 默认

无

## 使用说明

一条静态的 IP 绑定条目包括一个 IP 地址，一个 MAC 地址，以及 VLAN ID 和接口名字。

同一个 IP 地址或 MAC 地址只能出现在一个绑定条目中，不允许重复出现。绑定条目配置以后不能修改，只能删除重配。

默认情况下系统未配置任何绑定条目。

## 举例说明

绑定 MAC 0001.1234.1234，VLAN 1，IP 172.20.50.5 和接口 eth-0-1 到一个绑定条目中。

```
Switch(config)# ip source binding mac 0001.1234.1234 vlan 1 ip 172.20.50.5
interface eth-0-1
```

## 相关命令

**show ip source binding**

**no ip source binding**

## 6.10.2 no ip source binding

使用“no ip source binding”命令，删除所有已经配置的绑定条目。

### 命令语法

**no ip source binding entries**

**no ip source binding entries vlan *VLAN-ID***

**no ip source binding entries interface *INTERFACE-ID***

VLAN-ID	绑定到该 VLAN 的条目，范围是 1 ~ 4094
INTERFACE-ID	绑定到该接口的条目

### 命令模式

全局配置模式

### 默认

无

### 使用说明

如果不指定 VLAN 或者接口，那么所有的绑定条目都将被删除。

### 举例说明

- 删除所有绑定到接口 eth-0-1 的条目：

```
Switch(config)# no ip source binding entries interface eth-0-1
```

- 删除所有绑定到 vlan 2 的条目：

```
Switch(config)# no ip source binding entries vlan 2
```

- 删除所有绑定条目：

```
Switch(config)# no ip source binding entries
```

### 相关命令

**ip source binding**

**show ip source binding**

## 6.10.3 ip source maximal binding

使用“ip source maximal binding”命令，配置每个端口上最多绑定的条目数。

在原命令之前加上关键字“no”恢复该配置为默认值。

## 命令语法

**ip source maximal binding number per-port** *NUMBER*

**no ip source maximal binding number per-port**

NUMBER	指定端口上最多绑定的条目数，范围在 0~30 之间
--------	---------------------------

## 命令模式

全局配置模式

## 默认

10

## 使用说明

指定端口上最多绑定的条目数，范围在 0~30 之间。0 表示不限定。默认为 10 条。

## 举例说明

设置每个端口上最多绑定的条目数为 20:

```
Switch(config)# ip source maximal binding number per-port 20
```

## 相关命令

**show ip source binding**

### 6.10.4 ip verify source

使用“ip verify source”在接口上使能 IP 绑定检查功能，并指定检查项。

在原命令前加上关键字“no”删除该配置。

## 命令语法

**ip verify source** (**ip** | **ip-mac** | **ip-vlan** | **ip-mac-vlan**)

**no ip verify source**

ip	检查源 IP 地址
ip-mac	检查源 IP 地址和源 MAC 地址
ip-vlan	检查源 IP 地址和源 VLAN

ip-mac-vlan	检查源 IP 地址、源 MAC 地址，和源 VLAN
-------------	----------------------------

## 命令模式

端口配置模式

## 默认

无

## 使用说明

在 access 端口上，不带 tag 的报文是可以通过源 VLAN 检查的。

默认情况下接口不使能 IP 绑定检查功能。

## 举例说明

在接口上使能 IP 绑定检查功能，检查源 IP 和 MAC。

```
Switch(config-if)# ip verify source ip-mac
```

## 相关命令

**ip source binding**

**show ip source binding**

## 6.10.5 show ip source binding

使用“show ip source binding”显示 ip 绑定检查的功能的相关配置和绑定条目。

## 命令语法

**show ip source binding (interface *INTERFACE-ID* |)**

<b>interface</b> <i>INTERFACE-ID</i>	显示绑定到指定端口的条目
--------------------------------------	--------------

## 命令模式

特权模式

## 默认

无

## 使用说明

如果不指定端口，那么所有绑定表项都会被显示出来。

## 举例说明

显示命令输出结果：

```
Switch# show ip source binding
The total number of ip binding is 1, the max ip number limit is 127
The total number of ipv6 binding is 0, the max ipv6 number limit is 128
IP source guard binding table:
VLAN MAC Address      Type   Interface      State   IP Address
=====
3      0001.0002.0003 static eth-0-1       ip      10.0.0.2
```

## 相关命令

**ip source binding**

**no ip source binding**

## 6.11 AAA 命令

### 6.11.1 aaa new-model

使能鉴权，授权，统计(AAA)访问控制模块。

## 命令语法

**aaa new-model**

**no aaa new-model**

## 命令模式

全局配置模式

## 使用说明

使能 AAA 访问控制模块。

## 举例说明

下面举例，使能 AAA 访问控制模块。

```
Switch(config)#aaa new-model
```

## 相关命令

**show aaa status**



## 6.11.2 aaa authentication login

设置用户登录鉴权方式链表。

### 命令语法

**aaa authentication login (default|LISTNAME) {enable|line|none|radius|local|tacacs-plus}**

**no aaa authentication login (default|LISTNAME)**

default	默认方式链表
LISTNAME	鉴权方式链表名
enable	Enable 密码
line	Line 密码
none	无鉴权
radius	RADIUS 方式
local	本地用户
tacacs-plus	TACACS+方式

### 命令模式

全局配置模式

### 使用说明

使用该命令，设置用户登录鉴权方式链表。

### 举例说明

下面举例，配置用户登录鉴权方式使用本地用户，RADIUS，无鉴权。

```
Switch(config)# aaa authentication login default local radius none
```

### 相关命令

**show aaa method-lists authentication**

## 6.11.3 aaa authorization exec

设置用户登录授权方式链表。

### 命令语法

**aaa authorization exec (default|LISTNAME) { none|radius|local|tacacs-plus}**

**no aaa authorization exec (default|LISTNAME)**

default	默认方式链表
LISTNAME	授权方式链表名
none	无授权
radius	RADIUS 方式
local	本地用户
tacacs-plus	TACACS+方式

## 命令模式

全局配置模式

## 使用说明

使用该命令设置用户登录授权方式链表。

## 举例说明

下面举例，配置用户登录授权方式使用 TACACS+和无授权。

```
Switch(config)# aaa authorization exec default tacacs-plus none
```

## 相关命令

### 6.11.4 aaa accounting exec

设置用户 exec 计费方式链表。

## 命令语法

**aaa accounting exec (default|LISTNAME) (((start-stop|stop-only) {radius|tacacs-plus} (none|)) | none)**

**no aaa accounting exec (default|LISTNAME)**

default	默认方式链表
LISTNAME	计费方式链表名
start-stop	用户登录和退出都会发送计费请求
stop-only	用户退出时会发送计费请求
radius	RADIUS 方式
tacacs-plus	TACACS+方式
none	前面计费方式失败则不计费（否则如果计费失败会强制用户下线）

## 命令模式

全局配置模式

## 使用说明

使用该命令设置用户 `exec` 计费方式链表。

## 举例说明

下面举例，配置用户 `exec` 计费方式使用 TACACS+。

```
Switch(config)# aaa accounting exec default start-stop tacacs-plus
```

## 相关命令

### 6.11.5 aaa accounting commands

设置用户命令行计费方式链表。

## 命令语法

**aaa accounting commands (default|LISTNAME) ((tacacs-plus (none)) | none)**

**no aaa accounting commands (default|LISTNAME)**

default	默认方式链表
LISTNAME	计费方式链表名
tacacs-plus	TACACS+方式
none	前面计费方式失败则不计费（否则如果计费失败会记录到日志中）

## 命令模式

全局配置模式

## 使用说明

使用该命令，设置用户命令行计费方式链表。

## 举例说明

下面举例，配置用户命令行计费方式使用 TACACS+。

```
Switch(config)# aaa accounting commands default tacacs-plus
```

## 相关命令

### 6.11.6 aaa privilege mapping

设置设备和服务器之间的级别映射关系。

## 命令语法

**aaa privilege mapping** <0-12> <0-13> <0-14>

**no aaa privilege mapping**

<0-12>	设备级别 1 对应 server 中级别的最大值
<1-13>	设备级别 2 对应 server 中级别的最大值
<2-14>	设备级别 3 对应 server 中级别的最大值

## 命令模式

全局配置模式

## 使用说明

Server 中 privilege 的级别一般是 0~15 而设备中的级别范围是 1~4。默认三参数是 0、1、10:

0: 表示 server 级别 0 映射到设备级别 1

1: 表示 server 级别 1 映射到设备级别 2

9: 表示 server 级别 2~9 映射到设备级别 3

剩下的 10~15 则映射到设备级别 4

## 举例说明

下面举例，配置设备和服务器之间的级别映射关系。

```
Switch(config)# aaa privilege mapping 0 1 14
```

## 相关命令

**show aaa privilege mapping**

### 6.11.7 login authentication

设置用户登录鉴权方式链表。

## 命令语法

**login authentication (default|LISTNAME)**

**no login authentication**

default	默认 AAA 鉴权方式链表名。
LISTNAME	AAA 鉴权方式链表名。

**命令模式**

Line 模式

**使用说明**

使能 AAA 鉴权用户登录。

**举例说明**

下面举例，使能 AAA 鉴权用户登录。

```
Switch# configure terminal
Switch(config)# line vty 0 7
Switch(config-line)# login authentication default
```

**相关命令****show aaa method-lists authentication****6.11.8 authorization exec**

设置用户登录鉴权方式链表。

**命令语法****authorization exec (default|LISTNAME)****no authorization exec**

default	默认 AAA 授权方式链表名。
LISTNAME	AAA 授权方式链表名。

**命令模式**

Line 模式

**使用说明**

使能 AAA 授权用户登录。

**举例说明**

下面举例，使能 AAA 授权用户登录。

```
Switch# configure terminal
Switch(config)# line vty 0 7
Switch(config-line)# authorization exec default
```

## 相关命令

### 6.11.9 accounting exec

设置用户登录 `exec` 计费方式链表。

## 命令语法

**accounting exec (default|LISTNAME)**

**no accounting exec**

default	默认 AAA exec 计费方式链表名。
LISTNAME	AAA exec 计费方式链表名。

## 命令模式

Line 模式

## 使用说明

使能 AAA 用户 `exec` 计费。

## 举例说明

下面举例，使能 AAA `exec` 计费

```
Switch# configure terminal
Switch(config)# line vty 0 7
Switch(config-line)# accounting exec default
```

## 相关命令

### 6.11.10 accounting commands

设置用户命令行计费方式链表。

## 命令语法

**accounting commands (default|LISTNAME)**

**no accounting commands**

default	默认 AAA 命令行计费方式链表名。
LISTNAME	AAA 命令行计费方式链表名。

## 命令模式

Line 模式

## 使用说明

使能 AAA 用户命令行计费。

## 举例说明

下面举例，使能 AAA 命令行计费

```
Switch# configure terminal
Switch(config)# line vty 0 7
Switch(config-line)# accounting commands default
```

## 相关命令

### 6.11.11 show aaa method-lists authentication

使用此命令，显示鉴权，授权，统计方式链表。

## 命令语法

**show aaa method-lists authentication**

## 命令模式

特权模式

## 使用说明

使用此命令，显示鉴权，授权，统计方式链表。

## 举例说明

下面举例，显示系统中鉴权方式链表。

```
Switch# show aaa method-lists authentication
authen queue = AAA_ML_AUTHEN_LOGIN
      name = default  state = ALIVE :   radius
authen queue = AAA_ML_AUTHEN_LOGIN
      name = group_a  state = ALIVE :   radius local line enable none
authen queue=AAA_ML_AUTHEN_LOGIN
      name = group_b  state = ALIVE :   local line none
```

## 相关命令

**aaa authentication login**

## 6.11.12 show aaa status

使用此命令，显示鉴权，授权，统计（AAA）状态。

### 命令语法

```
show aaa status
```

### 命令模式

特权模式

### 使用说明

使用此命令，显示鉴权，授权，统计（AAA）状态。

### 举例说明

下面举例，显示系统 AAA 状态。

```
aaa stats:  
  Authentication enable
```

### 相关命令

```
aaa new-model
```

## 6.11.13 show aaa privilege mapping

使用此命令显示设备和服务器之间的级别映射关系。

### 命令语法

```
show aaa privilege mapping
```

### 命令模式

特权模式

### 使用说明

使用此命令显示设备和服务器之间的级别映射关系。

### 举例说明

下面举例，显示设备和服务器之间的级别映射关系。

```
Switch# show aaa privilege mapping  
  Server      Switch      Server  
=====
```

0	1	0
1	2	1



2~10	3	10
11~15	4	15

## 相关命令

**aaa privilege mapping**

## 6.12 RADIUS 认证命令

### 6.12.1 radius-server deadtime

使用“radius-server deadtime”命令配置重新激活认证服务器的时间间隔。

在原命令之前加上关键字“no”，恢复该配置为默认值。

## 命令语法

**radius-server deadtime** *minutes*

**no radius-server deadtime**

<i>minutes</i>	设置重新激活认证服务器的时间间隔；以分钟为单位，取值范围<1-20>
----------------	------------------------------------

## 命令模式

全局配置模式

## 默认

默认重新激活认证服务器的时间间隔为5分钟。

## 使用说明

当某一个用户在一个服务器上认证失败若干次以后，这个服务器将被标记为“未激活”。设备不会向一个未激活的服务器发出任何认证请求。防止对服务器造成冲击。

设置重新激活认证服务器的时间间隔有助于认证失败后能及时更新

缺省重新激活认证服务器的时间间隔为5分钟。

## 举例说明

设置重新激活认证服务器的时间间隔为10分钟:

```
Switch(config)# radius deadtime 10
```

## 相关命令

**radius-server host**

### 6.12.2 radius-server host

使用“radius-server host”命令添加认证服务器。

在原命令之前加上关键字“no”，删除该配置。

## 命令语法

**radius-server host** (**mgmt-if**) (*ipv4-address* | *ipv6-address*) (**auth-port** *PORT-NUMber*) (**timeout** *seconds*) (**retransmit** *retries*) (**key string**) (source-interface *IFNAME*|source-ip *A.B.C.D*)

**no radius-server host** (*ipv4-address* | *ipv6-address*) (**auth-port** *PORT-NUMber*)

<b>mgmt-if</b>	通过管理口认证
<i>ipv4-address</i>	Radius 服务器的 IPv4 地址
<i>ipv6-address</i>	Radius 服务器的 IPv6 地址
<b>auth-port</b> <i>port-number</i>	Radius 服务器的认证的端口，UDP 端口号，默认值 1812
<b>timeout</b> <i>seconds</i>	设备和服务器之间的报文等待超时时间 设置范围 1-1000，默认是 5，单位“秒”
<b>retransmit</b> <i>retries</i>	设备到服务器之间的 request 报文，设置范围 1-100，默认为 3 次
<b>key string</b>	指定密钥字符串
<b>IFNAME</b>	指定源接口名称
<b>A.B.C.D</b>	指定源 IP 地址

## 命令模式

全局配置模式

## 默认

无

## 使用说明

用户可以使用" radius-server host "命令添加多个认证服务器。系统会以配置先后顺序依次向这些服务器发起认证请求。

如果没有单独为某个服务器指定超时时间、重传次数、密钥等，系统将会使用全局配置的属性。如果指定源接口或者源IP地址，将会使用对应的IP地址作为发出报文的源IP地址。

## 举例说明

添加认证服务器，地址为10.10.1.1，密钥为abcde。

```
Switch(config)# radius-server host 10.10.1.1 key abcde
```

## 相关命令

**radius-server key**

**radius-server timeout**

### 6.12.3 radius-server retransmit

使用“radius-server retransmit”命令设置交换机发往RADIUS服务器的Request报文的最大重传次数。

在原命令之前加上关键字“no”，恢复该配置为默认值。

## 命令语法

**radius-server retransmit** *retries*

**no radius-server retransmit**

retries	交换机发往 RADIUS 服务器的 <b>Request 报文</b> 的最大重传次数，取值范围<1-100>，默认为 3 次
---------	---

## 命令模式

全局配置模式

## 默认

交换机发往RADIUS服务器的Request报文的默认重传次数为3次。

## 使用说明

交换机会尝试所有的服务器，分别计算重传次数。如果设备到RADIUS服务器之间跳数较多，我们建议您配置RADIUS服务器重传次数为5。默认值是3次尝试。

## 举例说明

设置交换机发往RADIUS服务器的Request报文的默认重传次数为5次。

```
Switch(config)# radius retransmit 5
```

## 相关命令

**radius-server host**

**radius-server key**

### 6.12.4 radius-server timeout

使用"radius-server timeout"命令设置交换机等待来自RADIUS服务器的Response报文的超时时间。

在原命令之前加上关键字"no"，恢复该配置为默认值。

## 命令语法

**radius-server timeout** *seconds*

**no radius-server timeout**

seconds	设置交换机等待来自 RADIUS Server 的 Response 的超时时间。 默认 5 秒
---------	---

## 命令模式

全局配置模式

## 默认

默认值是5秒。

## 使用说明

使用此命令来设置一个交换机和一台服务器response报文超时之前等待的秒数。如果设备到RADIUS服务器之间跳数较多，我们建议您配置RADIUS服务器超时为15秒。举例说明。

设置交换机等待来自RADIUS Server的Response的超时时间为15秒。

```
Switch(config)# radius retransmit 15
```

## 相关命令

**radius-server host**

**radius-server key**

## 6.12.5 radius-server key

使用“radius-server key”命令设置交换机与认证服务器交互的共享密钥。  
在原命令之前加上关键字“no”，删除该配置。

### 命令语法

**radius-server key** *key-string*

**no radius-server key**

key-string	交换机与认证服务器交互的共享密钥
------------	------------------

### 命令模式

全局配置模式

### 默认

无

### 使用说明

缺省没有共享密钥；  
共享密钥的长度在1-64个字符之间。

### 举例说明

设置交换机与认证服务器交互的共享密钥为“simple-key”

```
Switch(config)# radius-server key simple-key
```

### 相关命令

**radius-server host**

## 6.12.6 show radius-server

使用“show radius-server”命令显示dot1x的Radius服务器状态。

### 命令语法

**show radius-server**

### 命令模式

特权模式

## 默认

无

## 使用说明

使用此命令显示每个会话中除以激活状态和非激活状态下的所有Radius服务器。

## 举例说明

在特权模式下使用“show radius-server”命令。

```
Switch# show radius-server
=====
802.1X session on interface eth-0-9:
current radius server:
  retransmit count   : 3
  server address     : 3.3.3.3:1812
  socket descriptor  : 15
  last state         :
radius servers in dead list:
  N/A
=====
```

## 相关命令

**radius-server host**

## 6.13 TACACS+认证命令

### 6.13.1 clear tacacs statistics

使用此命令，清空所有 TACACS 统计值。

## 命令语法

**clear tacacs statistics**

## 命令模式

特权模式

## 使用说明

使用此命令，清空所有 TACACS 统计值。

## 举例说明

下面举例，清空所有 TACACS 统计值。

```
Switch(config)# clear tacacs statistics
```

## 相关命令

**show tacacs**

### 6.13.2 show tacacs

使用此命令，显示 TACACS+ 相关统计。

## 命令语法

**show tacacs**

## 命令模式

特权模式

## 使用说明

使用此命令，显示 TACACS+ 相关统计。

## 举例说明

下面举例，显示系统中 TACACS+ 相关统计信息。

```
Switch# show tacacs
Tacacs+ Server      : 1.2.3.4/49
      Socket opens:      1
      Socket closes:    0
      Socket aborts:    0
      Socket errors:    0
      Socket Timeouts:  0
Failed Connect Attempts: 0
      Total Packets Sent: 2
      Total Packets Recv: 2
```

区域	描述
Tacacs+ Server	TACACS+服务器的 IP 地址
Socket opens	成功通过 TCP 连接到 TACACS+服务器连接数量
Socket closes	成功关闭 TCP 连接通信数量
Socket aborts	到 TACACS+服务器的 TCP 连接异常中断的数量
Socket errors	类似错误数据包格式或长度的其他连接读写错误
Failed Connect Attempts	连接 TACACS+服务器失败的 TCP 连接通信数量
Total Packets Sent	TACACS+服务器收到数据包数量

区域	描述
Total Packets Recv	TACACS+服务器发送的回复数据包数量

## 相关命令

**tacacs-server host**

### 6.13.3 tacacs-server host

使用此命令，增删 TACACS+服务器。

## 命令语法

**tacacs-server host** [ **mgmt-if** ] *ip-address* [ **single-connection** | **port** *port-number* | **timeout** *integer* | **key** *string* ] \* [ **single-connection** | **port** *port-number* | **timeout** *integer* | **key** *string* | **source-interface** *IFNAME* | **source-ip** *source-ip-address* ] \*

**no tacacs-server host** [ **mgmt-if** ] *ip-address*

mgmt-if	通过管理口认证
ip-address	服务器 IP 地址
single-connection	维持 TCP 连接
port-number	TACACS+ 端口号
integer	服务器应答超时时间，取值范围为 1~20
string	TACACS+ 加密字
IFNAME	指定源接口名称
source-ip-address	指定源 IP 地址

## 命令模式

全局配置模式

## 默认

TACACS+ 端口号的默认值为 49；服务器应答超时时间的默认值为 5 秒。

## 使用说明

此命令可用来增删 TACACS+ 服务器。如果指定了源接口或者源 IP 地址，将会使用对应的 IP 地址作为发出报文的源 IP 地址。



## 举例说明

配置 10.10.10.1 的 TACACS+ 服务器：

```
Switch(config)# tacacs-server host 10.10.10.1 port 55 key my_key
```

## 6.14 Port-Isolate 命令

### 6.14.1 port-isolate group

使用 “port-isolate group” 指定端口所在的隔离组号。

在原命令前加上关键字 “no” 删除该配置。

## 命令语法

**port-isolate group** *group*

**no port-isolate group**

group	隔离组号。有效范围 1-30
-------	----------------

## 命令模式

端口配置模式

## 使用说明

属于同一隔离组的两个端口之间将受端口隔离功能的控制。属于不同隔离组的两个端口不受该功能影响。

隔离组可以配在物理端口或者聚合端口上。

## 举例

设置端口属于隔离组 4。

```
Switch(config-if)# port-isolate group 4
```

## 相关命令

**port-isolate mode**

### 6.14.2 port-isolate mode

使用 “port-isolate mode” 命令配置端口隔离的模式。有隔离二层报文和全部隔离两种模式可供选择。

在原命令前加上关键字 “no” 恢复该配置为默认值。

## 命令语法

**port-isolate mode (all | l2)**

**no port-isolate mode**

all	隔离所有二层报文和三层报文
l2	仅隔离二层报文

## 命令模式

全局配置模式

## 使用说明

如果隔离模式为隔离二层，三层报文将不受影响。

如果隔离模式为全部隔离，所有报文都将受端口隔离功能的控制。

默认值为仅隔离二层。

## 举例

配置端口隔离模式为全部隔离。

```
Switch(config)# port-isolate mode all
```

## 相关命令

**port-isolate group**

### 6.14.3 show port-isolate

使用“show port-isolate”命令显示端口隔离相关配置。

## 命令语法

**show port-isolate (group isolate-group-id)**

<b>group</b> isolate-group-id	隔离组号。有效范围 1-
-------------------------------	--------------

## 命令模式

特权模式

## 使用说明

如果不指定隔离组号，所有端口隔离信息都将被显示。

## 举例

显示命令的输出结果

```
switch # show port-isolate group 12
Port Isolate Mode : L2
-----
Port Isolate Groups:
-----
Groups ID: 12
eth-0-1   eth-0-2   eth-0-3   eth-0-4   eth-0-5
eth-0-6
-----
```

## 相关命令

**port-isolate group**

## 6.15 私有 Vlan 命令

### 6.15.1 switchport mode private-vlan

在接口下使用“switchport mode private-vlan”，将交换机端口模式配置为私有 vlan。

## 命令语法

**switchport mode private-vlan** (*host* | *promiscuous*)

host	设置私有 vlan 端口类型为主机端口
promiscuous	设置私有 vlan 端口类型为混杂端口

## 命令模式

接口模式

## 默认值

默认交换机端口模式是 access 端口。

## 使用说明

在接口下使用“switchport mode private-vlan”，将交换机端口模式配置为私有 vlan。

只可在二层端口使用该命令。

## 举例

```
Switch(config)# interface eth-0-1
Switch (config-if)# switchport mode private-vlan host
Switch (config-if)# switchport mode private-vlan promiscuous
```

## 相关命令

**switchport private-vlan**

### 6.15.2 switchport private-vlan

在接口模式下使用“witchport private-vlan”命令指定私有 vlan 的主 vlan 和子 vlan。

使用该命令的 no 模式来恢复默认值。

## 命令语法

**switchport private-vlan <1-4094> (isolate | community-vlan <1-4094> |)**

private-vlan <1-4094>	设置主 vlan，范围在 1-4094
isolate	配置为隔离端口
community-vlan <1-4094>	配置为互通端口，设置子 vlan，范围在 1-4094

## 命令模式

接口模式

## 默认值

默认主 vlan 都是 1。

主机端口的默认是隔离端口，主 vlan1。隔离端口不存在子 vlan。

混杂端口默认主 vlan 是 1。

## 用法

在接口模式下使用“witchport private-vlan”命令指定私有 vlan 的主 vlan 和子 vlan。

只可在二层端口使用该命令。

## 举例

```
Switch (config)# interface eth-0-1
Switch (config-if)# switchport mode private-vlan host
Switch (config-if)# switchport private-vlan 1 isolate
```

```
Switch (config-if)# quit
Switch (config)# interface eth-0-2
Switch (config-if)# switchport mode private-vlan host
Switch (config-if)# switchport private-vlan 1 community-vlan 2
Switch (config-if)# quit
Switch (config)# interface eth-0-3
Switch (config-if)# switchport mode private-vlan promiscuous
Switch (config-if)# switchport private-vlan 1
```

## 相关命令

switchport mode private-vlan

### 6.15.3 show private-vlan

在 EXEC 模式下使用该命令，显示私有 vlan 配置情况。

## 命令语法

**show private-vlan (vlan <1-4094> | interface IFPHYSICAL | interface IFAGG )**

vlan <1-4094>	根据主 vlan 显示
interface IFPHYSICAL   interface IFAGG	根据接口显示

## 命令模式

特权模式

## 默认值

无

## 用法

无.

## 举例

```
Switch# show private-vlan
Primary   Secondary Type          Ports
-----
1         N/A        promiscuous    eth-0-3
1         N/A        isloate       eth-0-1
1         2         community     eth-0-2
DUT1# show private-vlan vlan 1
Primary   Secondary Type          Ports
-----
```

```

1          N/A          promiscuous   eth-0-3
1          N/A          isolate      eth-0-1
1          2            community     eth-0-2
DUT1# show private-vlan interface eth-0-1
-----
Private vlan mode: isolate
Primary vlan id   : 1

```

## 相关命令

**switchport mode private-vlan**

**switchport private-vlan**

## 6.16 DDOS 命令

### 6.16.1 ip icmp intercept

可以用在全局配置模式下的 **ip icmp intercept** 命令，来配置交换机防御 ICMP 泛洪攻击。使用命令相应的 **no** 形式关闭该项功能。

## 命令语法

**ip icmp intercept [maxcount *NUMBER*]**

**no ip icmp intercept**

maxcount	设定最大接收数据包的速率
NUMBER	每秒接收相应数据包的个数，范围为 0-1000，默认值为 500

## 命令模式

全局配置模式

## 默认

默认情况下此功能未打开。

## 使用说明

使用该条命令可以设置系统限制接收 ICMP 报文的速率。

## 举例说明

下面的例子表明了如何在设备上启用 ICMP 泛洪攻击检测：

```
Switch(config)# ip icmp intercept maxcount 100
```

下面的例子为关闭 ICMP 泛洪攻击检测：

```
Switch(config)# no ip icmp intercept
```

## 相关命令

**show ip-intercept config**

### 6.16.2 ip smurf intercept

在全局配置模式下使用 `ip smurf intercept` 命令，来配置交换机防御 smurf 攻击。使用命令相应的 `no` 形式关闭该项功能。

## 命令语法

**ip smurf intercept**

**no ip smurf intercept**

## 命令模式

全局配置模式

## 默认

默认情况下此功能未打开。

## 使用说明

使用该条命令可以配置系统抵御 smurf 攻击。

## 举例说明

下面的例子为配置防御 smurf 攻击检测：

```
Switch(config)# ip smurf intercept
```

下面的例子为关闭 smurf 攻击检测：

```
Switch(config)# no ip smurf intercept
```

## 相关命令

**show ip-intercept config**

### 6.16.3 ip fraggle intercept

在全局配置模式下使用 `ip fraggle intercept` 命令，来配置交换机防御 fraggle 攻击。使用命令相应的 `no` 形式关闭该项功能。

## 命令语法

**ip fraggle intercept**  
**no ip fraggle intercept**

## 命令模式

全局配置模式

## 默认

默认情况下此功能未打开。

## 使用说明

使用该条命令可以配置系统抵御 fraggle 攻击。

## 举例说明

下面的例子为配置防御攻击检测：

```
Switch(config)# ip fraggle intercept
```

下面的例子为关闭 fraggle 攻击检测：

```
Switch(config)# no ip fraggle intercept
```

## 相关命令

**show ip-intercept config**

### 6.16.4 ip udp intercept

在全局配置模式下使用 `ip udp intercept` 命令，来配置交换机防御 UDP 泛洪攻击。使用命令相应的 `no` 形式关闭该项功能。

## 命令语法

**ip udp intercept (maxcount NUMBER |)**  
**no ip udp intercept**

maxcount	设定最大接收数据包的速率
NUMBER	每秒接收相应数据包的个数，范围为 0-1000，默认值为 500

## 命令模式

全局配置模式



## 默认

默认情况下此功能未打开。

## 使用说明

使用该条命令可以设置系统限制接收 UDP 报文的速率。

## 举例说明

下面的例子为配置防御 UDP 泛洪攻击检测：

```
Switch(config)# ip udp intercept maxcount 100
```

下面的例子为关闭 UDP 泛洪检测：

```
Switch(config)# no ip udp intercept
```

## 相关命令

**show ip-intercept config**

### 6.16.5 ip tcp intercept

可以用在全局配置模式下的 **ip tcp intercept** 命令，来配置交换机防御 SYN 泛洪攻击。使用命令相应的 **no** 形式关闭该项功能。

## 命令语法

**ip tcp intercept (maxcount NUMBER|)**

**no ip tcp intercept**

maxcount	设定最大接收数据包的速率
NUMBER	每秒接收相应数据包的个数，范围为 0-1000，默认值为 500

## 命令模式

全局配置模式

## 默认

默认情况下此功能未打开。

## 使用说明

使用该条命令可以设置系统限制接收 TCP 协议的 SYN 报文的速率。

## 举例说明

下面的例子为配置防御 SYN 泛洪攻击检测：

```
Switch(config)# ip tcp intercept maxcount 100
```

下面的例子为关闭 SYN 泛洪攻击检测：

```
Switch(config)# no ip tcp intercept
```

## 相关命令

**show ip-intercept config**

### 6.16.6 ip small-packet intercept

在全局配置模式下，使用 `ip small-packet intercept` 命令配置系统过滤 ip 小报文。使用命令相应的 `no` 形式关闭该项功能。

## 命令语法

**ip small-packet intercept (length *NUMber* |)**

**no ip small-packet intercept**

length	设定 ip 小报文的长度
NUMber	接收 IP 报文的最小长度，范围为 28-65535，默认值为 28

## 命令模式

全局配置模式

## 默认

默认情况下此功能未打开。

## 使用说明

使用该条命令可以设置系统丢弃 IP 报文长度小于命令配置长度。

## 举例说明

下面的例子为配置防御 IP 小报文攻击检测：

```
Switch(config)# ip small-packet intercept length 32
```

下面的例子为关闭 IP 小报文检测：

```
Switch(config)# no small-packet intercept
```

## 相关命令

**show ip-intercept config**

### 6.16.7 ip maceq intercept

在全局配置模式下，使用 **ip maceq intercept** 命令配置系统过滤源 MAC 地址等于目的 MAC 地址的报文。使用命令相应的 **no** 形式关闭该项功能。

## 命令语法

**ip maceq intercept**

**no ip maceq intercept**

## 命令模式

全局配置模式

## 默认

默认情况下此功能未打开。

## 使用说明

使用该条命令可以设置系统丢弃源 MAC 地址等于目的 MAC 地址的报文。

## 举例说明

下面的例子为配置防御目的 MAC 地址等于源 MAC 地址的报文攻击检测：

```
Switch(config)# ip maceq intercept
```

下面的例子为关闭目的 MAC 地址等于源 MAC 地址的报文攻击检测：

```
Switch(config)# no ip maceq intercept
```

## 相关命令

**show ip-intercept config**

### 6.16.8 ip ipeq intercept

在全局配置模式下，使用 **ip ipeq intercept** 命令配置系统过滤源 IP 地址等于目的 IP 地址的报文。使用命令相应的 **no** 形式关闭该项功能。

## 命令语法

**ip ipeq intercept**

**no ip ipeq intercept**

## 命令模式

全局配置模式

## 默认

默认情况下此功能未打开。

## 使用说明

使用该条命令可以设置系统丢弃源 MAC 地址等于目的 MAC 地址的报文。

## 举例说明

下面的例子为配置防御目的 IP 地址等于源 IP 地址的报文攻击检测：

```
Switch(config)# ip ipeq intercept
```

下面的例子为关闭目的 IP 地址等于源 IP 地址的报文攻击检测：

```
Switch(config)# no ip ipeq intercept
```

## 相关命令

**show ip-intercept config**

### 6.16.9 show ip-intercept config

在特权模式下，使用 show ip-intercept config 命令显示当前 DDoS 防御配置。

## 命令语法

**show ip-intercept config**

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面的例子显示系统当前 DDoS 防御配置：

```
Switch# show ip-intercept config  
Current DDoS Prevent configuration:
```

```

=====
ICMP Flood Intercept           :Enable  Maxconut:100
UDP Flood Intercept           :Enable  Maxconut:100
SYN Flood Intercept           :Enable  Maxconut:100
Small-packet Attack Intercept :Enable  Packet Length:32
Sumrf Attack Intercept        :Enable
Fraggle Attack Intercept      :Enable
MAC Equal Intercept           :Disable
IP Equal Intercept            :Disable

```

## 相关命令

**ip icmp intercept**

**ip smurf intercept**

**ip udp intercept**

**ip tcp intercept**

**ip small-packet intercept**

**ip maceq intercept**

**ip ipeq intercept**

## 6.16.10 show ip-intercept statistics

在特权模式下，使用 `show ip-intercept statistics` 命令显示当前攻击检测丢包统计信息。

## 命令语法

**show ip-intercept statistics**

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面的例子显示当前系统攻击检测丢包统计信息：

```

Switch# show ip-intercept statistics
Current DDoS Prevent statistics:
=====
Resist Small-packet Attack packets number   : 108
Resist ICMP Flood packets number            : 0

```

```
Resist Smurf Attack packets number      : 0
Resist SYN Flood packets number         : 0
Resist Fraggle Attack packets number    : 0
Resist UDP Flood packets number         : 0
```

## 相关命令

**clear ip-intercept statistics**

### 6.16.11 clear ip-intercept statistics

在特权模式下，使用 `clear ip-intercept statistics` 命令清除攻击检测丢包统计信息。

## 命令语法

**clear ip-intercept statistics**

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面的例子为清除攻击检测丢包统计信息：

```
Switch# clear ip-intercept statistics
Switch# show ip-intercept statistics
Current DDoS Prevent statistics:
=====
Resist Small-packet Attack packets number      : 0
Resist ICMP Flood packets number               : 0
Resist Smurf Attack packets number             : 0
Resist SYN Flood packets number                : 0
Resist Fraggle Attack packets number           : 0
Resist UDP Flood packets number                : 0
```

## 相关命令

**show ip-intercept statistics**

## 6.17 Key Chain 命令

### 6.17.1 key chain

在全局配置模式下，使用命令 `key chain` 创建密钥链。使用该命令的 `no` 形式删除配置。

#### 命令语法

**key chain** *WORD*

**no key chain** *WORD*

WORD	密钥链名称，不超过 20 个字符
------	------------------

#### 命令模式

全局配置模式

#### 默认

没有密钥链被创建

#### 使用说明

密钥链通常使用在路由协议或网络应用中，具体的应用配置参见相关章节的配置文档。

#### 举例说明

配置密钥链：

```
Switch(config)# key chain test
```

#### 相关命令

**key**

**key-string**

**show key chain**

### 6.17.2 key

在密钥链配置模式下，使用命令 `key` 创建密钥。使用命令相关的 `no` 形式删除该配置。

#### 命令语法

**key** <0-31>

**no key <0-31>**

## 命令模式

密钥链配置模式

## 默认

密钥链中没有配置密钥。

## 使用说明

只有密钥中配置了密钥字符串，该密钥才会被使用。

## 举例说明

配置密钥 1:

```
Switch(config-keychain)# key 1
```

## 相关命令

**key chain**

**key-string**

**accept-lifetime**

**send-lifetime**

### 6.17.3 key-string

在密钥配置模式下，使用命令 **key-string** 配置密钥字符串。使用命令相关的 **no** 形式删除配置。

## 命令语法

**key-string** *LINE*

**no key-string** *LINE*

LINE	密钥字符串，允许长度为 0~255
------	-------------------

## 命令模式

密钥配置模式



## 默认

没有配置密钥字符串

## 使用说明

使用该命令配置密钥的字符串，如果不设置发送或接收的有效时间，则密钥永久有效。

## 举例说明

配置密钥字符串：

```
Switch(config-keychain-key)# key-string ##test_keywords##
```

## 相关命令

**key**

**accept-lifetime**

**send-lifetime**

### 6.17.4 accept-lifetime

在密钥配置模式下，使用 **accept-lifetime** 命令配置密钥的有效接收时间。使用命令的 **no** 形式删除配置。

## 命令语法

**accept-lifetime** *START-TIME EXPIRE-TIME*

**no accept-lifetime**

<b>START-TIME</b>	密钥有效接收开始时间，格式可以为： <b>HH:MM:SS &lt;1-31&gt; MONTH &lt;1993-2035&gt;</b> 或 <b>HH:MM:SS MONTH &lt;1-31&gt; &lt;1993-2035&gt;</b> ，其中 <b>MONTH</b> 为月份英文首位三个字母
<b>EXPIRE-TIME</b>	密钥有效接收结束时间，格式可以为： <b>HH:MM:SS &lt;1-31&gt; MONTH &lt;1993-2035&gt;</b> ， <b>HH:MM:SS MONTH &lt;1-31&gt; &lt;1993-2035&gt;</b> ， <b>Infinite</b> ， <b>duration &lt;1-2147483646&gt;</b> ，其中 <b>MONTH</b> 为月份英文首位三个字母

## 命令模式

密钥配置模式

## 默认

密钥接收永久有效。

## 使用说明

该命令配置密钥的接收有效时间，当时间到期以后该密钥无效。

## 举例说明

配置密钥有效接收时间从 2012-1-2 00:00:01 开始：

```
Switch(config-keychain-key)# accept-lifetime 0:0:1 2 jan 2012 infinite
```

## 相关命令

**key**

**key-string**

## 6.17.5 send-lifetime

在密钥配置模式下，使用 `send-lifetime` 命令配置密钥的有效发送时间。使用命令的 `no` 形式删除配置。

## 命令语法

**send-lifetime** *START-TIME EXPIRE-TIME*

**no send-lifetime**

START-TIME	密钥有效接收开始时间，格式可以为：HH:MM:SS <1-31> MONTH <1993-2035> 或 HH:MM:SS MONTH <1-31> <1993-2035>，其中 MONTH 为月份英文首位三个字母
EXPIRE-TIME	密钥有效接收结束时间，格式可以为：HH:MM:SS <1-31> MONTH <1993-2035>，HH:MM:SS MONTH <1-31> <1993-2035>，Infinite，duration <1-2147483646>，其中 MONTH 为月份英文首位三个字母

## 命令模式

密钥配置模式

## 默认

密钥发送永久有效。

## 使用说明

该命令配置密钥的发送有效时间，当时间到期以后该密钥无效。

## 举例说明

配置密钥有效发送时间从 2012-1-2 00:00:01 开始：

```
Switch(config-keychain-key)# send-lifetime 0:0:1 2 jan 2012 infinite
```

## 相关命令

**key**

**key-string**

### 6.17.6 show key chain

使用 show key chain 显示密钥链信息。

## 命令语法

**show key chain** (*WORD*)

WORD	密钥链名称
------	-------

## 命令模式

特权模式

## 默认

无。

## 使用说明

无

## 举例说明

显示密钥链 test-chain 信息：

```
Switch# show key chain test
key chain test:
  key 1 -- text "key-string ##test_keywords_1##"
    accept-lifetime <00:00:01 Jan 01 2012> - <infinite>
    send-lifetime <always valid> - <always valid> [valid now]
  key 2 -- text "key-string ##test_keywords_2##"
    accept-lifetime <always valid> - <always valid> [valid now]
```

```
send-lifetime <00:00:01 Jan 02 2012> - <infinite>
```

## 相关命令

**key chain**

**key**

**key-string**

## 6.18 Port Block 命令

### 6.18.1 port-block

在端口配置模式下，使用命令 `port-block` 创建端口阻塞。使用该命令的 `no` 形式删除配置。

## 命令语法

**port-block (known-unicast | known-multicast | unknown-unicast | unknown-multicast | broadcast)**

**no port-block (known-unicast | known-multicast | unknown-unicast | unknown-multicast | broadcast)**

known-unicast	对目的 MAC 地址已知的单播进行阻塞
known-multicast	对目的 MAC 地址已知的组播进行阻塞
unknown-unicast	对目的 MAC 地址未知的单播进行阻塞
unknown-multicast	对目的 MAC 地址未知的组播进行阻塞
broadcast	对广播进行阻塞

## 命令模式

端口配置模式

## 默认

对 MAC 地址已知的单播和组播都是不阻塞的；

对 MAC 地址未知的单播和组播都是不阻塞的；

广播也是不阻塞的。

## 使用说明

默认情况下，MAC 地址未知的单播或组播可以传输到所有端口。用户在端口上可以配置该命令行对这些报文进行阻塞。在被保护的端口没有对这类报文进行阻塞，将可能出现安全问题。

port-block 只对二层组播报文有效，包含三层头信息的组播报文将不被阻塞。

## 举例说明

对已知单播进行阻塞配置：

```
Switch(config-if)# port-block known-unicast
```

## 相关命令

**show port-block (interface IFPHYSICAL | interface IFAGG |)**

### 6.18.2 show port-block

在特权模式下，显示指定端口的 port-block 配置信息。

## 命令语法

**show port-block (interface IFPHYSICAL | interface IFAGG |)**

IFPHYSICAL	指定物理端口
IFAGG	指定 agg 端口

## 命令模式

特权模式

## 默认

N/A

## 使用说明

显示指定端口的 port-block 配置信息。

## 举例说明

显示端口的 port-block 配置信息：

```
Switch# show port-block interface eth-0-1
```

## 相关命令

**port-block (known-unicast | known-multicast | unknown-unicast | unknown-multicast | broadcast)**

## 6.19 设备管理安全命令

### 6.19.1 telnet server acl

在全局配置模式下，使用该命令可以过滤 telnet client ip。使用该命令的 no 形式删除配置。

#### 命令语法

**telnet server acl NAME**

**no telnet server acl**

<b>NAME</b>	对应创建的 policy-map 名字，该 policy-map
-------------	----------------------------------

#### 命令模式

全局配置模式

#### 默认

不过滤任何 telnet client ip;

#### 使用说明

为了防止网络上的暴力破解，可以使用该命令过滤指定的 telnet client ip。

#### 举例说明

启用 telnet acl，过滤源 ip 为 1.1.1.1 的报文：

```
Switch(config)# ip access-list telnetACL
Switch(config-ip-acl)# 10 deny tcp host 1.1.1.1 any
Switch(config-ip-acl)# class-map match-any cmap
Switch(config-cmap)# match access-group telnetACL
Switch(config-cmap)# policy-map pmap
Switch(config-pmap)# class cmap
Switch(config-pmap-c)# telnet server acl pmap
```

#### 相关命令

无

## 6.19.2 ssh server acl

在全局配置模式下，使用该命令可以过滤 ssh client ip。使用该命令的 no 形式删除配置。

### 命令语法

**ssh server acl NAME**

**no ssh server acl**

<b>NAME</b>	对应创建的 policy-map 名字
-------------	---------------------

### 命令模式

全局配置模式

### 默认

不过滤任何 ssh client ip;

### 使用说明

为了防止暴力破解，可以使用该命令过滤指定的 ssh client ip。

### 举例说明

启用 ssh acl:

启用 ssh acl，过滤源 ip 为 1.1.1.1 的报文:

```
Switch(config)# ip access-list sshACL
Switch(config-ip-acl)# 10 deny tcp host 1.1.1.1 any
Switch(config-ip-acl)# class-map match-any cmap
Switch(config-cmap)# match access-group sshACL
Switch(config-cmap)# policy-map pmap
Switch(config-pmap)# class cmap
Switch(config-pmap-c)# ssh server acl pmap
```

### 相关命令

无

# 7 IP 业务命令行参考

## 7.1 ARP 命令

### 7.1.1 arp

此命令添加一条静态 ARP，使用该命令的 no 形式来删除静态配置的 ARP。

#### 命令语法

**arp** ( *vrf VRF-NAME* | ) *IP-ADDRESS HARDWARE-ADDRESS*

**no arp** ( *vrf VRF-NAME* | ) *IP-ADDRESS*

<i>vrf VRF-NAME</i>	VRF 实例名字
<i>IP-ADDRESS</i>	要添加的静态映射的 IP 地址
<i>HARDWARE-ADDRESS</i>	要添加的静态映射的 MAC 地址，格式为 HHHH.HHHH.HHHH

#### 命令模式

全局配置模式

#### 默认

无

#### 使用说明

所添加的 IP 地址不能为广播地址、多播地址或者本地环回地址；或者形如 0.X.X.X/8 的地址；所添加的 MAC 地址不能为广播地址、多播地址，设备本身地址，或者全 0 地址；添加的静态 ARP 不能被 `clear arp-cache` 命令删除。

#### 举例说明

下面的例子显示了如何添加一条静态 ARP：

```
Switch(config)# arp 10.31.7.19 0800.900.1834
```



## 相关命令

**clear arp-cache**

### 7.1.2 arp retry-interval

此命令设置本地发送 ARP 请求报文的频率，即解析同一个 IP 地址，发送连续 2 次 ARP 请求报文的时间间隔。使用关键字 **no** 恢复此时间间隔为默认值。

## 命令语法

**arp retry-interval** *SECONDS*

**no arp retry-interval**

<i>SECONDS</i>	发送 ARP 请求报文的时间间隔，以秒为单位，范围<1,10>
----------------	---------------------------------

## 命令模式

端口配置模式

## 默认

10 秒

## 使用说明

默认重发 ARP 请求报文的时间间隔为 10 秒；此功能不能配置在 2 层端口上；使用 **no switchport** 命令关闭端口的二层功能。

## 举例说明

设置设备发送 ARP 请求报文的时间间隔为 3 秒：

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# arp retry-interval 3
```

## 相关命令

**show interface**

### 7.1.3 arp timeout

此命令设置动态 ARP 表项的老化时间。使用关键字 **no** 恢复老化时间为默认值。

## 命令语法

**arp timeout** *SECONDS*

**no arp timeout**

<i>SECONDS</i>	ARP 表项的老化时间，以秒为单位，范围<1-2147483>
----------------	---------------------------------

## 命令模式

端口配置模式

## 默认

3600 秒

## 使用说明

默认老化时间是 3600 秒；

此功能不能配置在 2 层端口上。

## 举例说明

设置动态 ARP 表项的老化时间为 1200 秒：

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# arp timeout 1200
```

## 相关命令

**show interface**

### 7.1.4 clear arp-cache

使用此命令更新 ARP cache。使用此命令后，系统将探测 ARP cache 中的各项，探测失败的项将被清除。

## 命令语法

**clear arp-cache** [ *vrf vrf-name* ] [ *interface interface-name* ] [ **force-delete** ]

<i>vrf-name</i>	如果指定了此项，则更新此 VRF 内的 ARP cache；如果没有指定此项，则更新公网内学习的 ARP 表项
<i>interface-name</i>	如果指定了此项，则更新此端口的 ARP cache；如果没有指定此项，则更新所有端口学习的 ARP 表项

<b>force-delete</b>	如果指定了此项，则强制删除指定 ARP cache 中的所有非静态 ARP 表项；如果没有指定此项，则更新指定 ARP cache 中的 ARP 表项
---------------------	---

## 命令模式

特权模式

## 默认

无

## 使用说明

此命令不能更新静态 ARP 表项。

## 举例说明

更新公网内所有动态 ARP 表项：

```
Switch# clear arp-cache
```

## 7.1.5 clear ip arp

使用此命令更新某个指定的动态 ARP 表项。使用此命令后，系统将探测这条 ARP，若探测失败则该 ARP 被清除。

## 命令语法

```
clear ip arp [ vrf vrf-name ] ip-address [ force-delete ]
```

vrf-name	如果指定了此项，则更新此 VRF 内的 ARP cache；如果没有指定此项，则更新公网内学习的 ARP 表项
ip-address	更新指定的 ARP 表项
force-delete	如果指定了此项，则强制删除指定 ARP 表项，不触发老化学习机制；如果没有指定此项，则更新指定 ARP 表项

## 命令模式

特权模式

## 默认

无

## 使用说明

此命令用于更新指定 IP 地址的动态 ARP 表项。force-delete 命令无法强制删除静态 ARP 表项。

## 举例说明

更新公网内的指定 ARP 表项：

```
Switch# clear ip arp 10.10.10.10
```

## 7.1.6 clear ip arp statistics

使用此命令清除 ARP 报文统计消息。

## 命令语法

**clear ip arp (vrf *VRF-NAME* |) statistics**

<b>vrf <i>VRF-NAME</i></b>	如果指定了此项，则清除此 VRF 内的 ARP 统计信息；如果没有指定此项，则清除公网内 ARP 统计信息
----------------------------	---

## 命令模式

特权模式

## 默认

无

## 使用说明

此命令用于清除 ARP 统计信息。

## 举例说明

下面的例子描述了如何清除 ARP 统计信息：

```
Switch# clear ip arp statistics
```

## 相关命令

**show ip arp summary**

## 7.1.7 show ip arp

使用此命令查看所有 ARP 条目，包括动态的和静态的。

## 命令语法

**show ip arp ((vrf *VRF-NAME*) interface *INTERFACE-NAME* )**

<b>vrf <i>VRF-NAME</i></b>	如果指定了此项，则查看此 VRF 内的 ARP cache；如果没有指定此项，则查看公网内学习的 ARP 表项
<b><i>INTERFACE-NAME</i></b>	如果指定了此项，则查看此端口的 ARP cache；如果没有指定此项，则查看所有端口学习的 ARP 表项

## 命令模式

特权模式

## 默认

无

## 使用说明

显示所有的 ARP 表项信息。

## 举例说明

下面的例子描述了如何查看公网内所有的 ARP 表项信息：

Switch# show ip arp

Protocol	Address	Age (min)	Hardware Addr	Interface
Internet	1.1.1.1	-	7cb5.0157.0c00	eth-0-1
Internet	2.2.2.1	-	7cb5.0157.0c00	eth-0-2
Internet	3.3.3.1	-	7cb5.0157.0c00	eth-0-3
Internet	10.0.20.1	-	7cb5.0157.0c00	eth-0-10
Internet	10.0.20.254	-	0000.5e00.0101	eth-0-10

## 相关命令

**clear ip arp**

### 7.1.8 show ip arp summary

使用此命令查看 ARP 表项的统计信息。

## 命令语法

**show ip arp ( vrf *VRF-NAME* ) summary**

<b>vrf VRF-NAME</b>	VRF 名称；如果指定了此项，则表示查看此 VRF 内的 ARP 表项统计信息；否则查看公网内的 ARP 表项统计信息
---------------------	---

## 命令模式

特权模式

## 默认

无

## 使用说明

显示 ARP 表项的统计信息。

## 举例说明

下面的例子描述了如何查看公网内 ARP 表项的统计信息：

```
Switch# show ip arp summary
```

```
Gratuitous ARP learning is disabled
2 IP ARP entries, with 0 of them incomplete
(Static:1, Dyamic:0, Interface:1)
ARP Pkt Received is: 0
ARP Pkt Send number is: 1
ARP Pkt Dicard number is: 0
```

## 相关命令

**clear ip arp statistics**

## 7.1.9 debug arp

使用此命令打开 ARP 的调试开关，使用该命令的 no 形式关掉 ARP 调试。

## 命令语法

**debug arp (vrf VRF-NAME |)**

<b>vrf VRF-NAME</b>	VRF 名称；如果指定了此项，则表示只打开此 VRF 内的 ARP 调试开关；否则打开公网内的 ARP 调试开关
---------------------	--

## 命令模式

特权模式

## 默认

无

## 使用说明

打开 ARP 的调试开关，用户可以看到 ARP 报文的接收和发送信息，以及 ARP 表项的创建，更新和删除过程。

## 举例说明

下面的例子描述了如何打开 ARP 调试开关：

```
Switch# debug arp
```

```
Sep  7 03:34:08 SWITCH ARP-7: IP ARP: creating entry for IP address: 7.7.7.7, hw:
e64d. 0445. df00
```

```
Sep  7 03:34:08 SWITCH ARP-7: IP ARP: send req src 7.7.7.7 e64d. 0445. df00, dst
7.7.7.7 eth-0-1
```

## 相关命令

**show debugging arp**

### 7.1.10 show debugging arp

使用此命令查看 ARP 调试开关是否打开。

## 命令语法

**show debugging arp (vrf *VRF-NAME* )**

<b>vrf <i>VRF-NAME</i></b>	VRF 名称；如果指定了此项，则表示只打开此 VRF 内的 ARP 调试开关；否则打开公网内的 ARP 调试开关
----------------------------	--

## 命令模式

特权模式

## 默认

无

## 使用说明

显示 ARP 调试开关是否打开。

## 举例说明

下面的例子描述了如何查看公网内 ARP 调试开关是否打开：

```
Switch# show debugging arp

ARP debugging status:
  ARP packet debugging is on
```

## 相关命令

**debug arp**

### 7.1.11 proxy-arp enable

使用 **proxy-arp enable** 命令用来开启代理 ARP 功能。使用该命令的 **no** 形式来关闭代理 ARP 功能。

## 命令语法

**proxy-arp enable**  
**no proxy-arp enable**

## 命令模式

端口配置模式

## 默认

缺省情况下，关闭 ARP 代理功能。

## 使用说明

当 ARP 代理功能没有启用的时候，设备只会回复那些目的 IP 是设备自己的 ARP 请求报文。

## 举例说明

下面的例子显示了如何在端口 eth-0-1 上使能代理功能。

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# no shutdown
Switch(config-if)# ip address 1.1.1.1/24
Switch(config-if)# proxy-arp enable
```

## 相关命令

**local-proxy-arp enable**



## 7.1.12 local-proxy-arp enable

本地 ARP 代理功能使得 3 层设备可以回复那些目的 IP 和接收端口是同一个子网的 ARP 请求报文。使用 `local-proxy-arp enable` 命令使能本地 ARP 代理功能，使用该命令的 `no` 形式关闭本地 ARP 代理功能。

### 命令语法

**local-proxy-arp enable**

**no local-proxy-arp enable**

### 命令模式

端口配置模式

### 默认

缺省情况下，本地 ARP 代理功能不使能。

### 使用说明

本地 ARP 代理最常见的应用场景是交换机或其下挂的交换机开启了二层端口隔离功能。使能本地 ARP 代理功能的时候，ICMP 重定向功能被自动关闭。

### 举例说明

下面的例子显示了如何在端口 `eth-0-1` 上使能本地 ARP 代理功能：

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# no shutdown
Switch(config-if)# ip address 1.1.1.1/24
Switch(config-if)# local-proxy-arp enable
```

### 相关命令

**proxy-arp enable**

## 7.1.13 gratuitous-arp-learning enable

使用命令 **gratuitous-arp-learning enable** 来使能设备的免费 ARP 学习功能，使用该命令的 `no` 形式关闭免费 ARP 学习功能。

### 命令语法

**gratuitous-arp-learning enable**

**no gratuitous-arp-learning enable**

## 命令模式

全局配置模式

## 默认

缺省情况下，关闭设备的免费 ARP 学习功能

## 使用说明

无

## 举例说明

下面的例子显示了如何使能端口 eth-0-1 上的免费 ARP 学习功能：

```
Switch(config)# gratuitous-arp-learning enable
```

## 相关命令

```
show ip arp summary
```

## 7.2 DHCP Client 命令

### 7.2.1 ip address dhcp

使用此命令通过 DHCP 获得 ip 地址。使用关键字 no 删除获得的 ip 地址，并取消 DHCP client 功能。

## 命令语法

```
ip address dhcp
```

```
no ip address dhcp
```

## 命令模式

端口配置模式

## 默认

没有启用 DHCP client。

## 使用说明

此命令在接口上启用 DHCP client 功能；如果接口处于打开状态，则立即开始通过 DHCP 获得 ip 地址。否则该接口的 DHCP client 功能处于挂起状态，在接口打开后，开始启用 DHCP client；使用 no 关键字，会释放获得的 ip 地址，并发送 DHCP RELEASE 消息。

## 举例说明

使用 DHCP 获得 ip 地址。

```
Switch(config-if)# ip address dhcp
```

取消 DHCP client 功能，并释放通过 DHCP 获得的 ip 地址。

```
Switch(config-if)# no ip address dhcp
```

## 相关命令

**dhcp client request**

**dhcp client client-id**

**dhcp client class-id**

**dhcp client lease**

**dhcp client hostname**

**management ip address dhcp**

**show dhcp client**

## 7.2.2 management ip address dhcp

使用此命令在管理口上通过 DHCP 获得 ip 地址。

使用关键字 no 删除获得的 ip 地址，并取消 DHCP client 功能。

## 命令语法

**management ip address dhcp**

**no management ip address dhcp**

## 命令模式

全局配置模式

## 默认

没有在管理口启用 DHCP client。

## 使用说明

此命令在管理口上启用 DHCP client 功能；使用 no 关键字，会释放获得的 ip 地址，并发送 DHCP RELEASE 消息。

## 举例说明

使用 DHCP 为管理口获得 ip 地址。

```
Switch(config)# management ip address dhcp
```

取消 DHCP client 功能，并释放通过 DHCP 获得的 ip 地址。

```
Switch(config-if)# no management ip address dhcp
```

## 相关命令

**show dhcp client**

### 7.2.3 dhcp client request

使用此命令设置 client 通过 DHCP 获得指定的配置参数。使用 no 关键字，取消请求的参数。

## 命令语法

**dhcp client request ( router | static-route | classless-static-route | classless-static-route-ms | tftp-server-address | dns-nameserver | domain-name | netbios-nameserver | vendor-specific )**

**no dhcp client request ( router | static-route | classless-static-route | classless-static-route-ms | tftp-server-address | dns-nameserver | domain-name | netbios-nameserver | vendor-specific )**

<b>router</b>	默认路由器选项 (3)
<b>static-route</b>	静态路由选项 (33)
<b>classless-static-route</b>	无类静态路由选项(121)
<b>classless-static-route-ms</b>	Microsoft 无类静态路由选项 (249)
<b>tftp-server-address</b>	TFTP 服务器 ip 地址选项 (150)
<b>dns-nameserver</b>	DNS 服务器选项 (6)
<b>domain-name</b>	域名选项 (15)
<b>netbios-nameserver</b>	Netbios 服务器选项 (44)
<b>vendor-specific</b>	厂商相关配置选项 (43)

## 命令模式

端口配置模式

## 默认

router, static-route, classless-static-route, classless-static-route-ms, tftp-server-address 为默认请求。

## 使用说明

此命令向 DHCP server 请求指定的配置参数，可以分多次指定所需要的参数，也可以一次指定所有需要的参数。此命令需要在 ip address dhcp 之前执行，否则只有在下一条 ip address dhcp 命令后才会生效。选项 33,121,249 之间存在优先级关系：选项 121 优先于选项 33 和选项 249，选项 249 优先于选项 33。

## 举例说明

指定请求 TFTP 服务器 ip 地址和静态路由：

```
Switch(config-if)# dhcp client request static-route tftp-server-address
```

指定请求默认路由器：

```
Switch(config-if)# dhcp client request router
```

取消默认路由器请求：

```
Switch(config-if)# no dhcp client request router
```

## 相关命令

**ip address dhcp**

### 7.2.4 dhcp client client-id

使用此命令设置 DHCP client ID, 作为 DHCP client 的标记。

使用 no 关键字删除设置的 client ID, 并使用默认的 client ID。

## 命令语法

**dhcp client client-id ( *ascii WORD* | *hex HEX-STRING* | *IFVLAN* | *IFAGG* | *IFPHYSICAL* )**

**no dhcp client client-id**

<b>ascii WORD</b>	ascii 字符串
<b>hex HEX-STRING</b>	十六进制字符串
<b>IFVLAN</b>	vlan 接口名称
<b>IFAGG</b>	agg 接口名称
<b>IFPHYSICAL</b>	物理接口名称

## 命令模式

端口配置模式

## 默认

缺省采用格式“Switch-HWADDR-IFNAME”。

## 使用说明

此命令需要在 `ip address dhcp` 之前执行，否则只有在下一条 `ip address dhcp` 命令后才会生效。

## 举例说明

设置 DHCP client ID 为 `switch-client`。

```
Switch(config-if)# dhcp client client-id ascii switch-client
```

删除设置的 DHCP client ID。

```
Switch(config-if)# no dhcp client client-id
```

## 相关命令

**ip address dhcp**

### 7.2.5 dhcp client class-id

使用此命令设置 DHCP client 的 `class-id`。

使用关键字 `no` 删除设置的 `class-id`。

## 命令语法

**dhcp client class-id** ( *WORD* | **hex** *HEX-STRING* )

**no dhcp client class-id**

<i>WORD</i>	ascii 字符串
<b>hex</b> <i>HEX-STRING</i>	十六进制字符串

## 命令模式

端口配置模式

## 默认

无

## 使用说明

DHCP client 使用 `class-id` 标记自己需要的配置参数类型。不同的厂商会定义自己的 `class-id` 标记自己的特殊配置，DHCP client 通过 `class-id` 向 server 请求这些与厂商相关的配置参数。此命令需要在 `ip address dhcp` 之前执行，否则只有在下一条 `ip address dhcp` 命令后才会生效。

## 举例说明

指定 DHCP client 的 `class-id`:

```
Switch(config-if)# dhcp client class-id acsii switch
```

删除指定的 `class-id`:

```
Switch(config-if)# no dhcp client class-id
```

## 相关命令

**ip address dhcp**

### 7.2.6 dhcp client lease

使用此命令设置 DHCP client 期望获得的租期。

使用关键字 `no` 取消设置的期望租期。

## 命令语法

**dhcp client lease** (*DAYS* (*HOURS* (*MINUTES* | )) | **infinite**)

**no dhcp client lease**

<i>DAYS</i>	租期时间，单位为天
<i>HOURS</i>	租期时间，单位为小时
<i>MINUTES</i>	租期时间，单位为分
<b>infinite</b>	租期时间为永久

## 命令模式

端口配置模式

## 默认

无

## 使用说明

设置 DHCP client 期望获得的租期，DHCP server 可以接受该租期，也可以忽略 client 的请求，分配自己设置的租期。此命令需要在 ip address dhcp 之前执行，否则只有在下一条 ip address dhcp 命令后才会生效。

## 举例说明

设置 DHCP client 期望租期为 20 分钟：

```
Switch(config-if)# dhcp client lease 0 0 20
```

删除设置的期望租期：

```
Switch(config-if)# no dhcp client lease
```

## 相关命令

**ip address dhcp**

### 7.2.7 dhcp client hostname

使用此命令设置在 DHCP 报文中使用的主机名称。

使用关键字 no 取消设置的主机名称。

## 命令语法

**dhcp client hostname** *WORD*

**no dhcp client hostname**

<i>WORD</i>	主机名称
-------------	------

## 命令模式

端口配置模式

## 默认

默认使用系统主机名称。

## 使用说明

此命令设置 DHCP 报文中的主机名称。此命令需要在 ip address dhcp 之前执行，否则只有在下一条 ip address dhcp 命令后才会生效。



## 举例说明

设置 DHCP 报文中主机名称为 switch  
 Switch(config-if)# dhcp client hostname switch  
 删除设置的主机名称  
 Switch(config-if)# no dhcp client hostname

## 相关命令

**ip address dhcp**

### 7.2.8 dhcp client default-router distance

使用此命令为从 DHCP server 获得的路由设置默认的路由器的距离。  
 使用 no 关键字删除设置的默认路由器距离。

## 命令语法

**dhcp client default-router distance *METRIC***  
**no dhcp client default-router distance**

<i>METRIC</i>	默认的路由器距离，值的范围：<1-255>
---------------	-----------------------

## 命令模式

全局配置模式

## 默认

DHCP server 获得的路由的路由器距离将被设置为默认值 254。

## 使用说明

无

## 举例说明

设置默认路由器距离为 233：  
 Switch(config)# dhcp client default-router distance 233  
 删除设置的默认路由器距离：  
 Switch(config)# no dhcp client default-router distance

## 相关命令

**ip address dhcp**

### 7.2.9 dhcp client broadcast-flag

使用此命令在 DHCP 消息中设置 broadcast flag。

使用 no 关键字，删除 broadcast flag。

## 命令语法

**dhcp client broadcast-flag**

**no dhcp client broadcast-flag**

## 命令模式

全局配置模式

## 默认

默认在请求 IP 地址阶段的 DHCP 消息中设置该标记。

## 使用说明

Broadcast flag 表示 DHCP client 在获得 IP 地址前不能接受单播 IP 报文，所以如果设置 broadcast flag，则 DHCP 服务器或 DHCP relay agent 将会广播 DHCP 消息到 client 所在的子网。

## 举例说明

设置 broadcast flag:

```
Switch(config)# dhcp client broadcast-flag
```

删除 broadcast flag:

```
Switch(config)# no dhcp client broadcast-flag
```

## 相关命令

**ip address dhcp**

### 7.2.10 debug dhcp client

使用此命令可以打开 dhcp client 的模块的调试功能。

在原命令之前加上关键字 “no”，关闭调试功能。

## 命令语法

**debug dhcp client ( events | error | packet | dump | all )**

**no debug dhcp client ( events | error | packet | dump | all )**

<b>events</b>	调试 dhcp client 事件信息
<b>error</b>	调试 dhcp client 错误信息
<b>packet</b>	调试 dhcp client 的数据包信息
<b>dump</b>	以十六进制调试 dhcp client 的数据包信息
<b>all</b>	上面提到的所有调试信息

**命令模式**

特权模式

**默认**

无

**使用说明**

使用“terminal monitor”打印消息

**举例说明**

使用如下命令，打开dhcp client的所有调试信息。

```
Switch# debug dhcp client all
```

**相关命令**

**terminal monitor**

**show logging buffer**

**7.2.11 show dhcp client**

此命令显示 DHCP client 的工作状态。

**命令语法**

**show dhcp client ( management | IFVLAN | IFAGG | IFPHYSICAL | ) (verbose)**

<b>management</b>	显示管理口的 DHCP client 工作状态
<i>IFVLAN</i>	vlan 接口名称

<i>IFAGG</i>	agg 接口名称
<i>IFPHYSICAL</i>	物理接口名称
<b>verbose</b>	详细信息

## 命令模式

特权模式

## 默认

无

## 使用说明

使用此命令查看一个或多个接口上 DHCP client 的工作状态，添加 **verbose** 查看详细信息。

## 举例说明

查看所有接口上 DHCP client 工作状态。

```
Switch# show dhcp client verbose
```

```
DHCP client informations:
=====
vlan1 DHCP client information:
  Current state: SELECT
  Transaction ID: 0x3ac1c1c7
=====
eth-0-1 DHCP client information:
  Current state: SELECT
  Transaction ID: 0x2fd3f55b
```

## 相关命令

**ip address dhcp**

### 7.2.12 show dhcp client statistics

使用此命令查看 DHCP client 统计信息。

## 命令语法

**show dhcp client statistics**

## 命令模式

特权模式

## 默认

无

## 使用说明

此命令显示 DHCP 消息的统计信息。

## 举例说明

查看 DHCP 消息统计信息：

```
Switch# show dhcp client statistics
```

```
DHCP client packet statistics:
```

```
=====
DHCP OFFERS      received: 0
DHCP ACKs        received: 0
DHCP NAKs        received: 0
DHCP Others      received: 0
DHCP DISCOVER    sent: 0
DHCP DECLINE     sent: 0
DHCP RELEASE     sent: 0
DHCP REQUEST     sent: 0
DHCP packet send failed: 0
```

## 相关命令

**ip address dhcp**

**clear dhcp client statistics**

### 7.2.13 clear dhcp client statistics

使用此命令清除 DHCP client 计数器。

## 命令语法

**clear dhcp client statistics**

## 命令模式

特权模式

## 默认

无

## 使用说明

此命令将 DHCP client 消息计数器清零。

## 举例说明

将 DHCP client 消息计数器清零。

```
Switch# clear dhcp client statistics
```

## 相关命令

**ip address dhcp**

**show dhcp client statistics**

## 7.3 DHCP Relay 命令

### 7.3.1 dhcp relay

在全局配置模式下，使用 `dhcp relay` 命令来启用 DHCP relay 服务。使用命令相应的 `no` 形式关闭该项功能。

## 命令语法

**dhcp relay**

**no dhcp relay**

## 命令模式

全局配置模式

## 默认

默认情况下此功能未打开。

## 使用说明

在启用 DHCP relay 服务前，必需先使用 `dhcp service` 命令使能 DHCP 功能，DHCP relay 功能要在系统使能 DHCP 功能后才生效。

## 举例说明

启用 dhcp relay 服务：

```
Switch(config)# dhcp relay
```

## 相关命令

**service dhcp**

## 7.3.2 dhcp-server(全局)

在全局模式下使用 `dhcp-server` 命令创建 DHCP 服务器组。使用命令相应的 `no` 形式，删除一个 DHCP 服务器组。

### 命令语法

**dhcp-server** *NUMBER SERVER-LIST*

**no dhcp-server** *NUMBER (SERVER-LIST)*

<i>NUMBER</i>	DHCP 服务器组的序号，范围为 1 到 16
<i>SERVER-LIST</i>	加入服务器组中的 DHCP 服务器的 IP 地址列表。一个服务器组下 DHCP 服务器个数的范围为 1 到 16

### 命令模式

全局配置模式

### 默认

默认情况下，系统未设置任何 DHCP 服务器组。

### 使用说明

该命令用于配置远程 DHCP 服务器。注意 `dhcp server` 功能和 `dhcp snooping` 功能不要在同一个 `vlan` 上设置。

### 举例说明

在 DHCP 服务器组 1 中添加 IP 地址为 1.1.1.1,2.2.2.2,3.3.3.3 这 3 个 DHCP 服务器：

```
Switch(config)# dhcp-server 1 1.1.1.1 2.2.2.2 3.3.3.3
```

### 相关命令

**service dhcp**

**dhcp-server (interface)**

## 7.3.3 dhcp-server (接口)

在接口模式下，使用 `dhcp-server` 命令将一个接口添加到一个 DHCP 服务器组中去。使用命令相应的 `no` 形式，将这个接口从 DHCP 服务器组中删除。

## 命令语法

**dhcp-server** *NUMBER*

**no dhcp-server**

<i>NUMBER</i>	DHCP 服务器组的序号，范围为 1 到 16
---------------	-------------------------

## 命令模式

端口配置模式

## 默认

默认情况下，接口没有加到任何 DHCP 服务器组。

## 使用说明

该命令用于在接口启用全局模式下配置的 DHCP 服务器组。

## 举例说明

在接口启用 DHCP 服务器组 1:

```
Switch(config-if)# dhcp-server 1
```

## 相关命令

**service dhcp**

### 7.3.4 dhcp relay information check

在全局模式下，使用 **dhcp relay information check** 命令配置 DHCP 服务器对转发的 BOOTREPLY 消息进行中继代理信息验证。使用命令相应的 **no** 形式取消中继代理信息的验证。

## 命令语法

**dhcp relay information check**

**no dhcp relay information check**

## 命令模式

全局配置模式

## 默认

DHCP 服务器对转发的 BOOTREPLY 消息检查中继信息。无效的信息会被丢弃。



## 使用说明

该条命令用于电缆接入路由器终端系统。默认情况下，DHCP 服务器检查中继信息，无效的信息会被丢弃。

## 举例说明

配置 DHCP 服务器对转发的 BOOTREPLY 消息进行中继代理信息验证：

```
Switch(config)# dhcp relay information check
```

## 相关命令

**dhcp relay information option**

### 7.3.5 dhcp relay information option

在全局模式下，使用 `dhcp relay information option` 命令，使能系统转发 BOOTREQUEST 消息到 DHCP 服务器时，插入 Option82 选项功能。使用命令相应的 `no` 形式关闭该项功能。

## 命令语法

**dhcp relay information option**

**no dhcp relay information option**

## 命令模式

全局配置模式

## 默认

默认情况下，不对 DHCP 报文插入 Option82 选项。

## 使用说明

该命令使能 DHCP 服务器检测用户发送的请求，在 Option82 选项中添加适当的内容。默认情况下，系统不对 DHCP 报文插入 Option82 选项。

`dhcp relay information option` 命令会在报文中加入电路 ID 和远端 ID。

## 举例说明

使能系统对 DHCP 报文插入 Option82 选项：

```
Switch(config)# dhcp relay information option
```

## 相关命令

**dhcp relay information check**

**dhcp relay information policy**

### 7.3.6 dhcp relay information policy

在全局模式下，使用 `dhcp relay information policy` 命令配置 DHCP 报文 Option82 选项转发策略。使用命令相应的 `no` 形式设置为默认的转发策略。

#### 命令语法

**dhcp relay information policy (drop | keep | replace)**

**no dhcp relay information policy**

<b>drop</b>	带 Option82 选项的报文直接丢弃
<b>keep</b>	带 Option82 选项的报文原样转发
<b>replace</b>	替换原报文中的 Option 82 选项，然后进行转发

#### 命令模式

全局配置模式

#### 默认

默认情况下，替换原报文中的 Option 82 选项，然后进行转发。

#### 使用说明

该条命令用于电缆接入路由器终端系统。一个 DHCP 中继代理可能收到从另一个 DHCP 中继代理处发送的含有 Option82 信息的 DHCP 报文。默认情况下，使用当前 relay 的 Option82 替换原报文中的 Option82 选项，然后进行转发。

#### 举例说明

设置带 Option82 选项的报文直接丢弃：

```
Switch(config)# dhcp relay information policy drop
```

#### 相关命令

**dhcp relay information option**

**dhcp relay information policy**

### 7.3.7 dhcp relay information trust-all

在全局模式下，使用 `dhcp relay information trust-all` 命令配置路由器上所有接口为 DHCP 中继代理信息选项的信任源接口。使用命令相应的 `no` 形式将接口设置为默认配置。

## 命令语法

```
dhcp relay information trust-all  
no dhcp relay information trust-all
```

## 命令模式

全局配置模式

## 默认

默认情况下，交换机上的所有接口都为不信任中继代理信息。

## 使用说明

默认情况下，如果在 DHCP 报文中的网关地址被设置为 0.0.0.0 并且该报文中已经包含 Option82 选项，DHCP 中继代理会丢弃该报文。如果在全局配置了 `dhcp relay information trust-all` 命令，即使 DHCP 报文的网关地址被设置为全 0，DHCP 中继代理也不会丢弃该 DHCP 报文。取而代之，收到的 DHCP DISCOVER 或者 DHCP REQUEST 报文会按照普通的 DHCP 中继操作被转发到命令 `dhcp-server` 所配置的地址。

## 举例说明

配置所有接口为 DHCP 中继代理信息选项的信任源接口：

```
Switch(config)# dhcp relay information trust-all
```

## 相关命令

```
dhcp relay information trusted
```

### 7.3.8 dhcp relay information trusted

在接口模式下，使用命令配置某接口为 DHCP 中继代理信息选项的信任源接口。使用命令相应的 `no` 形式将接口设置为默认配置。

## 命令语法

```
dhcp relay information trusted  
no dhcp relay information trusted
```

## 命令模式

端口配置模式

## 默认

默认情况下，所有接口都为不信任中继代理信息。

## 使用说明

默认情况下，如果在 DHCP 报文中的网关地址被设置为 0.0.0.0 并且该报文中已经包含 Option82 选项，DHCP 中继代理会丢弃该报文。如果在全局配置了 `dhcp relay information trust-all` 命令，即使 DHCP 报文的网关地址被设置为全 0，DHCP 中继代理也不会丢弃该 DHCP 报文。取而代之，收到的 DHCP DISCOVER 或者 DHCP REQUEST 报文会按照普通的 DHCP 中继操作被转发到命令 `dhcp-server` 所配置的地址。

## 举例说明

配置某接口为 DHCP 中继代理信息选项的信任源接口：

```
Switch(config-if)# dhcp relay information trusted
```

## 相关命令

**dhcp relay information trust-all**

### 7.3.9 dhcp relay gateway

在接口模式下，使用命令配置 DHCP 报文中的中继地址字段。使用命令相应的 `no` 形式将接口设置为默认配置。

## 命令语法

**dhcp relay gateway *A.B.C.D***

**no dhcp relay gateway**

## 命令模式

端口配置模式

## 默认

DHCP 报文中携带默认中继地址。

## 使用说明

无

## 举例说明

配置 DHCP 报文中的中继地址为 10.10.10.1：

```
Switch(config-if)# dhcp relay gateway 10.10.10.1
```

## 相关命令

**dhcp-server (interface)**

### 7.3.10 service dhcp

在全局模式下，使用命令 `service dhcp` 使能 DHCP snooping 和中继代理功能。使用命令相应的 `no` 形式关闭 DHCP snooping 和中继代理功能。

#### 命令语法

**service dhcp enable**

**service dhcp disable**

#### 命令模式

全局配置模式

#### 默认

默认情况下，未使能 DHCP 功能。

#### 使用说明

只有在用 `service dhcp` 命令总开关使能了 DHCP 服务，`dhcp snooping`，`dhcp relay` 等 DHCP 功能才会生效。

#### 举例说明

配置全局使能 DHCP 功能：

```
Switch(config)# service dhcp enable
```

#### 相关命令

**dhcp relay**

**dhcp snooping**

### 7.3.11 debug dhcp relay

使用此命令可以打开 `dhcp relay` 的模块的调试功能。

在原命令之前加上关键字 “no”，关闭调试功能。

#### 命令语法

**debug dhcp relay ( events | error | packet | dump | all )**

**no debug dhcp relay ( events | error | packet | dump | all )**

<b>events</b>	调试 dhcp relay 事件信息
<b>error</b>	调试 dhcp relay 错误信息

<b>packet</b>	调试 dhcp relay 的数据包信息
<b>dump</b>	以十六进制调试 dhcp relay 的数据包信息
<b>all</b>	上面提到的所有调试信息

## 命令模式

特权模式

## 默认

无

## 使用说明

使用“terminal monitor”打印消息

## 举例说明

使用如下命令，打开dhcp relay的所有调试信息。

```
Switch# debug dhcp relay all
```

## 相关命令

**terminal monitor**

**show logging buffer**

## 7.3.12 show dhcp-server

在特权模式下，使用 show dhcp-server 命令查看 DHCP 服务器组的配置信息。

## 命令语法

**show dhcp-server**

## 命令模式

特权模式

## 默认

无

## 使用说明

该命令用于显示全局模式下使用 dhcp-server 命令配置的所有 DHCP 服务器组。

## 举例说明

在特权模式下使用 show dhcp-server 命令：

```
Switch# show dhcp-server
```

```
DHCP server group information:
```

```
=====
```

```
group 1 ip address list:
```

```
  [1] 1.1.1.1  
  [2] 2.2.2.2  
  [3] 3.3.3.3  
  [4] 4.4.4.4  
  [5] 5.5.5.5  
  [6] 6.6.6.6  
  [7] 7.7.7.7  
  [8] 8.8.8.8
```

## 相关命令

**dhcp-server (global)**

### 7.3.13 show dhcp relay interfaces

在特权模式下，使用 show dhcp relay interfaces 命令显示 DHCP 服务器组下的接口属性。

## 命令语法

**show dhcp relay interfaces**

## 命令模式

特权模式

## 默认

无

## 使用说明

该命令用于显示属于 DHCP 中继的接口信息。

## 举例说明

在特权模式下使用 show dhcp relay interfaces 命令：

```
Switch# show dhcp relay interfaces
```

```
List of DHCP relay enabled interface(s):
```

```
DHCP relay service status: enabled
```

```
Interface Name          DHCP server group
```

```
=====
```

```
eth-0-1
```

```
1
```

## 相关命令

**show dhcp-server**

### 7.3.14 show dhcp relay information config

在特权模式下，使用 `show dhcp relay information config` 命令显示 DHCP 中继信息（Option82 选项）配置信息。

## 命令语法

**show dhcp relay information config**

## 命令模式

特权模式

## 默认

无

## 使用说明

该命令用于显示 DHCP 中继的配置信息。

## 举例说明

在特权模式下使用 `show dhcp relay information config` 命令：

```
Switch# show dhcp relay information config
```

```
DHCP relay agent information configuration:
```

```
=====
no dhcp relay information option
dhcp relay information check
dhcp relay information policy keep
```

## 相关命令

**dhcp relay information option**

### 7.3.15 show dhcp relay information trusted-sources

在特权模式下，使用 `show dhcp relay information trusted-sources` 命令显示所有接口是否配置为 DHCP 中继信息选项的信任源信息。

## 命令语法

**show dhcp relay information trusted-sources**



## 命令模式

特权模式

## 默认

无

## 使用说明

该命令用于显示所有接口被设置为 DHCP 中继的信任源。

## 举例说明

特权模式下使用 `show dhcp relay information trusted-sources` 命令：

```
Switch# show dhcp relay information trusted-sources
```

```
List of trusted sources of relay agent information option:
```

```
=====
```

```
All interfaces are trusted source of relay agent information option
```

## 相关命令

**dhcp relay information trusted**

### 7.3.16 show dhcp relay statistics

在特权模式下，使用 `show dhcp relay statistics` 命令显示交换机中继的 DHCP 报文统计信息。

## 命令语法

**show dhcp relay statistics**

## 命令模式

特权模式

## 默认

无

## 使用说明

该命令用于显示交换机处理的 DHCP 统计的详情。

## 举例说明

在特权模式下使用 `show dhcp relay statistics` 命令：

```
Switch# show dhcp relay statistics
```

```
DHCP relay packet statistics:
=====
Client relayed packets: 101
Server relayed packets: 88
Client error packets: 0
Server error packets: 0
Bogus GIADDR drops: 15
Bad circuit ID packets: 0
Corrupted agent options: 0
Missing agent options: 0
Missing circuit IDs: 0
```

## 相关命令

**clear dhcp relay statistics**

### 7.3.17 clear dhcp relay statistics

在特权模式下，使用 `clear dhcp relay statistics` 命令清除交换机中继的 DHCP 报文统计信息。

## 命令语法

**clear dhcp relay statistics**

## 命令模式

特权模式

## 默认

无

## 使用说明

该命令用于清除交换机处理的 DHCP 统计的详情。

## 举例说明

在特权模式下使用 `clear dhcp relay statistics` 命令：

```
Switch# clear dhcp relay statistics
```

## 相关命令

**show dhcp relay statistics**

## 7.4 DHCP Server 命令

### 7.4.1 service dhcp

在全局配置模式下使用 `service dhcp` 命令使能 DHCP snooping, server 或 relay 功能。使用命令的 `no` 形式去使能 DHCP 功能。

#### 命令语法

**service dhcp enable**

**service dhcp disable**

#### 命令模式

全局配置模式

#### 默认

DHCP 服务缺省处于去使能状态。

#### 使用说明

只有在用 `service dhcp` 命令总开关使能了 DHCP 服务, `dhcp snooping`, `dhcp relay`, `dhcp server` 等 DHCP 功能才会生效。

#### 举例说明

配置全局使能 DHCP 功能:

```
Switch(config)# service dhcp enable
```

#### 相关命令

**dhcp server**

**dhcp relay**

**dhcp snooping**

### 7.4.2 dhcp server(全局)

在全局模式下使用 `dhcp server` 使能 DHCP server 功能。使用命令相关的 `no` 形式去使能 DHCP server 功能。

#### 命令语法

**dhcp-server**

**no dhcp-server**

## 命令模式

全局配置模式

## 默认

DHCP server 缺省处于去使能状态。

## 使用说明

在使能 DHCP server 功能前，必需先使用 `dhcp service` 命令使能 DHCP 功能，DHCP server 功能要在系统使能 DHCP 功能后才生效。注意 `dhcp server` 功能和 `dhcp snooping` 功能不要在同一个 vlan 上设置。

## 举例说明

配置全局使能 DHCP server 功能：

```
Switch(config)# dhcp server
```

## 相关命令

**service dhcp**

### 7.4.3 dhcp server (接口)

在接口模式下，使用 `dhcp server` 在接口上启用 DHCP server 功能。使用命令相关的 `disable` 形式关闭 DHCP server 功能。

## 命令语法

**dhcp server** [*enable* | *disable*]

enable	使能接口的 DHCP server 模式
disable	去使能接口的 DHCP server 模式

## 命令模式

端口配置模式

## 默认

接口上的 DHCP server 和 DHCP relay 模式都处于去使能状态。

## 使用说明

该命令选择接口工作在 DHCP Server 模式。

## 举例说明

配置接口使能 DHCP Server 模式:

```
Switch(config-if)# dhcp server enable
```

## 相关命令

```
service dhcp
```

```
dhcp server(global)
```

### 7.4.4 dhcp server database {enable|disable}

此命令可以用来开启或关闭 DHCP 数据保存功能。

## 命令语法

```
dhcp server database { enable | disable }
```

## 命令模式

全局配置模式

## 默认

开启

## 使用说明

交换机设备在正常情况下开启 DHCP 数据保存功能，当设备重启或出现异常情况，可以防止数据丢失。

## 举例说明

开启 DHCP 数据保存功能:

```
Switch# config terminal
```

```
Switch (config)# dhcp server database enable
```

### 7.4.5 dhcp server database auto-save interval

此命令可以用来设置数据自动保存的时间间隔。

使用 **no** 命令取消该配置。

## 命令语法

```
dhcp server database auto-save interval interval-value
```

```
no dhcp server database auto-save interval
```

interval-value	DHCP 数据自动保存的时间间隔，取值范围为 300~86400，单位：秒
----------------	---------------------------------------

## 命令模式

全局配置模式

## 默认

300 秒

## 使用说明

系统每隔一段时间会自动保存当前的 dhcp 数据，并覆盖之前的数据文件，通过该命令可以设置自动更新的时间间隔。

## 举例说明

设置数据自动保存的时间间隔为 400 秒：

```
Switch# config terminal
```

```
Switch (config)# dhcp server database auto-save interval 400
```

## 7.4.6 dhcp ping packets

在全局模式下使用 dhcp ping packets 命令配置在分配地址前需要发出 ping 的包的个数。使用命令相关的 no 形式恢复默认值。

## 命令语法

**dhcp ping packets number**

**no dhcp ping packets**

number	<0-10> 需要设置的 ping 发出的包个数
--------	--------------------------

## 命令模式

全局配置模式

## 默认

默认在 ping 的时候发出 1 个 ICMP 消息。

## 使用说明

DHCP server 在分配地址之前会 ping 所要分配的地址。使用该命令指定 ping 发出的包的个数，如果这些包都没有回应，则将地址分配给 DHCP client，否则不回应。

## 举例说明

配置 ping 发出的包的个数为 10:

```
Switch(config)# dhcp ping packets 10
```

## 相关命令

**service dhcp**

**dhcp ping timeout**

## 7.4.7 dhcp ping timeout

在全局模式下，使用 `dhcp ping timeout` 命令配置 ping 超时时间。使用命令相关的 `no` 形式恢复默认值。

## 命令语法

**dhcp ping timeout number**

**no dhcp ping timeout**

number	<1-10> 设置 ping 超时的时间，单位秒（s）。
--------	------------------------------

## 命令模式

全局配置模式

## 默认

默认 ping 的超时等待时间为 1 秒。

## 使用说明

DHCP server 在分配地址前会 ping 该地址，并等待该命令指定的时间。如果在指定时间内没有回应，则认为该地址没有被使用。

## 举例说明

配置 dhcp ping 超时时间为 3 秒:

```
Switch(config)# dhcp ping timeout 3
```

## 相关命令

**service dhcp**

**dhcp ping packets**

## 7.4.8 dhcp pool

在全局模式下，使用 `dhcp pool` 命令创建 DHCP 地址池，并进入 DHCP 地址池配置模式。使用命令相关的 `no` 形式删除创建的 DHCP 地址池。

### 命令语法

**dhcp pool WORD**

**no dhcp pool WORD**

WORD	DHCP 地址池名称： 1) 名称长度范围 [1, 32) 2) 名称合法的字符 [0-9a-zA-Z.-_], 3) 名称必须以字母开头，字母或数字结束
------	--

### 命令模式

全局配置模式

### 默认

默认系统中没有 DHCP 地址池。

### 使用说明

命令执行中，系统会从全局模式进入 DHCP 地址池配置模式，显示 "`(config-dhcp)#`"。在 DHCP 地址池配置模式下，可以配置地址池的参数，例如，可分配的子网地址段，默认网关等。

### 举例说明

创建 DHCP 地址池 pool1:

```
Switch(config)# dhcp pool pool1
```

### 相关命令

**service dhcp**

**dhcp select**

**static-bind**

**dhcp excluded-address**

**network (DHCP)**



## 7.4.9 static-bind

在 DHCP 地址池配置模式下，使用 `static-bind` 命令配置静态绑定的地址。使用该命令的 `no` 形式，删除该地址的静态绑定。

### 命令语法

**static-bind ip-address** {[ip-address wildcard-mask | ip-address/prefix-length] [mac-address HHHH.HHHH.HHHH | client-identifier (ascii WORD | hex hex-string)]}

**no static-bind ip-address** A.B.C.D

ip-address	ip 地址
wildcard-mask	掩码
prefix-length	掩码位数
mac-address HHHH.HHHH.HHHH	DHCP client 的 mac 地址
ascii WORD	ascii 形式的 client id
hex hex-string	hex string 形式的 client id

### 命令模式

全局配置模式

### 默认

默认 DHCP 地址池中没有静态绑定的地址。

### 使用说明

该命令会使当前 DHCP 地址池成为静态地址池。每个静态地址池中，只能配置一条静态绑定地址。

### 举例说明

配置静态绑定的地址：

```
Switch(dhcp-config)# static-bind ip-address 10.10.10.10/24 mac-address 0012.2222.2222
```

### 相关命令

**dhcp pool**

## 7.4.10 dns-server address

在 DHCP 地址池配置模式下，使用 `dns-server` 命令配置 DNS 服务器 IP 地址。使用该命令的 `no` 形式删除配置的服务器地址。

### 命令语法

**dns-server** A.B.C.D (A.B.C.D... A.B.C.D)

**no dns-server**

A.B.C.D	DNS 服务器 IP 地址（至少配置一个）
A.B.C.D... A.B.C.D (Optional)	最多配置 8 个地址

### 命令模式

DHCP 地址池配置模式

### 默认

默认 DHCP 地址池没有配置 DNS 服务器地址。

### 使用说明

最多可以配置 8 个 DNS 服务器地址。

### 举例说明

配置 DNS 服务器地址：

```
Switch(dhcp-config)# dns-server 1.1.1.1 2.2.2.2
```

### 相关命令

**dhcp pool**

## 7.4.11 domain-name

在 DHCP 地址池配置模式下，使用 `domain-name` 命令配置域名。使用该命令的 `no` 形式删除配置的域名。

### 命令语法

**domain-name** WORD

**no domain-name**

WORD	DHCP 客户端使用的域名前缀。 1) 名称长度范围 [1, 64)
------	---------------------------------------

	2) 名称合法的字符 [0-9a-zA-Z.-_], 3) 名称必须以字母开头, 字母或数字结束
--	---

## 命令模式

DHCP 地址池配置模式

## 默认

默认 DHCP 地址池没有配置域名。

## 使用说明

通过设置域名前缀, DHCP 客户端只需要输入部分域名, 系统会自动添加设置的域名前缀。

## 举例说明

配置 DHCP 地址池的域名:

```
Switch(dhcp-config)# domain-name centec.org
```

## 相关命令

**dhcp pool**

### 7.4.12 bootfile-name

在DHCP地址池配置模式下, 使用bootfile-name命令配置DHCP客户端需要的启动镜像文件名。使用该命令的no形式删除配置的启动文件名。

## 命令语法

**bootfile-name WORD**

**no bootfile-name**

WORD	配置的启动文件的文件名。 1) 名称长度范围[1, 64) 2) 名称合法的字符[0-9a-zA-Z.-_], 3) 名称必须以字母开头, 字母或数字结束
------	--

## 命令模式

DHCP 地址池配置模式

## 默认

默认没有配置启动文件名。

## 使用说明

通过配置地址池中的TFTP服务器地址和启动文件名称，DHCP客户端可以从TFTP服务器请求启动文件，完成自动配置。

## 举例说明

配置启动文件名称为dhclient\_startup\_config。

```
Switch(dhcp-config)# bootfile dhclient_startup_config
```

## 相关命令

**dhcp pool**

**tftp-server-address**

### 7.4.13 tftp-server-address

在地址池配置模式下，使用命令 **tftp-server-address** 配置 TFTP 服务器地址。使用该命令相关的 **no** 形式删除配置。

## 命令语法

**tftp-server-address** A.B.C.D (A.B.C.D... A.B.C.D)

**no tftp-server-address**

A.B.C.D	TFTP 服务器 IP 地址
A.B.C.D... A.B.C.D (Optional)	TFTP 服务器 IP 地址列表（最多可以设置 8 个）

## 命令模式

地址池配置模式

## 默认

默认没有配置配置 TFTP 服务器地址

## 使用说明

最多可以设置 8 个 TFTP 服务器地址。列表中地址按照先后顺序使用。

## 举例说明

配置 TFTP 服务器地址为 1.1.1.1,2.2.2.2:

```
Switch(dhcp-config)# tftp-server-address 1.1.1.1 2.2.2.2
```

## 相关命令

**dhcp pool**

**bootfile-name**

### 7.4.14 gateway address

在地址池配置模式下，使用命令 **gateway** 配置默认网关。使用该命令相关的 **no** 形式删除配置。

## 命令语法

**gateway** A.B.C.D (A.B.C.D... A.B.C.D)

**no gateway**

A.B.C.D	IP 地址
A.B.C.D... A.B.C.D (Optional)	IP 地址列表（最多可以设置 8 个）

## 命令模式

地址池配置模式

## 默认

默认没有配置默认网关

## 使用说明

默认网关需要和地址池中的地址在同一子网内。最多可以设置 8 个默认网关地址。列表中地址按照先后顺序使用。

## 举例说明

配置默认网关为 1.1.1.1, 2.2.2.2:

```
Switch(dhcp-config)# gateway 1.1.1.1 2.2.2.2
```

## 相关命令

**dhcp pool**

## 7.4.15 netbios-name-server

在地址池配置模式下，使用命令 `netbios-name-server` 配置 `netbios` 域名服务器。使用该命令相关的 `no` 形式删除配置。

### 命令语法

**netbios-name-server** A.B.C.D (A.B.C.D... A.B.C.D)

**no netbios-name-server**

A.B.C.D	IP 地址
A.B.C.D... A.B.C.D (Optional)	IP 地址列表（最多可以设置 8 个）

### 命令模式

地址池配置模式

### 默认

默认没有配置 `netbios` 域名服务器

### 使用说明

最多可以设置 8 个 `netbios` 域名服务器地址。列表中地址按照先后顺序使用。

### 举例说明

配置 `netbios` 域名服务器 1.1.1.1 2.2.2.2:

```
Switch(dhcp-config)# netbios-name-server 1.1.1.1 2.2.2.2
```

### 相关命令

**dhcp pool**

## 7.4.16 netbios-node-type

在地址池配置模式下，使用 `netbios-node-type` 配置 NetBIOS node type。使用该命令相关的 `no` 形式删除配置。

### 命令语法

**netbios-node-type** [b-node|p-node|m-node|h-node]

**no netbios-node-type**

b-node	广播
--------	----

p-node	点到点
m-node	混合的
h-node	混合的（推荐使用）

## 命令模式

地址池配置模式

## 默认

默认没有配置 NetBIOS 节点类型

## 使用说明

使用该命令配置地址池中 NetBIOS node type 参数。

## 举例说明

配置 NetBIOS node type 为 h-node:

```
Switch(dhcp-config)# netbios-node-type h-node
```

## 相关命令

**dhcp pool**

### 7.4.17 network

在地址池配置模式下，使用命令 `network` 配置要分配的地址段。使用该命令相关的 `no` 形式删除配置。

## 命令语法

**network [ip-address wildcard-mask | ip-address/prefix-length]**

**no network**

ip-address	IP 地址
wildcard-mask	IP 地址掩码
prefix-length	IP 网络位

## 命令模式

地址池配置模式

## 默认

默认没有配置分配的地址段

## 使用说明

该命令配置地址池中可分配的地址段。所有的主机地址都是可分配的，可以使用命令 `dhcp excluded-address` 禁止分配其中的地址。不同地址池的地址段不能有重叠，并且不能再配置静态绑定。

## 举例说明

配置分配的地址段为 1.1.1.0/24:

```
Switch(dhcp-config)# network 1.1.1.0/24
```

## 相关命令

**dhcp pool**

### 7.4.18 lease

在地址池配置模式下，使用命令 `lease` 配置地址池中分配的地址的租约时间。使用该命令相关的 `no` 形式恢复默认配置。

## 命令语法

**lease days [ hours ][ minutes ]**

days	天数，范围 [0, 365]
hours (可选的)	小时数，范围 [0, 23].
minutes (可选的)	分钟数，范围[0, 59]

## 命令模式

地址池配置模式

## 默认

默认配置为 1 天

## 使用说明

无。

## 举例说明

配置租约为 2 天:



```
Switch(dhcp-config)# lease 2
```

配置租约为 1 天 2 小时：

```
Switch(dhcp-config)# lease 1 2
```

配置租约为 30 分钟：

```
Switch(dhcp-config)# lease 0 0 30
```

## 相关命令

**dhcp pool**

### 7.4.19 option

在 DHCP 地址池配置模式下，使用 `option` 命令配置 DHCP 选项。使用该命令的 `no` 形式删除配置的 DHCP 选项。

## 命令语法

```
option {code [ascii ascii-string | hex hex-string | ip-address ip-address]}
```

```
no option [ code ]
```

code	DHCP 选项代码
ascii-string	NVT ASCII 字符串
hex-string	十六进制字符串
ip-address	IP 地址

## 命令模式

DHCP 地址池配置模式

## 默认

默认没有 DHCP 选项被配置。

## 使用说明

DHCP 提供一个 TCP/IP 网络上的参数配置框架。不同的参数以 DHCP 选项的形式存储。当前的 DHCP 选项参考 RFC 2131, Dynamic Host Configuration Protocol。

## 举例说明

配置代码为 72 的 DHCP 选项：

```
Switch (dhcp-config)# option 72 ip-address 10.10.10.10 11.11.11.11
```

## 相关命令

### dhcp pool

## 7.4.20 dhcp excluded-address

在全局模式下，使用dhcp excluded-address 命令配置禁止分配的地址段。使用该命令的no形式删除配置的禁止分配地址。

## 命令语法

**dhcp excluded-address** A.B.C.D [A.B.C.D]

**no dhcp excluded-address** A.B.C.D [A.B.C.D]

A.B.C.D	IP 地址
A.B.C.D (Optional)	高位的 IP 地址

## 命令模式

DHCP地址池配置模式

## 默认

所有地址池中的地址都可以分配。

## 使用说明

使用该命令选择地址池中禁止分配的地址。DHCP服务器在分配地址时，会检查该地址是否被禁用。

## 举例说明

配置禁止分配地址10.10.1.100 -10.10.1.199:

```
Switch(dhcp-config)# ip dhcp excluded-address 10.10.1.100 10.10.1.199
```

## 相关命令

### dhcp pool

## 7.4.21 show dhcp server conflict

在特权模式下，使用命令 show dhcp server conflict 显示发现并记录的冲突地址。

## 命令语法

**show dhcp server conflict** [ip A.B.C.D | all]

ip A.B.C.D	IP 地址
all	所有地址

## 命令模式

特权模式

## 默认

无

## 使用说明

DHCP 服务器在分配地址之前，会检测地址是否已使用，并将冲突的地址记录下来。

## 举例说明

显示冲突的地址：

```
Switch# show ip dhcp conflict all
```

## 相关命令

**clear dhcp server conflict**

**dhcp ping packets**

**dhcp ping timeout**

## 7.4.22 show dhcp server binding

在特权模式下，使用命令 `show dhcp server binding` 显示 DHCP 服务器中绑定的地址信息。

## 命令语法

**show dhcp server binding [ip A.B.C.D | pool WORD | all]**

ip A.B.C.D	IP 地址
pool WORD	地址池名称
all	所有地址

## 命令模式

特权模式

## 默认

无

## 使用说明

绑定地址的信息包括 IP 地址，MAC 地址，租约时间，地址类型。

## 举例说明

显示 DHCP 服务器绑定地址信息：

```
Switch# show ip dhcp binding 1.1.1.1
```

## 相关命令

**clear dhcp server binding**

## 7.4.23 show dhcp server statistics

在特权模式下，使用命令 show dhcp server statistics 显示 DHCP 服务器统计。

## 命令语法

**show dhcp server statistics**

## 命令模式

特权模式

## 默认

无

## 使用说明

无。

## 举例说明

显示 DHCP 服务器统计：

```
Switch#show dhcp server statistics
```

```
DHCP server packet statistics:
```

```
=====
Message Received
BOOTREQUEST      12
DHCPDISCOVER    200
DHCPREQUEST      178
DHCPDECLINE      0
DHCPRELEASE      0
DHCPIFORM        0
```

```
Message Sent
BOOTREPLY      12
DHCPOFFER     190
DHCPACK       172
DHCNPAK        6
```

## 相关命令

**clear dhcp server statistics**

## 7.4.24 show dhcp server config

在特权模式下，使用 show dhcp server config 命令显示 DHCP 服务器配置。

## 命令语法

**show dhcp server config**

## 命令模式

特权模式

## 默认

无

## 使用说明

显示 DHCP 服务器配置。

## 举例说明

显示 DHCP 服务器配置：

```
Switch# show dhcp server config
```

```
DHCP server configuration:
```

```
=====
Pool name: pool10
network 10.1.1.0 mask 255.255.255.0
gateway 10.1.1.1
```

## 相关命令

无

## 7.4.25 clear dhcp server conflict

在特权模式下，使用 clear dhcp server conflict 命令清除记录的冲突地址。

## 命令语法

**clear dhcp server conflict [ip A.B.C.D | all]**

ip A.B.C.D	IP 地址
all	所有地址

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

清除地址 1.1.1.99:

```
Switch# clear ip dhcp conflict 1.1.1.99
```

## 相关命令

无

## 7.4.26 clear dhcp server binding

在特权模式下，使用 `clear dhcp server binding` 从 DHCP 服务器数据库中清除动态绑定的地址。

## 命令语法

**clear dhcp server binding [ip A.B.C.D | pool WORD | all]**

ip A.B.C.D	IP 地址
pool WORD	地址池名字
all	所有地址

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

清除地址绑定 1.1.1.99:

```
Switch# clear ip dhcp binding 1.1.1.99
```

## 相关命令

**show dhcp server binding**

### 7.4.27 clear dhcp server statistics

在特权模式下，使用 `clear dhcp server statistics` 命令清除 DHCP 服务器统计信息。

## 命令语法

**clear dhcp server statistics**

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

清除 DHCP 服务器计数器:

```
Switch# clear dhcp server statistics
```

## 相关命令

**clear dhcp server statistics**

## 7.5 DNS 命令

### 7.5.1 ip host

此命令用来在域名系统（DNS）中设置主机名及其对应的 IP 地址。

使用 **no** 命令用来删除主机名与 IP 地址的对应关系。

#### 命令语法

**ip host** *hostname ip-address*

**no ip host** *hostname*

hostname	主机名
ip-address	与主机名对应的 IP 地址

#### 命令模式

全局配置模式

#### 默认

域名缓存中无静态配置的主机名及其对应的 IP 地址。

#### 使用说明

全局模式下，使用 **ip host** 命令在域名系统(DNS)中设置主机名及其对应的 IP 地址。如果当前域名缓存中不存在此对应关系，系统会自动创建。

#### 举例说明

全局模式下，设置主机名及对应 IP 地址：

```
Switch(config)# ip host www.example1.com 192.0.2.141
```

### 7.5.2 dns domain

全局模式下使用 **dns domain** 命令在域名系统(DNS)下设置一个缺省域名。本命令的 **no** 格式用来删除指定的域名。

#### 命令语法

**dns domain** *domain-NAME*

**no dns domain** *domain-NAME*

<i>domain-NAME</i>	域名
--------------------	----



## 命令模式

全局配置模式

## 默认

无

## 使用说明

无

## 举例说明

全局模式下,在域名系统中设置缺省域名:

```
Switch(config)# dns domain www.example1.com
```

## 相关命令

**show dns domain**

### 7.5.3 dns server

此命令可以用来在域名系统(DNS)的域名服务器列表中新增一个域名服务器。

使用 **no** 命令可以从服务器列表中删除域名服务器。

## 命令语法

```
dns server ip-address [ source-interface IFNAME | source-ip source-ip-address ]
```

```
no dns server ip-address
```

ip-address	域名服务器的 ip 地址
IFNAME	指定源接口名称
source-ip-address	指定源 IP 地址

## 命令模式

全局配置模式

## 默认

域名服务器列表中不存在域名服务器。

## 使用说明

本命令最多能添加三个域名解析服务器。如果指定源接口或者源 IP 地址，将会使用对应的 IP 地作为发出报文的源 IP 地址。

## 举例说明

全局模式下，新增一个域名服务器：

```
Switch(config)# dns server 10.10.1.1
```

## 7.5.4 show dns

特权模式下使用 show dns 命令显示域名系统(DNS)的配置信息。

## 命令语法

**show dns {domain | server}**

<b>domain</b>	显示域名列表
<b>server</b>	显示域名服务器列表

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

特权模式下,显示域名系统的配置信息

```
Switch# show dns domain
Current DNS domain configuration:
      Domain                Suffix
-----
1   domain                  domain. com
2   domain                  aa. com
```

## 相关命令

**dns server**

**dns domain**

## 7.5.5 show ip host

特权模式下,使用 `show ip host` 命令显示指定 ip 主机的配置信息。

### 命令语法

**show ip host**

### 命令模式

特权模式

### 默认

无

### 使用说明

无

### 举例说明

特权模式下,显示指定主机的配置信息

```
Switch# show ip host
Current IP host configuration:
      Host                               Address
-----
1     www.sampledomain.com              1. 1. 1. 1
```

### 相关命令

**ip host**

## 7.5.6 ip dns server

此命令可以用来全局使能 DNS 功能。

使用 **no** 命令取消该配置。

### 命令语法

**ip dns server**

**no ip dns server**

### 命令模式

全局配置模式

### 默认

关闭

### 使用说明

无

### 举例说明

全局使能 DNS 功能：

```
Switch(config)# ip dns server
```

## 7.6 DNS 调试命令

### 7.6.1 show ip dns servers

特权模式下，使用此命令显示 DNS 的状态及配置条目。

### 命令语法

**show ip dns servers**

### 命令模式

特权模式

### 默认

无

## 使用说明

使用本命令之前，必须用 **ip dns server** 命令打开 DNS 功能。

## 举例说明

特权模式下，显示 DNS 的状态及配置条目：

```
Switch# show ip dns servers
```

```
ip dns server
```

```
Current IP host configuration:
```

Host	Address
------	---------

```
-----  
1 www.example1.com      192.0.2.141
```

```
Current DNS name server configuration:
```

Server	IP Address
--------	------------

```
-----  
1 nameserver           10.10.1.1
```

## 7.7 NAT 配置命令

### 7.7.1 ip nat inside

接口上使能 NAT 功能（此命令用于 snat 的入接口）。

#### 命令语法

```
ip nat inside  
no ip nat inside
```

#### 命令模式

端口配置模式

#### 默认

无

#### 使用说明

无

#### 举例说明

端口配置模式下,使能 NAT 功能:

```
Switch(config)# inter eth-0-1  
Switch(config-if)# no switchport  
Switch(config-if)# ip nat inside
```

### 7.7.2 ip nat outside

接口上使能 NAT 功能（此命令用于 snat 的出接口）。

#### 命令语法

```
ip nat outside  
no ip nat outside
```

#### 命令模式

端口配置模式

#### 默认

无

## 使用说明

无

## 举例说明

端口配置模式下,使能 NAT 功能:

```
Switch(config)# inter eth-0-1
```

```
Switch(config-if)# ip nat outside
```

### 7.7.3 ip nat-sa outside-ip

全局配置 snat 条目。

## 命令语法

```
ip nat-sa inside-ip-address outside-ip outside-ip-address [ dynamic | static ]
```

```
no ip nat-sa inside-ip-address outside-ip outside-ip-address
```

inside-ip-address	源 IP 地址
outside-ip-address	NAT 转换后的 IP 地址
dynamic	源 NAT 动态分配源端口号
static	源 NAT 端口号不变, 只替换 IP 地址

## 命令模式

全局配置模式

## 默认

无

## 使用说明

无

## 举例说明

全局配置 snat 条目:

```
Switch(config)# ip nat-sa 1.1.1.1 outside-ip 2.2.2.2 static
```

```
Switch(config)# ip nat-sa 1.1.1.1 outside-ip 2.2.2.2 dynamic
```

## 7.7.4 ip nat-da protocol

全局配置 dnat 条目（带端口号及协议）。

### 命令语法

**ip nat-da** *outside-ip-address* *outside-port-number* **protocol** { **tcp** | **udp** } *inside-ip-address*  
*inside-port-number*

**no ip nat-da** *outside-ip-address* *outside-port-number* **protocol** { **tcp** | **udp** } *inside-ip-address*  
*inside-port-number*

outside-ip-address	转换后的 IP 地址
outside-port-number	转换后端口，取值范围为 1~65535
protocol	端口协议类型
inside-ip-address	源 IP 地址
inside- port-number	源端口，取值范围为 1~65535

### 命令模式

全局配置模式

### 默认

无

### 使用说明

无

### 举例说明

全局配置 dnat 条目（带端口号及协议）：

```
Switch(config)# ip nat-da 2.2.2.2 9000 protocol tcp 1.1.1.1 23
```

## 7.7.5 ip nat-da inside

全局配置 dnat 条目（不带端口号）。

### 命令语法

**ip nat-da** *outside-ip-address* **inside** *inside-ip-address*

**no nat-da** *outside-ip-address* **inside** *inside-ip-address*



outside-ip-address	外网 IP 地址
inside-ip-address	NAT 转换后的内网 IP 地址

## 命令模式

全局配置模式

## 默认

无

## 使用说明

无

## 举例说明

全局配置 dnat 条目（不带端口号）：

```
Switch(config)# ip nat-da 2.2.2.2 inside 1.1.1.1
```

## 7.7.6 clear ip nat session

清除全部或指定 IP 地址的源 NAT 会话。

## 命令语法

**clear ip nat session**

**clear ip nat session** *inside-ip-address* [ *inside-port-number* ]

inside-ip-address	源 IP 地址
inside-port-number	源端口号

## 命令模式

特权模式

## 默认

无

## 使用说明

使用本命令前，需配置源 NAT 会话。

## 举例说明

清除指定 IP 地址和端口的源 NAT 会话：

```
Switch# clear ip nat session 1.1.1.1 23
```

## 7.7.7 arp scan for-nat

开启 **arp scan for-nat** 命令后，设备默认每隔 5 分钟向外发送 nat 相关 IP 网段的 ARP 请求报文。

### 命令语法

```
arp scan for-nat
```

### 命令模式

端口配置模式

### 默认

无

### 使用说明

无

### 举例说明

设备默认每隔 5 分钟向外发送 nat 相关 IP 网段的 ARP 请求报文：

```
Switch(config-if)# arp scan for-nat
```

## 7.7.8 nat session max-count

配置 NAT 会话阈值。

### 命令语法

```
nat session max-count max-count-value
```

max-count-value	NAT 会话阈值,取值范围为 1000~5000,默认值为 3000
-----------------	------------------------------------

### 命令模式

全局配置模式

**默认**

3000

**使用说明**

无

**举例说明**

配置 NAT 会话阈值为 5000:

Switch(config)# nat session max-count 5000

**7.7.9 nat session aging-timer**

配置 NAT 老化定时器周期。

**命令语法****nat session aging-timer { 0 | aging-timer-value }**

0	NAT 会话不老化
aging-timer-value	NAT 会话老化时间，取值范围为 10~1000000，单位为秒，默认 60s

**命令模式**

全局配置模式

**默认**

60s

**使用说明**

无

**举例说明**

配置 NAT 老化定时器周期为 30s:

Switch(config)# nat session aging-timer 30

**7.7.10 nat session sync**

全局配置模式下同步 NAT 会话。

## 命令语法

**nat session sync**

**nat session sync** *inside-ip-address* [ *inside-port-number* ]

inside-ip-address	源 IP 地址
inside-port-number	源端口号

## 命令模式

全局配置模式

## 默认

无

## 使用说明

将本设备上的 NAT 会话同步到对端，即 MLAG 主用设备的 NAT 会话手动同步到 MLAG 备用设备。

## 举例说明

全局配置模式下同步 NAT 会话：

```
Switch(config)# nat session sync 1.1.1.1 23
```

## 7.8 NAT 调试命令

### 7.8.1 show ip nat session

显示全部或指定 IP 地址的 NAT 会话。

## 命令语法

**show ip nat session** [ *inside-ip-address* ]

inside-ip-address	源 IP 地址
-------------------	---------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

显示全部 NAT 会话：

```
Switch# show ip nat session
```

```
-----  
Inside-IP  Outside-IP  Nat-Type  State
```

```
NAT session number: 0
```

```
-----  
Inside-IP  Inside-Port  Outside-IP  Outside-Port  TCP/UDP  State
```

```
PAT session number: 0  
-----
```

## 7.8.2 show ip nat session statistics

显示全部 NAT 会话统计信息。

## 命令语法

```
show ip nat session statistics
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

显示全部 NAT 会话统计信息：

```
Switch# show ip nat session statistics
```

```
NAT session total number: 0
```

```
PAT session total number: 0
```

```
NAT inside interfaces:
```

```
eth-0-2
```

```
NAT outside interfaces:
```

```
eth-0-2
```

### 7.8.3 show resource nat

显示全部 NAT 资源使用信息。

#### 命令语法

```
show resource nat
```

#### 命令模式

特权模式

#### 默认

无

#### 使用说明

无

#### 举例说明

显示全部 NAT 资源使用信息：

```
Switch# show resource nat
```

```
NAT
```

Resource	Used	Capability
----------	------	------------

NAT config entry	0	127
------------------	---	-----

NAT session	0	127
-------------	---	-----

PAT session	0	3000
-------------	---	------

# 8 IP 路由命令行参考

## 8.1 IP Unicast-Routing 命令

### 8.1.1 ip address

在接口模式下使用 `ip address` 命令，来设定接口的主 IP 或者从 IP 地址。使用相应的 `no` 命令来移除这个 IP 地址。

#### 命令语法

`ip address (ADDRESS WILDCARD-MASK | ADDRESS /PREFIX-LENGTH) (secondary)`

ADDRESS	IPv4 地址
WILDCARD-MASK	子网掩码
PREFIX-LENGTH	掩码长度
secondary	(可选) 指定这个 IP 地址是从 IP 地址，没有这个关键词的话就是主 IP 地址

#### 命令模式

端口配置模式

#### 默认

接口上默认不配置 IP 地址。

#### 使用说明

一个接口上可以有一个主 IP 地址和多个从 IP 地址。交换机产生的报文使用主 IP 地址。因此，在同一网段的所有的交换机和接入服务器共享同一个网络号。

主机可以使用 ICMP 请求消息来决定其子网掩码。交换机会用 ICMP 子网应答消息来回复这个请求。

你可以使用 `no ip address` 命令删除接口的 IP 地址，从而禁用该端口上的 IP 路由功能。如果系统检测到另外一个主机正在使用这个 IP 地址，系统将会在控制台上输出错误消息。

`Secondary` 这个关键字允许用户配置最多 15 个从 IP 地址。从 IP 地址跟主 IP 地址差不多，除非系统从来没有生成过使用从 IP 地址以外的路由更新报文。在接口上发布 IP 路由表的时候，IP 广播和 ARP 请求将会被适当的进行处理。

从 IP 地址在很多情况下被使用，下面是一些比较常用的应用场景：

在一个特定的网段中，可能没有足够的主机地址。例如，你的每个逻辑子网只允许 254 个主机，但是你在一个物理子网中需要 300 个主机地址。使用从 IP 地址就允许你在交换机或者接入服务器中，在一个物理子网内建立两个逻辑子网。

许多比较古老的网络是建立在 2 层桥接的基础上的。合理的使用从 IP 地址可以有效的对一个基于路由的子网的传输起到帮助作用，在一个老的桥接网段中的交换机可以很容易的了解到在这个网段中的许多子网。

在同一个网络的两个子网可能被另外一个网络所分割。但如果启用了子网的话，这种情况是不允许的。第一个网络会被延伸，或使用从 IP 地址在第二个网络上分层。

## 举例说明

下面的例子中，10.108.1.27 是主 IP 地址，192.31.7.17 和 192.31.8.17 是从 IP 地址：

```
Switch(config)# interface eth-0-1
Switch(config-if)# ip address 10.108.1.27 255.255.255.0
Switch(config-if)# ip address 192.31.7.17/24 secondary
Switch(config-if)# ip address 192.31.8.17 255.255.255.0 secondary
```

## 相关命令

无

### 8.1.2 ip icmp error-interval

在全局模式使用 `ip icmp error-interval` 命令来设定交换机产生 ICMP 错误消息的间隔时间，使用相应的 `no` 命令来返回默认值。

## 命令语法

```
ip icmp error-interval INTERVAL
```

<code>INTERVAL</code>	范围 0~2147483647 毫秒
-----------------------	--------------------

## 命令模式

全局配置模式



## 默认

默认 1000 毫秒。

## 使用说明

无

## 举例说明

下面的例子中，用户设定了时间间隔为 10 秒：

```
Switch(config)# ip icmp error-interval 10000
```

## 相关命令

ip redirects

ip unreachable

### 8.1.3 ip redirects

在接口模式下，使用 `ip redirects` 命令，来启用交换机发送 ICMP 重定向报文的功能。使用相应的 `no` 命令让系统禁止发送。

## 命令语法

ip redirects

no ip redirects

## 命令模式

端口配置模式

## 默认

默认 IP 重定向是开启的。

## 使用说明

无

## 举例说明

下面的例子中，用户关闭了 ICMP 重定向报文的发送：

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.10.10.1/24
Switch(config-if)# no ip redirects
```

## 相关命令

ip unreachable  
ip icmp error-interval

### 8.1.4 ip unreachable

在接口模式下，使用 `ip unreachable` 命令，来启用交换机发送 ICMP 不可达报文的功能。使用相应的 `no` 命令让系统禁止发送。

## 命令语法

ip unreachable  
no ip unreachable

## 命令模式

端口配置模式

## 默认

默认 IP 不可达是开启的。

## 使用说明

无

## 举例说明

下面的例子中，用户关闭了 ICMP 不可达报文的发送：

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.10.10.1/24
Switch(config-if)# no ip unreachable
```

## 相关命令

**ip redirects**  
**ip icmp error-interval**

### 8.1.5 ip verify unicast reverse-path

接口模式下，使用 `ip verify unicast reverse-path` 来启用 RPF 检测功能，使用相应的 `no` 命令返回默认值。

## 命令语法

ip verify unicast reverse-path

```
no ip verify unicast reverse-path
```

## 命令模式

端口配置模式

## 默认

RPF 检测功能默认关闭。

## 使用说明

无

## 举例说明

下面的例子中，用户在 eth-0-1 上启用了 RPF 检测：

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.10.10.1/24
Switch(config)# ip verify unicast reverse-path
```

## 相关命令

ip redirects

ip icmp error-interval

## 8.1.6 router-id (global)

在全局模式下，使用 `router-id` 命令，针对所有的路由协议，来使用一个固定的 Router ID。使用相应的 `no` 命令让交换机自动选择 Router ID。

## 命令语法

**router-id** IP-ADDRESS

no router-id

IP-ADDRESS	使用 IP 地址格式的 Router ID
------------	-----------------------

## 命令模式

全局配置模式

## 默认

Route ID 默认不定义。

## 使用说明

每个交换机上，Router ID 的 IP 地址格式是任意的，但是 Router ID 必须要保证唯一。

## 举例说明

下面的例子描述了如何指定一个 Router ID:

```
Switch(config)# router-id 1.1.1.1
```

## 相关命令

router-id (router)

## 8.1.7 ip route

在全局模式下，使用 **ip route** 命令来建立静态路由。

使用相应的 **no** 命令来删除这个静态路由。

## 命令语法

**ip route** [ *vrf name* ] { *prefix mask* | *prefix/prefix-length* } [ *nh-address* ] [ *distance* ] [ *vrf leakage-name* ] [ *track number* ] [ **default** ]

name	VRF 实例名
prefix	目的地址
mask	目的地址的子网掩码
prefix-length	子网前缀长度
nh-address	下一跳的 IP 地址
distance	(可选) 管理距离，静态路由默认是 1
leakage-name	路由泄露 VRF 实例名
number	指定 track ID，范围[1,500]
default	从默认 VRF 中泄露静态路由到其他 VRF 中

## 命令模式

全局配置模式

## 默认

静态路由默认不建立。

## 使用说明

交换机无法动态的和目的地址建立路由时，使用静态路由是个不错的选择。

## 举例说明

配置一条静态路由：

```
Switch(config)# ip route 172.31.0.0 255.255.0.0 172.31.6.6
```

配置静态路由泄露：

```
Switch(config)# ip route 22.12.31.0/24 23.0.0.2  
Switch(config)# ip route vrf test1 23.12.31.0/24 11.15.0.15  
Switch(config)# ip route vrf test2 24.12.31.0/24 103.0.0.15
```

将 vrf test1 中的路由发布到默认 vrf 中：

```
Switch(config)# ip route 23.12.31.0/24 11.15.0.15 vrf test1
```

将默认 vrf 中的路由发布到 vrf test1 中：

```
Switch(config)# ip route vrf test1 23.12.31.0/24 11.15.0.15 default
```

将 vrf test2 中的路由发布到 vrf test1 中：

```
Switch(config)# ip route vrf test1 24.12.31.0/24 103.0.0.15 vrf test2
```

## 8.1.8 ip host-collect

使用此命令可以使能或关闭 ARP 转主机路由功能。

### 命令语法

```
ip host-collect { enable | disable }
```

### 命令模式

接口配置模式

### 默认

关闭

### 使用说明

在使能 ARP 转主机路由功能后，可以将 ARP 转为 32 位主机路由。

### 举例说明

使能 ARP 转主机路由功能：

```
Switch(config-if)# ip host-collect enable
```

## 8.1.9 show ip route

在特权模式下，使用 show ip route 显示当前的路由表状态。

## 命令语法

**show ip route** (VRF NAME|) (IP-ADDRESS | PREFIX/PREFIX-LENGTH | PROTOCOL|)

VRF NAME	VRF 实例名
IP-ADDRESS	(可选) 选择显示哪个 IP 地址的路由
PREFIX	IP 路由前缀
PREFIX-LENGTH	路由前缀长度
PROTOCOL	(可选) 路由协议名, 或者关键字 <b>connected</b> , <b>static</b> , 或者 <b>summary</b> 。如果你指定了一个路由协议, 使用其中的一个关键字: <b>bgp</b> , <b>ospf</b> , 或者 <b>rip</b>

## 命令模式

特权模式

## 默认

无

## 使用说明

在路由被加入路由表后, 你可以用 `show ip route`, `show ip route static` 命令显示任何有效的动态和静态路由。

## 举例说明

下面的例子描述了 `show ip route` 命令的使用说明。

```
Switch# show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       [*] - [AD/Metric]
       * - candidate default
O      1.1.1.0/24 [110/2] via 10.10.1.1, eth-0-23, 00:34:17
O      2.2.2.0/24 [110/3] via 10.10.1.1, eth-0-23, 00:17:26
C      10.10.1.0/24 is directly connected, eth-0-23
C      10.10.1.23/32 is in local loopback, eth-0-23
O      10.10.2.0/24 [110/2] via 10.10.1.1, eth-0-23, 00:17:26
O      10.10.3.0/24 [110/3] via 10.10.1.1, eth-0-23, 00:17:26
```

## 相关命令

`ip route`

show ip route database

## 8.1.10 show ip route database

在特权模式下，使用 show ip route database 命令来显示路由信息表（RIB）。

### 命令语法

**show ip route database** (*VRF NAME*) (*PROTOCOL*)

PROTOCOL	(可选) 路由协议名，或者关键字 <b>connected</b> , <b>static</b> 。如果你指定了一个路由协议的话，使用这些关键字中的一个： <b>bgp</b> , <b>ospf</b> 和 <b>rip</b>
----------	--

### 命令模式

特权模式

### 默认

无

### 使用说明

在路由加入路由信息表（RIB）以后，你可以使用 show ip route database, show ip route database static 命令来显示所有的路由。

### 举例说明

下面的例子显示了使用 show ip route database 命令的输出结果：

```
Switch# show ip route database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       [*] - [AD/Metric]
       > - selected route, * - FIB route, p - stale info
O    *> 1.1.1.0/24 [110/2] via 10.10.1.1, eth-0-23, 00:48:58
O    *> 2.2.2.0/24 [110/3] via 10.10.1.1, eth-0-23, 00:32:07
S    6.6.6.0/24 [1/0] via 3.3.3.3 inactive
C    *> 10.10.1.0/24 is directly connected, eth-0-23
C    *> 10.10.1.23/32 is in local loopback, eth-0-23
O    *> 10.10.2.0/24 [110/2] via 10.10.1.1, eth-0-23, 00:32:07
O    *> 10.10.3.0/24 [110/3] via 10.10.1.1, eth-0-23, 00:32:07
```

### 相关命令

ip route

show ip route

## 8.1.11 show ip protocols

在特权模式下，使用 show ip protocols 命令来显示当前处于活动状态的路由协议及其参数。

### 命令语法

**show ip protocols** (vrf *NAME* |) (*PROTOCOL* |)

<b>vrf</b> <i>NAME</i>	VRF 实例名
<b>PROTOCOL</b>	(可选) 路由协议名。如果你指定了一个路由协议的话，使用这些关键字中的一个： <b>bgp</b> ， <b>ospf</b> 和 <b>rip</b>

### 命令模式

特权模式

### 默认

无

### 使用说明

在调试路由问题的时候，show ip protocols 命令所显示的信息是很有用的。show ip protocols 输出的信息可以帮助你识别一个交换机是否传输了错误的路由信息。

### 举例说明

下面是使用 show ip protocols 命令的例子：

```
Switch# show ip protocols
Routing Protocol is "ospf 0"
  Redistributing:
  Routing for Networks:
    3.3.3.0/24
    10.10.1.0/24
    10.10.4.0/24
  Distance: (default is 110)
```

### 相关命令

show ip route

## 8.1.12 show ip route summary

在特权模式下，用命令 show ip route summary 来显示各种类型路由的汇总信息。



## 命令语法

```
show ip route (vrf NAME |) summary
```

<b>vrf <i>NAME</i></b>	VRF 实例名
------------------------	---------

## 命令模式

特权模式

## 使用说明

无

## 举例说明

下面的例子显示了使用命令 `show ip route summary` 的输出结果：

```
Switch# show ip route summary
IP routing table name is Default-IP-Routing-Table(0)
IP routing table maximum-paths is 8
Route source      networks
connected         2
static            1
Total             3
```

## 相关命令

`show ip route`

### 8.1.13 show ip route add-fib-fail

在特权模式下，使用 `show ip route add-fib-fail` 命令，来显示由于硬件资源限制而无法进入 FIB 表的路由。

## 命令语法

```
show ip route add-fib-fail
```

## 命令模式

特权模式

## 默认

无

## 使用说明

如果用命令行 `show ip route` 可以看到该路由，而用命令行 `show ip route add-fib-fail` 也能看到该路由，说明该路由由于硬件资源限制无法进入路由转发表(FIB)，该路由将不能转发报文。您可以等到硬件资源空闲的时候，删除该路由然后重新配置，此时该路由可以重新转发报文。

## 举例说明

下面是使用 `show ip route add-fib-fail` 命令的一个例子：

```
Switch# show ip route add-fib-fail
=====
VRF          Route
default      1.1.1.1/32
default      1.1.1.0/24
test         2.2.2.2/32
test         2.2.2.0/24
```

## 相关命令

`show ip route`

### 8.1.14 max-static-routes

在全局模式下使用命令 **max-static-routes** 来配置系统最大可配置的静态路由条目数，使用该命令的 **no** 形式恢复系统的静态路由配置数目默认值。

## 命令语法

`max-static-routes COUNT`

`no max-static-routes COUNT`

COUNT	范围是 1~65535，默认值 1024 条
-------	------------------------

## 命令模式

全局配置模式

## 默认

1024

## 使用说明

用户可配置的最大静态路由条目不得小于当前已配置的静态路由条目数，不得大于系统的路由规格。

## 举例说明

下面的例子显示了如何将系统的可配最大静态路由条目数改为 10。

```
Switch# confi terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# max-static-routes 10
```

## 相关命令

show ip route summary

### 8.1.15 show resource fib

使用该命令显示系统中路由占用的硬件资源统计。

## 命令语法

show resource fib

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面的例子显示了使用命令 show resource fib 后的结果：

```
Switch# show resource fib
RIBFIB
Resource                               Used      Capability
=====
Indirect Routes                         0         6144
Host Routes                             0         3072
Static Routes                           0         1024
```

## 相关命令

show ip route summary

### 8.1.16 ecmp load-balance-mode dynamic

使用该命令设置 ECMP 的动态负载均衡模式。

## 命令语法

```
ecmp load-balance-mode dynamic
no ecmp load-balance-mode dynamic
```

## 命令模式

全局配置模式

## 默认

静态负载

## 使用说明

配置或取消 **ecmp** 动态负载均衡模式时交换机路由信息必须为空。

## 举例说明

下面的例子显示了如何配置 **ecmp** 负载均衡模式为动态负载：

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ecmp load-balance-mode dynamic
```

## 相关命令

无

### 8.1.17 ecmp load-balance-mode dynamic (efd-only | tcp-only)

使用该命令设置只对 **tcp** 流或者只对 **efd** 流做 ECMP 的动态负载。

## 命令语法

```
ecmp load-balance-mode dynamic (efd-only | tcp-only)
no ecmp load-balance-mode dynamic
```

## 命令模式

全局配置模式

## 默认

可以对所有的流做 **ecmp** 的动态负载

## 使用说明

无

## 举例说明

下面的例子显示了如何配置只对 tcp 流做 ecmp 的动态负载:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ecmp load-balance-mode dynamic tcp-only
```

## 相关命令

无

### 8.1.18 ecmp load-balance-mode static

使用该命令设置 ECMP 的静态 hash 负载均衡模式。

## 命令语法

```
ecmp load-balance-mode static
```

## 命令模式

全局配置模式

## 默认

无

## 使用说明

配置该模式时交换机路由信息必须为空。

## 举例说明

下面的例子显示了如何配置 ecmp 负载均衡模式为静态负载:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ecmp load-balance-mode static
```

## 相关命令

无

### 8.1.19 ecmp load-balance-mode static self-healing

使用该命令设置 ECMP 的 self-healing 负载均衡模式。

## 命令语法

```
ecmp load-balance-mode static self-healing
```

```
no ecmp load-balance-mode static self-healing
```

## 命令模式

全局配置模式

## 默认

无

## 使用说明

无

## 举例说明

下面的例子显示了如何配置 ecmp 负载均衡模式为 self-healing 负载：

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ecmp load-balance-mode static self-healing
```

## 相关命令

无

## 8.1.20 ecmp load-balance-mode round-robin

使用这个命令来设置对哪些前缀的路由做 ECMP round-robin 负载。

使用相应的 no 命令来删除这个配置。

## 命令语法

```
ecmp load-balance-mode round-robin A.B.C.D/E
no ecmp load-balance-mode round-robin A.B.C.D/E
```

## 命令模式

全局配置模式

## 使用说明

最多可配置 16 组

## 默认

无

## 举例说明

下面的例子显示了如何配置 **ecmp** 负载均衡模式为 **round-robin** 负载：

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ecmp load-balance-mode round-robin 1.1.1.0/24
```

## 相关命令

无

### 8.1.21 ecmp hash-field-select

使用该命令设置 ECMP 负载均衡模式使用哪些字段来计算 hash 值。

## 命令语法

```
ecmp hash-field-select {ipda | ipsa | ip-protocol | sourceport | destport | vxlan-vni| nvgre-vsids | inner-ipda | inner-ipsa | inner-ip-protocol | inner-sourceport | inner-destport}
```

## 命令模式

全局配置模式

## 默认

Ipsa ipda(外层头)

## 使用说明

无

## 举例说明

下面的例子显示了如何配置 **ecmp** 负载均衡模式使用外层头的源 ip 地址，目的 ip 地址以及内层头的目的 ip 地址来计算 hash 值：

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ecmp hash-field-select ipda ipsa inner-ipda
```

## 相关命令

无

### 8.1.22 show ecmp information

使用该命令显示当前 ECMP 的配置。

## 命令语法

show ecmp information

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

用 show ecmp information 命令显示当前 ecmp 的配置信息：

```
Switch# show ecmp information
Ecmp load balance enable mode: Static
Ecmp hash-field-select:
    ipsa ipda
```

## 相关命令

无

### 8.1.23 ecmp load-balance hash-arithmetic

使用该命令配置 ECMP 哈希算法。

使用该命令的 no 格式恢复默认值。

## 命令语法

ecmp load-balance hash-arithmetic (xor|crc)

no ecmp load-balance hash-arithmetic

## 命令模式

全局配置模式

## 默认

XOR

## 使用说明

使用该命令配置 ECMP 哈希算法。



使用该命令的 **no** 格式恢复默认值。

## 举例说明

下面例子修改了 ECMP 哈希算法：

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# load-balance hash-arithmetic crc
```

## 相关命令

无

## 8.2 RIP 命令

### 8.2.1 aggregate-address

该命令用来配置 RIP 交换机发布一个聚合的本地 IP 地址。

## 命令语法

**aggregate-address** *ip-address/M* [ **avoid-feedback** ] *IFNAME*

**no aggregate-address** *ip-address/M IFNAME*

ip-address/M	指定需要聚合的网络 IP 地址以及掩码
avoid-feedback	禁止从此接口学习到相同的聚合路由
IFNAME	接口名

## 命令模式

路由模式

## 默认

系统中没有配置 RIP 交换机发布聚合的本地 IP 地址。

## 使用说明

通过指定 **avoid-feedback** 关键字，接口将不再学习到和已发布的聚合 IP 地址相同的聚合路由，从而可以起到防止产生路由环路的作用。

## 举例说明

配置 rip 路由聚合：

```
Switch(config)# router rip
Switch(config-router)# aggregate-address 10.1.1.1/24 avoid-feedback eth-0-1
```

## 8.2.2 default-information originate (RIP)

使用此命令在 RIP 路由表中生成一条默认路由。

使用关键字 `no` 删除这条默认路由。

### 命令语法

```
default-information originate (route-map)
no default-information originate
```

route-map	路由映射
-----------	------

### 命令模式

路由模式

### 默认

无

### 使用说明

该命令生成的默认路由不会下到 FIB 表中，只会被 RIP 邻居学到。

### 举例说明

在 RIP 路由表中生成一条默认路由。

```
Switch(config)# router rip
Switch(config-router)# version 2
Switch(config-router)# network 192.168.16.0/24
Switch(config-router)# default-information originate
```

### 相关命令

无

## 8.2.3 default-metric (RIP)

配置 RIP 路由的缺省度量值。使用该命令的缺省形式恢复 RIP 路由的默认值。

### 命令语法

```
default-metric NUMBER-VALUE
```

no default-metric

NUMBER-VALUE	范围取值 1~16 跳
--------------	-------------

## 命令模式

路由模式

## 默认

默认跳数为 1。

## 使用说明

该命令要和重发布命令一起使用，这可以使经过 RIP 路由协议重发布出去的所有路由的度量值是一样的。

## 举例说明

下面的例子中，在设备上同时启用了 RIP 和 OSPF。同时在 RIP 中重发布 OSPF，并将所有从 OSPF 引入的路由的度量值设为 10。

```
Switch(config)# router rip
Switch(config-router)# default-metric 10
Switch(config-router)# redistribute ospf
```

## 相关命令

redistribute (RIP)

### 8.2.4 distance (RIP)

此命令设置加入 RIP 路由表路由的管理距离。

使用关键字 no 恢复此项设置为默认值。

## 命令语法

**distance** DISTANCE PREFIX/PREFIX-LENGTH (ACCESSS-LIST-NAME)

no distance

DISTANCE	管理值范围为 1-255，管理距离为 255 的路由无效
PREFIX	路由源的前缀，只对符合条件的源 IP 发过来的路由修改管理距离

PREFIX-LENGTH	路由源的前缀长度
ACCESSS-LIST-NAME	访问控制列表，只对符合条件的路由更新报文的路由修改管理距离

## 命令模式

路由模式

## 默认

默认值是 120。

## 使用说明

类型	管理值
直连接口	0
静态路由	1
外部 BGP	20
OSPF	110
RIP	120
内部 BGP	200
未知	255

管理距离表明了对一个路由源的信任度，它是从 0 到 255 之间的一个整数。一般情况下，值越高，信任等级越低。如果管理距离为 255，说明这个路由源不被信任，从这样的源来的所有路由都应该被忽略。

当用户配置了管理距离，那么当路由准备加入路由表的时候，系统就会根据发布路由更新的交换机的 IP 地址进行过滤，同时对符合条件的路由修改管理距离。举个例子，它可以用来过滤那些不在管理员控制范围内的不正确的路由。可选项访问控制列表通常用于过滤路由更新里的路由表项。

## 举例说明

设置从 20.20.0.0 的网段来的路由的管理距离值为 200:

```
Switch(config)# router rip
Switch(config-router)# network 10.10.0.0/24
Switch(config-router)# network 20.20.0.0/24
Switch(config-router)# distance 200 20.20.0.0/24
```

## 相关命令

distance (OSPF)

### 8.2.5 ip rip authentication

该命令用来使能 RIPv2 的认证功能，您可以在接口模式下用这条命令设置 MD5 认证使用的密钥链或者明文认证使用的密码。使用关键字 **no** 删除指定的密钥链或密码。

## 命令语法

ip rip authentication (key-chain *NAME-OF-CHAIN* | string *STRING*)

no ip rip authentication (key-chain | string)

<b>key-chain</b> <i>NAME-OF-CHAIN</i>	RIP 进行 MD5 认证所使用的 key-chain
<b>string</b> <i>STRING</i>	RIP 进行明文认证所用的密码

## 命令模式

端口配置模式

## 默认

默认无验证

## 使用说明

如果 **key-chain** 后面没有跟任何的内容或者 **string** 后面没有跟任何的内容，那么该接口上接收和发送报文不需要进行认证。**key-chain** 和 **string** 不能同时出现，您在使用一种方式的认证方式之前，请确保另一种认证不被使用。

## 举例说明

下面的例子描述了在 rip 报文发送和接收的时候使用密钥链 **trees**：

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip rip authentication key-chain trees
```

## 相关命令

ip rip authentication mode

### 8.2.6 ip rip authentication mode

此命令设置 RIPv2 的认证方式。使用关键字 **no** 恢复 RIP 的认证方式为默认值。

## 命令语法

```
ip rip authentication mode (text | md5)
```

```
no ip rip authentication mode
```

text	明文验证
md5	MD5 加密验证

## 命令模式

端口配置模式

## 默认

默认不进行验证。

## 使用说明

RIP v1 版本不支持验证功能。

## 举例说明

下面的例子描述了如何配置接口 RIP 验证的类型为 MD5:

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip rip authentication mode md5
```

## 相关命令

```
ip rip authentication key-chain
```

## 8.2.7 ip rip receive version

此命令设置端口可接收的 RIP 报文的版本。

使用关键字 no 恢复此设置为默认值。

## 命令语法

```
ip rip receive version [1 | 2]
```

```
no ip rip receive version
```

1	设置端口只可接收 RIPv1 的报文
2	设置端口只可接收 RIPv2 的报文

## 命令模式

端口配置模式

## 默认

默认端口只接收 V2 报文。

## 使用说明

使用此命令改变 RIP 接收报文的版本，该命令只能作用于 3 层接口，您可以配置该接口同时接收 RIPv1 和 RIPv2 的报文。

## 举例说明

下面的例子描述了如何设置接口 RIP 接收报文的类型为 v1 和 v2：

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip rip receive version 1 2
```

## 相关命令

version (RIP)

## 8.2.8 ip rip receive-packet

此命令设置端口可接收 RIP 报文。

使用关键字 no 设置端口不可接收 RIP 报文。

## 命令语法

```
ip rip receive-packet
no ip rip receive-packet
```

## 命令模式

端口配置模式

## 默认

端口可接收 RIP 报文。

## 使用说明

使用此命令来启用或禁用接口接收 RIP 报文的能力，而不管该接口相对应的网络有没有被加到 RIP 中。

## 举例说明

下面的例子描述了如何设置端口可接收 RIP 报文：

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip rip receive-packet
```

## 相关命令

ip rip receive version

### 8.2.9 ip rip send version

此命令设置端口发送 RIP 报文的版本。

使用关键字 no 恢复端口发送的 RIP 报文的版本为默认值。

## 命令语法

ip rip send version (( [1 | 2]) | 1-compatible)

no ip rip send version

1	接口发送 v1 的报文
2	接口发送 v2 的报文
1-compatible	接口发送 v2 的报文兼容 v1 的版本

## 命令模式

端口配置模式

## 默认

默认是 v2 版本。

## 使用说明

使用此命令改变 RIP 发送报文的版本，该命令只能作用于 3 层接口，您可以配置该接口既可以发送 RIPv1 的报文，也可以发送 RIPv2 的报文。

## 举例说明

下面的例子描述了如何设置接口可以发送两种类型的 RIP 报文：

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip rip send version 1 2
```



## 相关命令

ip rip receive version

### 8.2.10 ip rip send-packet

此命令设置端口可发送 RIP 报文。

使用关键字 **no** 设置端口不可发送 RIP 报文。

## 命令语法

ip rip send-packet

no ip rip send-packet

## 命令模式

端口配置模式

## 默认

端口可发送 RIP 报文

## 使用说明

使用此命令来启用或禁用接口发送 RIP 报文的能力，而不管该接口相对应的网络有没有被加到 RIP 中。

## 举例说明

下面的例子描述了如何设置此端口可发送 RIP 报文：

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip rip send-packet
```

## 相关命令

ip rip send version

### 8.2.11 ip rip split-horizon

此命令设置端口防止形成路由环路的方式：毒性逆转或水平分割。

使用关键字 **no** 恢复此设置为默认值。

## 命令语法

ip rip split-horizon (poisoned|)

no ip rip split-horizon

poisoned	如果指定此项，则采用毒性逆转的方式防止路由环路；否则，采用水平分割防止路由环路
----------	---

## 命令模式

端口配置模式

## 默认

端口采用毒性逆转防止路由环路。

## 使用说明

在一般情况下，不建议用 `ip rip split-horizon` 命令改变默认的状态，除非您确定您的应用程序需要变更以正确的宣告路由。

## 举例说明

下面的例子显示了如何使能水平分割来防止路由环路。

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip rip split-horizon
```

## 相关命令

无

## 8.2.12 network (RIP)

使用此命令在指定网段或者接口上使能 RIP 协议。

使用关键字 `no` 在指定网段或者接口上关闭 RIP 协议。

## 命令语法

**network** (PREFIX / PREFIX-LENGTH | INTERFACE-ID)

**no network** (PREFIX / PREFIX-LENGTH | INTERFACE-ID)

PREFIX	网段的前缀
PREFIX-LENGTH	前缀长度
INTERFACE-ID	网络的接口 ID

## 命令模式

路由模式

## 默认

无

## 使用说明

系统对配置多少个 RIP 网段并没有限制。RIP 协议只工作在那些使能了 RIP 的网段相关的接口上。

## 举例说明

下面的例子将在网段 10.99.0.0/16 和 192.168.7.0/24 使能 RIP 路由协议。

```
Switch(config)# router rip
Switch(config-router)# network 10.99.0.0/16
Switch(config-router)# network 192.168.7.0/24
```

## 相关命令

router rip

### 8.2.13 neighbor (RIP)

使用此命令定义一个用于交换路由信息的邻居路由器。

使用关键字 no 删除该邻居路由器。

## 命令语法

**neighbor** IP-ADDRESS

**no neighbor** *IP-ADDRESS*

IP- ADDRESS	与此路由器直接相连的路由器地址
----------------	-----------------

## 命令模式

路由模式

## 默认

无邻居被指定

## 使用说明

此命令用来配置 NBMA（Non-Broadcast Multi-Access，非广播多点可达）网络中 RIP 邻居的 IP 地址，并使更新报文以单播形式发送到对端，而不采用正常的组播或广播的形式。通常情况下，要结合 `passive interface`（被动接口）一起使用。您可以配置多个 RIP 邻居。

## 举例说明

下面的例子中，RIP 更新报文将会在网段 10.108.0.0/16 相关的所有接口上发送，但是接口 eth-0-1 除外。在这种情况下，我们可以使用 `neighbor` 命令，系统将会发送路由更新报文到指定的邻居。

```
Switch(config)# router rip
Switch(config-router)# network 10.108.0.0/16
Switch(config-router)# passive-interface eth-0-1
Switch(config-router)# neighbor 10.108.20.4
```

## 相关命令

`router rip`

### 8.2.14 offset-list (RIP)

设置接口接收或发送 RIP 路由时的附加度量值。使用此命令的 `no` 形式命令删除路由附加值。

## 命令语法

**offset-list** ACCESSS-LIST-NAME (**in** | **out**) METRIC-OFFSET (INTERFACE-ID)

**no offset-list** (**in** | **out**) (INTERFACE-ID|)

ACCESSS-LIST-NAME	访问控制列表
in	在进口方向应用
out	在出口方向应用
METRIC- OFFSET	应用到路由的附加度量值
INTERFACE-ID	接口的 ID

## 命令模式

路由模式

## 默认

默认不开启。

## 使用说明

偏移量列表可以用来改变路由的度量值，以达到某些目的（如做备份链路或者负载均衡）。

## 举例说明

下面的例子描述了在接口上设置 Offset 列表以增加发送的路由的度量值：

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-router)# offset-list 21 out 10
```

## 相关命令

无

### 8.2.15 passive-interface (RIP)

使用此命令设置端口上禁止发送 RIP 报文，使用关键字 `no` 使能发送 RIP 报文。

## 命令语法

```
passive-interface INTERFACE-ID
no passive-interface INTERFACE-ID
```

INTERFACE-ID	接口 ID
--------------	-------

## 命令模式

路由模式

## 默认

默认不开启。

## 使用说明

在 RIP 协议中，路由器被分为两类：主动式和被动式。

主动式路由器会定期在网络中广播路由更新信息，而被动式路由器只能被动接收来自主动式路由器的路由更新信息，以此来更新路由。而此命令就是设置路由器端口工作

在被动模式下。当该接口上被禁止发送 **RIP** 报文后，该接口所在的网段还是能被发布出去，而且同样也可以接收和处理 **RIP** 路由更新报文。

## 举例说明

下面的例子将 **eth-0-1** 设置为被动接口：

```
Switch(config)# router rip
Switch(config-router)# network 10.108.0.0/16
Switch(config-router)# passive-interface eth-0-1
```

## 相关命令

**router rip**

### 8.2.16 redistribute (RIP)

用此命令设置路由重发布。

使用关键字 **no** 删除重发布的路由。

## 命令语法

**redistribute** *PROTOCOL* {[**metric** *VALUE*] | **route-map** *WORD*}

**no redistribute** *PROTOCOL*

<b>PROTOCOL</b>	可引入的源路由协议，包括 OSPF, BGP, static, connected
<b>metric</b> <i>VALUE</i>	所发布的路由的度量值
<b>route-map</b>	路由映射
<b>WORD</b>	路由映射名字

## 命令模式

路由模式

## 默认

默认不使能重发布，度量值的默认值为 1。

## 使用说明

**redistribute** 命令中指定的 **metric** 值将会取代默认度量命令指定的度量值。

## 举例说明

设置重发布的静态路由的度量值为 10：

```
Switch(config)# router rip
Switch(config-router)# network 10.108.0.0/16
Switch(config-router)# redistribute static metric 10
```

## 相关命令

default-metric

## 8.2.17 router rip

使用此命令进入 RIP 协议配置模式。

## 命令语法

```
router rip
no router rip
```

## 命令模式

全局配置模式

## 默认

无

## 使用说明

无

## 举例说明

全局模式下开启 RIP 路由协议：

```
Switch(config)# router rip
```

## 相关命令

network (RIP)

## 8.2.18 timers basic (RIP)

此命令用来配置 RIP 各个定时器的值，可通过调节 RIP 定时器来调整路由协议的性能，以满足网络需要。

使用关键字 **no** 恢复设置为默认值。

## 命令语法

```
timers basic UPDATE TIMEOUT INVALID
no timers basic
```

UPDATE	路由更新时间，范围<5-2147483647>，默认 30s
TIMEOUT	路由老化时间，如果在老化时间内没有收到关于某条路由的更新报文，则该条路由在路由表中的度量值将会被设置为 16，此时该条路由将不能用于转发报文，范围<5-2147483647>，默认 180s
INVALID	路由的垃圾回收时间，定义了一条路由从度量值变为 16 开始，直到它从路由表里被删除所经过的时间。在垃圾回收时间内，RIP 以 16 作为度量值向外发送这条路由的更新，如果垃圾回收定时器超时，该路由仍没有得到更新，则该路由将从路由表中被彻底删除，范围<5-2147483647>，默认 120

## 命令模式

路由模式

## 默认

路由更新时间：30 秒；

路由老化时间：180 秒；

路由的垃圾回收时间：120 秒。

## 使用说明

RIP 协议的这些时间参数时可调整的。由于 RIP 是一个分布式的，异步的路由协议，因此，各个定时器的值在网络中的所有路由器上需要保持一致。同时，您也可以显示的指定地址族，这样，这些定时器的设置将只在该地址族内生效。

## 举例说明

下面的例子设置 RIP 路由的报文更新时间 5 秒，当超过 15 秒没有收到路由更新报文时，路由将失效。再过 15 秒，路由将从 RIP 路由表中删除。

```
Switch(config)# router rip
Switch(config-router)# timers basic 5 15 15
```

## 相关命令

无

### 8.2.19 show ip rip database

此命令用来查看 RIP 的数据库。



## 命令语法

```
show ip rip database (vrf |)
```

vrf	VPN 转发实例
-----	----------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

用 `show ip rip database` 命令显示 RIP 数据库的内容。

```
Switch# show ip rip database
Codes: R - RIP, Rc - RIP connected, Rs - RIP static, K - Kernel,
       C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP
   Network      Next Hop      Metric From      If      Time
Rc 1.1.1.0/24          1          eth-0-1
Rc 2.2.2.0/24          1          eth-0-2
Rc 10.0.0.0/24         1          vlan10
```

## 相关命令

```
show ip rip interface
```

### 8.2.20 show ip rip interface

使用此命令显示接口的 RIP 信息。

## 命令语法

```
show ip rip interface (INTERFACE-ID |)
```

INTERFACE-ID	接口 ID
--------------	-------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

使用 `show ip rip interface` 命令查看接口的 RIP 信息。

```
Switch# show ip rip interface eth-0-1
eth-0-1 is up, line protocol is up
  Routing Protocol: RIP
    Receive RIP packets
    Send RIP packets
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IP interface address:
      1.1.1.1/24
```

## 相关命令

`show ip rip database`

### 8.2.21 version (RIP)

使用此命令设置 RIP 协议版本信息。

使用关键字 `no` 设置 RIP 版本为默认值。

## 命令语法

`version (1 | 2)`

`no version`

1	指定 RIP v1
2	指定 RIP v2

## 命令模式

路由模式

## 默认

默认系统接收 v1 和 v2 的报文,只发送 v2 的报文。

## 使用说明

接口上指定 RIP 的发送和接收的版本信息会覆盖路由模式下配置的 RIP 版本信息。

## 举例说明

指定 RIP 路由中发送和接收的版本为 v2:

```
Switch(config)# router rip
Switch(config-router)# version 2
```

## 相关命令

ip rip receive version

ip rip send version

## 8.2.22 distribute-list

使用此命令过滤网络中路由更新,使用该命令的 no 形式恢复默认设置。

## 命令语法

distribute-list (prefix |) *WORD* (in|out)

no distribute-list (prefix |) *WORD* (in|out)

prefix	过滤列表
WORD	访问控制列表名字
in	进口方向过滤
out	出口方向过滤

## 命令模式

路由模式

## 默认

无

## 使用说明

关键字 in 用于过滤接收的 RIP 路由,关键字 out 用于过滤发送的 RIP 更新报文。

## 举例说明

下面的例子对所有的 RIP 接收的路由进行过滤：

```
Switch(config)# router rip
Switch(config-router)# distribute-list prefix 1 in
```

## 相关命令

ip prefix-list

### 8.2.23 address-family

此命令进入地址族模式。

## 命令语法

```
address-family ipv4 vrf WORD
```

WORD	VPN 实例
------	--------

## 命令模式

路由模式

## 默认

无

## 使用说明

无

## 举例说明

下面的例子显示如何进入地址族模式：

```
Switch(config-router)# address-family ipv4 vrf 1
```

## 相关命令

无

### 8.2.24 show ip protocol rip

此命令显示 RIP 协议的信息。

## 命令语法

```
show ip protocol rip
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

使用 `show ip rip interface` 命令显示 RIP 的协议信息。

```
Switch# show ip protocol rip
Routing protocol is "rip"
  Sending updates every 30 seconds with +/-5 seconds
  Timeout after 180 seconds, Garbage collect after 120 seconds
  Outgoing update filter list for all interface is not set
  Incoming update filter list for all interface is not set
  Default redistribution metric is 1
  Redistributing:
    connected metric default
  Default version control: send version 2, receive version 2
  Interface          Send          Recv   Key-chain
Routing for Networks:
  10.10.11.0/24
Routing Information Sources:
  Gateway            Distance  Last Update  Bad Packets  Bad Routes
Number of routes (excluding connected): 0
Distance: (default is 120)
```

## 相关命令

无

### 8.2.25 debug rip

使用该命令来打开 RIP 的调试开关，主要包括 `events` 和 `packet` 开关。使用该命令的 `no` 形式关闭 RIP 调试开关。

## 命令语法

```
debug rip (all|events|PACKET|)
```

```
no debug rip (all|events|PACKET|)
```

no debug all (rip | )

all	打开 RIP 的所有调试开关
events	打开 RIP 的事件调试开关
PACKET	RIP 报文调试开关, 包括 recv, send 以及 detail
recv	接收报文的调试开关
send	发送报文的调试开关
detail	接收或发送报文的详细信息调试开关

## 命令模式

特权模式

## 默认

调试功能关闭。

## 使用说明

无

## 举例说明

下面的例子显示了如何打开 RIP 报文的调试开关:

```
Switch# debug rip packet
```

## 相关命令

show debugging rip

### 8.2.26 show debugging rip

使用该命令来显示 RIP 调试开关的状态信息。

## 命令语法

show debugging rip

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面的例子显示了 RIP 调试开关的状态信息。

```
Switch# show debugging rip
RIP debugging status:
  RIP packet debugging is on
```

## 相关命令

debug rip

## 8.2.27 show ip rip database database-summary

使用该命令显示 RIP 路由的统计值。

## 命令语法

```
show ip rip database database-summary (vrf NAME |)
```

<b>vrf</b> <i>NAME</i>	VRF 实例名
------------------------	---------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面的例子显示了使用命令 show ip rip database database-summary 的输出结果：

```
Switch# show ip rip database database-summary
Type                Count
```

```
RIP connected      1
RIP                 1
Total               2
```

## 相关命令

```
show ip rip database
```

## 8.2.28 show resource rip

使用该命令显示 RIP 路由占用的硬件资源统计。

## 命令语法

```
show resource rip
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面的例子显示了使用命令 `show resource rip` 的输出结果：

```
Switch# show resource rip
RIP
Resource                Used          Capability
=====
Routes                   2            6144
```

## 相关命令

```
show ip rip database
```

## 8.3 OSPF 命令

### 8.3.1 area authentication

启用 OSPF 的区域验证，可以在 OSPF 路由模式下使用 `area authentication` 命令。使用该命令的 `no` 形式删除 OSPF 的区域验证功能。



## 命令语法

area *AREA-ID* authentication (message-digest|)

no area *AREA-ID* authentication

AREA-ID	区域标识符，指定了哪个区域被启用验证功能。标识符可以是十进制的或者是 IP 地址
message-digest	(可选) 启用 MD5 验证

## 命令模式

路由模式

## 默认

不使用验证功能。

## 使用说明

RFC 1247 规定类型 1 为明文验证，如果命令中没有该选项，默认不使用验证功能。

一个区域的所有路由器之间身份验证类型必须是相同。网络上的所有 OSPF 路由器的身份验证密码也必须是相同的，在接口模式下使用 `ip ospf authentication-key` 来指定认证密码。

如果要启用 MD5 验证，你必须在接口模式下用 `ip ospf message-digest-key` 指定 keyid。

## 举例说明

下面例子讲述了在 OSPF 进程 201 内如何配置区域 0 的 OSPF 的验证。

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip address 192.168.251.201/24
Switch(config-if)# ip ospf authentication-key adcdefgh
Switch(config)# interface eth-0-2
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.56.0.201/16
Switch(config-if)# ip ospf authentication-key ijklmnop
Switch(config)# router ospf 201
Switch(config-router)# network 10.0.0.0 0.255.255.255 area 10.0.0.0
Switch(config-router)# network 192.168.0.0/16 area 0
Switch(config-router)# area 10.0.0.0 authentication
Switch(config-router)# area 0 authentication
```

## 相关命令

`ip ospf authentication-key`

## 8.3.2 area default-cost

要指定一个发送到 Stub 区域默认的汇总路由的开销，在路由模式下使用命令 `area default-cost`。如果要删除配置， 只要用该命令的 `no` 形式。

### 命令语法

```
area AREA-ID default-cost COST
```

```
no area AREA-ID default-cost
```

AREA-ID	区域标识符，标识符可以是十进制的或者是 IP 地址
COST	Cost 的范围 0-16777214

### 命令模式

路由模式

### 默认

默认为 1。

### 使用说明

此命令只用在连接 stub 区域的区域边缘路由器（ABR）上。

有两种 Stub 区域的路由配置命令：`stub` 和 `default-cost` 命令。

配置 Stub 区域后只学习类型为 1(router-lsa)， 2(network lsa)和 3(summary lsa)的 LSA。

### 举例说明

下面例子讲述如何配置 Stub 区域和如何配置 Stub 区域的 Cost 值：

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.56.0.201/16
Switch(config)# router ospf 201
Switch(config-router)# network 10.0.0.0/8 area 10.0.0.0
Switch(config-router)# area 10.0.0.0 stub
Switch(config-router)# area 10.0.0.0 default-cost 20
```

### 相关命令

无

### 8.3.3 area filter-list

使用此命令来过滤本区域内收到或发出的 3 类 LSA，该命令只能作用于 ABR 上。

使用关键字 no 删除过滤列表对指定区域的应用。

#### 命令语法

**area** *AREA-ID* **filter-list** (**access** *ACCESSSS-LIST-NAME* | **prefix** *PREFIX-LIST-NAME*) (**in** | **out**)

**no area** *AREA-ID* **filter-list** (**access** *ACCESSSS-LIST-NAME* | **prefix** *PREFIX-LIST-NAME*) (**in** | **out**)

AREA-ID	以 ID 标识的 OSPF 区域
access	表示后面所跟为接入列表；即根据接入列表对报文进行过滤
ACCESSSS-LIST-NAME	ACL 名字
prefix	表示后面所跟为前缀列表；即根据前缀列表对报文进行过滤
PREFIX-LIST-NAME	前缀列表名字
in	对进入此区域的报文按指定的列表进行过滤
out	对出此区域的报文按指定的列表进行过滤

#### 命令模式

路由模式

#### 默认

默认无配置

#### 使用说明

当该特性的方向配置为 in 时，所有从其他区域进入该区域的 3 类 LSA 将被过滤，包括 ABR 上生成的 3 类汇总 LSA。所有不符合路由前缀列表的路由将被忽视。当该特性的方向配置为 out 时，所有从该区域进入其他区域的 3 类 LSA 将被过滤。如果在该区域上配置汇总路由，那么只要有一条匹配的 3 类 LSA 被发送到其他区域，那么该汇总路由也将被发布到其他区域。如果一条匹配的 3 类 LSA 都没有，那么该汇总路由也不会被发送到其他区域。被前缀列表或 ACL deny 掉的 3 类 LSA 将被隐式的忽略。

#### 举例说明

下面例子讲述如何使用 Filter-List 来过滤从其他区域发到区域 1 的 3 类 LSA：

```
Switch(config)# router ospf 201
Switch(config-router)# area 1 filter-list prefix AREA_1 in
```

## 相关命令

area range

### 8.3.4 area range

使用此命令在 OSPF 区域边界上对路由进行合并和汇总，使用关键字 **no** 取消此项功能。

## 命令语法

**area** *AREA-ID* **range** (*ADDRESS MASK* | *ADDRESS / PREFIX-LENGTH*) (**advertise** | **not-advertise**)

**no area** *AREA-ID* **range** (*ADDRESS MASK* | *ADDRESS / PREFIX-LENGTH*)

AREA-ID	以 ID 标识的 OSPF 区域。
ADDRESS	聚合路由的目的 IPv4 地址
PREFIX-LENGTH	聚合路由的地址前缀长度
advertise	发布这条聚合路由
not-advertise	不发布这条聚合路由

## 命令模式

路由模式

## 默认

不对路由进行聚合。

## 使用说明

**area range** 只能用在 ABR 路由器上。用来对当前区域进行路由聚合。聚合的结果是由 ABR 把单一的汇总路由宣告给其他区域。一个区域可配置多条聚合网段，这样 OSPF 可对多个网段进行聚合。

## 举例说明

下面的例子讲述了如何在 ABR 路由器上对子网 10.0.0.0 进行路由汇总以及对 192.168.110.0 网络内的所有主机路由进行汇总。

```
Switch(config)# interface eth-0-1
```

```

Switch(config-if)# no switchport
Switch(config-if)# ip address 192.168.110.201/24
Switch(config)# interface eth-0-2
Switch(config-if)# no switchport
Switch(config-if)# ip address 192.168.120.201/24
Switch(config)# interface eth-0-3
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.0.0.0/8
Switch(config)# router ospf 201
Switch(config-router)# network 192.168.110.0/24 area 0
Switch(config-router)# area 10.0.0.0 range 10.0.0.0/8
Switch(config-router)# area 0 range 192.168.110.0 255.255.0.0

```

## 相关命令

无

### 8.3.5 area stub

使用此命令设置指定区域为 Stub（存根）区域，使用关键字 **no** 取消对此区域为存根区域的设置。

## 命令语法

```

area AREA-ID stub (no-summary|)
no area AREA-ID stub (no-summary|)

```

AREA-ID	以 ID 或者 IP 地址标识的 OSPF 区域
no-summary	如果指定了此项，则配置此区域为完全存根区域

## 命令模式

路由模式

## 默认

默认无 Stub 区域

## 使用说明

缺省情况下，没有区域被设置为 Stub（存根）区域。Stub 区域的所有路由器都必须用 **area stub** 进行设置。

如果一个区域被配置为存根区域，则当 5 类 LSA 在整个 AS 内进行洪泛时，不会被洪泛进此存根区域。典型的可以被配置为存根区域的是一个 IP 子网，此时所有主机都通过路由器访问外网；把此 IP 子网配置为存根区域，可以减少路由信息的流量并减少连接状态数据库的大小；存根区域中的 ABR 会向存根区域发布汇总路由，以通告存根区

域到达 AS 内其它区域的路由；所以存根区域可以避免 AS 外的路由变化对此存根区域的影响，但它并不能阻止 AS 内的其他区域对它的影响。完全存根区域不仅能阻止 5 类 LSA 的进入，而且能阻止其他的 3 类 LSA 的进入；所以完全存根区域不仅避免了 AS 外的路由变化对此存根区域的影响，而且避免了 AS 内其它区域对它的影响。可以用关键字 `no-summary` 将区域配置为完全存根区域，此时 ABR 向存根区域只宣告一条缺省路由的 3 类 LSA。

## 举例说明

下面例子讲述了如何配置 Stub 区域以及设置默认的 Cost 值：

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.56.0.201/16
Switch(config)# router ospf 201
Switch(config-router)# network 10.0.0.0/8 area 10.0.0.0
Switch(config-router)# area 10.0.0.0 stub
Switch(config-router)# area 10.0.0.0 default-cost 20
```

## 相关命令

无

### 8.3.6 auto-cost

使用此命令设置计算链路开销时所依据的参考带宽，使用关键字 `no` 把参考带宽设置为默认值。

## 命令语法

`auto-cost reference-bandwidth RATE`

`no auto-cost reference-bandwidth`

RATE	带宽，以 Mbps 为单位. 范围从 1 到 4294967；默认是 100
------	--

## 命令模式

路由模式

## 默认

100 Mbps

## 使用说明

使用 `ip ospf cost` 命令设置的端口 Cost 值将会覆盖用该命令计算出来的 cost 值。计算链路开销的公式为：参考带宽/端口速率。

## 举例说明

下面例子讲述了如何在链路上设置带宽为 1G

```
Switch(config)# router ospf 1
Switch(config-router)# auto-cost reference-bandwidth 1000
```

## 相关命令

ip ospf cost

### 8.3.7 clear ip ospf

使用此命令重启 OSPF 进程。

## 命令语法

```
clear ip ospf (PID | ) process
```

PID	(可选)进程 ID
-----	-----------

## 命令模式

特权模式

## 默认

无

## 使用说明

<0-65535>: OSPF 进程编号; 如果没有指定此项, 则重启所有 OSPF 进程。

## 举例说明

下面例子讲述如何重启所有 OSPF 进程:

```
Switch# clear ip ospf process
```

## 相关命令

无

### 8.3.8 compatible rfc1583

使用此命令用来使能兼容 RFC1583 的路由选择优先规则。使用关键字 no 来禁用此规则。

## 命令语法

```
compatible rfc1583
no compatible rfc1583
```

## 命令模式

路由模式

## 默认

不兼容 RFC 1583。

## 使用说明

为了减少路由环路，所有 OSPF 域内的路由器的 RFC1583 兼容模式需要设置成一样的。当有多个 AS-External-LSA 发布了到相同目的地址的路由时，在如何选择最优路由的问题上，RFC1583 和 RFC2328 所定义的优先规则是不相同的。如果到达同一个外部路径有多个最小距离项时，如果 RFC1583Compatibility 设为 disable，则选择 OSPF 的区域标志最大的项；否则如果 enable，就认为是 ecmp 了。

## 举例说明

下面的例子讲述了如何将路由器设置为 RFC1583 兼容模式。

```
Switch(config)# router ospf 1
Switch(config-router)# compatible rfc1583
```

## 相关命令

无

### 8.3.9 default-information originate (OSPF)

使用此命令用来将缺省路由引入 OSPF 区域，使用关键字 no 取消引入缺省路由。

## 命令语法

```
default-information originate [route-map WORD ] | [always] | [metric METRIC-VALUE]
[metric-type TYPE-VALUE]
```

```
no default-information originate [always] [metric] [metric-type] [route-map]
```

always	(可选) 在没有配置静态默认路由的情况下始终向 OSPF 网络通告默认路由，如果没有指定该关键字，本机必须要配置缺省路由才可以引入产生缺省路由的 ASE LSA。
metric	(可选) 被用作生成默认路由的 Metric。假如你没有指定相应的值，默认值是 1。



metric-type	(可选) 外部链路的路由类型: 1—type 1 的 5 类 LSA 2—type 2 类型的 5 类 LSA 默认是 Type2
route-map	路由策略

## 命令模式

路由模式

## 默认

默认关闭

## 使用说明

当你使用重发布命令(`redistribute`)或引入缺省路由命令(`default-information-originate`)时, 路由器自动成为自治系统边界路由器(ASBR)。ASBR 默认不会向 OSPF 域生成默认路由, 除非系统本身已经存在默认路由或者指定了 `always` 关键字。

## 举例说明

下面例子讲述了如何设置默认路由以及修改对应的 Metric 值和类型:

```
Switch(config)# router ospf 109
Switch(config-router)# redistribute rip metric 100
Switch(config-router)# default-information originate metric 100 metric-type 1
```

## 相关命令

`redistribute (OSPF)`

### 8.3.10 default-metric (OSPF)

使用此命令设置 OSPF 引入外部路由时的开销, 使用关键字 `no` 恢复路由开销为默认值。

## 命令语法

`default-metric METRIC-VALUE`

`no default-metric (METRIC-VALUE)`

METRIC-VALUE	设置指定的路由开销, 范围<0-16777214>
--------------	---------------------------

## 命令模式

路由模式

## 默认

默认值为 20。

## 使用说明

`default-metric` 命令通常和 `redistribute` 路由器配置命令一起使用。

## 举例说明

下面例子讲述了如何将 RIP 路由引入到 OSPF，并将引入时的路由开销设为 10。

```
Switch(config)# router ospf
Switch(config-router)# default-metric 10
Switch(config-router)# redistribute rip
```

## 相关命令

`redistribute (OSPF)`

### 8.3.11 distance (OSPF)

设置 OSPF 的管理距离，使用 `no` 命令恢复默认配置。

## 命令语法

**distance** {*DISTANCE* | **ospf** [**external** *DIST1*] [**inter-area** *DIST2*] | [**intra-area** *DIST3*]}

**no distance** {*DISTANCE* | **ospf**}

<i>DISTANCE</i>	管理距离，范围：1 到 255。（255 个距离值的路由在路由表中无效。）
<b>external</b> <i>DIST1</i>	(可选)对区域外路由设置管理距离
<b>inter-area</b> <i>DIST2</i>	(可选)对区域间路由设置管理距离
<b>intra-area</b> <i>DIST3</i>	(可选)对区域内路由设置管理距离

## 命令模式

路由模式

## 默认

*DIST1*: 110

*DIST2*: 110

*DIST3*: 110

## 使用说明

默认情况下，区域内、区域间、区域外路由的管理距离都为 110。

管理距离表征的是对路由的可信度；管理距离越小，此种路由的可信度越高。

当有不止一条的路由可以到达目标时，路由器根据路由的可信度，即根据管理距离选择采用何种路由。只在本地有效。

## 举例说明

下面例子讲述了如何设置 OSPF 的管理距离：

```
Switch(config)# router ospf
Switch(config-router)# distance 90
Switch(config-router)# redistribute rip
```

## 相关命令

无

### 8.3.12 distribute-list (OSPF)

使用该命令对 OSPF 接收的路由或要发布的 5 类路由进行过滤。使用关键字 **no** 取消过滤行为。

## 命令语法

**distribute-list** *ACCESSS-LIST-NAME* (**in** | **out**)

**no distribute-list** *ACCESSS-LIST-NAME* (**in** | **out**)

ACCESSS-LIST-NAME	ACL 名称
in	过滤接收到的路由
out	抑制某些被发布的路由

## 命令模式

路由模式

## 默认

默认无配置

## 使用说明

必须要指定一个 ACL。in 方向用来设置路由信息的过滤条件，只有通过过滤的路由信息才能被接收；out 方向用来配置对引入的路由信息进行过滤。

## 举例说明

下面的例子讲述了如何只接收 20.0.0.0 和 10.108.0.0 两个网段的路由：

```
Switch(config)# ip access-list acl1
Switch(config-ip-acl)# permit any 20.0.0.0 0.0.255.255 any
Switch(config-ip-acl)# permit any 10.108.0.0 0.0.255.255 any
Switch(config-ip-acl)# deny any any any
Switch(config)# router ospf 1
Switch(config-router)# network 10.108.0.0/16 area 1
Switch(config-router)# distribute-list acl1 in
```

## 相关命令

ip access-list

### 8.3.13 ip ospf authentication

使用此命令设置端口的认证方式，使用关键字 no 设置端口的认证方式为默认值。

## 命令语法

**ip ospf authentication** (*MESSAGE-DIGEST* | *NULL*)

no ip ospf authentication

MESSAGE-DIGEST	(可选) 采用 MD5 加密认证方式
NULL	(可选) 不采用认证，在不需要使用密码或者消息认证的场景比较有用

## 命令模式

端口配置模式

## 默认

默认端口不进行认证。

## 使用说明

认证类型和认证密码必须是匹配的。如果你准备使用明文认证，那么除了要用命令 `ip ospf authentication` 外，还需要在接口上指定 `ip ospf authentication-key`；如果你准备使用 MD5 认证，那么除了使用命令 `ip ospf authentication message-digest` 外，还需要在接口上指定 `ip ospf message-digest-key`。为了向前兼容，区域认证类型还是可以设置的，如果接口上没有设置认证类型，就将使用对应的区域认证类型。

## 举例说明

下面例子讲述了如何设置 OSPF 验证的类型为 MD5：

```
Switch(config-if)# ip ospf authentication message-digest
```

## 相关命令

```
area authentication
ip ospf authentication-key
ip ospf message-digest-key
```

### 8.3.14 ip ospf authentication-key

使用此命令设置端口的认证密码，使用关键字 `no` 取消端口的认证密码。

## 命令语法

```
ip ospf authentication-key PASSWORD
no ip ospf authentication-key
```

PASSWORD	所设置的端口认证密码，长度为 8 bytes
----------	------------------------

## 命令模式

端口配置模式

## 默认

默认端口认证密码为空。

## 使用说明

在同一网络内的邻居路由器接口密码必须一致。这个密码将会被附加到报文上被发送出去，不同的接口上使用的密码可以是不一样的。

## 举例说明

下面例子讲述如何配置 OSPF 接口密码：

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip ospf authentication-key yourpass
```

## 相关命令

```
area authentication
ip ospf authentication
```

### 8.3.15 ip ospf cost

使用此命令设置端口开销，使用关键字 **no** 设置端口开销为默认值。

## 命令语法

```
ip ospf cost INTERFACE-COST
no ip ospf cost
```

INTERFACE-COST	设置端口的范围值 1 到 65535
----------------	--------------------

## 命令模式

端口配置模式

## 默认

端口的速率不一样，默认开销也可能不一样。

## 使用说明

如果你不想使用默认的端口开销，可以用该命令来改变开销值。也可以使用 **reference bandwidth** 来改变端口开销。

## 举例说明

下面例子讲述了如何设置端口的开销为 65：

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip ospf cost 65
```

## 相关命令

auto-cost reference bandwidth

### 8.3.16 ip ospf database-filter all out

使用此命令过滤端口的链路状态通告报文，使用关键字 **no** 恢复端口对链路状态通告报文的转发。

## 命令语法

```
ip ospf database-filter all out
```

```
no ip ospf database-filter
```

## 命令模式

端口配置模式

## 默认

默认不开启，所有的 LSA 都可以被泛洪。

## 使用说明

正常情况下，OSPF 会从所有的邻居接口泛洪 LSA，除了接收报文的端口。这种机制在一定程度上保证了泛洪的鲁棒性。但是，过多的冗余报文将会消耗带宽，增加 CPU 负担，进而造成网络的不稳定。为了避免这种情况的发生，可以使用该命令阻止 LSA 报文从某个端口泛洪。

## 举例说明

下面例子讲述如何阻止 LSA 报文在广播网络，非广播网络和点对点网络上被发布出去：

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip ospf database-filter all out
```

## 相关命令

无

### 8.3.17 ip ospf dead-interval

邻居路由器失效时间。如果在该时间之后还没有收到邻居的任何 hello 报文，则宣告邻居死亡。使用关键字 **no** 恢复此时间段为默认值。

## 命令语法

```
ip ospf dead-interval SECONDS
```

no ip ospf dead-interval

SECONDS	设置的时间间隔值，范围<1-65535>
---------	----------------------

## 命令模式

端口配置模式

## 默认

*SECONDS*: 默认在宣告邻居死亡之前，端口等待的时间为 40 秒

## 使用说明

邻居路由器失效时间会在 hello 报文中被通告。在同一 OSPF 网络中的时间间隔必须一致。该值设置的越短，网络收敛时间也越短，但是会增加网络的不稳定性。

## 举例说明

设置 OSPF 的接口死亡时间间隔为 20 秒：

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip ospf dead-interval 20
```

## 相关命令

ip ospf hello-interval

show ip ospf interface

### 8.3.18 ip ospf hello-interval

使用此命令设置此端口发送 Hello 报文的时间间隔，使用关键字 no 设置此端口发送 Hello 报文的时间间隔为默认值。

## 命令语法

ip ospf hello-interval *SECONDS*

no ip ospf hello-interval

SECONDS	范围值 1~65535，期间路由器必须接收到一个 hello 报文，否则这个邻居就会在邻居表中被删除。网络上所有节点的 hello interval 必须要配置成一样的。
---------	---



## 命令模式

端口配置模式

## 默认

10 seconds (以太网);

30 seconds (非广播网)。

## 使用说明

该值将会在 hello 报文中被发送，同一网络内的路由器上设置的 hello 时间间隔必须一致。该值设置的越短，网络拓扑变化将能被越快的检测到，但这样也会造成网络上流量增加。

## 举例说明

下面的例子将端口发送 Hello 报文的时间间隔设置为 15 秒：

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip ospf hello-interval 15
```

## 相关命令

ip ospf dead-interval

### 8.3.19 ip ospf message-digest-key md5

使用此命令给此端口设定 MD5 认证的认证密码，使用关键字 no 取消端口的认证密码。

## 命令语法

```
ip ospf message-digest-key KEY-ID md5 KEY
```

```
no ip ospf message-digest-key KEY-ID
```

KEY-ID	key 标志，范围为 1 到 255
KEY	认证密码，最大 16 个字符

## 命令模式

端口配置模式

## 默认

默认不开启。

## 使用说明

使用该验证类型时，所有接入同一网络/子网的路由器配置有一个共享的密码。对于每一个 OSPF 路由协议包，该密码用于生成/检验加在 OSPF 包最后的"信息摘要"。该信息摘要是根据 OSPF 协议包和密码通过单向函数而得到的。一个接口上可能同时有多个密码被激活，这是为了平滑地过度到新密码。

## 举例说明

下面例子讲述了如何创建 Key 以及密码：

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip ospf message-digest-key 10 md5 xvv560q1e
Switch(config-if)# ip ospf message-digest-key 19 md5 8ry4222
```

## 相关命令

area authentication  
ip ospf authentication

### 8.3.20 ip ospf mtu

使用此命令设定端口发送数据库描述(DD)报文时所填入的 MTU 值，使用关键字 no 恢复端口 MTU 为默认值。

## 命令语法

```
ip ospf mtu MTU-VALUE
no ip ospf mtu
```

MTU-VALUE	MTU 范围 576 到 65535
-----------	--------------------

## 命令模式

端口配置模式

## 默认

1500

## 使用说明

当 OSPF 组装报文的时候，默认会将接口的 MTU 值填进去，该命令可以强制报文里使用用户配置的 MTU 值。这个命令配置的 MTU 值不会写进 kernel。

## 举例说明

下面例子讲述了如何配置接口的 MTU：

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip ospf mtu 1280
```

## 相关命令

```
ip ospf mtu-ignore
```

### 8.3.21 ip ospf mtu-ignore

使用此命令设置端口接收数据库描述报文时，忽略对 MTU 字段的检测。

使用关键字 `no` 设置对数据库描述报文的 MTU 字段进行检测。

## 命令语法

```
ip ospf mtu-ignore
no ip ospf mtu-ignore
```

## 命令模式

端口配置模式

## 默认

默认接口启用 MTU 的匹配功能。

## 使用说明

OSPF 检查邻居是否使用相同的 MTU 值。这个检查发生在互相交换数据库描述报文时，如果在接收到的 DD 报文里的 MTU 高于入接口上配置的 MTU，OSPF 邻接将无法建立。

## 举例说明

下面例子讲述了如何设置在端口上接收到 DD 报文时不对 MTU 值进行检测：

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip ospf mtu-ignore
```

## 相关命令

ip ospf mtu

### 8.3.22 ip ospf priority

使用此命令设置路由器端口优先权，这个值被用来在网络中选举指定路由器。使用关键字 `no` 恢复端口优先权为默认值。

## 命令语法

```
ip ospf priority NUMBER-VALUE
```

```
no ip ospf priority
```

NUMBER-VALUE	优先级范围 0~255
--------------	-------------

## 命令模式

端口配置模式

## 默认

优先级为 1。

## 使用说明

端口的默认优先权值为 1。

端口的优先权主要用来选举网络中的 DR 和 BDR；优先级高的会被选举为 DR。

如果优先级相等，则 Router-ID 大的会被选举为 DR；如果某一个端口的优先级被设置为 0，则此端口不会参加 DR 和 BDR 的选举。端口优先级只在多路访问的网络中起作用，也就是说，点对点网络无效。

## 举例说明

下面例子讲述了如何配置 OSPF 的接口优先级为 4：

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip ospf priority 4
```

## 相关命令

ip ospf network

neighbor (OSPF)

### 8.3.23 ip ospf retransmit-interval

使用此命令设置在邻接间交换 LSA 报文时的重传时间间隔，使用关键字 **no** 恢复在邻接间交换 LSA 报文时的重传时间间隔为默认值。

#### 命令语法

```
ip ospf retransmit-interval SECONDS
```

```
no ip ospf retransmit-interval
```

SECONDS	<1-65535>: 重传时间间隔，以秒为单位
---------	-------------------------

#### 命令模式

端口配置模式

#### 默认

默认为 5 秒。

#### 使用说明

当一个路由器发送 LSA 报文到它的邻居时，它会缓存该报文直到收到邻居的确认报文。如果在重传时间间隔内没有收到确认报文，该 LSA 将被重传。设置该值必须要谨慎，以免引起不必要的重传。通常，这个值要大于两个路由器之间的报文往返延迟。

#### 举例说明

下面例子讲述了如何设置接口的 LSA 报文交换时候的重传时间：

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip ospf retransmit-interval 8
```

#### 相关命令

无

### 8.3.24 ip ospf transmit-delay

使用此命令设置端口发送一个 LSA 报文的延迟时间，使用关键字 **no** 恢复此时间为默认值。

#### 命令语法

```
ip ospf transmit-delay SECONDS
```

```
no ip ospf transmit-delay
```

SECONDS	<1-65535>延迟时间，以秒为单位
---------	---------------------

## 命令模式

端口配置模式

## 默认

默认为 1 秒。

## 使用说明

LSA 在本路由器的链路状态数据库（LSDB）中会随时间老化（每秒钟加 1），但在网络的传输过程中却不会，所以有必要在发送之前在 LSA 的老化时间上增加一定的延迟时间。此配置对低速率的网络尤其重要。

## 举例说明

下面例子讲述如何设置 LSA 报文的延迟时间：

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip ospf transmit-delay 3
```

## 相关命令

无

## 8.3.25 ip ospf network

使用此命令设置端口所接入的网络类型，使用关键字 `no` 恢复端口所接入的网络类型为默认值。

## 命令语法

```
ip ospf network (broadcast|non-broadcast|point-to-multipoint[non-broadcast]|point-to-point)
no ip ospf network
```

broadcast	广播网络，如以太网，FDDI
non- broadcast	NBMA 网络
point-to-multipoint	点对多点网络

point-to-point	点对点网络
----------------	-------

## 命令模式

端口配置模式

## 默认

根据网络类型来决定

## 使用说明

缺省情况下，接口的网络类型根据物理接口而定。以太网接口的网络类型为 **broadcast**，串口的网络类型为 **p2p**，ATM 接口的网络类型为 **nbma**。如果在广播网络上有不支持组播地址的路由器，可以将接口的网络类型改为 **NBMA**。也可以将接口的网络类型由 **NBMA** 改为广播。这样，就不必再配置邻居路由器。

一个 **NBMA** 类型的网络可以改为广播类型的条件是：任意两台路由器之间都有一条虚电路直接可达，或者说，这个网络是全连通的。如果网络不满足这个条件，必须将接口的网络类型改为点到多点。这样，两台不能直接可达的路由器之间可以通过一台与两者都直接可达的路由器来交换路由信息。接口的网络类型改为点到多点后，就不必再配置邻居路由器。如果同一网段内只有两台路由器运行 **OSPF** 协议，也可以将接口的网络类型改为点到点。

## 举例说明

下面的例子讲述了如何配置 **OSPF** 的 **NBMA** 网络：

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip address 192.168.77.17/24
Switch(config-if)# ip ospf network non-bradcast
```

## 相关命令

Neighbor (OSPF)

### 8.3.26 neighbor (OSPF)

使用此命令在非广播网络内设置与本路由器直接相连的路由器，即此路由器的邻居，使用关键字 **no** 取消此关联。

## 命令语法

```
neighbor IP-ADDRESS {[priority NUMBER] [poll-interval SECONDS] | [cost NUMBER]}
no neighbor IP-ADDRESS [priority NUMBER] [poll-interval SECONDS] [cost NUMBER]
```

<b>IP-ADDRESS</b>	邻居的 IP 地址
<b>priority NUMBER</b>	(可选) 接口的优先级
<b>poll-interval SECONDS</b>	(可选) 非广播轮询时间间隔，以秒为单位；默认为 120 秒
<b>cost NUMBER</b>	(可选 1) 端口的开销

## 命令模式

路由模式

## 默认

默认没有指定。

## 使用说明

一般而言，OSPF 会使用 Hello 协议自动发现，建立和维持邻居关系；

但是在 NBMA 和 Point-to-Multipoint 网络中，有时候需要此命令手工配置邻居。

就算是邻居路由器失效了，系统还是需要向该邻居发送 hello 报文，但是发送报文的频率将会降低，此时发送的时间间隔就是轮询值(poll-interval)。一台路由器启动时，会向优先级大于 0 的接口发送 Hello 报文。当网段上选举出 DR 和 BDR 之后，它们就会向所有的邻居发送 Hello 报文，建立邻接关系。

## 举例说明

下面例子讲述了在非广播网络中的地址为 192.168.3.4 的路由器，将其优先级配置为 1，轮询时间配置为 180。

```
Switch(config)# router ospf
Switch(config-router)# neighbor 192.168.3.4 priority 1 poll-interval 180
```

## 相关命令

ip ospf priority

### 8.3.27 network area (OSPF)

使用此命令配置将接口加入指定的 OSPF 区域，使用该命令的 no 形式将接口退出 OSPF 域。

## 命令语法

```
network {IP-ADDRESS WILDCARD-MASK | IP-ADDRESS/PREFIX-LENGTH} area
AREA-ID
```



**no network** {IP-ADDRESS WILDCARD-MASK | IP-ADDRESS/PREFIX-LENGTH} **area**  
AREA-ID

IP-ADDRESS	IP 地址
WILDCARD-MASK	地址掩码
PREFIX-LENGTH	掩码长度
AREA-ID	区域 ID，可以用十进制或 IP 地址表示

## 命令模式

路由模式

## 默认

默认不开启。

## 使用说明

将 IP 地址和地址掩码一起使用可以将 1 个或多个接口加入指定的 OSPF 域。

## 举例说明

下面例子创建了 OSPF 进程 109，并且指定了 4 个区域：0，2，3 和 10.9.50.0：

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.108.20.1/24
Switch(config)# router ospf 109
Switch(config-router)# network 10.108.20.0/24 area 10.9.50.0
Switch(config-router)# network 10.108.0.0/16 area 2
Switch(config-router)# network 10.109.10.0/24 area 3
Switch(config-router)# network 0.0.0.0/0 area 0
```

## 相关命令

router ospf

### 8.3.28 overflow database external

使用此命令用来配置 OSPF 的 LSDB 中 External LSA 的最大条目数以及从溢出状态恢复的时间，使用关键字 no 将配置恢复为默认值。

## 命令语法

overflow database external *MAXLSAS RECOVERTIME*

no overflow database external

MAXLSAS	<0-2147483647> LSA 条目数的最大值，请注意，这个值应该在 AS 中所有路由器上都应该是相同的
RECOVERTIME	<0-65535>恢复时间，如果 LSA 的个数已经超出限制，那么会等待一个恢复时间，等这个时间到的时候，再看看是否可以重新添加新的 lsa

## 命令模式

路由模式

## 默认

无

## 使用说明

使用该命令来限制一个路由器可以接收的外部 LSA 的数量。如果是在邻接建立过程中，收到的外部 LSA 超过了此处所定义的数量，那么邻居状态将一直处于 Loading 状态。

## 举例说明

下面例子讲述了如何配置路由器可以接收的外部 LSA 的最大数量：

```
Switch(config)# router ospf 200
Switch(config-router)# network 10.108.0.0/16 area 0
Switch(config-router)# overflow database external 5 3
```

## 相关命令

router ospf

### 8.3.29 passive-interface (OSPF)

使用此命令抑制端口发送 Hello 报文，使用关键字 no 取消端口对发送 Hello 报文的抑制。

## 命令语法

passive-interface *INTERFACE-ID*

no passive-interface *INTERFACE-ID*

interface-id	接口名字
--------------	------

## 命令模式

路由模式

## 默认

默认不开启。

## 使用说明

如果在接口上禁用路由更新报文的发送，那么此接口还是能正常接收和处理 OSPF 报文的。

## 举例说明

下面例子讲述了如何将端口设备为被动接口：

```
Switch(config)# router ospf 200
Switch(config-router)# network 10.108.0.0/16 area 0
Switch(config-router)# passive-interface eth-0-1
```

## 相关命令

router ospf

### 8.3.30 redistribute (OSPF)

此命令设置路由重发布，即把别的路由协议生成的路由引入到 OSPF 路由域。使用该命令的 no 形式取消路由重发布。

## 命令语法

**redistribute** *PROTOCOL* [*process-id-ospf*] [**route-map** *WORD*] [**tag** *TAG-VALUE*]  
[**metric** *METRIC-VALUE*] [**metric-type** *TYPE-VALUE*]

**no redistribute** *PROTOCOL* [**metric** *METRIC -VALUE*] [**metric-type** *TYPE-VALUE*]

<b>route-map</b> <i>WORD</i>	路由策略
<i>PROTOCOL</i>	(可选)包含静态路由，直连路由，RIP，BGP 路由
<i>process-id-ospf</i>	(可选)对于 OSPF，可设置重分发的 OSPF 进程
<b>tag</b> <i>TAG-VALUE</i>	设置路由的 TAG
<b>metric</b> <i>METRIC-VALUE</i>	(可选)重发布路由时候的 Metric 值，默认 20

<b>metric-type TYPE-VALUE</b>	对于 OSPF，有两种类型的外部路由： 类型一的外部路由 类型二的外部路由 默认是二类路由。
-------------------------------	---

## 命令模式

路由模式

## 默认

默认重发布不开启。

**metric metric-value:** 默认值 20。

**metric-type type-value:** 类型 2 的外部路由。

## 使用说明

在该命令里配置的 **metric** 值将覆盖用命令 **default metric** 配置的值。

外部路由是指到达自治系统外部的路由。

Type-1 外部路由指接收的 IGP 路由，如 RIP 和 STATIC。此类路由有较高的可靠性，所以外部路由开销的计算结果等于自治系统的内部路由开销，并可与 OSPF 本身的路由开销相比较。也就是说，到达 Type-1 外部路由的开销等于路由器到达对应 ASBR 的开销加上 ASBR 到达目的地址的开销。

Type-2 外部路由指接收的 EGP 路由。此类路由可靠性较低，所以 OSPF 协议认为从 ASBR 到达自治系统外部的路由开销要远远高于自治系统内部到达 ASBR 的路由开销。因此在计算路由开销时主要考虑前者。也就是说，到达 Type-2 外部路由的开销等于 ASBR 到达目的地址的开销。

## 举例说明

下面例子讲述了如何重发布静态路由并将其 Metric 设置为 10:

```
Switch(config)# router ospf 119
Switch(config-router)# network 10.108.0.0/16 area 100
Switch(config-router)# redistribute static metric 10
```

## 相关命令

**default-metric**

### 8.3.31 router-id (OSPF)

使用此命令设置路由器标识为指定的值，使用关键字 **no** 设置标识为默认值。

## 命令语法

**router-id** *IP-ADDRESS*

no router-id

IP- ADDRESS	IP 地址

## 命令模式

路由模式

## 默认

无

## 使用说明

此参数是 OSPF 协议中一个很重要的参数；在 OSPF 协议中，路由器 ID 号是一个 32 比特无符号整数，是一台路由器在 OSPF 自治系统中的唯一标识。用户可以自行指定路由器 ID 号。如果用户没有指定路由器 ID 号，则路由器会自动从已配置的接口的 IP 地址中选一个作为本机的 ID 号。在选择路由器 ID 时，环回接口上的 IP 地址优于普通接口上的 IP 地址；若都是普通接口，则选择接口 IP 最大的作为路由器 ID。若路由器的所有接口上都未配置 IP 地址，则必须在 OSPF 视图下配置路由器 ID 号，否则 OSPF 将无法运行。在手工设置路由器 ID 号时，必须保证自治系统中任意两台路由器 ID 号都不相同。为此，不妨选择某个接口的 IP 地址作为本机 ID 号。若在已经有邻居的路由器上用此命令更改了路由器 ID，则该 ID 必须重新启用 OSPF 协议才能生效。

## 举例说明

下面例子讲述了如何配置 OSPF 的 Route-id:

```
Switch(config)# router ospf 119
Switch(config-router)# router-id 10.1.1.1
```

## 相关命令

clear ip ospf

router ospf

### 8.3.32 router ospf

使用此命令创建 OSPF 进程并进入 OSPF 配置模式，使用关键字 no 关闭 OSPF 进程。

## 命令语法

**router ospf** [*PROCESS-ID* [*vrf VPN-NAME*]]

no router ospf [*PROCESS-ID*]

PROCESS-ID	OSPF 进程编号；如果未指定，则进入 0 号进程。使用关键字 no 关闭 OSPF 进程时，如果没有指定进程编号，则关闭 OSPF 的 0 号进程；否则只关闭指定的 OSPF 进程
vrf VPN-NAME	(可选)VPN 中的 OSPF 的进程

## 命令模式

全局配置模式

## 默认

默认无配置。

## 使用说明

您可以在一台路由器上创建多个 OSPF 进程，如果没有指定进程编号，则创建默认的 0 号进程。

## 举例说明

下面例子讲述如何创建 OSPF 进程号为 109：

```
Switch(config)# router ospf 109
Switch(config-router)# router ospf 109
```

## 相关命令

network area

### 8.3.33 summary-address (OSPF)

使用此命令对外部路由进行汇总，使用关键字 no 取消汇总。

## 命令语法

**summary-address** *PREFIX / PREFIX-LENGTH* [**not-advertise**] [**tag** *TAG-VALUE*]

**no summary-address** *PREFIX / PREFIX-LENGTH* [**not-advertise**] [**tag** *TAG-VALUE*]

PREFIX	IP 路由的前缀
PREFIX-LENGTH	前缀长度
not-advertise	(可选) 如果指定了此项，则对指定网络的外部路由不进行宣告

<b>tag TAG- VALUE</b>	路由标记，范围<0-4294967295>，默认为 0
-----------------------	-----------------------------

## 命令模式

路由模式

## 默认

缺省情况下，不对外部路由进行聚合。

## 使用说明

从其他路由协议学到的路由可以在 ASBR 上进行汇总，汇总路由里的 **metric** 值选择的是所有被汇总的路由里值最大的一个。该命令可以用来帮助减少路由表的大小。配置 **summary-address** 命令后，对处于聚合地址范围内的外部路由，本地路由器只向邻居路由器发布一条聚合后的路由。您可以使用命令 **area range** 对 OSPF 区域间的路由进行汇总。OSPF 不支持 **summary-address 0.0.0.0/0** 这样的命令。

## 举例说明

下面例子讲述了如何配置汇总路由，汇总路由 10.1.0.0 包括了子网 10.1.1.0， 10.1.2.0， 10.1.3.0 等等。此时，只有 10.1.0.0 这条汇总路由会被发布出去。

```
Switch(config)# router ospf
Switch(config-router)# summary-address 10.1.0.0/16
```

## 相关命令

**area range**

### 8.3.34 show ip ospf

使用此命令查看指定 OSPF 路由进程相关信息。

## 命令语法

**show ip ospf (PROCESS-ID)**

<b>PROCESS-ID</b>	OSPF 进程号
-------------------	----------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子讲述了如何查看 OSPF 的进程信息：

```
Switch# show ip ospf
Routing Process "ospf 100" with ID 11.11.11.11
Process uptime is 0 minute
Process bound to VRF default
Conforms to RFC2328, and RFC1583 Compatibility flag is disabled
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Refresh timer 10 secs
Number of incoming current DD exchange neighbors 0/5
Number of outgoing current DD exchange neighbors 0/5
Number of external LSA 0. Checksum 0x000000
Number of opaque AS LSA 0. Checksum 0x000000
Number of non-default external LSA 0
External LSA database is unlimited.
Number of LSA originated 1
Number of LSA received 3
Number of areas attached to this router: 1
  Area 1
    Number of interfaces in this area is 1(1)
    Number of fully adjacent neighbors in this area is 1
    Number of fully adjacent virtual neighbors through this area is 0
    Area has no authentication
    SPF algorithm last executed 00:00:38.995 ago
    SPF algorithm executed 1 times
    Number of LSA 4. Checksum 0x0235ff
```

## 相关命令

无

### 8.3.35 show ip ospf border-routers

使用此命令查看指定 OSPF 路由进程的 ABR 和 ASBR 信息。

## 命令语法

```
show ip ospf border-routers
```



## 命令模式

特权模式

## 使用说明

无

## 举例说明

下面例子显示了查看 ABR 路由器的输出结果：

```
Switch# show ip ospf border-routers
OSPF process 100 internal Routing Table
Codes: i - Intra-area route, I - Inter-area route
i 22.22.22.22 [1] via 172.10.1.2, eth-0-10, ABR, Area 1
```

## 相关命令

无

### 8.3.36 show ip ospf database

使用此命令查看指定 OSPF 路由进程的链路状态数据库信息。

## 命令语法

```
show ip ospf (PROCESS-ID) database
show ip ospf (PROCESS-ID) database [adv-router [IP-ADDRESS]]
show ip ospf (PROCESS-ID) database [asbr-summary] [LINK-STATE-ID]
show ip ospf (PROCESS-ID) database [asbr-summary] [LINK-STATE-ID] [adv-router [IP-ADDRESS]]
show ip ospf (PROCESS-ID) database [asbr-summary] [LINK-STATE-ID] [self-originate] [LINK-STATE-ID]
show ip ospf (PROCESS-ID) database [external] [LINK-STATE-ID]
show ip ospf (PROCESS-ID) database [external] [LINK-STATE-ID] [adv-router [IP-ADDRESS]]
show ip ospf (PROCESS-ID) database [external] [LINK-STATE-ID] [self-originate] [LINK-STATE-ID]
show ip ospf (PROCESS-ID) database [network] [LINK-STATE-ID]
show ip ospf (PROCESS-ID) database [network] [LINK-STATE-ID] [adv-router [IP-ADDRESS]]
show ip ospf (PROCESS-ID) database [network] [LINK-STATE-ID] [self-originate] [LINK-STATE-ID]
show ip ospf (PROCESS-ID) database [router] [LINK-STATE-ID]
show ip ospf (PROCESS-ID) database [router] [adv-router [IP-ADDRESS]]
```

```
show ip ospf (PROCESS-ID) database [router] [self-originate] [LINK-STATE-ID]
```

```
show ip ospf (PROCESS-ID) database [self-originate] [LINK-STATE-ID]
```

```
show ip ospf (PROCESS-ID) database [summary] [LINK-STATE-ID]
```

```
show ip ospf (PROCESS-ID) database [summary] [LINK-STATE-ID] [adv-router [IP-ADDRESS]]
```

```
show ip ospf (PROCESS-ID) database [summary] [LINK-STATE-ID] [self-originate] [LINK-STATE-ID]
```

PROCESS-ID	(可选) OSPF 进程号
<b>adv-router</b> [IP-ADDRESS]	(可选) 查看指定 OSPF 宣告路由器的 LSA 信息
LINK-STATE-ID	(可选) 查看自治系统边界路由器的汇总 LSA 信息
asbr-summary	(可选) 查看自治系统边界路由器的汇总 LSA 信息
external	(可选) 查看指定 OSPF 路由进程的外部 LSA 信息
network	(可选) 查看指定 OSPF 路由进程的网络 LSA 信息
router	(可选) 查看指定 OSPF 路由进程的路由器 LSA 有关信息
self-originate	(可选) 查看路由器自生成 LSA 信息
summary	(可选) 查看区域边界路由器汇总 LSA 信息

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子讲述了如何使用此命令来查看相关的信息：

```
Switch# show ip ospf database
Router Link States (Area 3 [Stub])
Link ID      ADV Router   Age  Seq#          CkSum  Link count
10.0.0.1     10.0.0.1     546  0x80000089  0x4567  1
```

## 相关命令

无

### 8.3.37 show ip ospf interface

使用此命令显示 OSPF 接口的信息。

## 命令语法

show ip ospf interface (*INTERFACE-NAME*)

INTERFACE-NAME	(可选) 接口的名字
----------------	------------

## 命令模式

特权模式

## 使用说明

无

## 举例说明

下面例子讲述了如何显示 OSPF 的接口信息：

```
Switch# show ip ospf interface eth-0-3
eth-0-3 is up, line protocol is up
  Internet Address 3.3.3.1/24, Area 3 [Stub], MTU 1500
  Process ID 0, Router ID 10.0.0.1, Network Type NBMA, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 10.0.0.1, Interface Address 3.3.3.1
  No backup designated router on this network
  Timer intervals configured, Hello 30, Dead 120, Wait 120, Retransmit 5
    Hello due in 00:00:17
  Neighbor Count is 1, Adjacent neighbor count is 0
  Crypt Sequence Number is 1218176990
  Hello received 0 sent 80, DD received 0 sent 0
  LS-Req received 0 sent 0, LS-Upd received 0 sent 0
  LS-Ack received 0 sent 0, Discarded 0
```

## 相关命令

无

### 8.3.38 show ip ospf neighbor

使用此命令查看指定 OSPF 路由进程的邻居信息。

## 命令语法

**show ip ospf neighbor** [*INTERFACE-NAME*] [*NEIGHBOR-ID*] [**detail**] [**all**]

INTERFACE-NAME	(可选) 接口名字.
NEIGHBOR-ID	(可选) 邻居 ID
detail	(可选) 查看邻居的详细信息

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子讲述如何查看 OSPF 邻居的信息:

```
Switch# show ip ospf neighbor
Neighbor ID      Pri State           Dead Time Address           Interface
10.199.199.137  1 FULL/DR          0:00:31  192.168.80.37     eth-0-1
172.16.48.1     1 FULL/DROTHER    0:00:33  172.16.48.1      vlan1
172.16.48.200   1 FULL/DROTHER    0:00:33  172.16.48.200    vlan2
10.199.199.137  5 FULL/DR          0:00:33  172.16.48.189    eth-0-2
```

## 相关命令

无

### 8.3.39 show ip ospf summary-address

使用该命令显示 OSPF 的汇总路由信息。

## 命令语法

show ip ospf summary-address

## 命令模式

特权模式

## 默认

无

## 使用说明

度量值为 16777215 的路由不对外发布。

## 举例说明

下面例子讲述了如何使用此命令：

```
Switch# show ip ospf summary-address
OSPF process 0:
10.0.0.0/8 Metric 20, Type 2, Tag 0
20.0.0.0/8 Metric 16777215, Type 0, Tag 0
```

## 相关命令

无

### 8.3.40 show ip ospf database database-summary

使用此命令显示 OSPF 数据库信息的摘要和汇总。

## 命令语法

```
show ip ospf (PROCESS-ID) database database-summary
```

PROCESS-ID	(可选) OSPF 进程 ID
------------	-----------------

## 命令模式

特权模式

## 使用说明

无

## 举例说明

下面例子讲述了如何使用此命令：

```
Switch# show ip ospf database database-summary
          OSPF Router with ID (10.10.10.10) (Process ID 0)
Area 0 database summary
  LSA Type          Count      MaxAge
  Router             1          0
  Network            0          0
```

```

Summary Net          0          0
Summary ASBR        0          0
Subtotal             1          0
Process 0 database summary
LSA Type             Count       MaxAge
Router               1          0
Network              0          0
Summary Net          0          0
Summary ASBR        0          0
Type-5 Ext           1          0
Total                2          0

```

## 相关命令

无

### 8.3.41 show ip ospf route summary

使用此命令显示 OSPF 路由的信息汇总。

## 命令语法

```
show ip ospf (PROCESS-ID) route summary
```

PROCESS-ID	(可选) OSPF 进程 ID
------------	-----------------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子讲述了如何使用此命令：

```

Switch# show ip ospf summary-address
          OSPF Router with ID (10.10.10.10) (Process ID 0)
Route Type             Count
(C)Connected           1
(D)Discard              1
(O)Intra area          0
(IA)Inter area         0
(E1)Ext type 1         0
(E2)Ext type 2         0

```

```
(N1)NSSA Ext type 1          0
(N2)NSSA Ext type 2          0
Total                        2
```

## 相关命令

无

### 8.3.42 show ip protocols ospf

使用此命令查看 OSPF 协议的参数设置信息。

## 命令语法

```
show ip protocols ospf (vrf WORD )
```

vrf	VPN 转发实例
WORD	VPN 路由转发名字

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子讲述了如何显示 OSPF 协议的信息：

```
Switch# show ip protocols ospf
Routing Protocol is "ospf 0"
  Redistributing:
  Routing for Networks:
  Distance: (default is 110)
```

## 相关命令

无

### 8.3.43 show ip ospf processes-count

使用此命令查看 OSPF processes 当前配置数目和最大允许配置数目。

#### 命令语法

```
show ip ospf processes-count
```

#### 命令模式

特权模式

#### 默认

无

#### 使用说明

无

#### 举例说明

下面例子讲述了如何显示 OSPF processes 的当前配置数目和最大配置数目：

```
DUT1# show ip ospf processes-count
OSPF processes current count: 0
OSPF processes max count    : 200
```

#### 相关命令

无

### 8.3.44 timers spf

使用此命令设置收到拓扑变化报文而计算 SPF 的时间。

#### 命令语法

```
timers spf SPF-START SPF-HOLD
```

```
no timers spf
```

SPF-START	接收到网络变化报文开始计算 SPF 之前的延迟时间，以秒为单位。范围<0-2147483647>
SPF-HOLD	连续两次计算 SPF 的时间间隔，以秒为单位。范围<0-2147483647>



## 命令模式

路由模式

## 默认

spf-start: 5 秒

spf-hold: 10 秒

## 使用说明

无

## 举例说明

下面例子讲述了如何设置 OSPF 的 SPF 计算参数:

```
Switch(config)# router ospf 1
Switch(config-router)# router-id 10.10.10.2
Switch(config-router)# timers spf 5 10
Switch(config-router)# redistribute static
Switch(config-router)# network 10.21.21.0/24 area 0
Switch(config-router)# network 10.22.22.0/24 area 00
```

## 相关命令

无

### 8.3.45 max-concurrent-dd

使用此命令设置能够同时处理的最大的 DD 报文数目。

使用关键字 **no** 恢复为默认值。

## 命令语法

max-concurrent-dd *NUMBER-VALUE*

no max-concurrent-dd

NUMBER-VALUE	可同时处理的 DD 报文的最大数量。范围<1-65535>
--------------	-------------------------------

## 命令模式

路由模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子讲述了如何配置可同时处理的 DD 报文的最大数量：

```
Switch(config)# router ospf 100
Switch(config-router)# router-id 10.10.10.2
Switch(config-router)# max-concurrent-dd 10
```

## 相关命令

无

### 8.3.46 maximum-area

使用此命令设置此 OSPF 域中可以配置的最大区域数目，使用关键字 **no** 恢复为默认值。

## 命令语法

**maximum-area** *NUMBER-VALUE*

**no maximum-area**

number-value	配置最大的区域数目，范围<1-4294967294>
--------------	----------------------------

## 命令模式

路由模式

## 默认

3000

## 使用说明

OSPF 协议为了减少网络中的路由信息流量，并且减少路由器中连接状态数据库的大小，对区域进行了划分；可使用此命令设置一个 AS 中区域的最大数目。

## 举例说明

下面例子讲述如何使用此命令：

```
Switch(config)# router ospf 100
Switch(config-router)# router-id 10.10.10.2
Switch(config-router)# maximum-area 100
```

## 相关命令

无

### 8.3.47 refresh timer

使用此命令设置刷新链路状态数据库的时间间隔，使用关键字 **no** 恢复刷新链路状态数据库的时间间隔为默认值。

## 命令语法

```
refresh timer NUMBER-VALUE
```

```
no refresh timer (NUMBER-VALUE)
```

NUMBER-VALUE	刷新数据库时间间隔，范围为<10-1800>
--------------	------------------------

## 命令模式

路由模式

## 默认

10 秒

## 使用说明

一般不建议用户去修改这个配置。

## 举例说明

下面例子讲述了如何设置 **refresh timer**：

```
Switch(config)# router ospf 100
Switch(config-router)# router-id 10.10.10.2
Switch(config-router)# refresh timer 100
```

## 相关命令

无

### 8.3.48 debug ospf

使用该命令打开所有的 OSPF 调试开关。使用该命令的 **no** 形式关闭 OSPF 调试功能。

## 命令语法

```
debug ospf (all)
```

no debug ospf (all)

all	打开所有的调试开关
-----	-----------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch# debug ospf all
```

## 相关命令

无

### 8.3.49 debug ospf events

使用该命令打开 OSPF 的事件调试开关。使用该命令的 no 形式关闭 OSPF 的事件调试功能。

## 命令语法

```
debug ospf events (abr|asbr|lsa|os|router|vlink)
```

```
no debug ospf events (abr|asbr|lsa|os|router|vlink)
```

abr	打开 ABR 调试开关
asbr	打开 ASBR 调试开关
lsa	打开 LSA 调试开关
os	打开 OS 交互调试开关
router	打开路由器调试开关
vlink	打开虚链路调试开关

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch# debug ospf events lsa
```

## 相关命令

无

### 8.3.50 debug ospf ifsm

使用该命令打开 OSPF 的接口状态机调试开关。使用该命令的 no 形式关闭该功能的调试开关。

## 命令语法

```
debug ospf ifsm (status|events|timers)
```

```
no debug ospf ifsm (status|events|timers)
```

status	状态调试开关
events	事件调试开关
timers	定时器调试开关

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch# debug ospf ifsm timers
```

## 相关命令

无

### 8.3.51 debug ospf nfsm

使用该命令打开 OSPF 的邻居状态机调试开关。使用该命令的 `no` 形式关闭该功能的调试开关。

## 命令语法

```
debug ospf nfsm (status|events|timers)
```

```
no debug ospf nfsm (status|events|timers)
```

status	状态调试开关
events	事件调试开关
timers	定时器调试开关

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch# debug ospf nfsm timers
```

## 相关命令

无

### 8.3.52 debug ospf lsa

使用该命令打开 OSPF 的链路状态通告(LSA)调试开关。使用该命令的 `no` 形式关闭该功能的调试开关。

## 命令语法

```
debug ospf lsa (flooding|generate|install|maxage|refresh)
```

```
no debug ospf lsa (flooding|generate|install|maxage|refresh)
```

flooding	LSA 泛洪调试开关
generate	LSA 生成调试开关
install	LSA 安装调试开关
maxage	LSA 老化调试开关
refresh	LSA 刷新调试开关

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch# debug ospf lsa install
```

## 相关命令

无

### 8.3.53 debug ospf packet

使用该命令打开 OSPF 的报文调试开关，使用该命令的 **no** 形式关闭该功能的调试开关。

## 命令语法

```
debug ospf packet PARAMETERS
```

```
no debug ospf packet PARAMETERS
```

```
PARAMETERS = dd|detail|hello|ls-ack|ls-request|ls-update|rcv|send
```

dd	数据库描述报文调试开关
detail	报文详细信息调试开关
hello	hello 报文调试开关
ls-ack	链路状态确认报文调试开关
ls-request	链路状态请求报文调试开关
ls-update	链路状态更新报文调试开关
recv	打开报文接收的开关
send	打开报文发送的开关

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch# debug ospf packet dd send detail
```

## 相关命令

无

### 8.3.54 debug ospf route

使用该命令打开路由计算调试开关，使用该命令的 **no** 形式关闭该功能的调试开关。

## 命令语法

```
debug ospf route (ase|ia|install|spf)
```

```
no debug ospf route (ase|ia|install|spf)
```

ase	外部路由计算调试开关
ia	域间路由计算调试开关



install	路由计算调试开关
spf	SPF 计算调试开关

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch# debug ospf route install
```

## 相关命令

无

### 8.3.55 show debugging ospf

使用该命令查看 OSPF 的调试开关状态。

## 命令语法

```
show debugging ospf
```

## 命令模式

特权模式。

## 默认

无

## 使用说明

无

## 举例说明

下面的例子显示了 OSPF 调试开关的状态信息。

```
Switch# show debugging ospf
```

```
OSPF debugging status:
  OSPF packet Hello send debugging is on
  OSPF packet Database Description send debugging is on
  OSPF packet Link State Request send debugging is on
  OSPF packet Link State Update send debugging is on
  OSPF packet Link State Acknowledgment send debugging is on
  OSPF route installation debugging is on
```

## 相关命令

无

### 8.3.56 show resource ospf

使用该命令来显示 OSPF 路由占用的硬件资源统计。

## 命令语法

```
show resource ospf
```

## 命令模式

特权模式

## 默认

无

## 使用说明

只有在使用 OSPF 之后，Capability 的数值才不为 0。

## 举例说明

下面的例子显示了使用命令 show resource ospf 的输出结果：

```
Switch# show resource ospf
OSPF
Resource                Used                Capability
=====
Routes                   1                   6144
```

## 相关命令

```
show ip ospf route summary
```

### 8.3.57 area nssa

使用此命令设置指定区域为 Not-So-Stubby-Area (NSSA) 区域。

使用关键字 no 取消对此区域为 NSSA 区域的设置。

## 命令语法

**area** *area-id* **nssa translator-role** { **candidate** | **never** | **always** }

**area** *area-id* **nssa no-redistribution**

**area** *area-id* **nssa default-information-originate** [ **metric** *metric-value* ] [ **metric-type** *type-value* ]

**area** *area-id* **nssa no summary**

area-id	以 ID 或者 IP 地址标识的 OSPF 区域
candidate never always	candidate 表示如果路由器被选举为 translator，可以转换 Type 7 LSA 为 Type-5 LSA，默认为 candidate；never 表示路由器永不进行 Type 7 LSA 到 Type 5 LSA 的转换；always 表示路由器总是进行 Type 7 LSA 到 Type 5 LSA 的转换
no-redistribution	表示不分发 external-LSA 到 NSSA
metric-value	指定度量值，取值范围为 0~16777214
type-value	指定 external-LSA 的度量值类型，取值范围为 1~2，默认值为 2
no-summary	如果指定此项，则配置此区域为完全存根区域

## 命令模式

路由模式

## 默认

默认无 NSSA 区域

## 使用说明

缺省情况下，没有区域被设置为 NSSA 区域。NSSA 区域的所有路由器都必须用 **area nssa** 进行设置。

NSSA 区域能够将自治域外部路由引入并传播到整个 OSPF 自治域中，同时又不会学习来自 OSPF 网络其它区域的外部路由。

## 举例说明

配置不分发 external-LSA 到 NSSA：

```
Switch(config)# router ospf 201
Switch(config-router)# area 10.0.0.0 nssa no-redistribution
```

### 8.3.58 show ip ospf database

使用此命令查看指定 OSPF 路由进程的链路状态数据库信息。

## 命令语法

**show ip ospf** [*process-id*] **database** [*nssa-external* [*link-state-id*] | **adv-router** [*ip-address*] | [**self-originate**]]

process-id	(可选) OSPF 进程号
ip-address	(可选) 查看指定 OSPF 宣告路由器的 LSA 信息
link-state-id	(可选) 查看自治系统边界路由器的汇总 LSA 信息
nssa-external	(可选) 查看指定 OSPF 路由进程的 NSSA 区域外部 LSA 信息
self-originate	(可选) 查看路由器自生成 LSA 信息

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

查看指定 OSPF 路由进程的 NSSA 区域外部 LSA 信息：

```
Switch# show ip ospf database nssa-external
Switch#
```

## 8.4 Route-map 命令

### 8.4.1 route-map

在全局配置模式下，使用 route-map 的 match 和 set 命令，来定义各个路由协议间进行重分布的条件，或者启用 BGP 协议的条件路由功能。删除 route-map 的条目，使用相应的 no 命令。

## 命令语法

**route-map** *map-tag* [**permit** | **deny**] [*sequence-NUMBER*]

**no route-map** *map-tag* [**permit** | **deny**] [*sequence-NUMBER*]

map-tag	Route-map 的一个有意义的名字。路由重分布命令使用这个名字
---------	-----------------------------------

	字来引用这个 route-map。多个 route-map 的序列可以共享同一个 route-map 名。Route-map 的名字长度不得超过 20，并且它的首字母必须是'a'-'z', 'A'-'Z'或者'0'-'9'
permit	(可选) 如果 route-map 的 match 规则被匹配到了，并且指定了 permit 关键字，这个路由将会像 set 动作所指定的规则那样进行重分布
deny	(可选) 如果 route-map 的 match 规则被匹配到了，这个路由将不会被重分布
sequence-NUMBER	(可选) route-map 的序列号，表示这个 route-map 在同一个 route-map 名中所处的位置。如果使用了相应的 no 命令，这个序列将会被删除

## 命令模式

全局配置模式

## 默认

默认使用 permit 关键字。

## 使用说明

无

## 举例说明

下面的例子描述了如何创建一个 route-map 并进入 route-map 配置模式：

```
Switch(config)# route-map rip-to-ospf permit
Switch(config-route-map)# match metric 1
Switch(config-route-map)# set metric 2
```

## 相关命令

match as-path  
 match community  
 match interface  
 match ip address  
 match local-preference  
 match metric  
 match origin  
 match route-type

match tag  
set aggregator  
set as-path  
set atomic-aggregate  
set comm-list  
set community  
set dampening  
set extcommunity  
set ip address  
set local-preference  
set metric  
set metric-type  
set origin  
set originator-id  
set tag  
set vpv4  
set weight

## 8.4.2 match as-path

使用这个命令来匹配一个自治系统路径的 ACL。

使用 `no` 参数来删除这个条目。

`match as-path` 命令制定了自治系统匹配的路径。如果设置了这条命令的 `permit` 规则，路由将会被 `set` 规则所重分布或者被控制。反正，如果 `match` 规则被匹配到，但是配置的是 `deny` 规则的话，路由将不会被重分布或者控制。如果没有任何 `match` 规则被匹配的话，这个路由将不会被重分布。

被 `route-map` 策略所指定的路由可能跟路由协议所指定的不一样。设置这种策略会让报文发往不同的路径，如何转发则取决于他们的长度和内容。被策略所转发的报文会覆盖路由表指定要转发的报文。



这个命令只在 BGP 协议中起作用。

## 命令语法

**match as-path** *LISTNAME*

**no match as-path**

LISTNAME	指定自治系统路径的 ACL 名
----------	-----------------

## 命令模式

Route-map 模式

## 默认

默认 match as-path 不设置。

## 使用说明

无

## 举例说明

```
Switch# configure terminal
Switch(config)# route-map myroute deny 34
Switch(config-route-map)# match as-path myaccesslist
```

## 相关命令

match metric  
 match ip address  
 match community  
 set as-path  
 set community

### 8.4.3 match community

使用这个命令来指定匹配的团体属性(community)号。

使用相应的 no 命令来删除这个条目。

Community 是用来过滤路由和建立路由组用的。他们用来在大规模的路由上使用 match 或者 set 命令来启用策略。Community 表使用一组路由的共通属性来识别和过滤这组路由。

match community 命令设置的 match 值会覆盖全局值，如果有路由没有满足任何一个 match 规则的话，这个路由将会被忽略。



这个命令只在 BGP 协议中起作用。

## 命令语法

match community *WORD*

no match community

WORD	Community 表的名字
------	----------------

## 命令模式

Route-map 模式

## 默认

默认 match community 不设置。

## 使用说明

无

## 举例说明

```
Switch# configure terminal
Switch(config)# route-map myroute permit 3
Switch(config-route-map)# match community mylist
```

## 相关命令

match ip address

match as-path

set as-path

set community

match metric

### 8.4.4 match interface

使用这个命令来定义一个针对接口的 **match** 规则。

使用相应的 **no** 命令来删除这个规则。



这个命令只在 BGP 协议中起作用。

## 命令语法

match interface *IFNAME*

no match interface



IFNAME	待匹配的接口名
--------	---------

## 命令模式

Route-map 模式

## 默认

默认 `match interface` 不设置。

## 使用说明

无

## 举例说明

```
Switch# configure terminal
Switch(config)# route-map mymap1 permit 10
Switch(config-route-map)# match interface eth-0-1
```

## 相关命令

`match tag`  
`match route-type external`

## 8.4.5 match ip address

使用这个命令来指定 `match` 一个 ACL 的规则。

使用相应的 `no` 命令来删除这个规则。

`match ip address` 命令指定匹配了一个 ACL，如果指定了一个 `permit` 的 `match` 规则的话，路由将会被像 `set` 规则指定的那样进行重发布或者进行控制。相反，如果制定了相应的 `deny` 规则的话，满足条件的路由将不会被重发布或者控制。如果没有匹配到任何规则的话，路由将不会被接受或者转发。被策略指定的路由最好不要跟路由协议指定的路由一样。指定策略会导致报文根据他们的长度或者内容经过不同的路由转发。报文转发规则的优先级是策略转发大于普通的路由转发。



这个命令对 BGP, OSPF, RIP 和策略路由(PBR)有效。

## 命令语法

**match ip address** *ACCESSSLISTID*  
**no match ip address**

ACCESSLISTID	指定 IPV4 ACL 名
--------------	---------------

## 命令模式

Route-map 模式

## 默认

默认 match ip address 不设置。

## 使用说明

无

## 举例说明

```
Switch# configure terminal
Switch(config)# route-map myroute permit 3
Switch(config-route-map)# match ip address List1
```

## 相关命令

match community

match as-path

set as-path

set community

match metric

## 8.4.6 match ip address prefix-list

用这个命令来匹配前缀列表条目；使用相应的 no 命令来删除这个规则。

如果匹配了前缀并且指定是 permit 的语法的话，路由将会被重发布或者被 set 语法所受控。如果满足了 match 条件但是制定了 deny 语法的话，路由将不会被重发布或者被 set 语法受控。如果没有满足 match 条件，无论指定了 permit 还是 deny 语法，路由都不会被接收或者转发。

被指定的路由不能跟路由协议相同，指定的策略让报文能够按照他们的长度及内容通过不同的路由进行转发。相对于路由表指定的路径来说，报文将会优先以配置的策略来进行转发。



这个命令对 BGP, OSPF, RIP 有效。

## 命令语法

```
match ip address prefix-list LISTNAME  
no match ip address prefix-list [ LISTNAME ]
```

LISTNAME	IP 前缀列表名
----------	----------

## 命令模式

Route-map 模式

## 默认

默认 `match ip addressprefix-list` 不设置。

## 使用说明

无

## 举例说明

```
Switch# configure terminal  
Switch(config)# route-map rmap1 permit 3  
Switch(config-route-map)# match ip address prefix-list mylist
```

## 相关命令

```
match community  
match as-path  
set as-path  
set community  
match metric
```

### 8.4.7 match ip next-hop

使用这个命令来指定 `match` 一个下一跳的 IP 地址。

使用相应的 `no` 命令来删除这个规则。

如果匹配了 `nexthop` 地址并且指定是 `permit` 的语法的话，路由将会被重发布或者被 `set` 语法所受控。如果满足了 `match` 条件但是制定了 `deny` 语法的话，路由将不会被重发布或者被 `set` 语法受控。如果没有满足 `match` 条件，无论指定了 `permit` 还是 `deny` 语法，路由都不会被接收或者转发。



这个命令对 BGP, OSPF, RIP 有效。

## 命令语法

**match ip next-hop** *ACCESSSLISTID*

**no match ip next-hop** [*ACCESSSLISTID*]

ACCESSSLISTID	指定 IPV4 ACL 名
---------------	---------------

## 命令模式

Route-map 模式

## 默认

默认 **match ip next-hop** 不设置。

## 使用说明

无

## 举例说明

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# match ip next-hop mylist
```

## 相关命令

**match community**

**match as-path**

**set as-path**

**set community**

**match metric**

### 8.4.8 match ip next-hop prefix-list

用这个命令来匹配下一跳的前缀列表条目。

使用相应的 **no** 命令来删除这个规则。



这个命令对 BGP, OSPF, RIP 有效。

## 命令语法

```
match ip next-hop prefix-list LISTNAME  
no match ip next-hop prefix-list [ LISTNAME ]
```

LISTNAME	IP 前缀列表名
----------	----------

## 命令模式

Route-map 模式

## 默认

默认 `match ip next-hop prefix-list` 不设置。

## 使用说明

无

## 举例说明

```
Switch# configure terminal  
Switch(config)# route-map mymap permit 3  
Switch(config-route-map)# match ip next-hop prefix-list list1
```

## 相关命令

```
match metric  
match interface  
match ip next-hop
```

### 8.4.9 match local-preference

使用这个命令来指定匹配本地优先级。使用相应的 `no` 命令来删除这个规则。



这个命令对 BGP 有效。

## 命令语法

```
match local-preference LOCAL-PREFERENCE
```

no match local-preference

LOCAL-PREFERENCE	<0-4294967295> 指定优先级
------------------	----------------------

## 命令模式

Route-map 模式

## 默认

默认 match local-preference 不设置。

## 使用说明

无

## 举例说明

```
Switch# configure terminal
Switch(config)# route-map mymap permit 3
Switch(config-route-map)# match local-preference 100
```

## 相关命令

match community

match as-path

set as-path

set community

match ip next-hop

### 8.4.10 match metric

使用这个命令来 match metric 值。

使用相应的 no 命令来删除这个规则。

如果指定匹配了 metric 值并且指定是 permit 的语法的话，路由将会被重发布或者被 set 语法所受控。如果满足了 match 条件但是制定了 deny 语法的话，路由将不会被重发布或者被 set 语法受控。如果没有满足 match 条件，无论指定了 permit 还是 deny 语法，路由都不会被接收或者转发。



这个命令对 BGP, OSPF, RIP 有效。

## 命令语法

**match metric** *METRICVAL*

no match metric

METRICVAL	<+/-metric> <0-4294967295> metric 值
-----------	-------------------------------------

## 命令模式

Route-map 模式

## 默认

默认 match metric 不设置。

## 使用说明

无

## 举例说明

```
Switch# configure terminal
Switch(config)# route-map myroute permit 3
Switch(config-route-map)# match metric 2
```

## 相关命令

match community

match as-path

set as-path

set community

match ip next-hop

### 8.4.11 match origin

使用这个命令来匹配 BGP 中的起始(origin)属性。

使用相应的 **no** 命令来删除这个规则。

Origin 属性定义了路径的起始信息。EGP 参数用路由表中的 e 来表示，这表明这一条路由的起始信息是从外部网关协议(EGP)中学习到的。同样的，IGP 参数用路由表中的 i 来表示，它表示起始路径信息是通过内部网关协议(IGP)学习到的。

在路由表中，不完整的(incomplete)会用?来表示，这就是说，这个路由的原始路径是通过不清楚或者其他别的方式来学习到的。比如，一个静态路由被重发布到 BGP 的话，那它的原始路由就是不完整的。



这个命令只对 BGP 有效。

## 命令语法

```
match origin { egp | igp | incomplete }
```

```
no match origin
```

egp	从 EGP 学到
igp	本地 IGP
incomplete	未知源

## 命令模式

Route-map 模式

## 默认

默认 `match origin` 不设置。

## 使用说明

无

## 举例说明

```
Switch# configure terminal
Switch(config)# route-map myroute deny 34
Switch(config-route-map)# match origin egp
```

## 相关命令

无

### 8.4.12 match route-type external

使用这个命令来匹配指定的外部路由类型。

使用相应的 `no` 命令来删除这个规则。

使用 `match route-type external` 命令来匹配指定的外部路由类型。自治系统外部 LSA 即是类型 1 或者是类型 2。外部类型 1 值匹配类型 1 的外部路由，外部类型 2 只匹配类型 2 的外部路由。





这个命令仅对 OSPF 有效。

## 命令语法

```
match route-type external { type-1 | type-2 }
```

```
no match route-type external
```

type-1	匹配 OSPF 外部类型 1 metric
type-2	匹配 OSPF 外部类型 2 metric

## 命令模式

Route-map 模式

## 默认

默认 `match route-type` 不设置。

## 使用说明

无

## 举例说明

```
Switch# configure terminal
Switch(config)# route-map mymap1 permit 10
Switch(config-route-map)# match route-type external type-1
```

## 相关命令

`match tag`

### 8.4.13 match tag

使用这个命令来匹配指定的 `tag`。

使用相应的 `no` 命令来删除这个规则。



这个命令对 OSPF, RIP 有效。

## 命令语法

```
match tag TAG
```

no match tag

TAG	<0-4294967295> 指定 tag 值
-----	-------------------------

## 命令模式

Route-map 模式

## 默认

默认 match tag 不设置。

## 使用说明

无

## 举例说明

```
Switch# configure terminal
Switch(config)# route-map mymap1 permit 10
Switch(config-route-map)# match tag 100
```

## 相关命令

match metric

match route-type external

### 8.4.14 set aggregator

使用这个命令来设置 route-map 和 router ID 的 AS 号。

使用相应的 no 命令来删除这个规则。

自治系统(AS)是一个网络管理机构控制下的路由器和网络群组。他们被不同的区域所分离，被指派了一个独特的 16 位的号码。使用 set aggregator as 命令来指定这个 AS 号码。

为了使用 set aggregator 命令，你必须首先要有一个 match 规则。Match 和 set 命令设置了路由协议间重发布路由的规则。Match 命令制定了在满足什么样的条件下才能进行重发布，而 Set 命令则指定了满足条件后所执行的动作。

如果报文没有满足任何定义的条件，他们将会被正常的路由所转发。



这个命令仅对 BGP 有效。

## 命令语法

**set aggregator as** *ASNUM* *IPADDRESS*

no set aggregator

ASNUM	<1-65535> 指定集合的 AS 号
IPADDRESS	指定集合的 IP 地址

## 命令模式

Route-map 模式

## 默认

默认 set aggregator 不设置。

## 使用说明

无

## 举例说明

```
Switch# configure terminal
Switch(config)# route-map myroute permit 3
Switch(config-route-map)# set aggregator as 43 10.10.0.3
```

## 相关命令

无

### 8.4.15 set as-path

使用这个命令来修改自治系统(AS)的路径。

使用相应的 no 命令来删除这个规则。

使用 set as-path 命令来指定一个 AS 的路径。通过指定 AS-Path 的长度，路由器可以影响路径的最佳路径选择。在这个命令中使用 prepend 参数，来在已有的 AS-Path 中，再追加一个指定的 AS-path。



这个命令仅对 BGP 有效。

## 命令语法

set as-path prepend *ASN* [...*ASN*]

no set as-path

ASN	追加自治系统的 AS-path
prepend	系统会将这个号码加到现有的 AS-path 中去

## 命令模式

Route-map 模式

## 默认

默认 set as-path 不设置。

## 使用说明

无

## 举例说明

```
Switch# configure terminal
Switch(config)# route-map myroute permit 3
Switch(config-route-map)# set as-path prepend 8 24
```

## 相关命令

无

### 8.4.16 set atomic-aggregate

使用这个命令来设置 atomic aggregate 属性。

使用相应的 no 命令来删除这个规则。

使用该命令你首先要有个 match 规则，match 和 set 规则同时作用来进行路由重分布。Match 命令指定向其他路由协议重发布路由的规则。Set 命令指定在当前 route-map 下路由重分布的表现方式。

如果报文没有匹配到任何条件，将会被通常的路由表转发。



这个命令对 BGP 有效。

## 命令语法

set atomic-aggregate

no set atomic-aggregate

## 命令模式

Route-map 模式

## 默认

默认 `set atomic-aggregator` 不设置。

## 使用说明

无

## 举例说明

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set atomic-aggregate
```

## 相关命令

无

### 8.4.17 set comm-list delete

使用这个命令来删除从进入或者外发更新时，满足条件的 `community`。

使用相应的 `no` 命令来删除这个规则。



这个命令仅对 BGP 有效。

## 命令语法

**set comm-list** { <1-199>|<100-199>|WORD } delete

no set comm-list

<1-199>	标准 community 列表号
<100-199>	扩展 community 列表号
WORD	Community 列表名
delete	删除匹配条件的 community

## 命令模式

Route-map 模式

## 默认

默认 `set comm-list delete` 不设置。

## 使用说明

无

## 举例说明

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set comm-list 34 delete
```

## 相关命令

无

### 8.4.18 set community

用这个命令来设置 `community` 属性。

使用相应的 `no` 命令来删除这个规则。

使用这个命令来设置 `community` 属性和在某个特定的 `community` 中的组目的地址，已经，根据这些 `community` 来应用路由选择。



这个命令对 BGP 有效。

## 命令语法

```
set community [ AA:NN | internet | local-AS | no-advertise | no-export ]
```

```
set community none
```

```
no set community
```

AA:NN	AA:NN: 用这样的格式来描述 <code>community</code> 号 AA = AS 号 NN = 指定的 <code>community</code> 号
internet	指定 Internet 这个 <code>community</code> (公认的 <code>community</code> )
local-AS	指定不发往 local AS 以外的 AS (公认的 <code>community</code> )
no-advertise	指定不把这个路由对对等体宣告 (公认的 <code>community</code> )
no-export	指定不把这个路由对下一个 AS 宣告 (公认的 <code>community</code> )
none	把通过这个 <code>route-map</code> 的 <code>community</code> 属性删除

## 命令模式

Route-map 模式

## 默认

默认 set community 不设置。

## 使用说明

无

## 举例说明

下面是使用 set community 时的例子：

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set community no-export no-advertise
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set community no-advertise
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set community 10:01 23:34 12:14 no-export
```

## 相关命令

无

### 8.4.19 set dampening

使用这个命令来使能 route-flap 惩罚，并且设置它的参数。

使用相应的 no 命令来删除这个规则。

设置不可达的半衰期(half-life time)大于等于可达的半衰期。抑制门限值必须要比重用门限值大。



这个命令仅对 BGP 有效。

## 命令语法

```
set dampening REACHTIME REUSE SUPPRESS MAXSUPPRESS [ UNREACHTIME ]
```

```
no set dampening
```

REACHTIME	<1-45> 用分来表示可达的半衰期。时间衰减是当前值的一半，默认 15 分钟
REUSE	<1-20000> 指定重用门限值。当被一种的路由的惩罚值衰减到重用孟宪以下是，这个路由就不再被抑制。默认重用门限是 750
SUPPRESS	<1-20000> 指定抑制门限值。当一个路由的惩罚值超过抑制门限的时候，这个路由就被抑制了。默认的抑制门限是 2000
MAXSUPPRESS	<1-255> 指定最大抑制时间。一个被惩罚的路由的最大抑制时间。默认值是半衰期的 4 倍(60 分钟)
UNREACHTIME	<1-45> 指定不可达半衰期的惩罚值，默认 15 分钟

## 命令模式

Route-map 模式

## 默认

请参考命令语法中的描述。

## 使用说明

无

## 举例说明

```
Switch# configure terminal
Switch(config)# route-map R1 permit 24
Switch(config-route-map)# set dampening 20 333 534 30
```

## 相关命令

无

### 8.4.20 set extcommunity

使用这个命令来设置一个扩展的 `community` 属性。

使用相应的 `no` 命令来删除这个规则。

使用该命令你首先要有个 `match` 规则，`match` 和 `set` 规则同时作用来进行路由重分布。`Match` 命令指定向其他路由由协议重发布路由的规则。`Set` 命令指定在当前 `route-map` 下路由重分布的表现方式。

如果报文没有匹配到任何条件，将会被通常的路由表转发。





这个命令对 BGP 有效。

## 命令语法

```
set extcommunity { rt | soo} EXTCOMMNUMBER [...EXTCOMMNUMBER ]
```

```
no set extcommunity { rt | soo}
```

rt	指定扩展 community 的扩展对象
soo	指定扩展 community 的 site-of-origin 属性
EXTCOMMNUMBER	ASN:NN 或者 IP-address:nn VPN 扩展 comminty
ASN:NN	AS 号
IPADDRESS	以 IP 地址形式表示的 AS 号

## 命令模式

Route-map 模式

## 默认

默认 set extcommunity 不设置。

## 使用说明

无

## 举例说明

```
Switch# configure terminal
Switch (config)# route-map rmap1 permit 3
Switch (config-route-map)# set extcommunity rt 06:01
Switch# configure terminal
Switch (config)# route-map rmap1 permit 3
Switch (config-route-map)# set extcommunity rt 0.0.0.6:01
Switch# configure terminal
Switch (config)# route-map rmap1 permit 3
Switch (config-route-map)# set extcommunity soo 06:01
Switch# configure terminal
Switch (config-route-map)# route-map rmap1 permit 3
Switch (config-route-map)# set extcommunity soo 0.0.0.6:01
```

## 相关命令

无

## 8.4.21 set ip next-hop

使用这个命令来设置指定的下一跳的值。

使用相应的 `no` 命令来删除这个规则。

使用该命令你首先要有个 `match` 规则，`match` 和 `set` 规则同时作用来进行路由重分布。`Match` 命令指定向其他路由协议重发布路由的规则。`Set` 命令指定在当前 `route-map` 下路由重分布的表现方式。

如果报文没有匹配到任何条件，将会被通常的路由表转发。



这个命令对 BGP, OSPF, RIP 和策略路由有效。

### 命令语法

```
set ip next-hop A.B.C.D
```

```
no set ip next-hop
```

A.B.C.D	A.B.C.D: 指定下一跳的 IP 地址
---------	-----------------------

### 命令模式

Route-map 模式

### 使用说明

无

### 默认

默认 `set ip next-hop` 不设置。

### 举例说明

```
Switch# configure terminal
Switch(config)# route-map mymap permit 3
Switch(config-route-map)# set ip next-hop 10.10.0.67
```

### 相关命令

无

## 8.4.22 set ip nex-hop load-share

使用这个命令来设置指定多个下一跳的值并进行负载均衡。

使用相应的 `no` 命令来删除这个规则。

使用该命令你首先要有个 `match` 规则，`match` 和 `set` 规则同时作用来进行路由重分布。`Match` 命令指定向其他路由协议重发布路由的规则。`Set` 命令指定在当前 `route-map` 下路由重分布的表现方式。

如果报文没有匹配到任何条件，将会被通常的路由表转发。



这个命令对 BGP, OSPF, RIP 和策略路由有效。

## 命令语法

```
set ip next-hop A.B.C.D A.B.C.D [A.B.C.D ...] load-share
```

```
no set ip next-hop load-share
```

A.B.C.D	A.B.C.D: 指定下一跳的 IP 地址
---------	-----------------------

## 命令模式

Route-map 模式

## 使用说明

最多支持 4 个下一跳负载均衡

## 默认

默认 `set ip next-hop` 不设置。

## 举例说明

```
Switch# configure terminal
Switch(config)# route-map mymap permit 3
Switch(config-route-map)# set ip next-hop 10.10.0.67 10.11.0.100 load-share
```

## 相关命令

无

### 8.4.23 set local-preference

使用这个命令来设置本地优先级属性。

使用相应的 `no` 命令来删除这个规则。

使用该命令你首先要有个 **match** 规则，**match** 和 **set** 规则同时作用来进行路由重分布。**Match** 命令指定向其他路由协议重发布路由的规则。**Set** 命令指定在当前 **route-map** 下路由重分布的表现方式。

如果报文没有匹配到任何条件，将会被通常的路由表转发



这个命令仅对 BGP 有效。

## 命令语法

**set local-preference** *LOCAL-PREFERENCE*

**no set local-preference**

*LOCAL-PREFERENCE* <0-4294967295> 指定优先级

## 命令模式

Route-map 模式

## 默认

默认 **set local-preference** 不设置。

## 使用说明

无

## 举例说明

```
Switch# configure terminal
Switch(config)# route-map mymap permit 3
Switch(config-route-map)# set local-preference 100
```

## 相关命令

无

### 8.4.24 set metric

使用这个命令来设置一个路由的 **metric** 值。

使用相应的 **no** 命令来删除这个规则。

这个命令用于设置一条路由的 **metric** 值，以及关于一个关于 AS 的首选路径影响的外部邻居。首选路径是一个比较有较低 **metric** 值的路由。一个路由器比较在同一个 AS 中，

邻居路径的 metric 值。比较不同的 AS 邻居的 metric 值，使用 `bgp always-compare-med` 命令。



这个命令仅对 BGP, OSPF 和 RIP 有效。

## 命令语法

**set metric** *METRICVAL*

**no set metric**

METRICVAL	<+/-metric> <0-4294967295> metric 值
-----------	-------------------------------------

## 命令模式

Route-map 模式

## 默认

默认 `set metric` 不设置。

## 使用说明

无

## 举例说明

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set metric 600
```

## 相关命令

无

## 8.4.25 set metric-type

使用这个命令来设置目的路由协议的 metric 类型。

使用相应的 `no` 命令来删除这个规则。

当 `route-map` 匹配的时候，这个命令设置在 AS-external-LSA 中设置 Type-1 或者 Type-2 两种类型。



这个命令仅对 OSPF 有效。

## 命令语法

```
set metric-type {type1 | type2}
```

```
no set metric-type
```

type1	选择设置外部类型 1 的 metric
type2	选择设置外部类型 2 的 metric

## 命令模式

Route-map 模式

## 默认

默认 set metric-type 不设置。

## 使用说明

无

## 举例说明

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set metric-type 1
```

## 相关命令

无

### 8.4.26 set origin

使用这个命令来设置 BGP origin 代码。

使用相应的 no 命令来删除这个规则。

Origin 属性定义了路径的起始信息。EGP 参数用路由表中的 e 来表示，这表明这一条路由的起始信息是从外部网关协议(EGP)中学习到的。同样的，IGP 参数用路由表中的 i 来表示，它表示起始路径信息是通过内部网关协议(IGP)学习到的。这个路由的原始路径是通过不清楚或者其他别的方式来学习到的。比如，一个静态路由被重发布到 BGP 的话，那它的原始路由就是不完整的。



这个命令仅对 BGP 有效。

## 命令语法

```
set origin { egp | igp | incomplete }
```

```
no set origin
```

egp	指定一个远程 EGP 系统
igp	一个本地的 IGP 系统
incomplete	指定一个不明确的继承关系的系统

## 命令模式

Route-map 模式

## 默认

默认 set origin 不设置。

## 使用说明

无

## 举例说明

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set origin egp
```

## 相关命令

无

### 8.4.27 set originator-id

使用这个命令来设置 originator ID 属性。

使用相应的 no 命令来删除这个规则。

使用该命令你首先要有个 match 规则，match 和 set 规则同时作用来进行路由重分布。Match 命令指定向其他路由协议重发布路由的规则。Set 命令指定在当前 route-map 下路由重分布的表现方式。

如果报文没有匹配到任何条件，将会被通常的路由表转发。



这个命令仅对 BGP 有效。

## 命令语法

```
set originator-id IPADDRESS
no set originator-id
```

IPADDRESS	指定 originator 的 IP 地址
-----------	-----------------------

## 命令模式

Route-map 模式

## 默认

默认 set originator-id 不设置。

## 使用说明

无

## 举例说明

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set originator-id 1.1.1.1
```

## 相关命令

无

### 8.4.28 set tag

使用这个命令来设置一个指定的 tag 值。

使用相应的 no 命令来删除这个规则。

在这个命令中的 tag，被另外一个路由协议(重分布时的 BGP 或者其他 IGP)所标签，原因是 AS-external-LSA 在它的 LSA 中有一个 route-tag 区。并且，使用 route-map 的话，ZebOS 会使用合适的 tag 值对这个 LSA 上打上标签。有时候，这个 tag 会匹配 route-map，有时候，这个值会被其他应用程序所使用。



这个命令仅对 OSPF 和 RIP 有效。

## 命令语法

```
set tag TAGVALUE
```



no set tag

TAGVALUE	<0-4294967295> 目的路由协议的 tag 号
----------	------------------------------

## 命令模式

Route-map 模式

## 默认

默认 set tag 不设置。

## 使用说明

无

## 举例说明

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set tag 6
```

## 相关命令

redistribute

default-information

## 8.4.29 set vpnv4 next-hop

使用这个命令来设置一个 VPNv4 下一跳地址。

使用相应的 no 命令来删除这个规则。

在这个命令中的 tag，被另外一个路由协议(重分布时的 BGP 或者其他 IGP)所标签，原因是 AS-external-LSA 在它的 LSA 中有一个 route-tag 区。并且，使用 route-map 的话，ZebOS 会使用合适的 tag 值对这个 LSA 上打上标签。有时候，这个 tag 会匹配 route-map，有时候，这个值会被其他应用程序所使用。



这个命令仅对 BGP 有效。

## 命令语法

set vpnv4 next-hop *IPADDRESS*

no set vpnv4 next-hop

IPADDRESS	指定下一跳 IP 地址
-----------	-------------

## 命令模式

Route-map 模式

## 默认

默认 set vpnv4 next-hop 不设置。

## 使用说明

无

## 举例说明

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set vpnv4 next-hop 6.6.6.6
```

## 相关命令

无

### 8.4.30 set weight

使用这个命令来设置路由表的应用权重(weight)。

使用相应的 no 命令来删除这个规则。

Weight 值是用于帮助进行最优路径选择的。它在路由器本地被之地你个。当有多个路由器，他们的目的地都相同时，有比较高权重的路由器将会被优先选中。



这个命令仅对 BGP 有效。

## 命令语法

set weight *WEIGHT*

no set weight

WEIGHT	<0-4294967295> 指定权重值
--------	----------------------

## 命令模式

Route-map 模式

## 默认

默认 set weight 不设置。

## 使用说明

无

## 举例说明

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set weight 60
```

## 相关命令

match as-path

### 8.4.31 show route-map

使用这个命令来显示用户可读的 route-map 信息。

## 命令语法

```
show route-map [ NAME ]
```

NAME	route-map 名
------	-------------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch1# show route-map
route-map abc, permit, sequence 10
```

```

Match clauses:
  ip address acl1
Set clauses:
  local-preference 200
route-map abc, permit, sequence 20
Match clauses:
Set clauses:

```

## 相关命令

route-map

## 8.5 Prefix-list 命令

### 8.5.1 ip prefix-list

在全局配置模式下，使用命令 **ip prefix-list** 创建地址前缀列表或添加表项。使用该命令的 **no** 形式删除配置。

## 命令语法

```

ip prefix-list WORD (seq SEQUENCE-NUMBER) (deny | permit)
(any | A.B.C.D/M (ge GE-LENGTH) (le LE-LENGTH))
no ip prefix-list WORD (seq SEQUENCE-NUMBER) (deny | permit)
(any | A.B.C.D/M (ge GE-LENGTH) (le LE-LENGTH))
no ip prefix-list WORD (seq SEQUENCE-NUMBER)

```

<b>WORD</b>	地址前缀列表表名
<b>seq SEQUENCE-NUMBER</b>	地址前缀列表表项序号，范围 1~65535。如果输入命令的时候没有指定序号，将添加默认序号。默认序号为 5 的倍数，并且是剩下序号中大于当前已分配序号的最小的数
<b>deny</b>	指定地址前缀列表的匹配模式为拒绝。在该模式下，如果过滤的 IP 地址在定义的范围，该 IP 地址不能通过过滤从而不能进入下一表项的测试；否则，将进行下一表项的测试
<b>permit</b>	指定地址前缀列表的匹配模式为允许。在该模式下，如果过滤的 IP 地址在定义的范围，则通过过滤，进行相应的设置；否则，必须进行下一表项的测试
<b>A.B.C.D/M</b>	网络地址和掩码位数。掩码位数范围 0~32
<b>ge GE-LENGTH</b>	指定地址匹配的最小前缀长度
<b>le LE-LENGTH</b>	指定地址匹配的最大前缀长度

## 命令模式

全局配置模式

## 默认

没有地址前缀列表被创建。

使用说明

地址前缀列表用于 IP 地址过滤。同一个地址前缀列表可包含多个表项，一个表项包括地址和掩码位数。命令中的 **deny** 和 **permit** 关键字指定该匹配结果是拒绝或者允许。此时，多个表项之间是“或”的关系，即通过一个表项就可通过该地址前缀列表的过滤。没有通过任何一个表项的过滤就意味着没有通过该地址前缀列表的过滤。

地址前缀范围包括两个部分，分别由 **mask-length** 和 **[greater-equal-value, less-equal-value]** 决定。如果指定了这两部分，要被过滤的 IP 地址必须匹配这两部分规定的前缀范围。具体的匹配公式如下：

$$\text{network/length} < \text{ge ge-length} < \text{le le-length} \leq 32$$

例如，只指定 **ge-length**，则匹配范围为 **[ge-length,32]**；只指定 **le-length**，则匹配范围为 **[network/length, le-length]**；如果两者都指定，则匹配范围为 **[ge-length, le-length]**。

如果在输入命令中没有指定序号，则交换机会自动为表项添加默认序号。默认序号从 5 开始，并且每次递增 5，例如，5、10、15。默认序号将从当前大于已分配的序号中选择，并且是其中的最小值。

## 举例说明

- 配置匹配默认路由的拒绝表项：

```
Switch(config)# ip prefix-list abc deny 0.0.0.0/0
```

- 配置匹配 10.0.0.0/8 的允许表项：

```
Switch(config)# ip prefix-list abc permit 10.0.0.0/8
```

- 配置匹配长度为 [16,24]，地址为 192.168.0.0/16 的允许表项：

```
Switch(config)# ip prefix-list abc permit 192.168.0.0/16 le 24
```

- 配置匹配长度为 [25,32]，地址为 192.168.0.0/16 的拒绝表项：

```
Switch(config)# ip prefix-list abc deny 192.168.0.0/16 ge 25
```

## 相关命令

```
ip prefix-list description
```

```
ip prefix-list sequence
```

```
show ip prefix-list
```

```
clear ip prefix-list
```

## 8.5.2 ip prefix-list description

在全局配置模式下，使用命令 `ip prefix-list description` 添加地址前缀列表描述。使用命令相关的 `no` 形式删除该配置。

### 命令语法

```
ip prefix-list WORD description LINE
```

```
no ip prefix-list WORD description (LINE)
```

WORD	地址前缀列表表名
LINE	地址前缀列表描述，范围 0~80

### 命令模式

全局配置模式

### 默认

地址前缀列表默认没有描述。

### 使用说明

如果该地址前缀列表不存在，交换机将会自动创建。

### 举例说明

配置地址前缀列表描述为：Deny routes from router A

```
Switch(config)# ip prefix-list abc description Deny routes from router A
```

### 相关命令

```
ip prefix-list
```

```
ip prefix-list sequence
```

```
show ip prefix-list
```

```
clear ip prefix-list
```

## 8.5.3 ip prefix-list sequence-number

在全局配置模式下，使用命令 `ip prefix-list sequence-number` 启用地址前缀列表序号。使用命令相关的 `no` 形式关闭序号。

## 命令语法

```
ip prefix-list sequence-number
no ip prefix-list sequence-numbe
```

## 命令模式

全局配置模式

## 默认

地址前缀列表默认使用序号。

## 使用说明

该命令会使显示地址前缀列表配置的时候显示序号。

## 举例说明

配置启用地址前缀列表序号：

```
Switch(config)# ip prefix-list sequence-number
```

## 相关命令

```
ip prefix-list
show ip prefix-list
clear ip prefix-list
```

### 8.5.4 show ip prefix-list

使用命令 `show ip prefix-list` 显示当前地址前缀列表配置。

## 命令语法

```
show ip prefix-list (summary | detail) (WORD)
show ip prefix-list WORD (seq SEQUENCE-NUMBER|A.B.C.D/M (longer | first-match) |)
```

summary	地址前缀列表统计摘要
detail	地址前缀列表详细统计
WORD	地址前缀列表表名
seq SEQUENCE-NUMBER	表项序号
A.B.C.D/M	网络地址/掩码位数 e.g., 35.0.0.0/8
longer	只显示掩码位数大于 M 的表项

first-match	只显示第一个匹配的表项
-------------	-------------

## 命令模式

特权模式

## 默认

无

## 使用说明

只有 RIP 支持 `prefix` 的引用统计。

## 举例说明

显示地址前缀列表信息：

```
Switch# show ip prefix-list
ip prefix-list aa: 2 entries
  permit 1.1.1.0/24
  permit 1.2.3.0/24
```

## 相关命令

`ip prefix-list`

`clear ip prefix-list`

### 8.5.5 clear ip prefix-list

使用 `clear ip prefix-list` 清除地址前缀列表计数器的统计信息。

## 命令语法

**clear ip prefix-list** (*WORD (A.B.C.D/M)*)

WORD	地址前缀列表表名
A.B.C.D/M	网络地址/掩码位数 e.g., 35.0.0.0/8

## 命令模式

特权模式



## 默认

无

## 使用说明

无

## 举例说明

重置地址前缀列表计数器：

```
Switch# clear ip prefix-list abc
```

## 相关命令

ip prefix-list

# 8.6 PBR 命令

## 8.6.1 ip policy route-map

默认情况下，PBR 不在设备上启用，想要启用 PBR 的话，你首先要配置一个有 `match` 和 `set` 语句的 `route-map`，然后，你才可以在一个三层端口上启用 PBR 功能。所有进入这个端口上的报文，都会去匹配这个 `route-map` 制定的 `match` 策略，满足 `match` 策略的报文，将会按照 `set` 制定的规则进行相应的转发处理。

## 命令语法

```
ip policy route-map map-NAME
```

```
no ip policy route-map
```

map-NAME	策略路由映射名
----------	---------

## 命令模式

端口配置模式

## 默认

禁用

## 使用说明

这个命令可以在 `routed` 端口，`vlan` 端口 `routed` 汇聚端口上启用。

## 举例说明

下面的例子表明了如何在设备上启用 PBR。

```
switch (config)# ip access-list 1 extend
switch (config-ex-ip-acl)# 10 permit any any any
switch (config-route-map)# exit
switch (config)# route-map richard permit 10
switch (config-route-map)# match ip address 1
switch (config-route-map)# set ip next-hop 10.1.1.1
switch (config-route-map)# exit
switch (config)# interface eth-0-1
switch (config-if)# no switch port
switch (config-if)# no shutdown
switch (config-if)# ip policy route-map richrad
```

## 相关命令

route-map

### 8.6.2 show ip policy route-map

使用这个命令来表示 PBR 配置的详细信息。

## 命令语法

```
show ip policy route-map
```

## 命令模式

特权模式

## 默认

禁用

## 使用说明

查看 PBR 在接口的应用情况

## 举例说明

```
SWITCH# show ip policy route-map
Route-map                interface
richard                   eth-0-1
                           eth-0-3

Failed entry: no
sally                     eth-0-2
Failed entry: yes
Please use Policy Based-Routing CLI: show pbr failed entry to gain more detail.
```

## 相关命令

route-map

### 8.6.3 show resource pbr

使用这个命令来 PBR 模块的资源使用情况。

## 命令语法

```
show resource pbr
```

## 命令模式

特权模式

## 默认

禁用

## 使用说明

无

## 举例说明

```
SWITCH# show resource pbr
Policy Based Routing
Resource                               Used          Capability
=====
Policy Route Map                        0             32
Policy Based Routing ACE                0             64
```

## 相关命令

route-map

```
show ip policy route-map
```

## 8.7 BGP 命令

### 8.7.1 address-family

使用这个命令来进入 IPv4, VPNv4 address-family 命令模式。

## 命令语法

```
address-family ipv4 (unicast|vrf NAME |)
```

```
address-family vpnv4 (unicast)
```

vpn4	配置 VPN-IPV4 前缀的会话，这个参数使用 IPV4 风格的地址格式：A.B.C.D
unicast	指定单播前缀
vrf	VPN 路由/转发实例
NAME	VPN 路由/转发实例名

## 命令模式

路由模式

## 默认

N/A

## 使用说明

使用 `address-family` 命令，来进入路由模式，允许配置跟路由相关的参数。

退出该模式使用相应的 `exit`，或者 `exit-address-family` 命令。

## 举例说明

```
Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) address-family ipv4
```

## 相关命令

`exit`, `exit-address-family`

## 8.7.2 advertise l2vpn

### 命令语法

**advertise l2vpn**

### 命令模式

ipv4 VRF 地址族模式

### 默认

无

### 使用说明

在 vrf 内向其他 vtep 发布 type5 类性的路由

## 举例说明

```
Switch(config)# router bgp 65001

Switch(config-vrf)# address family ipv4 vrf evpn-tenant-1

Switch(config-router-af)# redistribute connected

Switch(config-router-af)# advertise l2vpn
```

## 相关命令

```
redistribute (BGP)
```

### 8.7.3 aggregate-address

使用这个命令来配置 BGP 集合条目。

使用相应的 no 命令来删除这个配置。

## 命令语法

```
(no) aggregate-address IPADDRESS {summary-only|as-set}
```

IPADDRESS	A.B.C.D/M 指定聚合的 IP 前缀
summary-only	从更新过程中，过滤更多的指定路由
as-set	生成 AS set 路径信息

## 命令模式

路由模式

## 默认

Disabled

## 使用说明

聚合用于将路由表的规模最小化。聚合通过一些特征，将不同的路由联合起来，并宣告为一条路由。如果更确定的 BGP 路由在可选择的范围的话，aggregate-address 命令在 BGP 路由表中创建了一个聚合条目。使用参数 summary-only 只宣告前缀，对所有邻居抑制更确定的路由。

## 举例说明

```
Switch# configure terminal
Switch(config)# router bgp 100
Switch(config-router)# aggregate-address 10.0.0.0/8 as-set summary-only
```

## 相关命令

N/A

### 8.7.4 bgp always-compare-med

使用这个命令来比较在不同 AS 中的邻居间距离的 Multi Exit Discriminator (MED)。

使用相应的 no 命令来删除这个配置。

## 命令语法

```
(no) bgp always-compare-med
```

## 命令模式

路由模式

## 默认

Disabled

## 使用说明

Multi Exit Discriminator (MED) 用于 BGP 的最佳路径选路。在 BGP 的属性: weight, local preference, AS-path 和 origin 的比较结果为相等以后, MED 将被进行比较。

MED 只在相同的 AS 的路径中进行比较。使用 bgp always-compare-med 命令来允许在不同的 AS 间比较 MED。MED 参数在选择最佳路径以后才被使用。一个具有低 MED 的路径会被优先使用。

## 举例说明

```
Switch# configure terminal
Switch(config)# router bgp 100
Switch(config-router)# bgp always-compare-med
```

## 相关命令

bgp bestpath med, bgp bestpath as-path ignore

### 8.7.5 bgp bestpath as-path ignore

使用这个命令来防止这个路由器被通过 AS-path 原则选中。

使用相应的 no 命令来让这个路由器可以通过 AS-path 原则选中。

## 命令语法

(no) bgp bestpath as-path ignore

## 命令模式

路由模式

## 默认

N/A

## 使用说明

N/A

## 举例说明

```
Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) bgp bestpath as-path ignore
```

## 相关命令

bgp always-compare-med, bgp bestpath med, bgp bestpath compare-routerid

### 8.7.6 bgp bestpath compare-confed-aspath

使用这个命令来允许比较 AS-path 的长度。

使用相应的 no 命令来反转这个选择，并且忽略在 BGP 最佳路径选择中的 AS 联合路径长度。

## 命令语法

(no) bgp bestpath compare-confed-aspath

## 命令模式

路由模式

## 默认

BGP 从 eBGP 对等体中使用相等的 eBGP 路径来接受路由，并选择接收到的第一条路由为最优路径。

## 使用说明

这个命令指定了，在 BGP 最佳路径选择中，当 AS 联合路径长度可用的时候，必须要使用这样一个规则。它只在 bgp bestpath as-path ignore 命令没有被指定的时候生效。

## 举例说明

```
Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) bgp bestpath compare-confed-aspath
```

## 相关命令

bgp bestpath as-path ignore

### 8.7.7 bgp bestpath compare-routerid

使用这个命令来比较对等的 eBGP 路径的 router-id。

使用相应的 no 命令来删除这个配置。

## 命令语法

(no) bgp bestpath compare-routerid

## 命令模式

路由模式

## 默认

BGP 从 eBGP 对等体中使用相等的 eBGP 路径来接受路由，并选择接收到的第一条路由为最优路径。

## 使用说明

当对比对等体中相同的路由的时候，BGP 路由器并不考虑路由器上的 router ID。默认情况下，它选择第一个接收到的路由。使用这个命令在选择过程中包括考虑 route ID 这样一个步骤，相同的路由将会被比较，并且拥有最小 route ID 的路由将会被选择。Route-id 是路由器中最高 IP 地址，这个 IP 地址优先会使用 loopback 地址。Route-id 可以被 bgp router-id 命令来手动设置。

## 举例说明

```
Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) bgp bestpath compare-routerid
```

## 相关命令

show ip bgp, show ip bgp neighbors

### 8.7.8 bgp bestpath med

使用这个命令来指定 Multi Exit Discriminator (MED) 属性的比较。

使用相应的 no 命令来防止 BGP 在选路时把 MED 作为考虑因素。



## 命令语法

```
bgp bestpath med confed [ missing-as-worst ]
```

```
bgp bestpath med missing-as-worst [confed]
```

confed	在联合路径中比较 MED
missing-as-worst	把丢失的 MED 作为优先选择的对象

## 命令模式

路由模式

## 默认

MED 值是 0

## 使用说明

使用这个命令来指定两个 MED 属性：`confed` 和 `missing-as-worst`。`Confed` 属性让 MED 通过联合对等体中学到的路径来进行比较。MED 仅在路径中没有扩展的 AS(不在联合中的 AS)比较。如果路径中只要有一个扩展的 AS，MED 比较就不会进行。

`Missing-as-worst` 属性则将丢失的 MED 作为路径中为无限大值来考虑，把丢失了 MED 的路径作为最差的路径来考虑。如果 `missing-as-worst` 没有使能的话，丢失的 MED 值是 0，这样的话这条路径就会作为最佳路径来考虑。

## 举例说明

```
Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) bgp bestpath med missing-as-worst
```

## 相关命令

`bgp-always-compare-med`, `bgp bestpath as-path ignore`, `bgp deterministic-med`

### 8.7.9 bgp client-to-client reflection

使用这个命令来从 BGP 路由反射客户端来回滚路由反射(route reflection, RR)。

使用相应的 `no` 命令来删除这个配置。

## 命令语法

```
(no) bgp client-to-client reflection
```

reflection	路由反射
------------	------

## 命令模式

路由模式

## 默认

当路由器被配置为路由反射时，client-to-client 的反射将会被默认使能。

## 使用说明

bgp client-to-client reflection 命令用于配置路由器为 RR。当所有的内部网关协议(iBGP)的 speaker 都没有全部两两互联的时候，会使用 RR。如果客户端已经全互联了，那 RR 就不必要了，使用 no bgp client-to-client reflection 命令来取消 client-to-client 的反射。

## 举例说明

```
Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) no bgp client-to-client reflection
```

## 相关命令

bgp cluster-id, neighbor route-reflector-client, show ip bgp

### 8.7.10 bgp cluster-id

如果 BGP 集群有一个以上的 RR 的话，使用这个命令来配置 cluster ID。

使用相应的 no 命令来删除这个配置。

## 命令语法

(no) bgp cluster-id CLUSTERID

CLUSTERID	A.B.C.D <1-4294967295> 指定这个路由器的 cluster ID，它会像一个 RR 一样活动。可以是一个 IP 地址，或者是一个最大为 4 字节的数值。
A.B.C.D	RR 的以 IP 地址形式的 cluster-id
<1-4294967295>	RR 的 32bit cluster-id

## 命令模式

路由模式

## 默认

N/A

## 使用说明

一个集群包括了 RR 和它的客户端。通常，一个集群被它的唯一的 RR 的 `route-id` 所标识，但是为了增加冗余，有时候，一个集群可能会有一个以上的 RR。所有在这样一个集群里面的 RR 都被同一个 `cluster ID` 所标识。`bgp cluster-id` 命令用于配置拥有一个以上 RR 集群的 32bit 的 `cluster ID`。

## 举例说明

```
Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) bgp cluster-id 1.1.1.1
```

## 相关命令

`bgp client-to-client reflection`, `neighbor route-reflector-client`, `show ip bgp`

## 8.7.11 bgp confederation identifier

使用这个命令来指定一个 Bgp confederation identifier.

使用相应的 `no` 命令来删除 Bgp confederation identifier.

## 命令语法

(no) `bgp confederation identifier ID`

ID= <1-65535> 设置路由域的联合 ASN

ID	<1-65535> 设置路由域的联合 ASN
----	------------------------

## 命令模式

路由模式

## 默认

N/A

## 使用说明

N/A

## 举例说明

```
Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) bgp confederation identifier 1
```

## 相关命令

bgp confederation peer

### 8.7.12 bgp confederation peers

使用这个命令来配置属于指定联合的自治系统(AS)。

使用相应的 no 命令来删除这个配置。

## 命令语法

(no) bgp confederation peers .ASN

ASN	<1-65535> 在同一个联合但不同 sub-AS 下的 eBGP 对等体的 ASN
-----	---

## 命令模式

路由模式

## 默认

N/A

## 使用说明

一个联合允许一个 AS 被分成几个 AS。AS 会被指定一个联合号。外部的路由器只能把整个联合看作一个 AS。每个 AS 在内部是全互联的，并且对这个联合来说，是内部可见的。使用 bgp confederation peers 命令来定义联合对等体列表。

## 举例说明

```
Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) bgp confederation peers 1234 21345
```

## 相关命令

bgp confederation identifier

## 8.7.13 bgp dampening

使用这个命令来指定 bgp dampening 的参数

使用相应的 no 命令来删除这个配置。

### 命令语法

(no) bgp dampening REACHTIME

(no) bgp dampening REACHTIME REUSE

(no) bgp dampening REACHTIME REUSE SUPPRESS MAXSUPPRESS  
(UNREACHTIME)

(no) bgp dampening ROUTEMAP

REACHTIME	<1-45> 指定可达半衰期(单位 min)。惩罚时间是当前值的一半。默认 15min。
REUSE	<1-20000> 指定重用门限值。当对一个抑制路由的惩罚，一直衰减到重用门限值以下时，这个路由就不再被抑制了。默认值是 750。
SUPPRESS	<1-20000> 指定抑制门限值。当对一个路由的惩罚超过这个抑制门限时，这个路由会被抑制。默认值 2000。
MAXSUPPRESS	<1-255> 指定最大抑制时间。惩罚路由被抑制的最长时间。默认是 4 倍的半衰期(60min)。
UNREACHTIME	<1-45> 指定不可达半衰期(单位 min)。
ROUTEMAP	route-map WORD 指定惩罚规则的 route-map。
WORD	指定 route-map 的名字。

### 命令模式

路由模式

地址族(单播 ipv4 | 单播 vpnv4 | ipv4 vrf)模式

### 默认

N/A

### 使用说明

路由惩罚最大限度的减少了由于路由翻动(route flapping)导致的不稳定性。每次翻动都会在这个翻动的路由上增加一个惩罚。一旦当总的惩罚值达到抑制门限，这个路由的

宣告就会被抑制。这个惩罚会根据配置的半衰期进行衰减。一旦惩罚比重用门限低的时候，路由的抑制就会被取消。

一旦惩罚值低于重用门限的一半时，惩罚信息会被立即取消。

## 举例说明

```
Switch# configure terminal
Switch(config)# router bgp 100
Switch(config-router)# bgp dampening 20 800 2500 80 25
```

## 相关命令

N/A

## 8.7.14 bgp default ipv4-unicast

使用这个命令来配置 BGP 默认状态并且激活对等体的 IPV4 单播默认状态。这将会影响 BGP 的全局配置。

使用相应的 no 命令来删除这个配置。

## 命令语法

```
(no) bgp default ipv4-unicast
```

## 命令模式

路由模式

## 默认

BGP 默认行为是 IPV4 单播。

## 使用说明

no bgp default ipv4-unicast 用于让 BGP 默认的路由行为(与 BGP 邻居交换 IPV4 地址)失效。

## 举例说明

```
Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) bgp default ipv4-unicast
```

## 相关命令

N/A

## 8.7.15 bgp default local-preference

使用这个命令来改变默认的 local-preference 值。

使用相应的 `no` 来返回默认设置。

## 命令语法

(no) `bgp default local-preference PREFERRED_VALUE`

PREFERRED_VALUE	<0-4294967295> 配置默认的 local preference 值，默认 100
-----------------	--

## 命令模式

路由模式

## 默认

N/A

## 使用说明

Local-preference 表示，当存在通往同一个目的的多条路径时，优先级比较高的那条路径。使用 `bgp default local-preference` 命令来定义特定的路径优先级。这个优先级是针对本地 AS 的所有路由器和接入服务器有效的。

## 举例说明

```
Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) bgp default local-preference 2345555
```

## 相关命令

N/A

## 8.7.16 bgp deterministic med

当在同一个 AS 中，从不同的对等体中选择宣告的路由时，使用这个命令来比较 Multi Exit Discriminator (MED) 参数。

使用相应的 `no` 命令来删除这个配置。

## 命令语法

(no) `bgp deterministic-med`

## 命令模式

路由模式

## 默认

Disabled

## 使用说明

Multi Exit Discriminator (MED) 用于在 BGP 中的最佳路径选择。在 BGP 的属性：weight, local preference, AS-path 和 origin 的比较结果为相等以后，MED 将被进行比较。在本地 AS 的所有的路由器上，使能 `bgp deterministic-med` 命令，用于获取一个比较结果。在使能这个命令以后，所有对同一前缀的路径，都会被组合在一起，并且根据他们的 MED 值来安排。

根据这个比较，就可以得出一个最佳路径。

这个命令，在同一个 AS 中，在选择被不同对等体宣告的路由时，根据 MED 值来进行比较。当在不同的 AS 上进行选路时要比较 MED 的话，要使用 `bgp always-compare-med` 命令。

## 举例说明

```
Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) bgp deterministic-med
```

## 相关命令

`show ip bgp`, `show ip bgp neighbors`

### 8.7.17 bgp enforce-first-as

使用这个命令来设置用来拒绝，第一个 AS-path 不是邻居配置的 ASN 的 update 消息。

使用相应的 `no` 命令来删除这个配置。

## 命令语法

(no) `bgp enforce-first-as`

## 命令模式

路由模式

## 默认

N/A

## 使用说明

使能这个特性，将会增加 BGP 网络的安全性，不允许接受未授权的系统发来的流量。

## 举例说明

```
Switch# configure terminal
```



```
Switch(config)# router bgp 100
Switch(config-router)# bgp enforce-first-as
```

## 相关命令

N/A

## 8.7.18 bgp fast-external-failover

使用这个命令，如果使用 BGP 的接口，连接 down 的话，立即重置一个 BGP 会话。

使用相应的 no 命令来删除这个配置。

## 命令语法

```
(no) bgp fast-external-failover
```

## 命令模式

路由模式

## 默认

Enabled

## 使用说明

N/A

## 举例说明

```
Switch# configure terminal
Switch(config)# router bgp 100
Switch(config-router)# bgp fast-external-failover
```

## 相关命令

N/A

## 8.7.19 bgp log-neighbor-changes

使用这个命令，在没有打开 debug bug 命令的条件下，用日志记录 BGP 状态迁移信息。

使用相应的 no 命令来删除这个配置。

## 命令语法

```
bgp log-neighbor-changes
```

## 命令模式

路由模式

## 默认

Disabled

## 使用说明

Centec 的系统提供了另外一种方法用于记录邻居状态的实现，比如，`debug bgp fsm`，`debug bgp events`，等。然而，这些命令会对日志系统的性能造成很严重的影响：

`bgp log-neighbor-changes` 命令，会记录如下事件

- 接收到 BGP 通告
- 接收到错误的 BGP 更新
- 用户重置请求
- 对等体超时
- 对等体关闭会话
- 接口震荡
- 变换
- 删除邻居
- 成员被增加到对等体组中
- 端口
- 远端 AS 变化
- 修改 RR 客户端配置
- 软件修改配置

## 举例说明

```
Switch# configure terminal
Switch(config)# router bgp 100
Switch(config-router)# bgp log-neighbor-changes
```

## 相关命令

N/A

### 8.7.20 bgp router-id

使用这个命令来配置 `router-id`。

使用相应的 `no` 命令来删除这个配置。

## 命令语法

(no) bgp router-id ROUTERID

ROUTERID	A.B.C.D 手动配置 router-id
----------	------------------------

## 命令模式

路由模式

地址族(ipv4 vrf)模式

## 默认

如果配置了环回口的话，route-id 将会设置为环回口地址，否则的话，最高的 IP 地址将会设置为 router-id。

## 使用说明

使用 bgp router-id 命令来手动配置一个固定的 route-id，作为 BGP 的路由器标识。

## 举例说明

```
Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) bgp router-id 1.1.2.3
```

## 相关命令

N/A

### 8.7.21 bgp scan-time

使用这个命令来设置 BGP 路由下一跳的扫描间隔。

使用相应的 no 命令来删除这个配置。

## 命令语法

(no) bgp scan-time TIME

TIME	<0-60> 以 s 为单位，默认值 60s
------	------------------------

## 命令模式

路由模式

## 默认

N/A

## 使用说明

使用这个命令来配置 BGP 路由器的扫描间隔，这个间隔是路由器检查在数据表中路由的可靠性的周期。

如果想要禁用 BGP 扫描机能的话，将扫描间隔设置为 0。

## 举例说明

```
Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) bgp scan-time 10
```

## 相关命令

N/A

### 8.7.22 clear ip bgp \*

使用这个命令来重置所有对等体的 BGP 连接。

## 命令语法

```
clear ip bgp * (in|out|SOFT)
clear ip bgp * ipv4 PREFIX ROUTES
clear ip bgp * vpnv4 unicast ROUTES
clear ip bgp * vrf NAME ROUTES
```

*	清除所有的 BGP 对等体
ipv4	清除所有 IPv4 地址族对等体
vpnv4	清除所有 VPNv4 地址族对等体
ROUTES	IN out SOFT
IN	in(前缀过滤)
in	表示入站的宣告路由将会被清除
prefix-filter	过滤特定的前缀

out	示出站的宣告路由将会被清除
SOFT	(in out)表示入站/出站的宣告路由都将会被清除
PREFIX	单播 组播
unicast	单播
multicast	组播
vrf VPN	路由/转发实例
NAME VPN	路由/转发实例名

## 命令模式

特权模式

## 默认

N/A

## 使用说明

BGP 的重置分硬重置和软重置两种，它们的区别就是：硬重置会导致 BGP 邻居关系切断并重新建立；软重置不会切断邻居关系，只会重新刷新路由表。

## 举例说明

```
Switch# clear ip bgp *
Switch# clear ip bgp * ipv4 unicast in prefix-filter
Switch# clear ip bgp * vpnv4 unicast in
```

## 相关命令

N/A

### 8.7.23 clear ip bgp A.B.C.D

使用这个命令来通过指定的 IP 地址重置 IPV4 BGP 的连接。

## 命令语法

```
clear ip bgp A.B.C.D (in|out|SOFT)
clear ip bgp A.B.C.D ipv4 PREFIX ROUTES
clear ip bgp A.B.C.D vpnv4 unicast ROUTES
```

A.B.C.D	要清除的 BGP 路由的 IP 地址
---------	--------------------

ipv4	清除所有 IPv4 地址族对等体
vpn4	清除所有 VPNv4 地址族对等体
ROUTES	IN out SOFT
IN	in(前缀过滤)
in	表示入站的宣告路由将会被清除
prefix-filter	过滤特定的前缀
out	示出站的宣告路由将会被清除
SOFT	(in out)表示入站/出站的宣告路由都将会被清除
PREFIX	单播 组播
unicast	单播
multicast	组播

## 命令模式

特权模式

## 默认

N/A

## 使用说明

N/A

## 举例说明

```
Switch# clear ip bgp 10.10.0.12 soft
Switch# clear ip bgp 10.10.0.10 vpn4 unicast out
```

## 相关命令

N/A

### 8.7.24 clear ip bgp dampening

使用这个命令来重置所有指定地址族的 BGP 惩罚路由。

## 命令语法

```
clear ip bgp dampening (A.B.C.D|A.B.C.D/M)
clear ip bgp ipv4 PREFIX dampening (A.B.C.D|A.B.C.D/M)
```

A.B.C.D	指定想要清除的 BGP 惩罚的 IPV4 地址
A.B.C.D/M	定想要清除的 BGP 惩罚的带子网的 IPV4 地址
ipv4	清除所有 IPV4 地址族对等体
PREFIX	单播 组播
unicast	单播
multicast	组播

## 命令模式

特权模式

## 默认

N/A

## 使用说明

N/A

## 举例说明

```
Switch# clear ip bgp dampening 10.10.0.121
Switch# clear ip bgp ipv4 unicast dampening
```

## 相关命令

N/A

### 8.7.25 clear ip bgp flap-statistics

使用这个命令来清除所有指定地址族的前缀的振荡次数和历史统计。

## 命令语法

clear ip bgp flap-statistics (A.B.C.D|A.B.C.D/M)

clear ip bgp ipv4 PREFIX flap-statistics (A.B.C.D|A.B.C.D/M)

A.B.C.D	指定想要清除的 BGP 惩罚的 IPV4 地址
A.B.C.D/M	定想要清除的 BGP 惩罚的带子网的 IPV4 地址
ipv4	清除所有 IPV4 地址族对等体

PREFIX	单播 组播
unicast	单播
multicast	组播

## 命令模式

特权模式

## 默认

N/A

## 使用说明

N/A

## 举例说明

```
Switch# clear ip bgp flap-statistics 10.10.0.121
Switch# clear ip bgp ipv4 unicast flap-statistics
```

## 相关命令

N/A

## 8.7.26 clear ip bgp ASN

使用这个命令来重置一个指定 AS 下的所有对等体的 BGP 连接。

## 命令语法

```
clear ip bgp ASN (IN|out|SOFT)
clear ip bgp ASN ipv4 PREFIX ROUTES
clear ip bgp ASN vpngv4 unicast ROUTES
```

ASN	<1-65535>= 指定要被删除的所有路由的 ASN
ipv4	清除所有 IPv4 地址族对等体
vpngv4	清除所有 VPNv4 地址族对等体
ROUTES	IN out  SOFT
IN	in(前缀过滤)
in	表示入站的宣告路由将会被清除



prefix-filter	过滤特定的前缀
SOFT	(in out)表示入站/出站的宣告路由都将会被清除
PREFIX	单播 组播
unicast	单播
multicast	组播

## 命令模式

特权模式

## 默认

N/A

## 使用说明

N/A

## 举例说明

```
Switch# clear ip bgp 100
Switch# clear ip bgp 200 ipv4 unicast in prefix-filter
Switch# clear ip bgp 500 vpnv4 unicast in
```

## 相关命令

N/A

## 8.7.27 clear ip bgp external

使用这个命令来对所有外部对等体的 BGP 连接进行重置。

## 命令语法

```
clear ip bgp external (In|out|SOFT)
clear ip bgp external ipv4 PREFIX ROUTES
```

external = 清除所有的外部对等体  
 ipv4 = 清除所有 IPv4 地址族对等体  
 ROUTES = In|out|soft  
 IN = in(前缀过滤)  
 in = 表示入站的宣告路由将会被清除  
 prefix-filter = 过滤特定的前缀

out = 表示出站的宣告路由将会被清除

SOFT = (in|out)表示入站/出站的宣告路由都将会被清除

PREFIX = 单播|组播

unicast = 单播

multicast = 组播

ipv4	清除所有 IPv4 地址族对等体
ROUTES	In out soft
IN	in(前缀过滤)
in	表示入站的宣告路由将会被清除
prefix-filter	过滤特定的前缀
out	表示出站的宣告路由将会被清除
SOFT	(in out)表示入站/出站的宣告路由都将会被清除
PREFIX	单播 组播
unicast	单播
multicast	组播

## 命令模式

特权模式

## 默认

N/A

## 使用说明

N/A

## 举例说明

```
Switch# clear ip bgp external out
Switch# clear ip bgp external ipv4 unicast in prefix-filter
```

## 相关命令

N/A

### 8.7.28 clear ip bgp peer-group

使用这个命令来重置一个对等组下的所有成员的 BGP 连接。

## 命令语法

```
clear ip bgp peer-group WORD(In|out|SOFT)
```

```
clear ip bgp peer-group WORD ipv4 PREFIX ROUTES
```

peer-group	清除一个对等组的所有成员
WORD	指定要清除的对等组的名字
ipv4	清除所有 IPv4 地址族对等体
ROUTES	In out soft
prefix-filter	过滤特定的前缀
IN	in(前缀过滤)
in	表示入站的宣告路由将会被清除
prefix-filter	过滤特定的前缀
out	表示出站的宣告路由将会被清除
SOFT	(in out)表示入站/出站的宣告路由都将会被清除
PREFIX	单播 组播
unicast	单播
multicast	组播

## 命令模式

特权模式

## 默认

N/A

## 使用说明

N/A

## 举例说明

```
Switch# clear ip bgp peer-group Peer1 out
Switch# clear ip bgp peer-group mypeer ipv4 unicast in prefix-filter
```

## 相关命令

N/A

## 8.7.29 clear ip bgp vrf

使用这个命令来重置指定的 BGP 连接的 VPN 路由/转发实例。

### 命令语法

```
clear ip bgp (A.B.C.D|*) vrf WORD (out|in|SOFT)
```

WORD 指定 VRF 名

A.B.C.D 指定要清楚的 BGP 路由的 IPV4 地址

\*清除所有对等体

in 进行 in 方向的软重置

out 进行 out 方向的软重置

SOFT = soft in|soft out|soft

WORD	指定 VRF 名
A.B.C.D	指定要清楚的 BGP 路由的 IPV4 地址
*	清除所有对等体
out	进行 out 方向的软重置
SOFT	soft in soft out soft

### 命令模式

特权模式

### 默认

N/A

### 使用说明

如果这个命令中，指定了邻居的地址的话，它将会把这个指定的连接给清除掉。如果没指定任何地址，这个命令将会清除所有的 BGP 路由。

### 举例说明

```
Switch# clear ip bgp 3.3.3.3 vrf VRF1 soft in
```

### 相关命令

N/A

## 8.7.30 debug bgp

使用这个命令来使能所有的 BGP 调试功能。

使用相应的 no 命令来删除这个配置。

### 命令语法

```
debug bgp (all|dampening|events|filters|fsm|keepalives|mpls| updates)
```

```
no debug all bgp
```

```
no debug bgp (all|dampening|events|filters|fsm|keepalives|mpls|nsm| updates)
```

all	打开或者关闭所有 BGP 调试开关。
dampening	BGP 惩罚调试模式
events	BGP 事件调试模式
filters	BGP 过滤调试模式
fsm	BGP 有限状态机(FSM)调试模式
mpls	BGP MPLS 调试模式
keepalives	BGP keepalive 信息调试模式
updates	BGP 更新通告调试模式

### 命令模式

特权模式

### 默认

N/A

### 使用说明

不带任何参数使用这个命令的话会打开所有通常的 BGP 调试开关。

### 举例说明

```
Switch# debug bgp
Switch# debug bgp events
```

### 相关命令

N/A

## 8.7.31 distance

使用这个命令来定义管理距离。

使用相应的 no 命令来删除这个配置。

### 命令语法

```
(no) distance ADMINDISTANCE | BGPDISTANCE
```

ADMINDISTANCE	<1-255> A.B.C.D/M (LISTNAME) 指定管理距离
1-255	管理距离
A.B.C.D/M	IP 源地址前缀
LISTNAME	引用到被选择的路由上的管理距离的 ACL 名
BGPDISTANCE	bgp EXT INT LOCAL 指定 IP 地址和子网掩码
EXT	<1-255> 指定 BGP 外部路由的管理距离。默认外部路由的管理距离是 20
INT	<1-255> 指定 BGP 内部路由的管理距离，默认内部路由的管理距离是 200
LOCAL	<1-255> 指定 BGP 本地路由的管理距离，默认本地路由的管理距离是 200

### 命令模式

路由模式

### 默认

N/A

### 使用说明

使用这个命令来试着 BGP 的管理距离。这个距离标识了一个路由器的可靠性。

这个值越高越不可靠。

管理距离可以对外部，内部和本地的路由进行设置。外部路径是从 AS 外部邻居学习到的路由。内部路由是在同一个 AS 的另外一个路由器中学习到的路由。而本地路由则是本路由器从别的进程中通过重发布学习到的路由。

如果管理距离被改变的话，将会在路由表中出现矛盾，并且阻塞路由。

## 举例说明

```
Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) distance 34 10.10.0.0/24 mylist
Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) distance bgp 34 23 15
```

## 相关命令

N/A

### 8.7.32 exit-address-family

使用这个命令来退出地址族模式。

## 命令语法

```
exit-address-family
```

## 命令模式

地址族模式

## 默认

N/A

## 使用说明

N/A

## 举例说明

下面的例子描述了 exit-address-family 命令的使用

```
Switch# configure terminal
Switch(config)# router bgp 100
Switch(config-router)# address-family ipv4 unicast
Switch(config-router-af)# exit-address-family
Switch(config-router)#
```

## 相关命令

地址族

### 8.7.33 ip as-path access-list

使用这个命令定义一个 BGP AS 路径的 ACL。

使用相应的 no 命令来删除这个配置。

## 命令语法

(no) ip as-path access-list LISTNAME (deny|permit) .LINE

LISTNAME 指定 ACL 的名字

deny (Optional) 匹配条件的 deny ACL

permit (Optional) 匹配条件的 permit ACL

.LINE 指定一个匹配 BGP AS-path 的常规描述。

LISTNAME	指定 ACL 的名字
deny	(Optional) 匹配条件的 deny ACL
permit	(Optional) 匹配条件的 permit ACL
.LINE	指定一个匹配 BGP AS-path 的常规描述。

## 命令模式

配置模式

## 默认

N/A

## 使用说明

命名联合表示一个基于常规表述的过滤规则。如果这个常规表述匹配了指定的用于代表某个路由的 AS-path 的字符串的话，则会应用相应的 permit 或者 deny 条件。使用这个命令来全局的定义 BGP ACL，使用 neighbor router configuration 命令来应用一个指定的 ACL。

## 举例说明

```
Switch# configure terminal
Switch(config)# ip as-path access-list mylist deny ^65535$
```

## 相关命令

N/A

### 8.7.34 ip community-list

使用这个命令来增加一个联合列表(community list)条目。

使用相应的 no 命令来删除这个配置。



## 命令语法

```
(no) ip community-list LISTNUM deny|permit .COMMUNITY
```

LISTNUM	指定联合列表的数量
<1-99>	联合列表号(标准)
<100-199>	联合列表号(扩展)
deny	指定拒绝这个联合
permit	指定允许这个联合
COMMUNITY	AA:NN internet local-AS no-advertise no-export
AA:NN	指定一个对于联合号来说有效的值。这个值的格式是一个 32bit 的值，AS 是高 16bit 而 VAL 是低 16bit。
internet	指定路由不被 internet 宣告。
local-AS	指定路由被外部 BGP 对等体宣告。
no-advertise	指定路由不被宣告到其他 BGP 对等体。
no-export	指定路由不被宣告到 AS 边界以外。

## 命令模式

配置模式

## 默认

N/A

## 使用说明

使用 community-lists 来指定 BGPcommunity 属性。community 属性用于实现策略路由。这是个可选的及物的属性，并且可以促进本地策略通过不同的 AS 来传输。它包括了 32bit 长度的联合值。

有两种 community-lists：扩展的和标准的。常规的 community-list 用指定的格式(非常规表述)来定义了 community 属性。而扩展的 community-list 则用常规表述来定义 community 属性。

## 举例说明

```
Switch# configure terminal
Switch(config)# ip community-list 20 permit 7675:80 7675:90
```

## 相关命令

ip community-list standard, ip community-list expanded

### 8.7.35 ip community-list expanded

使用这个命令来增加一个联合列表条目。

使用相应的 no 命令来删除这个配置。

## 命令语法

(no) ip community-list expanded WORD deny|permit .LINE

expanded	增加一个扩展联合列表条目
WORD	扩展联合扩展联合列表名
deny	指定拒绝这个联合列表
permit	指定允许这个联合列表
.LINE	指定使用常规表述来描述联合列表

## 命令模式

配置模式

## 默认

N/A

## 使用说明

使用 community-lists 来指定 BGPcommunity 属性。community 属性用于实现策略路由。这是个可选的及物的属性，并且可以促进本地策略通过不同的 AS 来传输。它包括了 32bit 长度的联合值。

有两种 community-lists：扩展的和标准的。常规的 community-list 用指定的格式(非常规表述)来定义了 community 属性。而扩展的 community-list 则用常规表述来定义 community 属性。

## 举例说明

```
Switch# configure terminal
Switch(config)# ip community-list expanded CLIST permit .*
```

## 相关命令

ip community-list, ip community-list standard

## 8.7.36 ip community-list standard

使用这个命令来增加一个标准的联合列表条目。

使用相应的 no 命令来删除这个配置。

### 命令语法

```
(no) ip community-list standard WORD deny|permit .COMMUNITY
```

standard	增加一个标准联合列表条目。
WORD	标准联合扩展联合列表名
deny	指定拒绝这个联合列表
permit	指定允许这个联合列表
COMMUNITY	AA:NN internet local-AS no-advertise no-export
AA: NN	指定一个对于联合号来说有效的值。这个值的格式是一个 32bit 的值，AS 是高 16bit 而 VAL 是低 16bit。
internet	指定路由不被 internet 宣告。
local-AS	指定路由不被外部 BGP 对等体宣告。
no-advertise	指定路由不被宣告到其他 BGP 对等体。
no-export	指定路由不被宣告到 AS 边界以外。

### 命令模式

配置模式

### 默认

N/A

### 使用说明

使用 community-lists 来指定 BGP community 属性。community 属性用于实现策略路由。这是个可选的及物的属性，并且可以促进本地策略通过不同的 AS 来传输。它包括了 32bit 长度的联合值。

有两种 community-lists：扩展的和标准的。常规的 community-list 用指定的格式(非常规表述)来定义了 community 属性。而扩展的 community-list 则用常规表述来定义 community 属性。

使用 ip community-list standard 来增加一个标准的 community-list 条目。标准的 community-list 被编译成了二进制格式，并且直接和 BGP 更新时的 BGPcommunity 属性

相比较。这个比较过程比扩展 `community-list` 要快。任何不匹配标准联合值的联合值都被自动的作为扩展联合值来对待。

## 举例说明

```
Switch# configure terminal
Switch(config)# ip community-list standard CLIST permit 7675:80 7675:90 no-export
```

## 相关命令

`ip community-list`, `ip community-list expanded`

### 8.7.37 neighbor activate

使用这个命令来使能和启用一个邻居路由器的指定 AF 路由信息交换功能。

使用相应的 `no` 命令来删除这个配置。

## 命令语法

(no) neighbor NEIGHBORID activate

NEIGHBORID	A.B.C.D TAG
A.B.C.D	以 IP 地址格式来指定 BGP 邻居的地址。
TAG	已经存在的对等组名。请参考 <code>neighbor peer-group</code> , <code>neighbor remote-as</code> 命令来创建对等组。当这个参数被命令使用的时候, 这个命令会被应用到指定组的所有对等体上。

## 命令模式

地址族模式和路由模式

## 默认

N/A

## 使用说明

在 TCP 连接被邻居打开以后, 这个命令被用于使能或者取消和邻居路由器之间指定 AF 信息交换。

使能组播和 VPNv4 地址前缀类型的交换, 邻居要在地址族模式下使用 `neighbor activate` 命令来激活。

## 举例说明

```
Switch# configure terminal
```

```
Switch(config)# router bgp 10
Switch(config-router)# neighbor 1.2.3.4 activate
```

## 相关命令

neighbor remote-as

### 8.7.38 neighbor advertisement-interval

使用这个命令来设置 BGP 路由更新的最小间隔。

使用相应的 no 参数来设置间隔为默认值。

## 命令语法

```
(no) neighbor NEIGHBORID advertisement-interval TIME
```

NEIGHBORID	A.B.C.D TAG
A.B.C.D	以 IP 地址格式来指定 BGP 邻居的地址。
TAG	已经存在的对等组名。请参考 neighbor peer-group, neighbor remote-as 命令来创建对等组。当这个参数被命令使用的时候, 这个命令会被应用到指定组的所有对等体上。
TIME	<0-600> 以 s 为单位的宣告间隔值。

## 命令模式

路由模式

## 默认

N/A

## 使用说明

使用这个命令来设置 BGP 路由更新发送的最小间隔。为了降低在 internet 中的路由抖动, 设定了一个最小的宣告间隔。所以 BGP 路由只会在每个时间间隔被发送。bgp dampening 也可以被用于控制路由抖动的效果。

## 举例说明

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 10.10.0.3 advertisement-interval 45
```

## 相关命令

N/A

### 8.7.39 neighbor allowas-in

使用这个命令来配置 PE 路由，用于运行对所有的含有重复 ASN(ASN)的前缀进行重宣告。

使用相应的 no 命令来删除这个配置。

## 命令语法

```
neighbor NEIGHBOR allowas-in [ NUMBER ]
```

```
no neighbor NEIGHBOR allowas-in
```

NEIGHBORID	A.B.C.D TAG
A.B.C.D	以 IP 地址格式来指定 BGP 邻居的地址。
TAG	已经存在的对等组名。请参考 neighbor peer-group, neighbor remote-as 命令来创建对等组。当这个参数被命令使用的时候，这个命令会被应用到指定组的所有对等体上。
NUMBER	<1-10> 发生的 ASN 的数量

## 命令模式

路由模式和地址族模式

## 默认

Disabled

## 使用说明

在一个 hub-and-spoke 系统中，一个 PE 路由器会重宣告所有包含重复 ASN 的 IP 前缀。使用 neighbor allowas-in 命令在每个 PE 路由器上配置两个 VRF，来接受和重宣告前缀。其中的一个 VRF 接受所有 PE 路由器宣告的带 ASN 的前缀，然后将它们宣告给邻居路由器。另外一个 VRF 则从 CE 路由器接受带 ASN 的前缀并将它们重宣告给所有的在 hub-and-spoke 系统中的 PE 路由器。

通过指定从 1~10 的数字，来控制 ASN 被宣告的次数。

## 举例说明

```
Switch (config-router)# address-family ipv4 vrf VRF_A
Switch (config-router-af)# neighbor 10.10.0.1 allowas-in 3
```

## 相关命令

N/A

### 8.7.40 neighbor attribute-unchanged

使用这个命令来向指定的邻居宣告没改变的 BGP 属性。

使用相应的 no 命令来删除这个配置。

## 命令语法

(no) neighbor NEIGHBORID attribute-unchanged {as-path|next-hop|med}

NEIGHBORID	A.B.C.D TAG
A.B.C.D	以 IP 地址格式来指定 BGP 邻居的地址。
TAG	已经存在的对等组名。请参考 neighbor peer-group, neighbor remote-as 命令来创建对等组。当这个参数被命令使用的时候, 这个命令会被应用到指定组的所有对等体上。
as-path	AS 路径属性
next-hop	下一跳属性
med	MED 值

## 命令模式

路由模式和地址族模式

## 默认

N/A

## 使用说明

N/A

## 举例说明

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 10.10.0.75 attribute-unchanged as-path med
```

## 相关命令

N/A

## 8.7.41 neighbor capability dynamic

使用这个命令在指定的对等体上使能动态容量。

使用相应的 no 命令来删除这个配置。

### 命令语法

(no) neighbor NEIGHBORID capability dynamic

NEIGHBORID	A.B.C.D TAG
A.B.C.D	以 IP 地址格式来指定 BGP 邻居的地址。
TAG	已经存在的对等组名。请参考 neighbor peer-group, neighbor remote-as 命令来创建对等组。当这个参数被命令使用的时候, 这个命令会被应用到指定组的所有对等体上。

### 命令模式

路由模式

### 默认

Disabled

### 使用说明

这个命令允许 BGP 的 speaker 来向一个对等体以非分裂方式来宣告或者回滚一个地址族的容量。

### 举例说明

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 10.10.10.1 capability dynamic
```

### 相关命令

N/A

## 8.7.42 neighbor capability orf prefix-list

使用这个命令来向邻居宣告 ORF 的最大容量(capability)。

使用相应的 no 命令来删除这个配置。



## 命令语法

(no) neighbor NEIGHBORID capability orf prefix-list (both|receive|send)

NEIGHBORID	A.B.C.D TAG
A.B.C.D	以 IP 地址格式来指定 BGP 邻居的地址。
TAG	已经存在的对等组名。请参考 <code>neighbor peer-group</code> , <code>neighbor remote-as</code> 命令来创建对等组。当这个参数被命令使用的时候, 这个命令会被应用到指定组的所有对等体上。
orf	向邻居宣告 ORF 容量
both	表示本地路由器既可以向他的对等体发送条目, 又可以接受 ORF 条目。
receive	只能接受 ORF 条目。
send	只能发送 ORF 条目。

## 命令模式

路由模式和地址族模式

## 默认

N/A

## 使用说明

出站路由过滤(ORF)发送和接受 `capability` 用来减轻邻居间的更新交互。通过过滤更新, 这个选项可以让生成和处理的更新最小化。

本地路由在发送模式下宣告 ORF `capability`, 远端路由在接受模式下接受这个宣告并应用这个过滤规则。两个路由器交互更新来维持他们各自的 ORF。

## 举例说明

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 1.1.1.1 capability orf prefix-list both
```

## 相关命令

N/A

### 8.7.43 neighbor capability route-refresh

使用这个命令来向指定邻居宣告路由更新的 `capbality`。

使用相应的 `no` 命令来删除这个配置。

## 命令语法

(no) neighbor NEIGHBORID capability route-refresh

NEIGHBORID	A.B.C.D TAG
A.B.C.D	以 IP 地址格式来指定 BGP 邻居的地址。
TAG	已经存在的对等组名。请参考 <code>neighbor peer-group</code> , <code>neighbor remote-as</code> 命令来创建对等组。当这个参数被命令使用的时候, 这个命令会被应用到指定组的所有对等体上。

## 命令模式

路由模式

## 默认

N/A

## 使用说明

使用这个命令来向对等体宣告, 最大支持的路由更新。

## 举例说明

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 10.10.10.1 capability route-refresh
```

## 相关命令

N/A

### 8.7.44 neighbor default-originate

使用这个命令来允许 BGP 本地路由来发送默认路由 0.0.0.0 到一个邻居, 作为它的默认路由。

使用相应的 `no` 命令来删除这个配置。

## 命令语法

(no) neighbor NEIGHBORID default-originate (ROUТЕMAP)

NEIGHBORID	A.B.C.D TAG
A.B.C.D	以 IP 地址格式来指定 BGP 邻居的地址。
TAG	已经存在的对等组名。请参考 <code>neighbor peer-group</code> ， <code>neighbor remote-as</code> 命令来创建对等组。当这个参数被命令使用的时候，这个命令会被应用到指定组的所有对等体上。
ROUTEMAP	route-map WORD
route-map	用于指定成为起始默认路由的标准的 route-map
WORD	Route-map 名

## 命令模式

路由模式和地址族模式

## 默认

N/A

## 使用说明

每个路由器都应该有个默认的路由，它应用于向不是在本本地 IP 路由表中的网络发送数据包。确保每个路由器都有一个默认路由的方法是，在每个路由器上配置一个静态路由，用来设置默认的路由。另一种方法是，创建一个默认路由并把这个路由广播到 BGP 邻居中。拥有默认路由的路由器，可以使用这个命令，来通过 BGP 广播这个路由。

## 举例说明

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 10.10.10.1 default-originate route-map myroute
```

## 相关命令

N/A

### 8.7.45 neighbor description

使用这个命令来将邻居和一个描述关联起来。

使用相应的 `no` 命令来删除这个配置。

## 命令语法

```
(no) neighbor NEIGHBORID description .LINE
```

NEIGHBORID	A.B.C.D TAG
A.B.C.D	以 IP 地址格式来指定 BGP 邻居的地址。
TAG	已经存在的对等组名。请参考 <code>neighbor peer-group</code> , <code>neighbor remote-as</code> 命令来创建对等组。当这个参数被命令使用的时候, 这个命令会被应用到指定组的所有对等体上。
LINE	描述这个邻居最多 80 个字符。

## 命令模式

路由模式和地址族 `ipv4 vrf` 模式 (需要 BGP/VPN 支持)

## 默认

N/A

## 使用说明

选项 `description` 的功能类似软件编程中的注释。这个功能只是用于帮助读者确定代码的作用, 或者在 BGP 中用来确定邻居。把一个邻居的描述加入到 BGP 配置中, 并不影响 BGP 的操作。这个描述应该表达有用的信息, 能够有助于迅速的确定邻居。对于只有几个邻居的简单方案, 它的作用就很有限。但是对于拥有多个邻居的 ISP 来说, 可以使用 `description` 来确定邻居, 而不需要记住它的 IP 地址。

## 举例说明

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 1.2.3.4 description Backup router for sales.
```

## 相关命令

N/A

### 8.7.46 neighbor distribute-list

使用这个命令来过滤来自特定 BGP 邻居的路由更新。

使用相应的 `no` 命令来删除这个配置。

## 命令语法

(no) neighbor NEIGHBORID distribute-list WORD in|out

NEIGHBORID	A.B.C.D TAG
A.B.C.D	以 IP 地址格式来指定 BGP 邻居的地址。

TAG	已经存在的对等组名。请参考 <code>neighbor peer-group</code> , <code>neighbor remote-as</code> 命令来创建对等组。当这个参数被命令使用的时候, 这个命令会被应用到指定组的所有对等体上。
WORD	IP ACL 的名字
in	表示入站的宣告路由将会被过滤
out	表示出站的宣告路由将会被过滤

## 命令模式

路由模式和地址族模式

## 默认

N/A

## 使用说明

每个 BGP 邻居只使用一个 `distribute-list`。

## 举例说明

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 1.2.3.4 distribute-list mylist out
```

## 相关命令

N/A

### 8.7.47 neighbor ebgp-multihop

使用这个命令来在不直连的网络上接受和与外部的对等体尝试 BGP 连接。

使用相应的 `no` 命令来删除这个配置。

## 命令语法

(no) neighbor NEIGHBORID ebgp-multihop (COUNT)

NEIGHBORID = A.B.C.D| TAG

A.B.C.D 以 IP 地址格式来指定 BGP 邻居的地址。

TAG 已经存在的对等组名。

COUNT = <1-255> 最大条数。如果没有设置的话那就是 255。

NEIGHBORID	A.B.C.D TAG
------------	-------------

A.B.C.D	以 IP 地址格式来指定 BGP 邻居的地址。
TAG	已经存在的对等组名。请参考 <code>neighbor peer-group</code> ， <code>neighbor remote-as</code> 命令来创建对等组。当这个参数被命令使用的时候，这个命令会被应用到指定组的所有对等体上。
COUNT	<1-255> 最大条数。如果没有设置的话那就是 255。

## 命令模式

路由模式

## 默认

N/A

## 使用说明

只有在到 `multihop` 对等体的路由时默认路由的时候，才会启用 `multihop`，这可以用来避免出现环路。

## 举例说明

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 10.10.10.34 remote-as 20
Switch(config-router)# neighbor 10.10.10.34 ebgp-multihop 5
```

## 相关命令

N/A

### 8.7.48 neighbor filter-list

使用这个命令来建立一个 BGP 过滤器。

使用相应的 `no` 命令来删除这个配置。

## 命令语法

```
(no) neighbor NEIGHBORID filter-list LISTNAME in|out
```

NEIGHBORID	A.B.C.D TAG
A.B.C.D	以 IP 地址格式来指定 BGP 邻居的地址。
TAG	已经存在的对等组名。请参考 <code>neighbor peer-group</code> ， <code>neighbor remote-as</code> 命令来创建对等组。当这个参数被命令使用的时候，这个命令会被应用到指定组的所有对等体上。

in	表示入站的宣告路由将会被过滤
out	表示出站的宣告路由将会被过滤

## 命令模式

路由模式和地址族模式

## 默认

N/A

## 使用说明

这个命令指定了基于 BGP AS-path 的 ACL 过滤器。每个过滤器都是一个基于常规表达的 ACL。

## 举例说明

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 10.10.0.34 filter-list listname out
```

## 相关命令

N/A

### 8.7.49 neighbor maximum-prefix

使用这个命令来控制可以被邻居接收到的前缀数量。

使用相应的 no 命令来删除这个配置。

## 命令语法

(no) neighbor NEIGHBORID maximum-prefix MAXIMUM

NEIGHBORID	A.B.C.D TAG
A.B.C.D	以 IP 地址格式来指定 BGP 邻居的地址。
TAG	已经存在的对等组名。请参考 neighbor peer-group, neighbor remote-as 命令来创建对等组。当这个参数被命令使用的时候, 这个命令会被应用到指定组的所有对等体上。
MAXIMUM	MAXPREFIX (THRESHOLD) (只有警告)
MAXPREFIX	<1-4294967295> 指定允许前缀的最大数量。

THRESHOLD	<1-100> 指定阈值，1%~100%。
warning-only	在超过限制时只发送警告信息。

## 命令模式

路由模式和地址族模式

## 默认

N/A

## 使用说明

`neighbor maximum-prefix` 命令，允许配置 BGP 路由器允许从邻居接收到的指定的前缀数量。当使用了 `warning-only` 选项的时候，如果接收到任何额外的前缀的话，那路由器将会结束对等状态。一个被结束的对等体，将会一直等到 `clear ip bgp` 命令被执行后，才会启用。

## 举例说明

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 10.10.0.72 maximum-prefix 1244 warning-only
```

## 相关命令

N/A

### 8.7.50 neighbor next-hop-self

使用这个命令来配置路由器作为一个 BGP-speaking 邻居或者一个对等体组。

使用相应的 `no` 命令来删除这个配置。

## 命令语法

(no) neighbor NEIGHBORID next-hop-self

NEIGHBORID	A.B.C.D TAG
A.B.C.D	以 IP 地址格式来指定 BGP 邻居的地址。
TAG	已经存在的对等组名。请参考 <code>neighbor peer-group</code> ， <code>neighbor remote-as</code> 命令来创建对等组。当这个参数被命令使用的时候，这个命令会被应用到指定组的所有对等体上。



## 命令模式

路由模式和地址族模式

## 默认

N/A

## 使用说明

当 BGP 路由器通过 eBGP 得到路由，并且这些路由需要广播给一个 iBGP 邻居时，发送的下一跳信息并不改变。使用这个命令，BGP 路由器可以改变发送给 iBGP 对等体的下一跳信息，把下一跳信息设置为这个邻居进行通信的接口的 IP 地址。

## 举例说明

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 10.10.0.72 remote-as 100
Switch(config-router)# neighbor 10.10.0.72 next-hop-self
```

## 相关命令

N/A

### 8.7.51 neighbor override-capability

使用这个命令来覆盖一个 capability 协商的结果。

使用相应的 no 命令来删除这个配置。

## 命令语法

(no) neighbor NEIGHBORID override-capability

NEIGHBORID	A.B.C.D TAG
A.B.C.D	以 IP 地址格式来指定 BGP 邻居的地址。
TAG	已经存在的对等组名。请参考 neighbor peer-group, neighbor remote-as 命令来创建对等组。当这个参数被命令使用的时候，这个命令会被应用到指定组的所有对等体上。

## 命令模式

路由模式

## 默认

N/A

## 使用说明

N/A

## 举例说明

```
Switch# configure terminal
Switch(config)# router bgp 12
Switch(config-router)# neighbor 10.10.10.10 override-capability
```

## 相关命令

N/A

## 8.7.52 neighbor passive

使用这个命令，来设定一个 BGP 邻居组为被动模式。

使用相应的 no 命令来删除这个配置。

## 命令语法

```
(no) neighbor NEIGHBORID passive
```

NEIGHBORID	A.B.C.D TAG
A.B.C.D	以 IP 地址格式来指定 BGP 邻居的地址。
TAG	已经存在的对等组名。请参考 neighbor peer-group, neighbor remote-as 命令来创建对等组。当这个参数被命令使用的时候，这个命令会被应用到指定组的所有对等体上。

## 命令模式

路由模式

## 默认

N/A

## 使用说明

N/A

## 举例说明

```
Switch# configure terminal
Switch(config)# router bgp 12
Switch(config-router)# neighbor 10.10.10.10 passive
```

## 相关命令

N/A

### 8.7.53 neighbor peer-group (adding a neighbor)

使用这个命令，来向一个已经存在的对等体组中增加一个邻居。

使用相应的 **no** 命令来删除这个配置。

## 命令语法

(no) neighbor IPADDRESS peer-group TAG

IPADDRESS	A.B.C.D 以 IP 地址格式来指定 BGP 邻居的地址。
-----------	---------------------------------

## 命令模式

路由模式

## 默认

N/A

## 使用说明

对邻居使用这个有同样更新策略的命令，将会把它加入到一个对等体组中。这个工具可以更新各种策略，比如分发和过滤器列表。对等组可以用任何 **neighbor** 命令来简单的进行配置。任何对对等组的修改会对所有的成员产生影响。

使用 **neighbor peer-group create** 命令来创建一个对等组，然后使用这个命令来把邻居加入这个组。

## 举例说明

下面是一个把邻居 10.10.0.63 加入一个新的对等组 group1 的例子。

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor group1 peer-group
Switch(config-router)# neighbor 10.10.0.63 peer-group group1
```

## 相关命令

N/A

### 8.7.54 neighbor peer-group (creating a peer-group)

使用这个命令来创建一个对等组。

使用相应的 `no` 命令来删除这个配置。

## 命令语法

(no) neighbor TAG peer-group

TAG 对等组名

TAG	已经存在的对等组名。请参考 <code>neighbor peer-group</code> ， <code>neighbor remote-as</code> 命令来创建对等组。当这个参数被命令使用的时候，这个命令会被应用到指定组的所有对等体上。
-----	--

## 命令模式

路由模式

## 默认

N/A

## 使用说明

这个命令可以更新各种策略，比如分发和过滤器列表。对等组可以用任何 `neighbor` 命令来简单的进行配置。任何对对等组的修改会对所有的成员产生影响。

## 举例说明

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor group1 peer-group
```

## 相关命令

N/A

### 8.7.55 neighbor prefix-list

使用这个命令在指定一个前缀列表的时候来分发 BGP 邻居信息。

使用相应的 `no` 命令来删除这个配置。

## 命令语法

(no) neighbor NEIGHBORID prefix-list LISTNAME in|out

NEIGHBORID	A.B.C.D TAG
A.B.C.D	以 IP 地址格式来指定 BGP 邻居的地址。
TAG	已经存在的对等组名。请参考 <code>neighbor peer-group</code> , <code>neighbor remote-as</code> 命令来创建对等组。当这个参数被命令使用的时候, 这个命令会被应用到指定组的所有对等体上。
LISTNAME	AS-path 的 ACL 号。
in	指定 ACL 应用到入站宣告上
out	指定 ACL 应用到出站宣告上

## 命令模式

路由模式和地址族模式

## 默认

N/A

## 使用说明

使用这个命令来指定一个用于过滤 BGP 宣告的前缀列表。如果有一个匹配到的话, 就使用这个路由。一个空的前缀列表将会允许所有的前缀。如果一个前缀没有匹配任何前缀列表的条目的话, 这个路由就会拒绝访问。当多个前缀列表的多个条目匹配了一个前缀的时候, 有最小序列号的条目就会被选择为真正的匹配。

路由器从前缀列表的最上面(序号 1)开始搜索。一旦匹配到 `match` 或者 `deny`, 下面的前缀列表就不需要继续往下搜索了。为了提高效率, 最常用的匹配要列在最前面。

`neighbor distribute-list` 命令对 `neighbor prefix-list` 命令来说是可选的, 并且, 只有他们中的一个才可以被用于对任意方向的同一个邻居进行过滤。

## 举例说明

```
Switch# configure terminal
Switch(config)# ip prefix-list list1 deny 30.0.0.0/24
Switch(config)# router bgp 12
Switch(config-router)# neighbor 10.10.10.10 prefix-list list1 in
```

## 相关命令

`ip prefix-list`

## 8.7.56 neighbor remote-as

使用这个命令来配置一个跟另一个路由器建立的内部或者外部的 BGP(iBGP 或者 eBGP)的 TCP 会话。

### 命令语法

```
neighbor NEIGHBORID remote-as ASNUM
```

NEIGHBORID	A.B.C.D TAG
A.B.C.D	以 IP 地址格式来指定 BGP 邻居的地址。
TAG	已经存在的对等组名。请参考 neighbor peer-group, neighbor remote-as 命令来创建对等组。当这个参数被命令使用的时候, 这个命令会被应用到指定组的所有对等体上。
ASNUM	<1-4294967295> 邻居 ASN

### 命令模式

路由模式

### 默认

N/A

### 使用说明

这个命令用来配置跟另外一个邻居的 iBGP 和 eBGP 的会话。一个对等组只在建立一个指定的对等组以后才会支持这个命令。

### 举例说明

```
Switch# configure terminal
Switch(config)# router bgp 11
Switch(config-router)# neighbor 10.10.0.73 remote-as 345
```

### 相关命令

N/A

## 8.7.57 neighbor remove-private-AS

使用这个命令来将私有 ASN 从出站更新中移除。

使用相应的 no 命令来删除这个配置并返回默认。

## 命令语法

(no)neighbor NEIGHBORID remove-private-AS

NEIGHBORID	A.B.C.D TAG
A.B.C.D	以 IP 地址格式来指定 BGP 邻居的地址。
TAG	已经存在的对等组名。请参考 <code>neighbor peer-group</code> ， <code>neighbor remote-as</code> 命令来创建对等组。当这个参数被命令使用的时候，这个命令会被应用到指定组的所有对等体上。

## 命令模式

路由模式 and 地址族 (ipv4 unicast | ipv4 multicast | vpnv4 unicast) mode

## 默认

Disabled

## 使用说明

私有 ASN 范围<64512-65535>。私有 ASN 不会被宣告到 Internet 上。这个命令只能和外部 BGP 对等体一起使用。路由器只会在更新中包含私有 ASN 的时候才会删除这个 ASN。如果更新中既有私有的又有公有的 ASN，系统作为 error 处理。

## 举例说明

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 10.10.0.63 remove-private-AS
```

## 相关命令

N/A

### 8.7.58 neighbor route-reflector-client

使用这个命令来配置路由器作为一个 BGP 的 RR，并且配置指定的邻居是他的客户端 (client)。

使用相应的 no 命令来删除这个配置

## 命令语法

(no) neighbor NEIGHBORID route-reflector-client

NEIGHBORID	A.B.C.D TAG
A.B.C.D	以 IP 地址格式来指定 BGP 邻居的地址。
TAG	已经存在的对等组名。请参考 <code>neighbor peer-group</code> , <code>neighbor remote-as</code> 命令来创建对等组。当这个参数被命令使用的时候, 这个命令会被应用到指定组的所有对等体上。

## 命令模式

路由模式和地址族模式

## 默认

N/A

## 使用说明

RR 是一个用来在 AS 中的 iBGP 对等体爆炸式增长的一个解决方案。通过 RR, 在 AS 中 iBGP 对等体的数量会减少。使用 `neighbor route-reflector-client` 命令, 来配置指定邻居作为它的 `client` 以及本地路由作为它的 RR。

由于 AS 可以有多个 RR。一个 RR 把另外一个 RR 作为另外一个 iBGP speaker 来对待。

## 举例说明

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 10.10.0.72 route-reflector-client
```

## 相关命令

N/A

### 8.7.59 neighbor send-community

使用这个命令来指定一个应该被发给一个 BGP 邻居的 `community` 属性。

使用相应的 `no` 命令来删除这个条目。使用 `extended` 和 `no` 参数来删除扩展的联合。不使用任何参数的话就只会删除标准联合。

## 命令语法

(no) neighbor NEIGHBORID send-community (both|extended|standard)

NEIGHBORID	A.B.C.D TAG
A.B.C.D	以 IP 地址格式来指定 BGP 邻居的地址。



TAG	已经存在的对等组名。请参考 <code>neighbor peer-group</code> , <code>neighbor remote-as</code> 命令来创建对等组。当这个参数被命令使用的时候, 这个命令会被应用到指定组的所有对等体上。
both	发送标准和扩展的 <code>community</code> 属性
extended	发送扩展 <code>community</code> 属性
standard	发送标准 <code>community</code> 属性

## 命令模式

路由模式和地址族模式

## 默认

物理是扩展还是标准的 `community` 属性都会发给邻居。

## 使用说明

默认情况下, 并不把 BGP 的 `community` 属性广播给对等体。但可以使用 `neighbor send-community` 命令来启动这项功能, 即发送 BGP 的 `community` 属性给它的对等体。路由策略可以基于邻居的地址, 对等组的名字或者是 AS 的路径信息。可能会出现这样一种情况, 在这种情况下, 需要把策略应用到某些特定的路由时, 而在这些路由中又不包含以前提到过的任何共有属性。`community` 属性的值可能是一个数字值, 也可能是可以附加到 BGP 路由时的一组值。可以把路由策略应用到包含特定 `community` 值或者属性的路由上。

## 举例说明

```
Switch# configure terminal
Switch(config)# bgp config-type standard
Switch(config)# router bgp 10
Switch(config-router)# neighbor 10.10.0.72 send-community extended
```

## 相关命令

N/A

### 8.7.60 neighbor shutdown

使用这个命令来关闭一个邻居。

使用相应的 `no` 命令来重新使能这个邻居。

## 命令语法

(no) neighbor NEIGHBORID shutdown

NEIGHBORID	A.B.C.D TAG
A.B.C.D	以 IP 地址格式来指定 BGP 邻居的地址。
TAG	已经存在的对等组名。请参考 <code>neighbor peer-group</code> , <code>neighbor remote-as</code> 命令来创建对等组。当这个参数被命令使用的时候, 这个命令会被应用到指定组的所有对等体上。

## 命令模式

路由模式

## 默认

N/A

## 使用说明

这个命令关闭任何指定邻居的活动会话, 并且清空相关的路由数据。

## 举例说明

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 10.10.0.72 shutdown
```

## 相关命令

N/A

### 8.7.61 neighbor soft-reconfiguration inbound

使用这个命令来配置启动存储更新。

使用相应的 `no` 命令来删除这个配置。

## 命令语法

(no) neighbor NEIGHBORID soft-reconfiguration inbound

NEIGHBORID	A.B.C.D TAG
A.B.C.D	以 IP 地址格式来指定 BGP 邻居的地址。
TAG	已经存在的对等组名。请参考 <code>neighbor peer-group</code> , <code>neighbor remote-as</code> 命令来创建对等组。当这个参数被命令使用的时候, 这个命令会被应用到指定组的所有对等体上。

## 命令模式

路由模式和地址族模式

## 默认

N/A

## 使用说明

如果在 BGP 邻居中已经配置了一个策略(如路由映射或者重分配列表)，并且需要改变这个策略的话，那么为了使新策略生效，就需要清除 BGP 会话。一旦清除了 BGP 会话，缓存就会无效。这会对路由有瞬间的影响。使用 `soft-reconfiguration inbound` 命令，就可以在不清除 BGP 会话的情况下改变策略。软件重新配置的情况是入站和出站。在使用入站时，从邻居来的软件重新配置的更新存储在内存中，而不管入站策略是什么。需要注意的是，使用入站软件配置比不使用入站软件配置需要更多的内存。出站软件重新配置不需要任何附加的内存，并且总是启动的。

## 举例说明

```
Switch# configure terminal
Switch(config)# router bgp 12
Switch(config-router)# neighbor 10.10.10.10 soft-reconfiguration inbound
```

## 相关命令

N/A

### 8.7.62 neighbor strict-capability-match

使用这个命令，如果 `capability` 值无法完全的匹配远端对等体的话，就关闭 BGP 连接。

使用相应的 `no` 命令来删除这个配置。

## 命令语法

(no) neighbor NEIGHBORID strict-capability-match

NEIGHBORID	A.B.C.D TAG
A.B.C.D	以 IP 地址格式来指定 BGP 邻居的地址。
TAG	已经存在的对等组名。请参考 <code>neighbor peer-group</code> ， <code>neighbor remote-as</code> 命令来创建对等组。当这个参数被命令使用的时候，这个命令会被应用到指定组的所有对等体上。

## 命令模式

路由模式

## 默认

N/A

## 使用说明

N/A

## 举例说明

```
Switch# configure terminal
Switch(config)# router bgp 12
Switch(config-router)# neighbor 10.10.10.10 strict-capability-match
```

## 相关命令

N/A

## 8.7.63 neighbor timers

使用这个命令来对一个指定的 BGP 邻居设定时钟。

使用相应的 no 命令来清除这个时钟。

## 命令语法

```
(no) neighbor NEIGHBORID timers KEEPALIVE
```

NEIGHBORID	A.B.C.D TAG
A.B.C.D	以 IP 地址格式来指定 BGP 邻居的地址。
TAG	已经存在的对等组名。请参考 neighbor peer-group, neighbor remote-as 命令来创建对等组。当这个参数被命令使用的时候, 这个命令会被应用到指定组的所有对等体上。
KEEPALIVE	<1-65535> 路由器发送给邻居 keepalive 信息的间隔时间, 默认 60s。
holdtime	<3-65535> 未接收到 keepalive 信息, 路由器宣告邻居死亡的等待时间, 默认 180s。

## 命令模式

路由模式

## 默认

N/A

## 使用说明

路由器发送 `keepalive` 信息用于通告另外一个路由器，两者之间的 BGP 连接仍然是活动的。`Keepalive` 间隔是每次发送 `keepalive` 信息的间隔时间。`Holdtime` 是路由器等待 `keepalive` 信息，宣告邻居死亡的超时时间。

## 举例说明

```
Switch# configure terminal
Switch(config)# router bgp 12
Switch(config-router)# neighbor 10.10.10.10 timers 60 120
```

## 相关命令

N/A

### 8.7.64 neighbor unsuppress-map

使用这个命令来选择性的对特定的邻居抑制更明确的路由。

## 命令语法

```
(no)neighbor NEIGHBORID unsuppress-map WORD
```

NEIGHBORID	A.B.C.D TAG
A.B.C.D	以 IP 地址格式来指定 BGP 邻居的地址。
TAG	已经存在的对等组名。请参考 <code>neighbor peer-group</code> ， <code>neighbor remote-as</code> 命令来创建对等组。当这个参数被命令使用的时候，这个命令会被应用到指定组的所有对等体上。

## 命令模式

路由模式和地址族 (`ipv4 unicast` | `ipv4 multicast`) 模式

## 默认

N/A

## 使用说明

当 `aggregate-address` 命令使用了 `summary-only` 选项时，会抑制聚合的更明确的路由。它会抑制更明确的路由到达所有的邻居。可以使用非抑制的映射，有选择的让特定的路由到达特定的邻居。

## 举例说明

```
Switch# configure terminal
```

```
Switch(config)# router bgp 10
Switch(config-router) neighbor 10.10.0.73 unsuppress-map mymap
Switch#configure terminal
Switch(config)#router bgp 10
Switch(config-router)address-family ipv4 unicast
Switch(config-router-af)neighbor 10.10.0.70 unsuppress-map mymap
```

## 相关命令

N/A

## 8.7.65 neighbor update-source

使用这个命令，来允许内部 BGP 会话使用任何对 TCP 连接可选的接口。

使用想要的 no 命令恢复默认，使用最接近的接口。

## 命令语法

(no) neighbor NEIGHBORID update-source IFNAME

NEIGHBORID	A.B.C.D TAG
A.B.C.D	以 IP 地址格式来指定 BGP 邻居的地址。
TAG	已经存在的对等组名。请参考 neighbor peer-group, neighbor remote-as 命令来创建对等组。当这个参数被命令使用的时候，这个命令会被应用到指定组的所有对等体上。

## 命令模式

路由模式

## 默认

N/A

## 使用说明

使用这个命令来与任在路由器上指定的接口结合使用。最常用的接口类型是 loopback 接口。使用 loopback 接口可以停止 BGP 对某个特定的 interface 进行 TCP 连接的依赖。

## 举例说明

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 10.10.0.72 update-source eth-0-1
```

## 相关命令

N/A

### 8.7.66 neighbor weight

使用这个命令，来设置路由到另据的默认 **weight**。

使用相应的 **no** 命令来删除这个配置。

## 命令语法

(no) neighbor NEIGHBORID weight WEIGHT

NEIGHBORID	A.B.C.D TAG
A.B.C.D	以 IP 地址格式来指定 BGP 邻居的地址。
TAG	已经存在的对等组名。请参考 <b>neighbor peer-group</b> ， <b>neighbor remote-as</b> 命令来创建对等组。当这个参数被命令使用的时候，这个命令会被应用到指定组的所有对等体上。

## 命令模式

路由模式

## 默认

N/A

## 使用说明

使用这个命令来指定所有从邻居学到的路由的 **weight** 值。具有最高 **weight** 值的路由，当网络上存在有其他路由的时候，有更高的优先级。

不像 **local-preference** 属性，**weight** 属性只跟本地路由器有关。

使用 **set weight** 命令将会覆盖使用本命令指定的 **weight** 值。

## 举例说明

```
Switch# configure terminal
Switch(config)# router bgp 12
Switch(config-router)# neighbor 10.10.10.10 weight 60
```

## 相关命令

N/A

## 8.7.67 neighbor fake-as

该命令用来配置指定对等体采用伪 AS 号与本端建立连接。

### 命令语法

**neighbor** { *group-name* | *ipv4-address* | *ipv6-address* } **fake-as** *as-number*

**no neighbor** { *group-name* | *ipv4-address* | *ipv6-address* } **fake-as**

group-name	对等体组的名称，为 1~47 个字符的字符串，区分大小写
ipv4-address	指定对等体的 IPv4 地址
ipv6-address	指定对等体的 IPv6 地址
as-number	本地自治系统号，取值范围为 1~4294967295

### 命令模式

路由模式

### 默认

无

### 使用说明

该命令常用于运营商修改网络部署的场景。例如，当运营商 A 收购了运营商 B 时，由于两者位于不同的 AS，因此需要把运营商 B 的 AS 合并到运营商 A 的 AS 中，即将原运营商 B 的 AS 号修改为运营商 A 的 AS 号。但是在网络合并过程中，原运营商 B 位于其他 AS 的 BGP 对等体可能不期望或者不便立即修改本地的 BGP 配置，此时就会造成与这些对等体的连接中断。

为了保证网络合并的顺利进行，可以在原运营商 B 的 ASBR 上执行 **neighbor fake-as** 命令，将原运营商 B 的 AS 号设置为合并后的运营商 A 的伪 AS 号，使原运营商 B 的 BGP 对等体能够继续使用伪 AS 号建立连接。

### 举例说明

配置指定对等体采用伪 AS 号与本端建立连接：

```
Switch(config)# router bgp 100
Switch(config-router)# neighbor 10.1.1.2 remote-as 200
Switch(config-router)# neighbor 10.1.1.2 fake-as 99
```

## 8.7.68 network

使用这个命令来指定被 BGP 路由进程宣告的网络。

使用相应的 no 命令来删除这个配置。



## 命令语法

(no) network A.B.C.D

(no) network A.B.C.D route-map WORD

A.B.C.D	IP 前缀, 例 35.0.0.0
WORD	Route-map 名

## 命令模式

路由模式 IPv4 单播地址族模式

## 默认

N/A

## 使用说明

N/A

## 举例说明

下面的例子举例说明说明了, 把一个 Class-A 的地址配置成一个网络路由。Class-A 的网络前缀掩码的长度 8 将会被在内部获得, 会是 2.0.0.0/8。

```
Switch(config)#router bgp 1
Switch(config-router)#network 2.0.0.0
Switch#show run
!
router bgp 1
no synchronization
network 2.0.0.0
!
```

下面的例子则列举了一个网络地址没有被捕获到, 所以被作为一个主机路由, 那是 1.2.3.0/32。

```
Switch(config)#router bgp 1
Switch(config-router)#network 1.2.3.0
Switch#show run
!
router bgp 1
no synchronization
network 1.2.3.0 mask 255.255.255.255
```

## 相关命令

N/A

## 8.7.69 network synchronization

使用这个命令，来保证被任何 `network` 命令指定的完全相同的静态网络前缀，是本地的或者在被 BGP RIB 介绍前是 IGP 可达的。

使用相应的 `no` 命令来删除这个配置。

### 命令语法

```
(no) network synchronization
```

### 命令模式

路由模式

地址族模式

IPv4 单播

IPv4 组播

### 默认

默认 `Network synchronization` 不使能

### 使用说明

N/A

### 举例说明

下面的例子在路由模式下使能了 BGP 静态网络路由的 IGP 同步。

```
Switch# configure terminal
Switch(config)# router bgp 11
Switch(config-router)# network synchronization
```

下面的例子在 IPv4 地址族模式下使能了 BGP 静态网络路由的 IGP 同步。

```
Switch# configure terminal
Switch(config)# router bgp 11
Switch(config)# address-family ipv4 unicast
Switch(config-af)# network synchronization
```

### 相关命令

N/A

## 8.7.70 synchronization

在配置模式或者地址族配置模式下，使用这个命令来使能 iBGP 学习路由的 IGP 同步。

使用相应的 `no` 命令来删除这个配置。

## 命令语法

(no) synchronization

## 命令模式

路由模式

地址族模式

ipv4 unicast

ipv4 multicast

## 默认

IGP 同步默认不使能。

## 使用说明

当 BGP 路由器无法宣告从 iBGP 邻居学到的路由时，需要使用 synchronization 功能，除非这些路由也会在 IGP(如 OSPF)中出现。在所有 AS 中的路由器都不进行 BGP 会话的时候，同步会被使能，并且 AS 就作为其他 AS 的传输者。no synchronization 命令在 BGP 路由器可以不等待 IGP 可达性出现的条件下宣告，从它的 iBGP 邻居学习到的路由时使用。

## 举例说明

下面示一个在路由模式下使能 IGP synchronization 的例子。

```
Switch# configure terminal
Switch(config)# router bgp 11
Switch(config-router)# synchronization
```

下面示一个在 IPV4 单播地址族模式下使能 IGP synchronization 的例子。

```
Switch# configure terminal
Switch(config)# router bgp 11
Switch(config)# address-family ipv4 unicast
Switch(config-af)# synchronization
```

## 相关命令

N/A

### 8.7.71 router bgp

使用这个命令，来配置一个 BGP 路由进程。

使用相应的 no 命令来删除这个配置。

## 命令语法

(no) router bgp ASN

ASN 指定 ASN <1-4294967295>.

ASN	指定 ASN <1-4294967295>.
-----	------------------------

## 命令模式

配置模式

## 默认

N/A

## 使用说明

router bgp 命令会启用一个 BGP 路由进程。

## 举例说明

```
Switch# configure terminal
Switch(config)# router bgp 12
Switch(config-router)#
```

## 相关命令

N/A

## 8.7.72 redistribute (BGP)

用此命令设置路由重发布。

使用关键字 no 删除重发布的路由。

## 命令语法

**redistribute** *PROTOCOL* {[**metric** *VALUE*] | **route-map** *WORD*}

no redistribute *PROTOCOL*

PROTOCOL	可引入的源路由协议，包括 OSPF, BGP, static, connected
<b>metric</b> <i>VALUE</i>	所发布的路由的度量值
route-map	路由映射
WORD	路由映射名字

## 命令模式

路由模式

## 默认

默认不使能重发布，度量值的默认值为 1。

## 使用说明

`redistribute` 命令中指定的 `metric` 值将会取代默认度量命令指定的度量值。

## 举例说明

设置重发布的静态路由的度量值为 10:

```
Switch(config)# router bgp 65001
Switch(config-router)# address family ipv4 vrf evpn-tenant-1
Switch(config-router)# redistribute connect
```

## 相关命令

`default-metric`

## 8.7.73 show debugging bgp

使用这个命令来表示设置的 BGP debugging 选项。

## 命令语法

```
show debugging bgp
```

## 命令模式

特权模式

## 默认

N/A

## 使用说明

N/A

## 举例说明

```
Switch# show debugging bgp
```

## 相关命令

N/A

## 8.7.74 show ip bgp

使用这个命令来显示 BGP 网络信息。

### 命令语法

```
show ip bgp(IPADDRESS)
```

```
show ip bgp ipv4 PREFIX (IPADDRESS)
```

IPADDRESS = A.B.C.D|A.B.C.D/M 指定 IP 地址及长度

ipv4 指定地址族。这决定了会被显示的路由表。

PREFIX = 单播|组播

unicast 指定 IPV4 单播地址族。这是默认选项。

multicast 指定 IPV4 组播地址族。

### 命令模式

特权模式

### 默认

N/A

### 使用说明

N/A

### 举例说明

```
Switch# show ip bgp 10.10.1.34/24
```

### 相关命令

N/A

## 8.7.75 show ip bgp attribute-info

使用这个命令来显示内部的 hash 信息。

### 命令语法

```
show ip bgp attribute-info
```

### 命令模式

特权模式

## 默认

N/A

## 使用说明

N/A

## 举例说明

这是一 `show ip bgp attribute-info` 命令显示的例子。  
 Switch# show ip bgp attribute-info

## 相关命令

N/A

## 8.7.76 show ip bgp cidr-only

使用这个命令来用非自然网络掩码来表示路由。

## 命令语法

```
show ip bgp cidr-only
show ip bgp ipv4 PREFIX cidr-only
```

ipv4	指定地址族。这决定了会被显示的路由表。
PREFIX	单播 组播
unicast	指定 IPV4 单播地址族。这是默认选项。
multicast	指定 IPV4 组播地址族。

## 命令模式

特权模式

## 默认

N/A

## 使用说明

N/A

## 举例说明

这是一个使用 `show ip bgp cidr-only` 来显示的命令。

```
Switch# show ip bgp cidr-only
```

## 相关命令

N/A

## 8.7.77 show ip bgp community

使用这个命令来显示匹配联合的路由。

## 命令语法

```
show ip bgp community TYPE (exact-match)
```

```
show ip bgp ipv4 PREFIX community TYPE (exact-match)
```

TYPE	AA:NN local-AS no-advertise no-export
AA:NN	对一个联合号码指定一个有效值。
local-AS	不向外发送本地 AS(公认联合)
no-advertise	不向任何对等体宣告(公认联合)
no-export	不像下一个 AS 输出(公认联合)
exact-match	指定显示精确匹配的联合

## 命令模式

特权模式

## 默认

N/A

## 使用说明

N/A

## 举例说明

```
Switch# show ip bgp community 10:23 exact-match
Switch# show ip bgp ipv4 multicast community 10:23 exact-match
```

## 相关命令

N/A



## 8.7.78 show ip bgp community-info

使用这个命令来列出所有的 BGP 联合体信息。

### 命令语法

```
show ip bgp community-info
```

### 命令模式

特权模式

### 默认

N/A

### 使用说明

N/A

### 举例说明

```
Switch# show ip bgp community-info
```

### 相关命令

N/A

## 8.7.79 show ip bgp community-list

使用这个命令来显示匹配 community-list 的路由。

### 命令语法

```
show ip bgp community-list LISTNAME (exact-match)
```

```
show ip bgp ipv4 PREFIX community-list LISTNAME (exact-match)
```

LISTNAME	指定 community list 名
exact-match	只表示那些有相同指定联合的路由。
ipv4	指定地址族。地址族的种类决定了显示的路由表
PREFIX	单播 组播
unicast	指定 IPV4 单播地址族。这是默认选项。
multicast	指定 IPV4 组播地址族。

## 命令模式

特权模式

## 默认

N/A

## 使用说明

N/A

## 举例说明

```
Switch# show ip bgp community-list mylist exact-match
Switch# show ip bgp ipv4 unicast community-list mylist
```

## 相关命令

N/A

## 8.7.80 show ip bgp dampening

使用这个命令来显示惩罚的详细信息。

## 命令语法

```
show ip bgp dampening dampened-paths|flap-statistics|parameters
show ip bgp ipv4 PREFIX dampening dampened-paths|flap-statistics|parameters
```

dampened-paths	显示惩罚路径
flap-statistics	显示路由 flap 统计
parameters	显示配置的惩罚参数的详细信息
ipv4	指定地址族。这决定了会被显示的路由表。
PREFIX	单播 组播
unicast	指定 IPV4 单播地址族。这是默认选项。
multicast	指定 IPV4 组播地址族。

## 命令模式

EXEC 模式 and 特权模式

## 默认

N/A

## 使用说明

N/A

## 举例说明

使能 `bgp dampening` 来在内存中保存 `dampened-path` 信息。

下面是一个显示所有惩罚参数的一个例子：

```
Switch# show ip bgp dampening parameters
```

下面的输出显示了内部路由 (i)，发生了 3 次震荡，被计入了历史 (h)。

```
Switch# show ip bgp dampening flap-statistics
```

下面的例子显示了一个被惩罚的路由

```
Switch# show ip bgp dampening dampened-paths
```

## 相关命令

N/A

### 8.7.81 show ip bgp filter-list

使用这个命令来显示符合 `filter-list` 的路由。

## 命令语法

```
show ip bgp filter-list LISTNAME
```

```
show ip bgp ipv4 PREFIX filter-list LISTNAME
```

LISTNAME	指定 ACL 名的常规表述
ipv4	指定地址族。地址族的种类决定了显示的路由表
PREFIX	单播/组播
unicast	指定 IPV4 单播地址族。这是默认选项。
multicast	指定 IPV4 组播地址族。

## 命令模式

特权模式

## 默认

N/A

## 使用说明

N/A

## 举例说明

```
Switch# show ip bgp filter-list mylist
Switch# show ip bgp ipv4 unicast filter-list Switch
```

## 相关命令

N/A

## 8.7.82 show ip bgp inconsistent-as

使用这个命令来显示与 AS-path 不匹配的路由。

## 命令语法

```
show ip bgp inconsistent-as
show ip bgp ipv4 PREFIX inconsistent-as
```

ipv4	指定地址族。地址族的种类决定了显示的路由表
PREFIX	单播 组播
unicast	指定 IPV4 单播地址族。这是默认选项。
multicast	指定 IPV4 组播地址族。

## 命令模式

特权模式

## 默认

N/A

## 使用说明

N/A

## 举例说明

```
Switch# show ip bgp inconsistent-as
Switch# show ip bgp ipv4 unicast inconsistent-as
```

## 相关命令

N/A

## 8.7.83 show ip bgp neighbors

使用这个命令来表示 TCP 和 BGP 邻居连接的详细信息。

### 命令语法

show ip bgp neighbors (IPADDRESS (advertised-routes|RECEIVED|receivedroutes|routes))

show ip bgp ipv4 PREFIX neighbors (IPADDRESS (advertised-routes|RECEIVED|receivedroutes|routes))

IPADDRESS	A.B.C.D 指定 IP 地址
A.B.C.D	指定 IPV4 的 IP 地址
advertised-routes	表示宣告给 BGP 邻居的路由
RECEIVED	接受到的 prefix-filter，显示所有接收到的路由(无论是接收的还是拒绝的)
prefix-filter	表示 prefix-list 的 filter
received-routes	表示从邻居接收到的路由。表示所有从邻居接收到的路由，先配置 BGP 软重置。这样就能显示所有从邻居学习到的接收路由。
PREFIX	单播 组播
unicast	指定 IPV4 单播地址族。这是默认选项。
multicast	指定 IPV4 组播地址族。

### 命令模式

特权模式

### 默认

N/A

### 使用说明

N/A

### 举例说明

这是一个使用 show ip bgp 命令来显示指定邻居的命令。

```
Switch# show ip bgp neighbors
```

## 相关命令

N/A

### 8.7.84 show ip bgp paths

使用这个命令来显示 BGP 路径信息。

## 命令语法

```
show ip bgp paths
```

```
show ip bgp ipv4 PREFIX paths
```

ipv4	指定地址族。这决定了会被显示的路由表。
PREFIX	单播 组播
unicast	指定 IPV4 单播地址族。这是默认选项。
multicast	指定 IPV4 组播地址族。

## 命令模式

特权模式

## 默认

N/A

## 使用说明

N/A

## 举例说明

```
Switch# show ip bgp paths
```

## 相关命令

N/A

### 8.7.85 show ip bgp prefix-list

使用这个命令来显示匹配 prefix-list 的路由。

## 命令语法

```
show ip bgp prefix-list LIST
```

show ip bgp ipv4 PREFIX prefix-list LIST

LIST	指定 IP prefix list 的名字
ipv4	指定地址族。这决定了会被显示的路由表。
PREFIX	单播 组播
unicast	指定 IPV4 单播地址族。这是默认选项。
multicast	指定 IPV4 组播地址族。

## 命令模式

特权模式

## 默认

N/A

## 使用说明

N/A

## 举例说明

```
Switch# show ip bgp prefix-list mylist
```

## 相关命令

N/A

## 8.7.86 show ip bgp quote-regexp

使用这个命令来显示匹配 AS path 常规表述的路由。

## 命令语法

show ip bgp quote-regexp WORD

show ip bgp ipv4 PREFIX regexp WORD

WORD	指定匹配 BGP AS-path 的常规表述
ipv4	指定地址族。这决定了会被显示的路由表。
PREFIX	单播 组播
unicast	指定 IPV4 单播地址族。这是默认选项。

multicast	指定 IPV4 组播地址族。
-----------	----------------

## 命令模式

特权模式

## 默认

N/A

## 使用说明

N/A

## 举例说明

```
Switch# show ip bgp quote-regexp "Switch"
```

## 相关命令

N/A

## 8.7.87 show ip bgp regexp

使用这个命令来显示匹配 AS-path 常规表述的路由。

## 命令语法

```
show ip bgp regexp .LINE
```

```
show ip bgp ipv4 PREFIX regexp .LINE
```

regexp	显示匹配 AS-path 常规表述的路由
LINE	指定一个常规表述来匹配 BGP AS-path
ipv4	指定地址族。这决定了会被显示的路由表。
PREFIX	单播 组播
unicast	指定 IPV4 单播地址族。这是默认选项。
multicast	指定 IPV4 组播地址族。

## 命令模式

特权模式



## 默认

N/A

## 使用说明

N/A

## 举例说明

```
Switch# show ip bgp regexp myexpression
```

## 相关命令

N/A

## 8.7.88 show ip bgp scan

使用这个命令来显示 BGP scan 状态

## 命令语法

```
show ip bgp scan
```

## 命令模式

特权模式

## 默认

N/A

## 使用说明

N/A

## 举例说明

```
Switch# show ip bgp scan
```

## 相关命令

N/A

## 8.7.89 show ip bgp summary

使用这个命令来显示 BGP 邻居状态的汇总信息。

## 命令语法

```
show ip bgp summary
```

show ip bgp ipv4 PREFIX summary

ipv4	指定地址族。这决定了会被显示的路由表。
PREFIX	单播 组播
unicast	指定 IPV4 单播地址族。这是默认选项。
multicast	指定 IPV4 组播地址族。

## 命令模式

特权模式

## 默认

N/A

## 使用说明

N/A

## 举例说明

这是一个使用 show ip bgp 命令显示的一个例子  
Switch# show ip bgp summary

## 相关命令

N/A

## 8.7.90 show ip bgp vpnv4 all

使用这个命令来显示 VPNv4 NLRI 的指定信息。

## 命令语法

show ip bgp vpnv4 all TYPE

all	显示所有跟 VPNv4 NLRI 有关的信息
TYPE	A.B.C.D neighbors summary
neighbors	显示所有 VPNv4 NLRI 的邻居信息
summary	显示 BGP 邻居状态的汇总信息
A.B.C.D	会在 BGP 路由表中显示的信息

## 命令模式

特权模式

## 默认

N/A

## 使用说明

N/A

## 举例说明

这是一个使用 `show ip bgp vpnv4 all` 来显示的一个例子。

```
Switch# show ip bgp vpnv4 all
```

## 相关命令

N/A

### 8.7.91 show ip bgp vpnv4 rd

使用这个命令来显示 VPNv4 NLRI 的指定信息。

## 命令语法

```
show ip bgp vpnv4 rd WORD TYPE
```

rd 显示路由的标识信息

WORD VPN 路由标识

TYPE = A.B.C.D |neighbors|summary

neighbors 显示 VPNv4 NLRIs 的信息

summary 显示 BGP 邻居状态的汇总信息

A.B.C.D 会在 BGP 路由表中显示的信息

rd	显示路由的标识信息
WORD	VPN 路由标识
TYPE	A.B.C.D  neighbors summary
neighbors	显示 VPNv4 NLRIs 的信息
summary	显示 BGP 邻居状态的汇总信息
A.B.C.D	会在 BGP 路由表中显示的信息

## 命令模式

特权模式

## 默认

N/A

## 使用说明

N/A

## 举例说明

这是一个使用 `show ip bgp vpnv4 rd` 来显示 VPNv4 指定信息的例子  
Switch# show ip bgp vpnv4 rd 123

## 相关命令

N/A

### 8.7.92 show ip bgp vpnv4 vrf

使用这个命令来显示 VPNv4 NLRI 指定信息

## 命令语法

show ip bgp vpnv4 vrf WORD TYPE

vrf	VPN 路由/转发 实例
WORD	VPN 路由/转发实例名
TYPE	A.B.C.D  neighbors summary
neighbors	显示 VPNv4 NLRI 的信息
summary	显示 BGP 邻居状态的汇总信息
A.B.C.D	会在 BGP 路由表中显示的信息

## 命令模式

特权模式

## 默认

N/A

## 使用说明

N/A

## 举例说明

这是一个使用 `show ip bgp vpnv4 rd` 命令来显示 VPNv4 指定信息的例子

```
Switch# show ip bgp vpnv4 vrf 123
```

## 相关命令

N/A

## 8.7.93 timers

使用这个命令并且设定 BGP `keepalive` 定时器和 `holdtime` 定时器的值。

使用相应的 `no` 命令来删除这个配置并返回默认值。

## 命令语法

```
timers bgp KEEPALIVE HOLDTIME
```

```
no timers bgp
```

KEEPALIVE	<0-65535> keepalive 信息被送往邻居的频率。默认 60s
HOLDTIME	<3-65535> 如果没有接收到 keepalive 信息的话，认为邻居死亡的间隔时间。默认 180s

## 命令模式

路由模式

## 默认

N/A

## 使用说明

这个命令在全局使用，用于设定/解除设定所有邻居的 `keepalive` 和 `holdtime` 值。

## 举例说明

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# timers bgp 40 120
```

## 相关命令

N/A

# 9 流量管理命令行参考

## 9.1 QOS 命令

### 9.1.1 bandwidth

用于指定队列占用端口带宽的百分比。

#### 命令语法

```
bandwidth percentage PERCENTAGE
```

```
no bandwidth percentage
```

<i>PERCENTAGE</i>
-------------------

设定链路带宽百分比。范围是 1-100。
----------------------

#### 命令模式

Policy map type 流分类配置模式

#### 默认

无

#### 使用说明

所有队列带宽的百分比之和为 100。

#### 举例说明

```
Switch# configure terminal
Switch(config)# policy-map type traffic-class pmap_tc
Switch(config-pmap-tc)# class type traffic-class cmap_tc
Switch(config-pmap-tc-c)# bandwidth percentage 20
```

#### 相关命令

priority level

## 9.1.2 class type qos

创建流分类的 `class-map` 并进入其配置模式。

### 命令语法

```
class type qos NAME
```

```
no class type qos NAME
```

<i>NAME</i>	流分类目录名。最大支持 40 个字节，只能是字母、数字、连字符、下划线组成。
-------------	--

### 命令模式

config-pmap 配置模式

### 默认

无

### 使用说明

流量监管用于流类型的匹配。通常，系统的每个 `policy map` 中都有默认的流类型。该映射不能人为更改，如果要更改，交换机将返回错误信息。

### 举例说明

```
Switch# configure terminal
Switch(config)# policy-map type qos pmap_qos
Switch(config-pmap)# class type qos cmap1
```

### 相关命令

`policy-map`

`class-map`

## 9.1.3 class type qos class-default

对于匹配不上的流类型，增加默认流类型。

### 命令语法

```
class type qos class-default
```

### 命令模式

config-pmap 配置模式



## 默认

无

## 使用说明

若某流无法匹配任何类型，那么就设定其为默认流类型。该默认类型不能人为删除。

## 举例说明

```
Switch# configure terminal
Switch(config)# policy-map type qos pmap_qos
Switch(config-pmap-qos)# class type qos class-default
```

## 相关命令

policy-map

### 9.1.4 class type traffic-class

在 policy map 中，引用已经存在的 class-map，并进入该目录的配置模式。

## 命令语法

class type traffic-class *NAME*

<i>NAME</i>	Class map 类型的目录名。最大支持 40 个字节，只能是字母、数字、连字符、下划线组成。
-------------	--

## 命令模式

config-pmap 配置模式

## 默认

无

## 使用说明

使用该命令可以依据流类型将流以不同属性加以划分，如优先级、带宽等。

## 举例说明

```
Switch# configure terminal
Switch(config)# policy-map type traffic-class pmap_tc
Switch(config-pmap-tc)# class type traffic-class cmap_tc
```

## 相关命令

policy-map traffic-class

set traffic-class

## 9.1.5 class-map type qos

创建或配置一个 class map，并进入该目录的配置模式。

### 命令语法

class-map type qos *NAME*

<i>NAME</i>	Class map 名。最大支持 40 个字节，只能是字母、数字、连字符、下划线组成。
-------------	---

### 命令模式

全局配置模式

### 默认

无

### 使用说明

用户可以为每一个流类型定义一个 class map 并用于 QoS policy。如果数据包匹配上 class map 中的任意一个条件，那么该数据包适用于该 class map。如果一条都没匹配上，那么该数据包将适用于一个默认值。

### 举例说明

```
Switch# configure terminal
Switch(config)# policy-map type qos pmap_qos
Switch(config-pmap-qos)# class type qos cmap_qos
```

### 相关命令

policy-map

class

## 9.1.6 class-map type traffic-class

创建或配置一个 class map，并进入该目录的配置模式。

### 命令语法

class-map type traffic-class *NAME*

<i>NAME</i>	Class map 名。最大支持 40 个字节，只能是字母、数字、连字符、下划线组成。
-------------	---

## 命令模式

全局配置模式

## 默认

无

## 使用说明

该类型的 `class-map` 使用不同流类型区别流。

## 举例说明

```
Switch# configure terminal
Switch(config)# class-map type traffic-class cmap_tc
```

## 相关命令

`policy-map`  
`class traffic-class`  
`set traffic-class`

## 9.1.7 clear qos aggregate-policer statistics

清空聚合流量监管的统计。

## 命令语法

```
clear qos aggregate-policer NAME statistics
```

<i>NAME</i>	聚合策略名
-------------	-------

## 命令模式

特权配置模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch# clear qos aggregate-policer example statistics
```

## 相关命令

```
show qos aggregate-policer
```

## 9.1.8 clear qos interface statistics policer flow

清空接口的流量监控的统计。

## 命令语法

```
clear qos interface NAME statistics policer flow
```

<i>NAME</i>	接口名
-------------	-----

## 命令模式

特权配置模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch# clear qos interface eth-0-1 statistics policer flow
```

## 相关命令

## 9.1.9 clear qos interface statistics policer port

清空端口的流量监管的统计。

## 命令语法

```
clear qos interface NAME statistics policer port {input|output}
```

<i>NAME</i>	接口名
-------------	-----

## 命令模式

特权配置模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch# clear qos interface eth-0-1 statistics policer port input
```

## 相关命令

show qos interface

### 9.1.10 clear qos interface statistics queue

清空接口上的队列的统计。

## 命令语法

```
clear qos interface NAME statistics queue
```

<i>NAME</i>	接口名
-------------	-----

## 命令模式

特权配置模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch# clear qos interface eth-0-1 statistics queue
```

## 相关命令

show qos interface queue statistics

## 9.1.11 match cos

在 class map 中使用 CoS (class of service) 值定义流类型。

### 命令语法

```
match cos COS
```

<i>COS</i>	CoS 值
------------	-------

### 命令模式

Class-map 配置模式

### 默认

无

### 使用说明

无

### 举例说明

```
Switch# configure terminal
Switch(config)# class-map type qos cmap_qos
Switch(config-cmap-qos)# match cos 5
```

### 相关命令

class-map

## 9.1.12 match dscp

使用 DSCP 值作为匹配的关键字。

### 命令语法

```
match dscp DSCP_STR
```

### 命令模式

Class-map 配置模式

### 默认

无

## 使用说明

作为匹配条件的 PHB 字符串：

PHB	DSCP
af11	10
af12	12
af13	14
af21	18
af22	20
af23	22
af31	26
af32	28
af33	30
af41	34
af42	36
af43	38
cs1	8
cs2	16
cs3	24
cs4	32
cs5	40
cs6	48
cs7	56
default	0

ef	46
dscp31	31

## 举例说明

```
Switch# configure terminal
Switch(config)# class-map type qos cmap_qos
Switch(config-cmap-qos)# match dscp af11
```

## 相关命令

class-map

### 9.1.13 match precedence

使用 IP 报文头的 ToS 字段中的优先级值作为 class map 中的匹配条件。

## 命令语法

match precedence *PREC\_STR*

<i>PREC_STR</i>	Precedence PHB string
-----------------	-----------------------

## 命令模式

Class-map 配置模式

## 默认

无

## 使用说明

作为匹配条件的 PHB 字符串：

PHB	Precedence
critical	Critical precedence (5)
flash	Flash precedence (3)
flash-override	Flash override precedence (4)



immediate	Immediate precedence (2)
internet	Internetwork control precedence (6)
network	Network control precedence (7)
priority	Priority precedence (1)
routine	Routine precedence (0)

## 举例说明

```
Switch# configure terminal
Switch(config)# class-map type qos cmap_qos
Switch(config-cmap-qos)# match precedence critical
```

## 相关命令

class-map

### 9.1.14 match access-group

通过引用 class map 中的 access-list 配置匹配条件。

## 命令语法

match access-group *NAME*

<i>NAME</i>	access-list 名
-------------	---------------

## 命令模式

Class-map 配置模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch# configure terminal
Switch(config)# class-map type qos cmap_qos
Switch(config-cmap-qos)# match access-group example
```

## 相关命令

class-map

### 9.1.15 acl-statistics exclude-drop enable

使能 policy-map 里面，acl 统计信息不包括丢弃报文的统计数据。

## 命令语法

```
acl-statistics exclude-drop enable
no acl-statistics exclude-drop enable
```

## 命令模式

Policy-map Class-map 配置模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch# configure terminal
Switch(config)acl-statistics exclude-drop enable
Switch(config)policy-map pmap
Switch(config-pmap)#class cmap
Switch(config-pmap-c)#statistics enable
```

## 相关命令

show policy-map statistics

### 9.1.16 match traffic-class

使用特定的 QoS 流类型值作为匹配条件。

## 命令语法

```
match traffic-class CLASS-ID
```

<i>CLASS-ID</i>	指定的流类型值。范围是 1—6
-----------------	-----------------

## 命令模式

Class-map 配置模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch# configure terminal
Switch(config)# class-map type traffic-class cmap_tc
Switch(config-cmap-tc)# match traffic-class 6
```

## 相关命令

class-map

## 9.1.17 policy-map type qos

创建一个 policy map。

## 命令语法

policy-map type qos *NAME*

no policy-map *NAME*

<i>NAME</i>	自定义的 policy-map 名
-------------	-------------------

## 命令模式

全局配置模式

## 默认

无

## 使用说明

policy map 应用于入方向的物理端口。

## 举例说明

```
Switch# configure terminal
Switch(config)# policy-map type qos pmap_qos
```

## 相关命令

service-policy

### 9.1.18 policy-map type traffic-class

创建一个队列设置的 policy map。

## 命令语法

```
policy-map type traffic-class NAME
```

<i>NAME</i>	自定义 policy-map 名
-------------	------------------

## 命令模式

全局配置模式

## 默认

无

## 使用说明

创建的 policy map 使用多个不同的流分类区别流。

## 举例说明

```
Switch# configure terminal
Switch(config)# policy-map type traffic-class pmap_tc
```

## 相关命令

service-policy traffic-class

### 9.1.19 pause buffer-size

设置基于优先级的流量控制(PFC)缓冲区临界值。

## 命令语法

```
pause buffer-size BUFFER-SIZE pause-threshold XOFF-SIZE resume-threshold XON-SIZE
pfc-cos COS
no pause
```

<i>BUFFER-SIZE</i>	入列通信流缓冲区大小
<i>XOFF-SIZE</i>	定义流分类暂停的缓冲区大小
<i>XON-SIZE</i>	定义流分类重传的缓冲区大小
<i>COS</i>	自定义暂停的优先级

## 命令模式

Policy map type 流分类配置模式

## 默认

无

## 使用说明

配置缓冲区大小、XON 和 XOFF 阈值。

## 举例说明

```
Switch# configure terminal
Switch(config)# policy-map type traffic-class pmap_tc
Switch(config-pmap-tc)# class type traffic-class cmap_tc
Switch(config-pmap-tc-c)# pause buffer-size 200 pause-threshold 150 resume-
threshold 100 pfc-cos 5
```

## 相关命令

### 9.1.20 priority level

设置队列调度的严格优先级。

## 命令语法

priority level *LEVEL*

no priority level

<i>LEVEL</i>	自定义严格的优先级。范围是 1 和 6。
--------------	----------------------

## 命令模式

Policy map type 流分类配置模式

## 默认

无

## 使用说明

无。

## 举例说明

```
Switch# configure terminal
Switch(config)# policy-map type traffic-class pmap_tc
Switch(config-pmap-tc)# class type traffic-class cmap_tc
Switch(config-pmap-tc-c)# priority level 5
```

## 相关命令

show qos interface

## 9.1.21 flow-policer number

设置可配 policer 资源数。

## 命令语法

flow-policer number (normal|extend)

<i>normal</i>	Normal 模式，可配的 policer 数为 576。
<i>extend</i>	extend 模式，可配的 policer 数为 3064。

## 命令模式

配置模式

## 默认

默认值为 normal 模式

## 使用说明

Normal 和 extend 模式之间相互切换，需要保存配置，再重启交换机才能生效。

## 举例说明

配置 flow 模式为 extend

```
Switch# configure terminal
Switch(config)# flow-policer number extend
```

```
% Configuration about flow-policer number has been stored, but cannot take effect
until the next reload.
% When setting the extend number of policers, It only supports the 10G rate of
policers, please check the rate of policers.
```

## 相关命令

```
show resource qos
```

### 9.1.22 qos aggregate-policer

创建一个聚合策略的实例，流类型可以共享聚合策略实例。

## 命令语法

```
qos aggregate-policer NAME {color-blind|color-aware} cir CIR [cbs CBS] [ebs EBS] {exceed
| violate} drop [statistics]
```

```
qos aggregate-policer NAME {color-blind|color-aware} cir CIR {cbs CBS|eir EIR} [ebs EBS]
{exceed | violate} drop [statistics]
```

```
no qos aggregate-policer NAME
```

<i>NAME</i>	实例名
<i>cir</i> <i>CIR-RATE</i>	CIR - Commit Information Rate, 范围是 0—100,000,000 kbps
<i>cbs</i> <i>CBS-SIZE</i>	CBS - Commit Burst Size, 范围是 0—640,000 bytes
<i>eir</i> <i>EIR-RATE</i>	EIR-Excess Information Rate, 范围是 0 —100,000,000 kbps
<i>ebs</i> <i>EBS-SIZE</i>	EBS - Excess Burst Size with the range of 0 to 640,000 bytes
<i>statistics</i>	使能聚合策略实例统计

## 命令模式

全局配置模式

## 默认

无

## 使用说明

无。

## 举例说明

```
Switch# configure terminals
Switch(config)# qos aggregate-policer example color-aware cir 1000 cbs 2000 eir
3000 ebs 4000 exceed drop statistics
```

## 相关命令

```
show qos aggregate-policer
```

### 9.1.23 aggregate-policer (policy-map)

对多条流应用流量监管策略，配置了其共享速率限制。

## 命令语法

```
aggregate-policer NAME
```

```
no aggregate-policer
```

<i>NAME</i>	聚合策略实例名
-------------	---------

## 命令模式

Policy map type 流分类配置模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch# configure terminal
Switch(config)# policy-map type qos pmap_qos
Switch(config-pmap-qos)# class type qos cmap_qos
Switch(config-pmap-qos-c)# aggregate-policer transmit1
```

## 相关命令

```
show qos aggregate policer
```

### 9.1.24 policer(policy-map)

对单条流应用流量监管策略，配置了其速率限制。



## 命令语法

```
policer {color-blind|color-aware} cir CIR [cbs CBS] [ebs EBS] {exceed | violate} drop
[statistics]
```

```
no policer
```

cir CIR-RATE	CIR - Commit Information Rate, 范围 0—100,000,000 kbps
cbs CBS-SIZE	CBS - Commit Burst Size, 范围 0—640,000 bytes
eir EIR-RATE	EIR-Excess Information Rate, 范围 0—100,000,000 kbps
ebs EBS-SIZE	EBS - Excess Burst Size, 范围 0—640,000 bytes
statistics	使能流量监管的统计

## 命令模式

Policy map type 流分类配置模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch# configure terminal
Switch(config)# policy-map type qos pmap_qos
Switch(config-pmap-qos)# class type qos cmap_qos
Switch(config-pmap-qos-c)# policer color-blind cir 50000 cbs 40000 ebs 30000 exceed
drop statistics
```

## 相关命令

```
show qos policy-map
```

### 9.1.25 qos policer(port)

使用该命令配置端口的流量监管策略。

## 命令语法

```
qos policer {input | output} {color-blind|color-aware} cir CIR [cbs CBS] [ebs EBS] {exceed | violate} drop [statistics]
```

```
qos policer {input | output} {color-blind|color-aware} cir CIR {cbs CBS|eir EIR} [ebs EBS] {exceed | violate} drop [statistics]
```

```
no qos policer {input | output}
```

<i>cir</i> <i>CIR-RATE</i>	CIR - Commit Information Rate, 范围 0—100,000,000 kbps
<i>cbs</i> <i>CBS-SIZE</i>	CBS - Commit Burst Size, 范围 0—640,000 bytes
<i>eir</i> <i>EIR-RATE</i>	EIR-Excess Information Rate, 范围 0—100,000,000 kbps
<i>ebs</i> <i>EBS-SIZE</i>	EBS - Excess Burst Size, 范围 0—640,000 bytes
<i>statistics</i>	使能流量监管的统计

## 命令模式

接口配置模式

## 默认

无

## 使用说明

在端口级别配置流量监控策略。

## 举例说明

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# qos policer input color-blind cir 50000 cbs 40000 ebs 30000
exceed drop statistics
```

## 相关命令

show qos domain map-table

### 9.1.26 qos shape rate(port)

物理端口上的流配置整形。

## 命令语法

qos shape rate *RATE* (ecn-percentage *PERCENTAGE*)

no qos shape rate

<i>RATE</i>	整形率范围：0—100,000,0000.
<i>PERCENTAGE</i>	ECN 设定的整形值

## 命令模式

接口配置模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# qos shape rate 1000
```

## 相关命令

show qos interface

### 9.1.27 shape rate(queue)

对物理端口上的 queue 配置整形。

## 命令语法

shape rate *RATE*

no shape rate

<i>RATE</i>	验证信息速率的值，范围是 0—100,000,000.
-------------	-----------------------------

## 命令模式

Policy map type 流分类配置模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch# configure terminal
Switch(config)# policy-map type traffic-class pmap_tc
Switch(config-pmap-tc)# class type traffic-class cmap_tc
Switch(config-pmap-tc-c)# shape rate 100000
```

## 相关命令

show qos interface queue

### 9.1.28 queue-limit

配置队列缓冲区大小。

## 命令语法

queue-limit *SIZE*

no queue-limit

<i>SIZE</i>	队列缓冲区单元个数，每个单元大小是 288Bytes
-------------	----------------------------

## 命令模式

Policy map type 流分类配置模式

## 默认

无

## 使用说明

对于控制流有 64 个单元；

non-drop 流有 256 个单元。

## 举例说明

```
Switch# configure terminal
Switch(config)# policy-map type traffic-class pmap_tc
Switch(config-pmap-tc)# class type traffic-class cmap_tc
Switch(config-pmap-tc-c)# queue-limit 200
```

## 相关命令

show qos interface

## 9.1.29 queue-limit dynamic

区分队列的动态缓冲区。

### 命令语法

queue-limit dynamic *LEVEL*

<i>LEVEL</i>	队列最大可用缓冲区，范围是 0—3： 3: 共享池的 15% 2: 共享池的 30% 1: 共享池的 50% 0: 共享池的 70%
--------------	--

### 命令模式

Policy map type 流分类配置模式

### 默认

队列使用共享池的 70%

### 使用说明

动态和静态的队列共享 4profile，如果 4profile 耗尽，有限队列的配置将返回错误信息。

### 举例说明

```
Switch# configure terminal
Switch(config)# policy-map type traffic-class pmap_tc
Switch(config-pmap-tc)# class type traffic-class cmap_tc
Switch(config-pmap-tc-c)# queue-limit dynamic 2
```

### 相关命令

show qos interface queue

## 9.1.30 random-detect

配置随机侦测变量。

### 命令语法

random-detect maximum-threshold *MAX* [minimum-threshold *MIN*] [ecn]

no random-detect

<i>MIN</i>	最小值（缓冲区单元）
------------	------------

<i>MAX</i>	最大值（缓冲区单元）
<i>ecn</i>	使能 ECN 模式

## 命令模式

Policy map type 流分类配置模式

## 默认

队列使用共享池的 70% Buffer 资源。

## 使用说明

动态和静态的队列共享 4profile，如果 4profile 耗尽，有限队列的配置将返回错误信息。

如果 *ecn* 是使能的，数据包将被标记而不是丢弃。

## 举例说明

```
Switch# configure terminal
Switch(config)# policy-map type traffic-class pmap_tc
Switch(config-pmap-tc)# class type traffic-class cmap_tc
Switch(config-pmap-tc-c)# random-detect maximum-threshold 200 ecn
```

## 相关命令

show qos interface

### 9.1.31 set cos

标记数据包 CoS 值。

## 命令语法

set cos *COS*

no set *COS*

## 命令模式

Policy map type 流分类配置模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch# configure terminal
Switch(config)# policy-map type qos pmap_qos
Switch(config-pmap-qos)# class type qos cmap_qos
Switch(config-pmap-qos-c)# set cos 3
```

## 相关命令

```
show policy-map
```

### 9.1.32 set dscp

配置 DSCP 值。

## 命令语法

```
set dscp DSCP_STR
no set dscp
```

## 命令模式

Policy map type 流分类配置模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch# configure terminal
Switch(config)# policy-map type qos pmap_qos
Switch(config-pmap-qos)# class type qos cmap_qos
Switch(config-pmap-qos-c)# set dscp cs3
```

## 相关命令

```
show policy-map
```

### 9.1.33 set precedence

配置优先级值。

## 命令语法

```
set precedence PREC_STR
no set precedence
```

## 命令模式

Policy map type 流分类配置模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch# configure terminal
Switch(config)# policy-map type qos pmap_qos
Switch(config-pmap-qos)# class type qos cmap_qos
Switch(config-pmap-qos-c)# set precedence network
```

## 相关命令

无

### 9.1.34 set traffic-class

配置流的服务队列。

## 命令语法

```
set traffic-class CLASS-ID
no set traffic-class
```

<i>CLASS-ID</i>	通信流 ID，范围 1—6
-----------------	---------------

## 命令模式

Policy map type 流分类配置模式

## 默认

无

## 使用说明

在收发报文的过程中不同的流将予以不同的处理。

## 举例说明

```
Switch# configure terminal
Switch(config)# policy-map type qos pmap_qos
Switch(config-pmap-qos)# class type qos cmap_qos
```



```
Switch(config-pmap-qos-c)# set traffic-class 3
```

## 相关命令

```
show policy-map
```

### 9.1.35 service-policy type qos

将 `policy-map` 应用到一个接口以影响其流分类规则。

## 命令语法

```
service-policy type qos input NAME
```

```
no service-policy input
```

<i>NAME</i>	Policy-map name
-------------	-----------------

## 命令模式

接口配置模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# service-policy type qos input pmap_qos
```

## 相关命令

```
clear qos statistics
```

### 9.1.36 service-policy type traffic-class

将 `policy-map` 应用到一个端口以影响其流队列规则。

## 命令语法

```
service-policy type traffic-class NAME
```

```
no service-policy type traffic-class
```

<i>NAME</i>	policy-map 名
-------------	--------------

## 命令模式

接口配置模式  
QoS 全局配置模式

## 默认

无

## 使用说明

用于将队列和优先流控制参数应用于接口上。

## 举例说明

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# service-policy type traffic-class pmap_tc
```

## 相关命令

show qos interface

## 9.1.37 show qos aggregate-policer statistics

show 聚合策略信息。

## 命令语法

show qos aggregator-policer *NAME* [statistics]

<i>NAME</i>	聚合策略名
<i>statistics</i>	聚合策略的统计信息

## 命令模式

特权配置模式

## 默认

无

## 使用说明

用于显示聚合策略信息。

## 举例说明

```
Switch# show qos aggregate-policer example
Aggregate policer: test
```

```
color blind
CIR 1000 kbps, CBS 640000 bytes, EBS 640000 bytes
drop violate packets
```

### 相关命令

aggregate-policer

## 9.1.38 show qos interface

显示接口上的每一个流分类的配置信息。

### 命令语法

show qos interface *NAME* egress

NAME	接口名
------	-----

### 命令模式

特权配置模式

### 默认

无

### 使用说明

无

### 举例说明

```
Switch# show qos interface eth-0-1egress
TC Priority Bandwidth Shaping(kbps) Drop-Mode Max-Queue-Limit(Cell) ECN
0 0 - - dynamic level 0 -
1 1 - - dynamic level 0 -
2 2 - - dynamic level 0 -
3 3 - - dynamic level 0 -
4 4 - - dynamic level 0 -
5 5 - - dynamic level 0 -
6 6 - - dynamic level 0 -
7 7 - - tail-drop 64 -
```

### 相关命令

show qos interface queue statistics

## 9.1.39 show qos interface statistics policer flow

显示接口上 policy-map 中 policy 的状态信息。

## 命令语法

```
show qos interface NAME statistics policer flow
```

NAME	接口名
------	-----

## 命令模式

特权配置模式

## 默认

无

## 使用说明

显示基于类型区分的流策略状态和流统计信息。

## 举例说明

```
Switch# show qos interface eth-0-1 statistics policer flow
Interface: eth-0-1
  Ingress service policy: b

  flow policer for class: class-default
  color blind
  CIR 100 kbps, CBS 640000 bytes, EBS 640000 bytes
  drop violate packets
Statistics:
Type      Packets      Bytes      Action
Confirm  0             0          Transmit
Exceed    0             0          Transmit
Violate   0             0          Drop
Total     0             0          -
```

## 相关命令

policy-map

### 9.1.40 show qos interface statistics policer port

显示端口策略统计信息。

## 命令语法

```
show qos interface NAME statistics policer port {input|output}
```

NAME	接口名
------	-----

## 命令模式

特权配置模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch# show qos interface eth-0-1 statistics policer port input
Interface: eth-0-1
input port policer:
  color blind
  CIR 100 kbps, CBS 640000 bytes, EBS 640000 bytes
  drop violate packets
Statistics:
  Type      Packets      Bytes      Action
  Confirm  0            0          Transmit
  Exceed   0            0          Transmit
  Violate  0            0          Drop
  Total    0            0          -
```

## 相关命令

qos policer

### 9.1.41 show qos interface statistics queue

显示每个接口上的流分类统计信息。

## 命令语法

```
show qos interface NAME statistics queue
```

NAME	接口名
------	-----

## 命令模式

特权配置模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch# show qos interface eth-0-1 statistics queue
Queue Transmit-packets    Transmit-Bytes    Drop-packets    Drop-Bytes
UC0    0                      0                 0                0
UC1    0                      0                 0                0
UC2    0                      0                 0                0
UC3    0                      0                 0                0
UC4    0                      0                 0                0
UC5    0                      0                 0                0
UC6    0                      0                 0                0
UC7    0                      0                 0                0
MC0    0                      0                 0                0
MC1    0                      0                 0                0
MC2    0                      0                 0                0
MC3    0                      0                 0                0
SPAN  0                      0                 0                0
```

## 相关命令

无

# 10 IPv6 安全命令行参考

## 10.1 DHCPv6 Snooping 命令

### 10.1.1 clear dhcpv6 snooping bindings learning

在特权模式下使用 `clear dhcpv6 snooping binding learning` 命令来清除 DHCP 绑定数据库中动态绑定的条目。

#### 命令语法

**clear dhcpv6 snooping bindings learning** (**ipv6** *IPv6-ADDRESS* | **mac** *MAC-ADDRESS* | **vlan** *VLAN-ID* | **interface** *IFNAME* |)

<b>ipv6</b> <i>IP-ADDRESS</i>	清除指定 IPv6 地址的绑定条目
<b>mac</b> <i>MAC-ADDRESS</i>	清除指定 MAC 地址的绑定条目
<b>interface</b> <i>IFNAME</i>	清除指定端口名称的绑定条目
<b>vlan</b> <i>VLAN-ID</i>	清除指定 VLAN 的绑定条目

#### 命令模式

特权模式

#### 默认

无

#### 使用说明

该命令用于清除 DHCPv6 snooping 动态绑定条目。

#### 举例说明

配置清除 DHCPv6 snooping 所有绑定条目：

```
Switch# clear dhcpv6 snooping bindings learning
```

## 相关命令

**show dhcpv6 snooping binding**

### 10.1.2 clear dhcpv6 snooping statistics

在特权模式下使用 `clear dhcpv6 snooping statistics` 命令来清除 DHCPv6 snooping 统计信息。

## 命令语法

**clear dhcpv6 snooping statistics**

## 命令模式

特权模式

## 默认

无

## 使用说明

该命令用于清除 DHCPv6 snooping 计数信息。

## 举例说明

配置清除 DHCPv6 snooping 计数：

```
Switch # clear dhcpv6 snooping statistics
```

## 相关命令

**show dhcpv6 snooping statistics**

### 10.1.3 dhcpv6 snooping

在全局配置模式下使用 `dhcpv6 snooping` 命令配置交换机全局使能 DHCPv6 snooping。使用命令相应的 `no` 形式恢复为默认设置。

## 命令语法

**dhcpv6 snooping**

**no dhcpv6 snooping**

## 命令模式

全局配置模式



## 默认

默认情况下，DHCPv6 snooping 未使能。

## 使用说明

必需在全局使能 DHCPv6 snooping，才可以使 DHCPv6 snooping 的配置生效。

只有在全局配置模式下使用 `dhcpv6 snooping vlan vlan-id` 命令在 VLAN 上使能 snooping，DHCPv6 snooping 才会起作用。

## 举例说明

配置使能 DHCPv6 snooping。

```
Switch(config)# dhcpv6 snooping
```

可以在特权模式下使用 `show dhcpv6 snooping config` 命令验证配置是否启用。

## 相关命令

**dhcpv6 snooping vlan**

**show dhcpv6 snooping config**

### 10.1.4 dhcpv6 snooping binding

在全局配置模式下，使用 `dhcpv6 snooping binding` 命令配置 DHCPv6 snooping 绑定数据库以及向数据库中添加静态绑定条目。

## 命令语法

**dhcpv6 snooping binding mac** *MAC-ADDRESS* **vlan** *VLAN-ID* **ipv6** *IP-ADDRESS*  
**interface** *IFNAME* **expiry** *SECONDS*

**no dhcpv6 snooping bindings** (**ipv6** *IP-ADDRESS* | **mac** *MAC-ADDRESS* | **vlan** *VLAN-ID* | **interface** *IFNAME* | )

<b>mac</b> <i>MAC-ADDRESS</i>	指定 MAC 地址
<b>vlan</b> <i>VLAN-ID</i>	指定 VLAN 序号。范围为 1 到 4094
<b>ipv6</b> <i>IP-ADDRESS</i>	指定 IPv6 地址
<b>interface</b> <i>IFNAME</i>	指定添加或删除绑定条目的接口
<b>expiry</b> <i>SECONDS</i>	指定时间间隔(单位为秒)后绑定条目无效。范围为 0 到 86400

## 命令模式

全局配置模式

## 默认

无

## 使用说明

当你在测试或调试交换机时使用该条命令。

在 DHCPv6 snooping 绑定数据库中，每一个数据条目都有一个 IPv6 地址，一个关联的 MAC 地址，一个租约时间，提供绑定数据的接口，以及该接口属于的 VLAN。

在特权模式下，使用 `show dhcpv6 snooping binding` 命令显示配置的绑定信息。

## 举例说明

为在 VLAN1 的接口 `eth-0-1` 上配置一个 DHCPv6 snooping 绑定，MAC 地址为 `0001.000c.01ef`，IPv6 地址为 `2001:1::1`，过期时间为 1200 秒。

```
Switch(config)# dhcpv6 snooping binding mac 0001.000c.01ef vlan 1 ipv6 2001:1::1
interface eth-0-1 expiry 1200
```

## 相关命令

**show dhcpv6 snooping binding**

### 10.1.5 dhcpv6 snooping database

在全局配置模式下，使用 `dhcpv6 snooping database` 命令配置交换机的 DHCPv6 snooping 绑定数据库代理。使用命令相应的 `no` 形式重置保存延期时间。

## 命令语法

**dhcpv6 snooping database auto-save interval *SECONDS***

<b>interval <i>SECONDS</i></b>	指定保存绑定数据库的时间间隔 (单位为秒)。范围为 15 到 1200
--------------------------------	-------------------------------------

## 命令模式

全局配置模式

## 默认

默认时间间隔为 600 秒。

## 使用说明

DHCPv6 snooping 绑定数据库存储在 `flash:/dhcpv6snooping` 中。

## 举例说明

配置 DHCPv6 snooping 自动保存数据库时间间隔为 120 秒:

```
Switch(config)# dhcpv6 snooping database auto-save interval 120
```

## 相关命令

**dhcpv6 snooping**

**dhcpv6 snooping binding**

### 10.1.6 dhcpv6 snooping trust

在端口配置模式下使用 **dhcpv6 snooping trust** 命令配置接口对 DHCPv6 snooping 为信任接口。使用命令相应的 **no** 形式恢复为默认设置。

## 命令语法

**dhcpv6 snooping trust**

**no dhcpv6 snooping trust**

## 命令模式

端口配置模式

## 默认

默认情况下，为 DHCPv6 snooping 不信任接口。

## 使用说明

配置连接 DHCPv6 服务器或其他交换机或路由器的接口为信任接口。配置连接 DHCPv6 客户端的接口为不信任接口。

## 举例说明

配置接口为 DHCPv6 snooping 信任接口:

```
Switch(config-if)# dhcpv6 snooping trust
```

## 相关命令

**show dhcpv6 snooping trusted-source**

### 10.1.7 dhcpv6 snooping vlan

在全局配置模式下使用 **dhcpv6 snooping vlan** 命令配置交换机在 VLAN 使能 DHCPv6 snooping。使用命令相应的 **no** 形式恢复为默认设置。

## 命令语法

**dhcpv6 snooping vlan** *VLAN-RANGE*

**no dhcpv6 snooping vlan** *VLAN-RANGE*

<b>vlan</b> <i>VLAN-RANGE</i>	指定使能 DHCP snooping 的 VLAN ID 或 VLAN 的范围。ID 范围为 1 到 4094
-------------------------------	---

## 命令模式

全局配置模式

## 默认

默认情况下 DHCPv6 snooping 在所有 VLAN 都未使能。

## 使用说明

你可以输入 VLAN 序号指定单独一个 VLAN ID，或者输入几个 VLAN 序号使用逗号间隔，或输入一个 VLAN 范围使用连字号间隔，或输入 VLAN 开始 ID 和 VLAN 结束 ID 使用空格间隔。在 VLAN 上使能 DHCPv6 snooping 前，必须先全局使能 DHCPv6 snooping。注意 dhcpv6 snooping 功能和 dhcpv6 server 功能不要在同一个 vlan 上设置。

## 举例说明

在 VLAN10 上配置 DHCPv6 snooping:

```
Switch(config)# dhcpv6 snooping vlan 10
```

## 相关命令

**show dhcpv6 snooping config**

### 10.1.8 show dhcpv6 snooping binding

在特权模式下使用 show dhcpv6 snooping binding 命令显示设备 DHCPv6 snooping 绑定数据库和所有接口的配置信息。

## 命令语法

**show dhcpv6 snooping binding** ( *all* | *manual* | *learning* ) ( *ipv4 IP-ADDRESS* | *mac MAC-ADDRESS* | *vlan VLAN-ID* | *interface IFNAME* | ) | **summary**

<b>all</b>	显示所有绑定条目
------------	----------

<b>manual</b>	显示静态绑定条目
<b>learning</b>	显示动态绑定条目
<b>mac</b> <i>MAC-ADDRESS</i>	指定 MAC 地址
<b>vlan</b> <i>VLAN-ID</i>	指定 VLAN 序号。范围为 1 到 4094
<b>ipv4</b> <i>IP-ADDRESS</i>	指定 IP 地址
<b>interface</b> <i>IFNAME</i>	指定添加或删除绑定条目的接口
<b>summary</b>	显示 DHCPv6 snooping 绑定的概要信息

## 命令模式

特权模式

## 默认

无

## 使用说明

如果使能了 DHCPv6 snooping 功能，即使接口变为断开状态，交换机也不会删除静态配置的绑定条目。

## 举例说明

显示 DHCPv6 snooping 绑定信息：

```
Switch# show dhcpv6 snooping binding all
DHCPv6 snooping binding table:
VLAN MAC Address      Interface  Lease(s)   IPv6 Address
=====
1      0001.0001.0001 eth-0-2    static     1:1::1:1
Switch# show dhcpv6 snooping binding summary
Total 1 DHCPv6 snooping binding entries
      0 learning entry, 1 configured entry
```

## 相关命令

**dhcpv6 snooping binding**

### 10.1.9 debug dhcpv6 snooping

使用此命令可以打开 dhcpv6 snooping 的模块的调试功能。

在原命令之前加上关键字 “no”，关闭调试功能。

## 命令语法

**debug dhcpv6 snooping ( events | error | packet | dump | all )**

**no debug dhcpv6 snooping ( events | error | packet | dump | all )**

<b>events</b>	调试 dhcpv6 snooping 事件信息
<b>error</b>	调试 dhcpv6 snooping 错误信息
<b>packet</b>	调试 dhcpv6 snooping 的数据包信息
<b>dump</b>	以十六进制调试 dhcpv6 snooping 的数据包信息
<b>all</b>	上面提到的所有调试信息

## 命令模式

特权模式

## 默认

无

## 使用说明

使用“terminal monitor”打印消息

## 举例说明

使用如下命令，打开D snooping的所有调试信息。

```
Switch# debug dhcpv6 snooping all
```

## 相关命令

**terminal monitor**

**show logging buffer**

### 10.1.10 show dhcpv6 snooping config

在特权模式下使用 show dhcpv6 snooping config 命令显示 DHCPv6 snooping 配置。

## 命令语法

**show dhcpv6 snooping config**

## 命令模式

特权模式

## 默认

无

## 使用说明

该命令用于显示 DHCPv6 snooping 配置信息。

## 举例说明

显示 dhcpv6 snooping 配置信息：

```
Switch# show dhcpv6 snooping config
dhcpv6 snooping service: enabled
dhcpv6 snooping switch: enabled
dhcpv6 snooping vlan 3
```

## 相关命令

**dhcpv6 snooping binding**

### 10.1.11 show dhcpv6 snooping trusted-sources

在特权模式下使用 show dhcpv6 snooping trusted-sources 命令显示 DHCPv6 snooping 的信任端口。

## 命令语法

**show dhcpv6 snooping trusted-sources**

## 命令模式

特权模式

## 默认

无

## 使用说明

该命令用于显示 DHCPv6 snooping 信任端口。

## 举例说明

显示 dhcpv6 snooping 信任端口：

```
Switch# show dhcpv6 snooping trusted-source
List of DHCPv6 snooping trusted interface(s):
```

```
=====
eth-0-20
```

## 相关命令

**dhcpv6 snooping trust**

### 10.1.12 show dhcpv6 snooping statistics

在特权模式下使用 `show dhcpv6 snooping statistics` 命令显示 DHCPv6 snooping 统计信息。

## 命令语法

**show dhcpv6 snooping statistics**

## 命令模式

特权模式

## 默认

无

## 使用说明

该命令用于显示 DHCPv6 snooping 统计信息。

## 举例说明

显示 DHCPv6 snooping 统计信息：

```
Switch# show dhcpv6 snooping statistics
DHCPv6 snooping statistics:
```

```
=====
DHCPv6 packets                137
Packets forwarded              137
Packets invalid                 0
Packets dropped                 0
```

## 相关命令

**clear dhcpv6 snooping statistics**



# 11 IPv6 路由命令行参考

## 11.1 OSPFv3 命令

### 11.1.1 router ipv6 ospf

使用此命令创建 OSPFv3 进程。

#### 命令语法

```
router ipv6 ospf [process ID]
```

<i>process ID</i>	OSPFv3 进程号，整数形式，取值范围是 1~65535。如果不指定进程号，缺省使用进程号 0。
-------------------	---

#### 命令模式

全局配置模式

#### 默认

无

#### 使用说明

只有在 OSPFv3 视图下配置了 Router ID，OSPFv3 进程才能正常运行，否则只能看到该进程，但无法生成 LSA。

#### 举例说明

下面例子讲述了创建 OSPFv3 进程 100。

```
Switch(config)# router ipv6 ospf 100
```

#### 相关命令

```
show ipv6 ospf
```

## 11.1.2 area default-cost

要指定一个发送到 Stub 区域或 NSSA 区域默认的汇总路由的开销，在路由模式下使用命令 `area default-cost`。如果要删除配置，只要用该命令的 `no` 形式。

### 命令语法

**area** *AREA-ID* **default-cost** *COST*

**no area** *AREA-ID* **default-cost**

<i>AREA-ID</i>	区域标识符，标识符可以是十进制的或者是 IP 地址
<i>COST</i>	Cost 的范围 0-16777215

### 命令模式

路由模式

### 默认

默认为 1。

### 使用说明

此命令只用在连接 stub 区域或 NSSA 区域的区域边缘路由器（ABR）上。

有两种 Stub 区域的路由配置命令：`stub` 和 `default-cost` 命令。

配置 Stub 区域后只学习类型为 1(router-lsa)，2(network lsa)和 3(summary lsa)的 LSA。

### 举例说明

下面例子讲述如何配置 Stub 区域和如何配置 Stub 区域的 Cost 值：

```
Switch(config)# router ipv6 ospf 201
Switch(config-router)# area 10.0.0.0 stub
Switch(config-router)# area 10.0.0.0 default-cost 20
```

### 相关命令

无

## 11.1.3 area range

使用此命令在 OSPF 区域边界上对路由进行合并和汇总，使用关键字 `no` 取消此项功能。

## 命令语法

**area** *AREA-ID* **range** *ADDRESS/MASK* (**not-advertise**)

**no area** *AREA-ID* **range** *ADDRESS/MASK*

<i>AREA-ID</i>	以 ID 标识的 OSPF 区域.
<i>ADDRESS</i>	聚合路由的目的 IPv6 地址
<i>MASK</i>	聚合路由的地址前缀长度
<b>not-advertise</b>	不发布这条聚合路由

## 命令模式

路由模式

## 默认

不对路由进行聚合。

## 使用说明

**area range** 只能用在 ABR 路由器上。用来对当前区域进行路由聚合。聚合的结果是由 ABR 把单一的汇总路由宣告给其他区域。一个区域可配置多条聚合网段，这样 OSPFv3 可对多个网段进行聚合。

## 举例说明

下面的例子讲述了如何在 ABR 路由器上对子网 2004::1/16 进行路由汇总

```
Switch(config)# router ipv6 ospf 201
```

```
Switch(config-router)# area 10.0.0.0 range 2004::1/16
```

## 相关命令

无

### 11.1.4 area stub

使用此命令设置指定区域为 Stub（存根）区域，使用关键字 **no** 取消对此区域为存根区域的设置。

## 命令语法

**area** *AREA-ID* **stub** (**no-summary**)

**no area** *AREA-ID* **stub** (**no-summary**)

<i>AREA-ID</i>	以 ID 或者 IP 地址标识的 OSPF 区域
<b>no-summary</b>	如果指定了此项，则配置此区域为完全存根区域

## 命令模式

路由模式

## 默认

默认无 Stub 区域

## 使用说明

缺省情况下，没有区域被设置为 Stub（存根）区域。Stub 区域的所有路由器都必须用 `area stub` 进行设置。

如果一个区域被配置为存根区域，则当 5 类 LSA 在整个 AS 内进行洪泛时，不会被洪泛进此存根区域。典型的可以被配置为存根区域的是一个 IP 子网，此时所有主机都通过路由器访问外网；把此 IP 子网配置为存根区域，可以减少路由信息的流量并减少连接状态数据库的大小；存根区域中的 ABR 会向存根区域发布汇总路由，以通告存根区域到达 AS 内其它区域的路由；所以存根区域可以避免 AS 外的路由变化对此存根区域的影响，但它并不能阻止 AS 内的其他区域对它的影响。完全存根区域不仅能阻止 5 类 LSA 的进入，而且能阻止其他的 3 类 LSA 的进入；所以完全存根区域不仅避免了 AS 外的路由变化对此存根区域的影响，而且避免了 AS 内其它区域对它的影响。可以用关键字 `no-summary` 将区域配置为完全存根区域，此时 ABR 向存根区域只宣告一条缺省路由的 3 类 LSA。

## 举例说明

下面例子讲述了如何配置 Stub 区域以及设置默认的 Cost 值：

```
Switch(config)# router ipv6 ospf 201
Switch(config-router)# area 10.0.0.0 stub
Switch(config-router)# area 10.0.0.0 default-cost 20
```

## 相关命令

无

### 11.1.5 auto-cost

使用此命令设置计算链路开销时所依据的参考带宽，使用关键字 `no` 把参考带宽设置为默认值。

## 命令语法

**auto-cost reference-bandwidth** *RATE*

**no auto-cost reference-bandwidth**

<i>RATE</i>	带宽，以 Mbps 为单位。范围从 1 到 4294967；默认是 100
-------------	---------------------------------------

## 命令模式

路由模式

## 默认

100 Mbps

## 使用说明

使用 `ipv6 ospf cost` 命令设置的端口 Cost 值将会覆盖用该命令计算出来的 cost 值。计算链路开销的公式为：参考带宽/端口速率。

## 举例说明

下面例子讲述了如何在链路上设置带宽为 1G

```
Switch(config)# router ipv6 ospf 1
```

```
Switch(config-router)# auto-cost reference-bandwidth 1000
```

## 相关命令

**ipv6 ospf cost**

### 11.1.6 clear ipv6 ospf

使用此命令重启 OSPFv3 进程。

## 命令语法

**clear ipv6 ospf** (*PID* | ) **process**

<i>PID</i>	(可选)进程 ID
------------	-----------

## 命令模式

特权模式

## 默认

无

## 使用说明

<0-65535>: OSPFv3 进程编号；如果没有指定此项，则重启所有 OSPFv3 进程。

## 举例说明

下面例子讲述如何重启所有 OSPFv3 进程：

```
Switch# clear ipv6 ospf process
```

## 相关命令

无

### 11.1.7 default-information originate (OSPFv3)

使用此命令用来将缺省路由引入 OSPFv3 区域，使用关键字 **no** 取消引入缺省路由。

## 命令语法

```
default-information originate [route-map WORD] | [always] | [metric METRIC-VALUE]  
[metric-type TYPE-VALUE]
```

```
no default-information originate [always] [metric] [metric-type] [route-map]
```

<b>always</b>	(可选) 在没有配置静态默认路由的情况下始终向 OSPFv3 网络通告默认路由，如果没有指定该关键字，本机必须要配置缺省路由才可以引入产生缺省路由的 ASE LSA。
<b>metric</b>	(可选) 被用作生成默认路由的 Metric。假如你没有指定相应的值，默认值是 1。
<b>metric-type</b>	(可选) 外部链路的路由类型： 1—type 1 的 5 类 LSA 2—type 2 类型的 5 类 LSA 默认是 Type2
<b>route-map</b>	路由策略

## 命令模式

路由模式

## 默认

默认关闭

## 使用说明

当你使用重发布命令(**redistribute**)或引入缺省路由命令(**default-information-originate**)时, 路由器自动成为自治系统边界路由器(ASBR)。ASBR 默认不会向 OSPFv3 域生成默认路由, 除非系统本身已经存在默认路由或者指定了 **always** 关键字。

IPv6 的 **route-map** 目前还没有支持, 如果配置了 **route-map** 当作 **route-map** 不存在时处理。

## 举例说明

下面例子讲述了如何设置默认路由以及修改对应的 Metric 值和类型:

```
Switch(config)# router ipv6 ospf 109
```

```
Switch(config-router)# default-information originate metric 100 metric-type 1
```

## 相关命令

**redistribute (OSPFv3)**

### 11.1.8 default-metric (OSPFv3)

使用此命令设置 OSPFv3 引入外部路由时的开销, 使用关键字 **no** 恢复路由开销为默认值。

## 命令语法

**default-metric** *METRIC-VALUE*

**no default-metric** (*METRIC-VALUE*)

<i>METRIC-VALUE</i>	设置指定的路由开销
---------------------	-----------

## 命令模式

路由模式

## 默认

默认值为 20。

## 使用说明

default-metric 命令通常和 redistribute 路由器配置命令一起使用。

## 举例说明

下面例子讲述了如何将 RIPng 路由引入到 OSPFv3，并将引入时的路由开销设为 10。

```
Switch(config)# router ipv6 ospf
Switch(config-router)# default-metric 10
Switch(config-router)# redistribute ripng
```

## 相关命令

**redistribute (OSPFv3)**

### 11.1.9 distance (OSPFv3)

设置 OSPFv3 的管理距离，使用 no 命令恢复默认配置。

## 命令语法

**distance** {*DISTANCE* | **ospfv3** [**external** *DIST1*] [**inter-area** *DIST2*] | [**intra-area** *DIST3*]}

**no distance** {*DISTANCE* | **ospfv3**}

<i>DISTANCE</i>	管理距离，范围：1 到 255。（255 个距离值的路由在路由表中无效。）
<b>external</b> <i>DIST1</i>	(可选)对区域外路由设置管理距离
<b>inter-area</b> <i>DIST2</i>	(可选)对区域间路由设置管理距离
<b>intra-area</b> <i>DIST3</i>	(可选)对区域内路由设置管理距离

## 命令模式

路由模式

## 默认

*DIST1*: 110

*DIST2*: 110

*DIST3*: 110



## 使用说明

默认情况下，区域内、区域间、区域外路由的管理距离都为 110。

管理距离表征的是对路由的可信度；管理距离越小，此种路由的可信度越高。

当有不止一条的路由可以到达目标时，路由器根据路由的可信度，即根据管理距离选择采用何种路由。只在本地有效。

## 举例说明

下面例子讲述了如何设置 OSPFv3 的管理距离：

```
Switch(config)# router ipv6 ospf
```

```
Switch(config-router)# distance 90
```

## 相关命令

无

### 11.1.10 distribute-list (OSPFv3)

使用该命令对 OSPFv3 计算出的路由或重发布到 OSPFv3 中的路由进行过滤。使用关键字 no 取消过滤行为。

## 命令语法

**distribute-list** *ACCESSS-LIST-NAME* (**in** | **out** (**bgp** | **connected** | **ospfv3** | **ripng** | **static**))

**no distribute-list** *ACCESSS-LIST-NAME* (**in** | **out**)

<i>ACCESSS-LIST-NAME</i>	ACL 名称
<b>in</b>	对 OSPFv3 计算出来的路由进行过滤
<b>out</b>	对重发布到 OSPFv3 中的路由进行过滤

## 命令模式

路由模式

## 默认

默认无配置

## 使用说明

必须要指定一个 ACL。in 方向用来设置路由信息的过滤条件，只有通过过滤的路由信息才下到 RIB 中；out 方向用来配置对引入的路由信息进行过滤。

## 举例说明

下面的例子讲述了如何只接收 2001:1::1/32 和 3001:1::1/32 两个网段的路由：

```
Switch(config)# ipv6 access-list filter-ospf-route
Switch(config-ip-acl)# permit any 2001:1::1/32 any
Switch(config-ip-acl)# permit any 3001:1::1/32 any
Switch(config-ip-acl)# deny any any any
Switch(config)# router ipv6 ospf 1
Switch(config-router)# distribute-list filter-ospf-route in
```

## 相关命令

**ipv6 access-list**

### 11.1.11 enable db-summary-opt

使用该命令对 OSPFv3 邻居间 Database Exchange 的过程进行优化，使用关键字 no 取消 database exchange 过程的优化。

## 命令语法

```
enable db-summary-opt
no enable db-summary-opt
```

## 命令模式

路由模式

## 默认

默认不使能

## 使用说明

使能了这个功能后，在 database exchange 的过程中，当路由器从邻居收到 DD 报文后，发现邻居的 LSA 比自己的新，那么将这个 LSA 从自己的 Database Summary list 中删除，没必要再发该 LSA 的 DD 报文给邻居了。

## 举例说明

下面的例子讲述了如何使能 Database Exchange 过程的优化：

```
Switch(config)# router ipv6 ospf 1
Switch(config-router)# enable db-summary-opt
```

## 相关命令

无

### 11.1.12 ipv6 ospf cost

使用此命令设置端口不同实例下开销，使用关键字 **no** 设置端口开销为默认值。

## 命令语法

```
ipv6 ospf cost INTERFACE-COST (instance ID |)
no ipv6 ospf cost (instance ID |)
```

<i>INTERFACE-COST</i>	设置端口的范围值 1 到 65535
<i>ID</i>	指定接口所属的实例 ID，取值范围是 0~255，缺省值是 0

## 命令模式

端口配置模式

## 默认

端口的速率不一样，默认开销也可能不一样。

## 使用说明

如果你不想使用默认的端口开销，可以用该命令来改变开销值。也可以使用 **reference bandwidth** 来改变端口开销。

## 举例说明

下面例子讲述了如何设置端口的开销为 65:

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ipv6 ospf cost 65
```

## 相关命令

**auto-cost reference bandwidth**

## 11.1.13 ipv6 ospf dead-interval

邻居路由器失效时间。如果在该时间之后还没有收到邻居的任何 hello 报文，则宣告邻居死亡。使用关键字 no 恢复此时间段为默认值。

### 命令语法

**ipv6 ospf dead-interval** *SECONDS* (*instance ID* |)

**no ipv6 ospf dead-interval** (*instance ID* |)

<i>SECONDS</i>	设置的时间间隔值，范围是 1-65535
<i>ID</i>	指定接口所属的实例 ID，取值范围是 0~255，缺省值是 0

### 命令模式

端口配置模式

### 默认

*SECONDS*: 默认在宣告邻居死亡之前，端口等待的时间为 40 秒

### 使用说明

邻居路由器失效时间会在 hello 报文中被通告。在同一 OSPFv3 网络中的时间间隔必须一致。该值设置的越短，网络收敛时间也越短，但是会增加网络的不稳定性。

### 举例说明

设置 OSPF 的接口死亡时间间隔为 20 秒：

```
Switch(config)# interface eth-0-1
```

```
Switch(config-if)# no switchport
```

```
Switch(config-if)# ipv6 ospf dead-interval 20
```

### 相关命令

**ipv6 ospf hello-interval**

**show ipv6 ospf interface**

## 11.1.14 ipv6 ospf hello-interval

使用此命令设置此端口发送 Hello 报文的时间间隔，使用关键字 no 设置此端口发送 Hello 报文的时间间隔为默认值。

## 命令语法

**ipv6 ospf hello-interval** *SECONDS* (*instance ID* |)

**no ipv6 ospf hello-interval** (*instance ID* |)

<i>SECONDS</i>	范围值 1~65535，期间路由器必须接收到一个 hello 报文，否则这个邻居就会在邻居表中被删除。网络上所有节点的 hello interval 必须要配置成一样的。
<i>ID</i>	指定接口所属的实例 ID，取值范围是 0~255，缺省值是 0

## 命令模式

端口配置模式

## 默认

10 seconds (以太网);

30 seconds (非广播网)。

## 使用说明

该值将会在 hello 报文中被发送，同一网络内的路由器上设置的 hello 时间间隔必须一致。该值设置的越短，网络拓扑变化将能被越快的检测到，但这样也会造成网络上流量增加。

## 举例说明

下面的例子将端口发送 Hello 报文的时间间隔设置为 15 秒：

```
Switch(config)# interface eth-0-1
```

```
Switch(config-if)# no switchport
```

```
Switch(config-if)# ipv6 ospf hello-interval 15
```

## 相关命令

**ipv6 ospf dead-interval**

### 11.1.15 ipv6 ospf mtu-ignore

使用此命令设置端口接收数据库描述报文时，忽略对 MTU 字段的检测。

使用关键字 no 设置对数据库描述报文的 MTU 字段进行检测。

## 命令语法

```
ipv6 ospf mtu-ignore (instance ID |)
no ipv6 ospf mtu-ignore (instance ID |)
```

<i>ID</i>	指定接口所属的实例 ID，取值范围是 0~255，缺省值是 0
-----------	---------------------------------

## 命令模式

端口配置模式

## 默认

默认接口启用 MTU 的匹配功能。

## 使用说明

OSPFv3 检查邻居是否使用相同的 MTU 值。这个检查发生在互相交换数据库描述报文时，如果在接收到的 DD 报文里的 MTU 高于入接口上配置的 MTU，OSPFv3s 邻接将无法建立。

## 举例说明

下面例子讲述了如何设置在端口上接收到 DD 报文时不对 MTU 值进行检测：

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ipv6 ospf mtu-ignore
```

## 相关命令

无

### 11.1.16 ipv6 ospf priority

使用此命令设置路由器端口优先权，这个值被用来在网络中选举指定路由器。使用关键字 `no` 恢复端口优先权为默认值。

## 命令语法

```
ipv6 ospf priority NUMBER-VALUE (instance ID |)
no ipv6 ospf priority (instance ID |)
```

<i>NUMBER-VALUE</i>	优先级范围 0~255，默认值是 1
---------------------	--------------------

<i>ID</i>	指定接口所属的实例 ID，取值范围是 0~255，缺省值是 0
-----------	---------------------------------

## 命令模式

端口配置模式

## 默认

优先级为 1。

## 使用说明

端口的默认优先权值为 1。

端口的优先权主要用来选举网络中的 DR 和 BDR；优先级高的会被选举为 DR。

如果优先级相等，则 Router-ID 大的会被选举为 DR；如果某一个端口的优先级被设置为 0，则此端口不会参加 DR 和 BDR 的选举。端口优先级只在多路访问的网络中起作用，也就是说，点对点网络无效。

## 举例说明

下面例子讲述了如何配置 OSPFv3 的接口优先级为 4：

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ipv6 ospf priority 4
```

## 相关命令

无

### 11.1.17 ipv6 ospf retransmit-interval

使用此命令设置在邻接间交换 LSA 报文时的重传时间间隔，使用关键字 **no** 恢复在邻接间交换 LSA 报文时的重传时间间隔为默认值。

## 命令语法

```
ipv6 ospf retransmit-interval SECONDS (instance ID |)
no ipv6 ospf retransmit-interval (instance ID |)
```

<i>SECONDS</i>	<1-65535>: 重传时间间隔，以秒为单位
<i>ID</i>	指定接口所属的实例 ID，取值范围是 0~255，缺省值是 0

## 命令模式

端口配置模式

## 默认

默认为 5 秒。

## 使用说明

当一个路由器发送 LSA 报文到它的邻居时，它会缓存该报文直到收到邻居的确认报文。如果在重传时间间隔内没有收到确认报文，该 LSA 将被重传。设置该值必须要谨慎，以免引起不必要的重传。通常，这个值要大于两个路由器之间的报文往返延迟。

## 举例说明

下面例子讲述了如何设置接口的 LSA 报文交换时候的重传时间：

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ipv6 ospf retransmit-interval 8
```

## 相关命令

无

### 11.1.18 ipv6 ospf transmit-delay

使用此命令设置端口发送一个 LSA 报文的延迟时间，使用关键字 **no** 恢复此时间为默认值。

## 命令语法

```
ipv6 ospf transmit-delay SECONDS (instance ID |)
no ipv6 ospf transmit-delay (instance ID |)
```

<i>SECONDS</i>	<1-65535>重传时间间隔，以秒为单位
<i>ID</i>	指定接口所属的实例 ID，取值范围是 0~255，缺省值是 0

## 命令模式

端口配置模式



## 默认

默认为 1 秒。

## 使用说明

LSA 在本路由器的链路状态数据库（LSDB）中会随时间老化（每秒钟加 1），但在网络的传输过程中却不会，所以有必要在发送之前在 LSA 的老化时间上增加一定的延迟时间。此配置对低速率的网络尤其重要。

## 举例说明

下面例子讲述如何设置 LSA 报文的延迟时间：

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ipv6 ospf transmit-delay 3
```

## 相关命令

无

### 11.1.19 passive-interface (OSPFv3)

使用此命令抑制端口发送 Hello 报文，使用关键字 **no** 取消端口对发送 Hello 报文的抑制。

## 命令语法

```
passive-interface INTERFACE-ID
no passive-interface INTERFACE-ID
```

<i>INTERFACE-ID</i>	接口名字
---------------------	------

## 命令模式

路由模式

## 默认

默认不开启。

## 使用说明

如果在接口上禁用路由更新报文的发送，那么此接口还是能正常接收和处理 OSPF 报文的。

## 举例说明

下面例子讲述了如何将端口设备为被动接口：

```
Switch(config)# router ipv6 ospf 200
```

```
Switch(config-router)# passive-interface eth-0-1
```

## 相关命令

**router ipv6 ospf**

### 11.1.20 redistribute (OSPFv3)

此命令设置路由重发布，即把别的路由协议生成的路由引入到 OSPFv3 路由域。使用该命令的 no 形式取消路由重发布。

## 命令语法

**redistribute (bgp | connected | ripng | static | ospfv3 [PID ]) [route-map WORD] [tag TAG-VALUE] [metric METRIC-VALUE] [metric-type TYPE-VALUE]**

**no redistribute PROTOCOL [metric METRIC -VALUE] [metric-type TYPE-VALUE]**

<b>route-map WORD</b>	路由策略
<b>ospfv3 [PID]</b>	指定重发布 ospfv3 的 process id
<b>tag TAG-VALUE</b>	设置路由的 TAG
<b>metric METRIC-VALUE</b>	(可选)重发布路由时候的 Metric 值，默认 20
<b>metric-type TYPE-VALUE</b>	对于 OSPF，有两种类型的外部路由： 类型一的外部路由 类型二的外部路由 默认是二类路由。

## 命令模式

路由模式

## 默认

默认重发布不开启。

metric metric-value: 默认值 20。

metric-type type-value: 类型 2 的外部路由。

## 使用说明

在该命令里配置的 `metric` 值将覆盖用命令 `default metric` 配置的值。

外部路由是指到达自治系统外部的路由。

Type-1 外部路由指接收的 IGP 路由，如 RIPng 和 STATIC。此类路由有较高的可靠性，所以外部路由开销的计算结果等于自治系统的内部路由开销，并可与 OSPF 本身的路由开销相比较。也就是说，到达 Type-1 外部路由的开销等于路由器到达对应 ASBR 的开销加上 ASBR 到达目的地址的开销。

Type-2 外部路由指接收的 EGP 路由。此类路由可靠性较低，所以 OSPF 协议认为从 ASBR 到达自治系统外部的路由开销要远远高于自治系统内部到达 ASBR 的路由开销。因此在计算路由开销时主要考虑前者。也就是说，到达 Type-2 外部路由的开销等于 ASBR 到达目的地址的开销。

BGP 和 route-map 不支持。

## 举例说明

下面例子讲述了如何重发布静态路由并将其 Metric 设置为 10:

```
Switch(config)# router ipv6 ospf 119
```

```
Switch(config-router)# redistribute static metric 10
```

## 相关命令

**default-metric**

### 11.1.21 router-id (OSPFv3)

使用此命令设置路由器标识为指定的值，使用关键字 `no` 设置标识为默认值。

## 命令语法

**router-id** *IP-ADDRESS*

**no router-id**

<i>IP-ADDRESS</i>	IP 地址
-------------------	-------

## 命令模式

路由模式

## 默认

无

## 使用说明

此参数是 OSPFv3 协议中一个很重要的参数；在 OSPFv3 协议中，路由器 ID 号是一个 32 比特无符号整数，是一台路由器在 OSPFv3 自治系统中的唯一标识。用户必须在 OSPFv3 视图下配置路由器 ID 号，否则 OSPFv3 将无法运行。在手工设置路由器 ID 号时，必须保证自治系统中任意两台路由器 ID 号都不相同。若在已经有邻居的路由器上用此命令更改了路由器 ID，则该 ID 必须重新启用 OSPF 协议才能生效。

## 举例说明

下面例子讲述了如何配置 OSPF 的 Route-id:

```
Switch(config)# router ipv6 ospf 119
```

```
Switch(config-router)# router-id 10.1.1.1
```

## 相关命令

```
clear ipv6 ospf
```

```
router ipv6 ospf
```

### 11.1.22 summary-address (OSPFv3)

使用此命令对外部路由进行汇总，使用关键字 no 取消汇总。

## 命令语法

```
summary-address PREFIX / PREFIX-LENGTH [not-advertise] [tag TAG-VALUE]
```

```
no summary-address PREFIX / PREFIX-LENGTH [not-advertise] [tag TAG-VALUE]
```

<i>PREFIX</i>	IPv6 路由的前缀
<i>PREFIX-LENGTH</i>	前缀长度
<b>not-advertise</b>	(可选) 如果指定了此项，则对指定网络的外部路由不进行宣告
<b>tag TAG-VALUE</b>	路由标记，范围<0-4294967295>，默认为 0

## 命令模式

路由模式

## 默认

缺省情况下，不对外部路由进行聚合。

## 使用说明

从其他路由协议学到的路由可以在 ASBR 上进行汇总，汇总路由里的 metric 值选择的是所有被汇总的路由里值最大的一个。该命令可以用来帮助减少路由表的大小。配置 `summary-address` 命令后，对处于聚合地址范围内的外部路由，本地路由器只向邻居路由器发布一条聚合后的路由。您可以使用命令 `area range` 对 OSPF 区域间的路由进行汇总。

## 举例说明

下面例子讲述了如何配置汇总路由，汇总路由 `2001:1:1::/48` 包括了子网 `2001:1:1:1::/64`，`2001:1:1:2::/64` 等等。此时，只有 `2001:1:1::/48` 这条汇总路由会被发布出去。

```
Switch(config)# router ipv6 ospf
```

```
Switch(config-router)# summary-address 2001:1:1::/48
```

## 相关命令

**area range**

### 11.1.23 show ipv6 ospf

使用此命令查看指定 OSPFv3 路由进程相关信息。

## 命令语法

```
show ipv6 ospf (PROCESS-ID)
```

<i>PROCESS-ID</i>	OSPF 进程号
-------------------	----------

## 命令模式

特权模式

## 默认

无

## 使用说明

不指定 OSPFv3 process ID 时，显示所有 process 的信息。

## 举例说明

下面例子讲述了如何查看 OSPFv3 的进程信息：

**Switch# show ipv6 ospf 65535**

```

Routing Process "OSPFv3 (65535)" with ID 1.1.1.1
Process uptime is 1 hour 52 minutes
SPF schedule delay min 0.500 secs, SPF schedule delay max 50.0 secs
Minimum LSA interval 5 secs, Minimum LSA arrival 1 secs
Number of incoming current DD exchange neighbors 0/5
Number of outgoing current DD exchange neighbors 0/5
Number of external LSA 0. Checksum Sum 0x0000
Number of AS-Scoped Unknown LSA 0
Number of LSA originated 3
Number of LSA received 19
Number of areas in this router is 1
  Area BACKBONE(0)
    Number of interfaces in this area is 1(1)
    SPF algorithm executed 6 times
    Number of LSA 4. Checksum Sum 0x16569
    Number of Unknown LSA 0

```

**相关命令**

无

**11.1.24 show ipv6 ospf database**

使用此命令查看指定 OSPFv3 路由进程的链路状态数据库信息。

**命令语法**

**show ipv6 ospf** (*PROCESS-ID*) **database**

**show ipv6 ospf** (*PROCESS-ID*) **database adv-router** *ROUTER-ID*

**show ipv6 ospf** (*PROCESS-ID*) **database** (**external** | **inter-prefix** | **inter-router** | **intra-prefix** | **link** | **network** | **router**) [*LINK-STATE-ID*] (**adv-router** *ROUTER-ID* | **self-originate**)

**show ipv6 ospf** (*PROCESS-ID*) **database max-age**

**show ipv6 ospf** (*PROCESS-ID*) **database self-originate**

<i>PROCESS-ID</i>	(可选) OSPFv3 进程号
<b>adv-router</b> <i>ROUTER-ID</i>	(可选) 查看指定 OSPFv3 宣告路由器的 LSA 信息
<i>LINK-STATE-ID</i>	(可选) 查看自治系统边界路由器的汇总 LSA 信息

**命令模式**

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子讲述了如何使用此命令来查看相关的信息：

```
Switch# show ipv6 ospf 65535 database
```

```

                OSPFv3 Router with ID (1.1.1.1) (Process 65535)
                Link-LSA (Interface vlan1000)
Link State ID  ADV Router      Age  Seq#          CkSum  Prefix
0.0.19.232    1.1.1.1          1492 0x80000002  0x27e3    1
0.0.19.232    2.2.2.2          1488 0x80000002  0xcc94    1
                Router-LSA (Area 0.0.0.0)
Link State ID  ADV Router      Age  Seq#          CkSum  Link
0.0.0.0       1.1.1.1          1452 0x80000003  0x42d6    1
0.0.0.0       2.2.2.2          1449 0x80000003  0x24f0    1
                Network-LSA (Area 0.0.0.0)
Link State ID  ADV Router      Age  Seq#          CkSum
0.0.19.232    2.2.2.2          1453 0x80000001  0x7f99
                Intra-Area-Prefix-LSA (Area 0.0.0.0)
Link State ID  ADV Router      Age  Seq#          CkSum  Prefix  Reference
0.0.0.2       2.2.2.2          1448 0x80000001  0x96fd    2  Network-LSA

```

## 相关命令

无

### 11.1.25 show ipv6 ospf interface

使用此命令显示 OSPFv3 接口的信息。

## 命令语法

```
show ipv6 ospf interface (INTERFACE-NAME)
```

<i>INTERFACE-NAME</i>	(可选) 接口的名字
-----------------------	------------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子讲述了如何显示 OSPFv3 的接口信息：

```
Switch# show ipv6 ospf interface vlan 12
```

```

vlan12 is up, line protocol is up
  Interface ID 4108
  IPv6 Prefixes
    fe80::8eb5:d5ff:fed9:ff00/10 (Link-Local Address)
    2004:12:0:12::1/96
  OSPFv3 Process (0), Area 0.0.0.0, Instance ID 0
  Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State Backup, Priority 1
  Designated Router (ID) 2.2.2.2
    Interface Address fe80::188f:beff:fe99:9800
  Backup Designated Router (ID) 1.1.1.1
    Interface Address fe80::8eb5:d5ff:fed9:ff00
  Timer interval configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:06
  Neighbor Count is 1, Adjacent neighbor count is 1

```

## 相关命令

无

### 11.1.26 show ipv6 ospf neighbor

使用此命令查看指定 OSPFv3 路由进程的邻居信息。

## 命令语法

```
show ipv6 ospf neighbor [INTERFACE-NAME] [NEIGHBOR-ID] [detail]
```

<i>INTERFACE-NAME</i>	(可选) 接口名字.
<i>NEIGHBOR-ID</i>	(可选) 邻居 ID
<b>detail</b>	(可选) 查看邻居的详细信息



## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子讲述如何查看 OSPFv3 邻居的信息：

```
Switch# show ipv6 ospf neighbor
```

```
OSPFv3 Process (0)
Neighbor ID      Pri   State           Dead Time   Interface   Instance ID
2.2.2.2          1    Full/DR         00:00:31   vlan12      0
2.2.2.2          1    Full/DR         00:00:33   vlan1212   0
OSPFv3 Process (65535)
Neighbor ID      Pri   State           Dead Time   Interface   Instance ID
2.2.2.2          1    Full/DR         00:00:31   vlan1000   0
```

## 相关命令

无

### 11.1.27 show ipv6 ospf database database-summary

使用此命令显示 OSPFv3 数据库信息的摘要和汇总。

## 命令语法

```
show ipv6 ospf (PROCESS-ID) database database-summary
```

<i>PROCESS-ID</i>	(可选) OSPFv3 进程 ID
-------------------	-------------------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子讲述了如何使用此命令：

```
Switch# show ipv6 ospf 65535 database database-summary
```

```
                OSPFv3 Router with ID (1.1.1.1) (Process ID 65535)
Area (0.0.0.0) database summary
  LSA Type          Count      MaxAge
  Router            2          0
  Network           1          0
  Inter-Prefix     0          0
  Inter-Router     0          0
  Intra-Prefix     1          0
  Subtotal         4          0
Process 65535 database summary
  LSA Type          Count      MaxAge
  Router            2          0
  Network           1          0
  Inter-Prefix     0          0
  Inter-Router     0          0
  Type-5 Ext       0          0
  Link              2          0
  Intra-Prefix     1          0
  Total             6          0
```

## 相关命令

无

### 11.1.28 show ipv6 ospf route

使用此命令显示 OSPFv3 路由的信息。

## 命令语法

```
show ipv6 ospf (PROCESS-ID) route
```

<i>PROCESS-ID</i>	(可选) OSPFv3 进程 ID
-------------------	-------------------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子讲述了如何使用此命令：

Switch# show ipv6 ospf route

```

OSPFv3 Process (0)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       E1 - OSPF external type 1, E2 - OSPF external type 2
Destination                                Metric
Next-hop
C 2004:1:0:10::/96                          1
   directly connected, vlan10, Area 0.0.0.0
C 2004:1:0:20::/96                          1
   directly connected, vlan20, Area 0.0.0.14
C 2004:1:0:100::/96                         1
   directly connected, vlan100, Area 0.0.0.0
C 2004:1:0:200::/96                         1
   directly connected, vlan200, Area 0.0.0.14
O 2004:2:0:10::/96                           2
   via fe80::188f:beff:fe99:9800, vlan1212, Area 0.0.0.0
   via fe80::188f:beff:fe99:9800, vlan12, Area 0.0.0.0
IA 2004:2:0:20::/96                          2
   via fe80::188f:beff:fe99:9800, vlan1212, Area 0.0.0.0
   via fe80::188f:beff:fe99:9800, vlan12, Area 0.0.0.0

```

## 相关命令

无

### 11.1.29 show ipv6 ospf route summary

使用此命令显示 OSPFv3 路由的信息汇总。

## 命令语法

**show ipv6 ospf (*PROCESS-ID*) route summary**

<i>PROCESS-ID</i>	(可选) OSPFv3 进程 ID
-------------------	-------------------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子讲述了如何使用此命令：

```
Switch# show ipv6 ospf route summary
```

```
                OSPFv3 Router with ID (1.1.1.1) (Process ID 0)
Route Type          Count
(C)Connected        8
(D)Discard           0
(O)Intra area       2
(IA)Inter area      4
(E1)Ext type 1      0
(E2)Ext type 2      0
(N1)NSSA Ext type 1 0
(N2)NSSA Ext type 2 0
Total               14

                OSPFv3 Router with ID (1.1.1.1) (Process ID 65535)
Route Type          Count
(C)Connected        1
(D)Discard           0
(O)Intra area       1
(IA)Inter area      0
(E1)Ext type 1      0
(E2)Ext type 2      0
(N1)NSSA Ext type 1 0
(N2)NSSA Ext type 2 0
Total               2
```

## 相关命令

无

### 11.1.30 show ipv6 protocols ospf

使用此命令查看 OSPFv3 协议的参数设置信息。

## 命令语法

```
show ipv6 protocols ospfv3
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子讲述了如何显示 OSPFv3 协议的信息：

```
Switch# show ipv6 protocols ospf
```

```

Routing Protocol is "OSPFv3 (0)" with ID 1.1.1.1
  Redistributing:
  Distance: (default is 110)
Routing Protocol is "OSPFv3 (65535)" with ID 1.1.1.1
  Redistributing:
  Distance: (default is 110)

```

## 相关命令

无

### 11.1.31 timers spf

使用此命令设置收到拓扑变化报文而计算 SPF 的时间。

## 命令语法

```
timers spf exp SPF-HOLD_MIN SPF-HOLD_MAX
```

```
no timers spf exp
```

<i>SPF-HOLD_MIN</i>	接收到网络变化报文开始计算 SPF 之前的最小延迟时间，以毫秒为单位
<i>SPF-HOLD_MAX</i>	接收到网络变化报文开始计算 SPF 之前的最大延迟时间，以毫秒为单位

## 命令模式

路由模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子讲述了如何设置 OSPFv3 的 SPF 计算参数：

```
Switch(config)# router ipv6 ospf 1
```

```
Switch(config)# timers spf exp 20 50
```

## 相关命令

无

### 11.1.32 max-concurrent-dd

使用此命令设置能够同时处理的最大的 DD 报文数目。

使用关键字 **no** 恢复为默认值。

## 命令语法

**max-concurrent-dd** *NUMBER-VALUE*

**no max-concurrent-dd**

<i>NUMBER-VALUE</i>	可同时处理的 DD 报文的最大数量
---------------------	-------------------

## 命令模式

路由模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子讲述了如何配置可同时处理的 DD 报文的最大数量：

```
Switch(config)# router ipv6 ospf 100
Switch(config-router)# router-id 10.10.10.2
Switch(config-router)# max-concurrent-dd 10
```

## 相关命令

无

### 11.1.33 debug ipv6 ospf

使用该命令打开所有的 OSPFv3 调试开关。使用该命令的 **no** 形式关闭 OSPF 调试功能。

## 命令语法

```
debug ipv6 ospf (all)
no debug ipv6 ospf (all)
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch# debug ipv6 ospf
```

## 相关命令

无

### 11.1.34 debug ipv6 ospf events

使用该命令打开 OSPFv3 的事件调试开关。使用该命令的 **no** 形式关闭 OSPFv3 的事件调试功能。

## 命令语法

```
debug ipv6 ospf events (abr|asbr|nssa|os|router|vlink)
no debug ipv6 ospf events (abr|asbr|nssa|os|router|vlink)
```

<b>abr</b>	打开 ABR 调试开关
<b>asbr</b>	打开 ASBR 调试开关
<b>nssa</b>	打开 NSSA 调试开关
<b>os</b>	打开 OS 交互调试开关
<b>router</b>	打开路由器调试开关
<b>vlink</b>	打开虚链路调试开关

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch# debug ipv6 ospf events lsa
```

## 相关命令

无

### 11.1.35 debug ipv6 ospf ifsm

使用该命令打开 OSPFv3 的接口状态机调试开关。使用该命令的 **no** 形式关闭该功能的调试开关。

## 命令语法

**debug ipv6 ospf ifsm (status|events|timers)**

**no debug ipv6 ospf ifsm (status|events|timers)**

<b>status</b>	状态调试开关
<b>events</b>	事件调试开关
<b>timers</b>	定时器调试开关



## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch# debug ipv6 ospf ifsm timers
```

## 相关命令

无

### 11.1.36 debug ipv6 ospf nfsm

使用该命令打开 OSPFv3 的邻居状态机调试开关。使用该命令的 no 形式关闭该功能的调试开关。

## 命令语法

```
debug ipv6 ospf nfsm (status|events|timers)
```

```
no debug ipv6 ospf nfsm (status|events|timers)
```

<b>status</b>	状态调试开关
<b>events</b>	事件调试开关
<b>timers</b>	定时器调试开关

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch# debug ipv6 ospf nfsm timers
```

## 相关命令

无

### 11.1.37 debug ipv6 ospf lsa

使用该命令打开 OSPFv3 的链路状态通告(LSA)调试开关。使用该命令的 no 形式关闭该功能的调试开关。

## 命令语法

```
debug ipv6 ospf lsa (flooding|generate|install|maxage|refresh)
```

```
no debug ipv6 ospf lsa (flooding|generate|install|maxage|refresh)
```

<b>flooding</b>	LSA 泛洪调试开关
<b>generate</b>	LSA 生成调试开关
<b>install</b>	LSA 安装调试开关
<b>maxage</b>	LSA 老化调试开关
<b>refresh</b>	LSA 刷新调试开关

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch# debug ipv6 ospf lsa install
```

## 相关命令

无

### 11.1.38 debug ipv6 ospf packet

使用该命令打开 OSPFv3 的报文调试开关，使用该命令的 **no** 形式关闭该功能的调试开关。

## 命令语法

**debug ipv6 ospf packet** *PARAMETERS*

**no debug ipv6 ospf packet** *PARAMETERS*

*PARAMETERS* = **dd|detail|hello|ls-ack|ls-request|ls-update|recv|send**

<b>dd</b>	数据库描述报文调试开关
<b>detail</b>	报文详细信息调试开关
<b>hello</b>	hello 报文调试开关
<b>ls-ack</b>	链路状态确认报文调试开关
<b>ls-request</b>	链路状态请求报文调试开关
<b>ls-update</b>	链路状态更新报文调试开关
<b>recv</b>	打开报文接收的开关
<b>send</b>	打开报文发送的开关

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

Switch# debug ipv6 ospf packet dd send detail

## 相关命令

无

### 11.1.39 debug ipv6 ospf route

使用该命令打开路由计算调试开关，使用该命令的 **no** 形式关闭该功能的调试开关。

## 命令语法

**debug ipv6 ospf route (ase|ia|install|spf)**

**no debug ipv6 ospf route (ase|ia|install|spf)**

<b>ase</b>	外部路由计算调试开关
<b>ia</b>	域间路由计算调试开关
<b>install</b>	路由计算调试开关
<b>spf</b>	SPF 计算调试开关

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch# debug ipv6 ospf route install
```

## 相关命令

无

### 11.1.40 show debuggin ipv6 ospf

使用该命令查看 OSPFv3 的调试开关状态。

## 命令语法

**show debugging ipv6 ospf**

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面的例子显示了 OSPF 调试开关的状态信息。

```
Switch# show debugging ipv6 ospf
```

```
OSPFv3 debugging status:
  OSPFv3 all packet detail debugging is on
  OSPFv3 all IFSM debugging is on
  OSPFv3 all NFSM debugging is on
  OSPFv3 all LSA debugging is on
  OSPFv3 all route calculation debugging is on
  OSPFv3 all event debugging is on
```

## 相关命令

无

### 11.1.41 show resource ipv6 ospf

使用该命令来显示 OSPFv3 路由占用的硬件资源统计。

## 命令语法

```
show resource ipv6 ospf
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面的例子显示了使用命令 `show resource ipv6 ospf` 的输出结果：

```
Switch# show resource ipv6 ospf
```

```
OSPFv3
Resource                               Used           Capability
=====
Routes                                  16             1913
```

## 相关命令

```
show ipv6 ospf route summary
```

# RIPng 命令

## 11.1.42 router ipv6 rip

使用此命令使能 RIPng 功能或者进入 RIPng 配置模式，使用关键字 `no` 关闭 RIPng 功能。

## 命令语法

```
router ipv6 rip
```

```
no router ipv6 rip
```

## 命令模式

全局配置模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子讲述了使能 RIPng 功能。

```
Switch(config)# router ipv6 rip
```

## 相关命令

无

## 11.1.43 ipv6 router rip

使用此命令可以在某个接口下使能 RIPng 功能，使用关键字 **no** 关闭接口的 RIPng 功能。

### 命令语法

```
ipv6 router rip  
no ipv6 router rip
```

### 命令模式

端口配置模式

### 默认

无

### 使用说明

无

### 举例说明

下面例子讲述了在接口 eth-0-1 上使能 RIPng 功能。

```
Switch (config)# interface eth-0-1  
Switch (config-if)# no switchport  
Switch (config-if)# ipv6 router rip
```

### 相关命令

```
router ipv6 rip
```

## 11.1.44 ipv6 rip metric-offset

使用此命令用来给 RIPng 接口设置接收附加度量值，使用关键字 **no** 恢复默认的接口接收附加度量值。

### 命令语法

```
ipv6 rip metric-offset NUMBER-VALUE  
no ipv6 rip metric-offset NUMBER-VALUE
```

<i>NUMBER-VALUE</i>	默认附加度量值是 1，取值范围是 1~16。
---------------------	------------------------

## 命令模式

端口配置模式

## 默认

默认附加度量值是 1

## 使用说明

当收到一条合法的 RIPng 路由，在其加入到路由表之前，接口接收度量值会附加到该路由上，再加入路由表中，因此路由表中的度量值发生变化。即是说，增加一个接口的接收度量值，该接口收到的 RIPng 路由度量值也会相应增加。

## 举例说明

下面例子讲述了给 RIPng 接口设置接收附加度量值配置为 2。

```
Switch(config)#interface eth-0-1
```

```
Switch (config-if)# ipv6 rip metric-offset 2
```

## 相关命令

无

### 11.1.45 ipv6 rip split-horizon

使用此命令配置对 RIPng 更新报文进行水平分割或者水平分割对性逆转，使用关键字 `no` 关闭水平分割功能。

## 命令语法

```
ipv6 rip split-horizon (poisoned|)
```

```
no ipv6 rip split-horizon
```

<b>poisoned</b>	水平分割对性逆转
-----------------	----------

## 命令模式

端口配置模式

## 默认

默认使能水平分割毒性逆转功能



## 使用说明

当水平分割毒性反转被使能时，从一个接口学到的路由还可以从这个接口向外发布，但 `metric` 值必须为 16。当水平分割功能被配置时，从一个接口学到的路由不能通过此接口向外发布。

## 举例说明

下面例子讲述了使能 RIPng 水平分割功能。

```
Switch(config)# interface eth-0-1
```

```
Switch(config-if)# ipv6 rip split- horizon
```

## 相关命令

无

### 11.1.46 default-information originate

使用此命令用来生成一条缺省路由到 RIPng 路由域中，使用关键字 `no` 关闭此功能。

## 命令语法

```
default-information originate (route-map name)
```

```
no default-information originate
```

<b>route-map</b>	Route map 引用
------------------	--------------

## 命令模式

路由模式

## 默认

无

## 使用说明

生成的 RIPng 缺省路由将强制通过指定接口的路由更新报文发布出去。

## 举例说明

下面例子讲述了生成一条缺省路由到 RIPng 路由域。

```
Switch(config)# router ipv6 rip
```

```
Switch(config-router)# default-information originate
```

## 相关命令

无

### 11.1.47 default-metric

使用此命令用来为再发布引入的路由设置 RIPng 度量值，使用关键字 **no** 恢复默认值。

## 命令语法

**default-metric** *NUMBER-VALUE*

**no default-metric**

<i>NUMBER-VALUE</i>	默认度量值是 1, 范围是 1 ~ 16
---------------------	----------------------

## 命令模式

路由模式

## 默认

默认度量值为 1

## 使用说明

使用此命令用来为再发布引入的路由设置 RIPng 度量值。该命令要和重发布命令一起使用，这可以使再发布引入的所有路由的度量值是一样的。

## 举例说明

下面的例子中，在设备上同时启用了 RIPng 和 OSPFv3。同时在 RIPng 中重发布 OSPFv3，并将所有从 OSPFv3 引入的路由的度量值设为 10。

```
Switch(config)# router ipv6 rip
```

```
Switch(config-router)#default-metric 10
```

```
Switch(config-router)#redistribute ospfv3
```

## 相关命令

**redistribute (RIPng)**

### 11.1.48 distance

使用此命令设置加入 RIPng 域的路由管理距离 AD 值，使用关键字 **no** 恢复默认值。

## 命令语法

**distance** *DISTANCE*

**no distance**

<i>DISTANCE</i>	管理值范围为 1-255，管理距离为 255 的路由无效
-----------------	------------------------------

## 命令模式

路由模式

## 默认

默认值是 120

## 使用说明

类型	管理值
直连接口	0
静态路由	1
外部 BGP	20
OSPFv3	110
RIPng	120
内部 BGP	200
未知	255

管理距离表明了对一个路由源的信任度，它是从 0 到 255 之间的一个整数。一般情况下，值越高，信任等级越低。如果管理距离为 255，说明这个路由源不被信任，从这样的源来的所有路由都应该被忽略。

## 举例说明

下面例子讲述了配置 RIPng 域的路由管理距离值。

```
Switch(config)#router ipv6 rip
```

```
Switch(config-router)#distance 200
```

## 相关命令

无

### 11.1.49 neighbor

使用此命令定义一个用于交换路由信息的邻居路由器。使用关键字 **no** 删除该邻居路由器。

## 命令语法

**neighbor** *IP-ADDRESS* *INTERFACE-NAME*

**no neighbor** *IP-ADDRESS* *INTERFACE-NAME*

<i>IP-ADDRESS</i>	与此路由器直接相连的路由器 Link-local 地址
<i>INTERFACE-NAME</i>	在某个接口上指定 RIPng 邻居

## 命令模式

路由模式

## 默认

无

## 使用说明

更新报文以单播形式发送到对端，而不采用正常的组播的形式。通常情况下，要结合 **passive interface**（被动接口）一起使用。您可以配置多个 RIP 邻居。

## 举例说明

下面例子讲述了 RIPng 更新不会通过 eth-0-1 发送出去，然而 **neighbor** 命令可以使更新发送到和 eth-0-1 直连的某个 link-local 地址邻居。

```
Switch(config)#router ipv6 rip
```

```
Switch(config-router)# passive-interface eth-0-1
```

```
Switch(config-router)# neighbor fe80:db8::1 eth-0-1
```

## 相关命令

**passive-interface**

## 11.1.50 offset-list

设置接口接收或发送 RIPng 路由时的偏移度量值。使用此命令的 **no** 形式命令删除路由偏移度量值。

### 命令语法

**offset-list** *ACCESSS-LIST-NAME* (**in** | **out**) *METRIC-OFFSET* (*INTERFACE-NAME* |)

**no offset-list** (**in** | **out**) (*INTERFACE-NAME*|)

<i>ACCESSS-LIST-NAME</i>	访问控制列表
<b>in</b>	在进口方向应用
<b>out</b>	在出口方向应用
<i>METRIC-OFFSET</i>	应用到路由的偏移度量值
<i>INTERFACE-ID</i>	接口的 ID

### 命令模式

路由模式

### 默认

无

### 使用说明

如果偏移度量值生效，那么接口接收附加度量值的增加被忽略。偏移量列表可以用来改变路由的度量值，以达到某些目的（如做备份链路或者负载均衡）。

### 举例说明

下面例子讲述了在接口上设置 offset 列表以增加发送的路由的度量值：

```
Switch(config)# interface eth-0-1
```

```
Switch(config-if)# no switchport
```

```
Switch(config-router)# offset-list 21 out 10
```

### 相关命令

无

## 11.1.51 passive-interface

使用此命令设置端口上禁止发送 RIPng 更新报文，使用关键字 **no** 使能发送 RIPng 更新报文。

### 命令语法

**passive-interface** *INTERFACE-NAME*

**no passive-interface** *INTERFACE-NAME*

<i>INTERFACE-NAME</i>	接口名字
-----------------------	------

### 命令模式

路由模式

### 默认

默认不开启

### 使用说明

此命令关闭路由更新的发送功能，且忽略指定接口的邻居发送的 RIPng request 报文，但是指定接口的邻居发送的路由更新能正常的接受和处理。

### 举例说明

下面例子讲述了将 eth-0-1 设置为被动接口：

```
Switch(config)#router ipv6 rip
```

```
Switch(config-router)# passive-interface eth-0-1
```

### 相关命令

**neighbor**

## 11.1.52 redistribute

用此命令设置路由再发布。使用关键字 **no** 删除再发布的路由。

### 命令语法

**redistribute** *PROTOCOL* {[**metric** *VALUE*] | **route-map** *WORD* }

**no redistribute** *PROTOCOL*

<i>PROTOCOL</i>	可引入的源路由协议，包括 OSPF, BGP, static, connected
<b>metric</b> <i>VALUE</i>	所发布的路由的度量值
<b>route-map</b>	路由映射
<i>WORD</i>	路由映射名字

## 命令模式

路由模式

## 默认

无

## 使用说明

redistribute 命令中指定的 metric 值将会取代默认度量命令指定的度量值。

## 举例说明

设置重发布的静态路由的度量值为 10:

```
Switch(config)#router ipv6 rip
```

```
Switch(config-router)#redistribute static metric 10
```

## 相关命令

**default-metric**

### 11.1.53 timers basic

此命令用来配置 RIPng 各个定时器的值，可通过调节 RIPng 定时器来调整路由协议的性能，以满足网络需要。使用关键字 no 恢复设置为默认值。

## 命令语法

**timers basic** *UPDATE TIMEOUT INVALID*

**no timers basic**

<i>UPDATE</i>	路由更新时间
<i>TIMEOUT</i>	路由老化时间，如果在老化时间内没有收到关于某条路由的更新报文，则该条路由在路由表中的度量值将会被设置为 16，此时该条路由将不能用于转发报文

<i>INVALID</i>	路由的垃圾回收时间，定义了一条路由从度量值变为 16 开始，直到它从路由表里被删除所经过的时间。在垃圾回收时间内，RIPng 以 16 作为度量值向外发送这条路由的更新，如果垃圾回收定时器超时，该路由仍没有得到更新，则该路由将从路由表中被彻底删除
----------------	---

## 命令模式

路由模式

## 默认

路由更新时间：30 秒；

路由老化时间：180 秒；

路由的垃圾回收时间：120 秒。

## 使用说明

RIPng 协议的这些时间参数时可调整的。由于 RIPng 是一个分布式的，异步的路由协议，因此，各个定时器的值在网络中的所有路由器上需要保持一致。

## 举例说明

下面的例子设置 RIPng 路由的报文更新时间 5 秒，当超过 15 秒没有收到路由更新报文时，路由将失效。再过 15 秒，路由将从 RIPng 路由表中删除：

```
Switch(config)# router rip
```

```
Switch(config-router)# timers basic 5 15 15
```

## 相关命令

无

### 11.1.54 distribute-list

使用此命令过滤网络中路由更新，使用该命令的 no 形式恢复默认设置。

## 命令语法

**distribute-list** (*prefix name* | *ACCESSSS-LIST-NAME*) (*in|out*) (*INTERFACE-NAME* |)

**no distribute-list** (*prefix name* | *ACCESSSS-LIST-NAME*) (*in|out*) (*INTERFACE-NAME* |)

<i>prefix name</i>	过滤列表
--------------------	------



<i>ACCESSS-LIST-NAME</i>	访问控制列表名字
<b>in</b>	进口方向过滤
<b>out</b>	出口方向过滤
<i>INTERFACE-NAME</i>	接口名字

## 命令模式

路由模式

## 默认

无

## 使用说明

关键字 **in** 用于过滤接收的 RIPng 路由，关键字 **out** 用于过滤发送的 RIPng 更新报文。

## 举例说明

下面例子讲述了对所有的 RIPng 接收的路由进行过滤：

```
Switch(config)# router rip
```

```
Switch(config-router)# distribute-list ripng_acl in
```

## 相关命令

**ipv6 access-list**

### 11.1.55 aggregate-address

使用此命令用来配置 RIPng 在接口发布聚合 IPv6 地址。使用该命令的 **no** 形式取消配置的聚合地址。

## 命令语法

**aggregate-address** *IP-ADDRESS* (**avoid-feedback**) *INTERFACE-NAME*

**no aggregate-address** *IP-ADDRESS* *INTERFACE-NAME*

<i>IP-ADDRESS</i>	指定的聚合地址
<b>avoid-feedback</b>	禁止从此接口学习到相同的聚合路由
<i>INTERFACE-NAME</i>	接口名字

## 命令模式

路由模式

## 默认

无

## 使用说明

如果一条路由的前缀和前缀长度与定义的 IPv6 前缀匹配，则这个自定义的 IPv6 前缀将取代原来的路由被发布出去。这样，多条路由将由一条路由所代替，并且，这条路由的度量值是原多条路由中最低的。

通过指定 **avoid-feedback** 关键字，本接口将不再学习到和已发布的聚合 IP 地址相同的聚合路由，从而可以起到防止产生路由环路的作用。

该命令只有在接口为三层口时才生效。

## 举例说明

下面例子讲述了在接口 eth-0-1 配置一个 RIPng 聚合地址：

```
Switch(config)#router ipv6 rip
```

```
Switch(config-router)# aggregate-address 2001:db8::/32 avoid-feedback eth-0-1
```

## 相关命令

无

### 11.1.56 route map

使用此命令设置接口收到和发送 RIPng 路由的路由策略，使用该命令的 **no** 形式关闭配置的路由策略。

## 命令语法

```
route-map name (in|out) INTERFACE-NAME
```

```
no route-map name (in|out) INTERFACE-NAME
```

<i>name</i>	route map 名字
<b>in</b>	收到报文
<b>out</b>	发送报文
<i>INTERFACE-NAME</i>	指定接口名字

## 命令模式

路由模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子讲述了在接口 eth-0-1 设置收到报文后的路由策略。

```
Switch (config)# router ipv6 rip
```

```
Switch (config-router)# route-map routemap10 in eth-0-1
```

## 相关命令

无

### 11.1.57 maximum-prefix

使用此命令限制 RIPng 域能存储的最大路由条数，使用命令的 no 形式恢复默认设置。

## 命令语法

**maximum-prefix** *NUMBER-VALUE* (*PERCENTAGE-VALUE* )

**no maximum-prefix**

<i>NUMBER-VALUE</i>	RIPng 域能存储的最大路由条数,范围是 1~65535
<i>PERCENTAGE-VALUE</i>	设置告警百分比的值, 范围是 1~100, 默认值 75%。

## 命令模式

路由模式

## 默认

默认 RIPng 域能存储的最大路由条数，这个和芯片 profile 有关，默认告警百分比是 75%。

## 使用说明

无

## 举例说明

下面例子讲述了设置最大条数 700，告警百分比为 70%。

```
Switch (config)# router ipv6 rip
Switch (config-router)# maximum-prefix 700 70
```

## 相关命令

无

### 11.1.58 show ipv6 rip database

使用此命令显示 RIPng 域的信息。

## 命令语法

```
show ipv6 rip database
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子讲述了显示 RIPng 域的信息:

```
Switch# show ipv6 rip database
```

```
Codes: R - RIP, Rc - RIP connected, Rs - RIP static, Ra - RIP aggregated,
        Rcx - RIP connect suppressed, Rsx - RIP static suppressed,
        K - Kernel, C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP
Network                Next Hop                If      Met Tag  Time
Rc 2001:db8:0:6::/64    ::                      eth-0-9  1    0
Rc 2001:db8:0:49::/64  ::                      eth-0-48 1    0
```

## 相关命令

```
show ipv6 rip interface
```

## 11.1.59 show ipv6 rip interface

使用此命令显示已经使能 RIPng 的接口的信息。

### 命令语法

**show ipv6 rip interface** (*INTERFACE-NAME* | )

<i>INTERFACE-NAME</i>	接口名字
-----------------------	------

### 命令模式

特权模式

### 默认

无

### 使用说明

无

### 举例说明

下面例子讲述了显示已经使能 RIPng 的接口的信息：

```
Switch# show ipv6 rip interface eth-0-9
```

```
eth-0-9 is up, line protocol is up
  Routing Protocol: RIPng
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
  IPv6 interface address:
    2001:db8:0:6::2/64
    fe80::b4df:82ff:fe70:ec00/10
```

### 相关命令

无

## 11.1.60 show ipv6 rip database database-summary

使用此命令显示 RIPng 域的概要信息。

### 命令语法

**show ipv6 rip database database-summary**

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子讲述了显示 RIPng 域的概要信息:

```
Switch# show ipv6 rip database database-summary
```

Type	Count
RIPng connected	2
Total	2

## 相关命令

无

### 11.1.61 show ipv6 protocol rip

使用此命令显示 RIPng 协议的信息。

## 命令语法

```
show ipv6 protocol rip
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子讲述了显示 RIPng 协议的信息:

```
Switch# show ipv6 protocol rip
```

```

Routing Protocol is "ripng"
  Sending updates every 30 seconds with +/-50%, next due in 2949331570 seconds
  Timeout after 180 seconds, garbage collect after 120 seconds
  Outgoing update filter list for all interface is not set
  Incoming update filter list for all interface is not set
  Default redistribute metric is 1
  Redistributing:
  Interface
    eth-0-9
    eth-0-48
  Routing for Networks:
  Number of routes (including connected): 2
  Distance: (default is 120)

```

## 相关命令

无

### 11.1.62 debug ipv6 rip

使用此命令打开 RIPng debug 调试功能，主要包括 events 和 packet 选项，使用命令的 no 形式关闭 debug 功能。

## 命令语法

**debug ipv6 rip (all|events|packet |)**

**no debug ipv6 (all|events|packet |)**

**no debug all ipv6 (rip |)**

<b>all</b>	打开 RIP 的所有调试开关
<b>events</b>	打开 RIP 的事件调试开关
<b>packet</b>	RIP 报文调试开关，包括 recv, send 以及 detail
<b>recv</b>	接收报文的调试开关
<b>send</b>	发送报文的调试开关
<b>detail</b>	接收或发送报文的详细信息调试开关

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子讲述了如何打开 RIPng 报文的调试开关。

```
Switch# debug ipv6 rip packet
```

## 相关命令

无

### 11.1.63 show debugging ipv6 rip

使用此命令显示 RIPng 调试开关的状态信息。

## 命令语法

```
show debugging rip
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子讲述了显示了 RIPng 调试开关的状态信息。

```
Switch# show debugging ipv6 rip
RIPng debugging status:
  RIPng event debugging is on
```

## 相关命令

```
debug ipv6 rip
```

### 11.1.64 show resource ipv6 rip

使用此命令显示 RIPng 路由存储资源的使用情况。



## 命令语法

**show resource ipv6 rip**

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子讲述了显示 RIPng 路由存储资源的使用情况：

```
Switch# show resource ipv6 rip
```

RIPng Resource	Used	Capability
Routes	2	728

## 相关命令

无

### 11.1.65 clear ipv6 rip router

使用此命令清除掉 RIPng 域中的路由。

## 命令语法

**clear ipv6 rip router** (*IP-ADDRESS*|**connected**|**static**|**ospfv3**|**bgp**|**all**)

<i>IP-ADDRESS</i>	清除指定地址的路由
<b>connected</b>	清除再发布直连路由
<b>static</b>	清除再发布静态路由
<b>ospfv3</b>	清除再发布 ospf 路由
<b>bgp</b>	清除再发布 bgp 路由
<b>all</b>	清除所有路由

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子讲述了清除掉 RIPng 域中所有路由。

```
Switch# clear ipv6 rip route all
```

## 相关命令

无

## 11.2 IPv6 单播配置

### 11.2.1 ipv6 enable

使用该命令使能 IPv6。

使用该命令的 no 格式去使能 IPv6。

## 命令语法

**ipv6 enable**

**no ipv6 enable**

## 命令模式

全局配置模式

## 默认配置

IPv6 默认不使能。

## 使用说明

使用该命令全局使能 IPv6 功能。

当 IPv6 不使能时候，IPv6 报文被当做普通二层报文处理。

## 举例说明

以下例子使能了 IPv6 功能:

```
Switch (config)# ipv6 enable
```

## 相关命令

无

### 11.2.2 max-static-v6routes

使用该命令配置系统允许的最大 IPv6 静态路由数。

使用该命令的 no 格式恢复默认值。

## 命令语法

```
max-static-v6routes count
```

```
no max-static-v6routes
```

<i>count</i>	范围 1-65535。
--------------	-------------

## 命令模式

全局配置模式

## 默认配置

根据不同的 TCAM profile，默认值可能有所不同。

## 使用说明

可配最大值受限于当前的 TCAM profile。

也受限于当前已经存在的静态路由条目数。

## 举例说明

以下例子将最大静态路由条目数限制为 10 条:

```
Switch (config)# max-staticv6-routes 10
```

## 相关命令

### 11.2.3 ipv6 route

使用该命令配置静态 IPv6 路由。

使用该命令的 no 格式删除静态路由。

## 命令语法

```

ipv6 route DEST_PREFIX (NEXTHOP | IFTUNNEL)
ipv6 route DEST_PREFIX (NEXTHOP | IFTUNNEL) ADMIN_DISTANCE
ipv6 route DEST_PREFIX NEXTHOP INTERFACE
ipv6 route DEST_PREFIX NEXTHOP INTERFACE ADMIN_DISTANCE
no ipv6 route DEST_PREFIX NEXTHOP INTERFACE
no ipv6 route DEST_PREFIX NEXTHOP
no ipv6 route DEST_PREFIX

```

<i>DEST_PREFIX</i>	目的地址前缀。格式为 X:X::X:X/M
<i>NEXTHOP</i>	下一跳 IPv6 地址。格式为 X:X::X:X
<i>IFTUNNEL</i>	IPv6 路由出口的隧道接口名字
<i>INTERFACE</i>	IPv6 路由出接口名字
<i>ADMIN_DISTANCE</i>	(可选项) 管理距离。范围 1-255。默认值 1。

## 命令模式

全局配置模式

## 默认配置

默认情况下，系统没有任何 IPv6 静态路由。

## 使用说明

无

## 举例说明

以下例子配置了一些静态路由：

```
Switch (config)# ipv6 route 3001::1/64 fe80::1234 eth-0-2
```

```
Switch (config)# ipv6 route 3002::1/64 3001::1
```

## 相关命令

```
show ipv6 route
```

## 11.2.4 ipv6 address

使用该命令配置接口上的 ipv6 地址。

使用该命令的 no 格式删除 ipv6 地址。

### 命令语法

**ipv6 address** *GOLBAL\_FREFIX* ( **eui-64** | **anycast** | )

**no ipv6 address** *GOLBAL\_FREFIX* ( **eui-64** | )

ipv6 address *LINK-LOCAL* link-local

no ipv6 address *LINK-LOCAL* link-local

**ipv6 address auto** link-local

**no ipv6 address auto** link-local

**no ipv6 address**

参数	描述
<i>GOLBAL_FREFIX</i>	全球单播地址。格式为 X:X::X:X/M format
<i>LINK-LOCAL</i>	链路本地地址。格式为 X:X::X:X

### 命令模式

端口配置模式

### 默认配置

默认情况，接口未配 IPv6 地址。

### 使用说明

使用该命令配置接口上的 IPv6 地址，使用该命令的 no 格式移除 IPv6 地址。IPv6 地址配置和 IPv4 地址相互不影响。

每个接口最多可配 1 个链路本地地址，8 个全球单播地址。

当接口上没有任何 IPv6 地址的时候，使用 auto 关键字可自动生成链路本地地址。使用该命令的 no 格式、配合 auto 关键字，可删除自动生成的链路本地地址，前提是接口上已经没有任何全球单播地址了。

可以在配置的时候指定一个全球单播地址为 anycast。

可以在配置的时候指定一个全球单播地址使用 eui-64 方式生成接口 ID。

如果配置全球单播地址的时候接口没有任何链路本地地址，那么会自动生成一个。如果之后用户又手动指定链路本地地址，那么用户指定的优先级高于自动生成的，将会发生覆盖。

如果不带任何参数的使用该命令的 **no** 格式，接口上所有的 IPv6 地址都会被删除。

## 举例说明

以下例子在接口上配置了链路本地地址和全局单播地址：

```
Switch (config-if)# ipv6 address fe80::1233 link-local
```

```
Switch (config-if)# ipv6 address 3001:1::1234/64
```

## 相关命令

**show ipv6 interface**

### 11.2.5 show ipv6 route

使用该命令显示 IPv6 路由

## 命令语法

**show ipv6 route ( database | )**

**show ipv6 route ( database | ) ( bgp | connected | ospf | rip | static )**

**show ipv6 route *IPV6\_ADDRESS***

**show ipv6 route *IPV6\_PREFIX***

**show ipv6 route**

**show ipv6 route summary**

<i>IPV6_ADDRESS</i>	IPv6 前缀。格式为 X:X::X:X/M
<i>IPV6_PREFIX</i>	IPv6 地址。格式为 X:X::X:X

## 命令模式

特权模式

## 默认配置

无

## 使用说明

无

## 举例说明

以下为显示结果:

### Switch # show ipv6 route

```
IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, O - OSPF, I - IS-IS, B - BGP
      [*] - [AD/Metric]
Timers: Uptime
S      3001::/64 [1/0]
      via fe80::1234, eth-0-2, 04:09:56
C      3001:1::/64
      via ::, eth-0-1, 01:39:07
C      3001:1::1234/128
      via ::1, eth-0-1, 01:39:07
S      3002::/64 [1/0]
      via 3001::1 (recursive via fe80::1234), eth-0-2, 04:09:19
C      3ffe:2::/64
      via ::, eth-0-2, 1d19h37m
C      3ffe:2::10/128
      via ::1, eth-0-2, 1d19h37m
C      fe80::/10
      via ::, Null0, 1d19h53m
```

### Switch # show ipv6 route database

```
IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, O - OSPF, I - IS-IS, B - BGP
      [*] - [AD/Metric]
      > - selected route, * - FIB route, p - stale info
Timers: Uptime
S      > 3001::/64 [1/0]
      * via fe80::1234, eth-0-2, 04:10:45
C      > 3001:1::/64
      * via ::, eth-0-1, 01:39:56
C      > 3001:1::1234/128
      * via ::1, eth-0-1, 01:39:56
S      > 3002::/64 [1/0]
      * via 3001::1 (recursive via fe80::1234), eth-0-2, 04:10:08
C      > 3ffe:2::/64
      * via ::, eth-0-2, 1d19h37m
C      > 3ffe:2::10/128
      * via ::1, eth-0-2, 1d19h37m
C      > fe80::/10
      * via ::, Null0, 1d19h54m
```

### Switch # show ipv6 route static

```
IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, O - OSPF, I - IS-IS, B - BGP
      [*] - [AD/Metric]
Timers: Uptime
S      3001::/64 [1/0]
      via fe80::1234, eth-0-2, 04:11:42
S      3002::/64 [1/0]
      via 3001::1 (recursive via fe80::1234), eth-0-2, 04:11:05
```

**Switch # show ipv6 route 3001::64**

```
Routing entry for 3001::/64
  Known via "static", distance 1, metric 0, best
  Last update 04:12:32 ago
  * via fe80::1234, eth-0-2
```

**Switch # show ipv6 route 3001::64/64**

```
Routing entry for 3001::/64
  Known via "static", distance 1, metric 0, best
  Last update 04:13:03 ago
  * via fe80::1234, eth-0-2
```

**Switch # show ipv6 route summary**

```
IPv6 routing table name is Default-IPv6-Routing-Table(0)
IPv6 routing table maximum-paths is 8
Route source networks
connected      5
static         2
Total          7
```

## 相关命令

**ipv6 route**

## 11.2.6 show ipv6 interface

使用该命令显示接口上的 IPv6 状态

## 命令语法

```
show ipv6 interface ( IFNAME | ) ( brief | )
```

<i>IFNAME</i>	指定接口的 IPv6 状态与配置
---------------	------------------

## 命令模式

特权模式

## 默认配置

无

## 使用说明

无



## 举例说明

以下为显示结果:

```
Switch # show ipv6 interface eth-0-1

Interface eth-0-1
  Interface current state: UP
  The maximum transmit unit is 1500 bytes
  IPv6 is enabled, link-local address is fe80::1233
  Global unicast address(es):
    3001:1::1234, subnet is 3001:1::/64
  Joined group address(es):
    ff02::1:ff00:1234
    ff02::1:ff00:0
    ff02::1:ff00:1233
    ff02::2
    ff02::1
  ICMP error messages limited to one every 2000 milliseconds
  ICMP redirects are always sent
  ND DAD is enabled, number of DAD attempts: 1
  ND router advertisement is disabled
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND retransmit interval is 1000 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements max interval: 600 secs
  ND router advertisements min interval: 198 secs
  ND router advertisements live for 1800 seconds
  ND router advertisements hop-limit is 0
  Hosts use stateless autoconfig for addresses.
Switch # show ipv6 interface eth-0-1 brief
*down: administratively down
Interface      Status Protocol IPv6 address
eth-0-1        up      up      3001:1::1234
                                     fe80::1233
```

## 相关命令

**ipv6 enable**

**ipv6 address**

### 11.2.7 ipv6 verify unicast reverse-path

使用该命令在接口上使能 IPv6 URPF（反向路径检查）

使用该命令的 **no** 格式去使能 URPF。

## 命令语法

**ipv6 verify unicast reverse-path**

**no ipv6 verify unicast reverse-path**

## 命令模式

端口配置模式

## 默认配置

URPF 默认不使能。

## 使用说明

无

## 举例说明

以下例子使能了 URPF:

```
Switch (config-if)# ipv6 verify unicast reverse-path
```

## 相关命令

**show ipv6 interface**

## 11.2.8 ipv6 icmp error-interval

使用该命令配置 ICMP 报文间隔。

使用该命令的 no 格式恢复默认值。

## 命令语法

**ipv6 icmp error-interval** *ERROR\_INTERVAL*

**no ipv6 icmp error-interval**

<b>error-interval</b> <i>ERROR_INTERVAL</i>	ICMP 报文间隔。范围是 0 – 2147483647。单位毫秒。
--	------------------------------------

## 命令模式

全局配置模式

## 默认配置

1000 毫秒

## 使用说明

无

## 举例说明

以下例子配置了 ICMP 报文间隔：

```
Switch (config)# ipv6 icmp error-interval 2000
```

## 相关命令

无

## 11.3 Ipv6 Prefix-list 命令

### 11.3.1 ipv6 prefix-list

在全局配置模式下，使用命令 `ipv6 prefix-list` 创建地址前缀列表或添加表项。使用该命令的 `no` 形式删除配置。

## 命令语法

```
ipv6 prefix-list WORD (seq SEQUENCE-NUMBER) (deny | permit)
(any | IPv6-ADDRESS /M (ge GE-LENGTH) (le LE-LENGTH) )
no ipv6 prefix-list WORD (seq SEQUENCE-NUMBER) (deny | permit)
(any | IPv6-ADDRESS /M (ge GE-LENGTH) (le LE-LENGTH))
no ipv6 prefix-list WORD (seq SEQUENCE-NUMBER)
```

<b>WORD</b>	地址前缀列表表名
<b>seq SEQUENCE-NUMBER</b>	地址前缀列表表项序号，范围 1~65535。如果输入命令的时候没有指定序号，将添加默认序号。默认序号为 5 的倍数，并且是剩下序号中大于当前已分配序号的最小的数
<b>deny</b>	指定地址前缀列表的匹配模式为拒绝。在该模式下，如果过滤的 IPv6 地址在定义的范围之内，该 IPv6 地址不能通过过滤从而不能进入下一表项的测试；否则，将进行下一表项的测试
<b>permit</b>	指定地址前缀列表的匹配模式为允许。在该模式下，如果过滤的 IPv6 地址在定义的范围之内，则通过过滤，进行相应的设置；否则，必须进行下一表项的测试
<b>IPv6-ADDRESS /M</b>	网络地址和掩码位数。掩码位数范围 0~128
<b>ge GE-LENGTH</b>	指定地址匹配的最小前缀长度
<b>le LE-LENGTH</b>	指定地址匹配的最大前缀长度

## 命令模式

全局配置模式

## 默认

没有地址前缀列表被创建。

## 使用说明

地址前缀列表用于 IPv6 地址过滤。同一个地址前缀列表可包含多个表项，一个表项包括地址和掩码位数。命令中的 **deny** 和 **permit** 关键字指定该匹配结果是拒绝或者允许。此时，多个表项之间是“或”的关系，即通过一个表项就可通过该地址前缀列表的过滤。没有通过任何一个表项的过滤就意味着没有通过该地址前缀列表的过滤。

地址前缀范围包括两个部分，分别由 **mask-length** 和 **[greater-equal-value, less-equal-value]** 决定。如果指定了这两部分，要被过滤的 IPv6 地址必须匹配这两部分规定的前缀范围。具体的匹配公式如下：

`network/length < ge ge-length < le le-length <= 128`

例如，只指定 **ge-length**，则匹配范围为 **[ge-length,128]**；只指定 **le-length**，则匹配范围为 **[network/length, le-length]**；如果两者都指定，则匹配范围为 **[ge-length, le-length]**。

如果在输入命令中没有指定序号，则交换机会自动为表项添加默认序号。默认序号从 5 开始，并且每次递增 5，例如，5、10、15。默认序号将从当前大于已分配的序号中选择，并且是其中的最小值。

## 举例说明

- 配置匹配默认路由的拒绝表项：  
`Switch(config)# ipv6 prefix-list abc deny ::/0`
- 配置匹配 2001:db8::/64 的允许表项：  
`Switch(config)# ipv6 prefix-list abc permit 2001:db8::/64`
- 配置匹配长度为 [32,64]，地址为 2001:db8::/32 的允许表项：  
`Switch(config)# ipv6 prefix-list abc permit 2001:db8::/32 le 64`
- 配置匹配长度为 [64,128]，地址为 2001:db8::/32 的拒绝表项：  
`Switch(config)# ip prefix-list abc deny 2001:db8::/32 ge 64`

## 相关命令

**ipv6 prefix-list description**

**ipv6 prefix-list sequence**

**show ipv6 prefix-list**

**clear ipv6 prefix-list**

## 11.3.2 ipv6 prefix-list description

在全局配置模式下，使用命令 `ipv6 prefix-list description` 添加地址前缀列表描述。使用命令相关的 `no` 形式删除该配置。

### 命令语法

**ipv6 prefix-list** *WORD* *description* *LINE*

**no ipv6 prefix-list** *WORD* *description* (*LINE*)

WORD	地址前缀列表表名
LINE	地址前缀列表描述，范围 0~80

### 命令模式

全局配置模式

### 默认

地址前缀列表默认没有描述。

### 使用说明

如果该地址前缀列表不存在，交换机将会自动创建。

### 举例说明说明

配置地址前缀列表描述为：Deny routes from router A

```
Switch(config)# ipv6 prefix-list abc description Deny routes from router A
```

### 相关命令

**ipv6 prefix-list**

**ipv6 prefix-list sequence**

**show ipv6 prefix-list**

**clear ipv6 prefix-list**

## 11.3.3 ipv6 prefix-list sequence-number

在全局配置模式下，使用命令 `ipv6 prefix-list sequence-number` 启用地址前缀列表序号。使用命令相关的 `no` 形式关闭序号。

## 命令语法

```

ipv6 prefix-list sequence-number
no ipv6 prefix-list sequence-numbe

```

## 命令模式

全局配置模式

## 默认

地址前缀列表默认使用序号。

## 使用说明

该命令会使显示地址前缀列表配置的时候显示序号。

## 举例说明说明

配置启用地址前缀列表序号：

```
Switch(config)# ipv6 prefix-list sequence-number
```

## 相关命令

```

ipv6 prefix-list
show ipv6 prefix-list
clear ipv6 prefix-list

```

### 11.3.4 show ipv6 prefix-list

使用命令 show ipv6 prefix-list 显示当前地址前缀列表配置。

## 命令语法

```

show ipv6 prefix-list (summary | detail) (WORD)
show ipv6 prefix-list WORD (seq SEQUENCE-NUMBER| IPv6-ADDRESS /M (longer | first-match) )

```

summary	地址前缀列表统计摘要
detail	地址前缀列表详细统计
WORD	地址前缀列表表名
seq SEQUENCE-NUMBER	表项序号
IPv6-ADDRESS M	网络地址/掩码位数 e.g., 2001:db8::/32

longer	只显示掩码位数大于 M 的表项
first-match	只显示第一个匹配的表项

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明说明

显示地址前缀列表信息：

```
Switch# show ipv6 prefix-list
Switch# show ipv6 prefix-list
ipv6 prefix-list ripng_pre: 5 entries
  seq 1 deny 2001:db8:9::/64
  seq 2 deny 2001:db8:10::/64
  seq 3 deny 2001:db8:11::/64
  seq 4 deny 2001:db8:12::/64
  seq 5 permit any
```

## 相关命令

**ipv6 prefix-list**

**clear ipv6 prefix-list**

### 11.3.5 clear ipv6 prefix-list

使用 clear ipv6 prefix-list 清除地址前缀列表计数器的统计信息。

## 命令语法

**clear ipv6 prefix-list** (*WORD* (*IPv6-ADDRESS* /*M*))

WORD	地址前缀列表表名
IPv6-ADDRESS /M	网络地址/掩码位数 e.g., 2001:db8::/32

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明说明

重置地址前缀列表计数器:

```
Switch# clear ipv6 prefix-list abc
```

## 相关命令

**ipv6 prefix-list**

# 11.4 Route-map 命令

## 11.4.1 route-map

在全局配置模式下，使用 `route-map` 的 `match` 和 `set` 命令，来定义各个路由协议间进行重分布的条件，或者启用 BGP 协议的条件路由功能。删除 `route-map` 的条目，使用相应的 `no` 命令。

## 命令语法

```
route-map map-tag [permit | deny] [sequence-NUMBER]
```

```
no route-map map-tag [permit | deny] [sequence-NUMBER]
```

map-tag	Route-map 的一个有意义的名字。路由重分布命令使用这个名字来引用这个 route-map。多个 route-map 的序列可以共享同一个 route-map 名。Route-map 的名字长度不得超过 20，并且它的首字母必须是'a'-'z', 'A'-'Z'或者'0'-'9'
permit	(可选) 如果 route-map 的 match 规则被匹配到了，并且指定了 permit 关键字，这个路由将会像 set 动作所指定的规则那样进行重分布
deny	(可选) 如果 route-map 的 match 规则被匹配到了，这个路由将不会被重分布
sequence-	(可选) route-map 的序列号，表示这个 route-map 在同一个 route-



NUMBER	map 名中所处的位置。如果使用了相应的 no 命令，这个序列将会被删除
--------	--------------------------------------

## 命令模式

全局配置模式

## 默认

默认使用 permit 关键字。

## 使用说明

无

## 举例说明

下面的例子描述了如何创建一个 route-map 并进入 route-map 配置模式：

```
Switch(config)# route-map rip-to-ospf permit
```

```
Switch(config-route-map)# match metric 1
```

```
Switch(config-route-map)# set metric 2
```

## 相关命令

**match as-path**

**match community**

**match interface**

**match ip address**

**match local-preference**

**match metric**

**match origin**

**match route-type**

**match tag**

**set aggregator**

**set as-path**

**set atomic-aggregate**

**set comm-list**

**set community**

**set dampening**

**set extcommunity**  
**set ip address**  
**set local-preference**  
**set metric**  
**set metric-type**  
**set origin**  
**set originator-id**  
**set tag**  
**set vpv4**  
**set weight**

## 11.4.2 match as-path

使用这个命令来匹配一个自治系统路径的 ACL。

使用 `no` 参数来删除这个条目。

`match as-path` 命令制定了自治系统匹配的路径。如果设置了这条命令的 `permit` 规则，路由将会被 `set` 规则所重分布或者被控制。反正，如果 `match` 规则被匹配到，但是配置的是 `deny` 规则的话，路由将不会被重分布或者控制。如果没有任何 `match` 规则被匹配的话，这个路由将不会被重分布。

被 `route-map` 策略所指定的路由可能跟路由协议所指定的不一样。设置这种策略会让报文发往不同的路径，如何转发则取决于他们的长度和内容。被策略所转发的报文会覆盖路由表指定要转发的报文。



这个命令只在 BGP 协议中起作用。

### 命令语法

**match as-path** *LISTNAME*

**no match as-path**

LISTNAME	指定自治系统路径的 ACL 名
----------	-----------------

### 命令模式

Route-map 模式

## 默认

默认 `match as-path` 不设置。

## 使用说明

无

## 举例说明

```
Switch# configure terminal
Switch(config)# route-map myroute deny 34
Switch(config-route-map)# match as-path myaccesslist
```

## 相关命令

**match metric**  
**match ip address**  
**match community**  
**set as-path**  
**set community**

### 11.4.3 match community

使用这个命令来指定匹配的团体属性(`community`)号。

使用相应的 `no` 命令来删除这个条目。

`Community` 是用来过滤路由和建立路由组用的。他们用来在大规模的路由上使用 `match` 或者 `set` 命令来启用策略。`Community` 表使用一组路由的共通属性来识别和过滤这组路由。

`match community` 命令设置的 `match` 值会覆盖全局值，如果有路由没有满足任何一个 `match` 规则的话，这个路由将会被忽略。



这个命令只在 BGP 协议中起作用。

## 命令语法

**match community** *WORD*  
**no match community**

WORD	Community 表的名字
------	----------------

## 命令模式

Route-map 模式

## 默认

默认 match community 不设置。

## 使用说明

无

## 举例说明

```
Switch# configure terminal
Switch(config)# route-map myroute permit 3
Switch(config-route-map)# match community mylist
```

## 相关命令

**match ip address**

**match as-path**

**set as-path**

**set community**

**match metric**

### 11.4.4 match interface

使用这个命令来定义一个针对接口的 match 规则。

使用相应的 **no** 命令来删除这个规则。



#### NOTE

这个命令只在 BGP 协议中起作用。

## 命令语法

**match interface** *IFNAME*

**no match interface**

IFNAME	待匹配的接口名
--------	---------

## 命令模式

Route-map 模式

## 默认

默认 `match interface` 不设置。

## 使用说明

无

## 举例说明

```
Switch# configure terminal
Switch(config)# route-map mymap1 permit 10
Switch(config-route-map)# match interface eth-0-1
```

## 相关命令

**match tag**  
**match route-type external**

### 11.4.5 match ipv6 address

使用这个命令来指定 `match` 一个 ipv6 ACL 的规则。

使用相应的 `no` 命令来删除这个规则。

`match ipv6 address` 命令指定匹配了一个 ACL，如果指定了一个 `permit` 的 `match` 规则的话，路由将会被像 `set` 规则指定的那样进行重发布或者进行控制。反正，如果制定了相应的 `deny` 规则的话，满足条件的路由将不会被重发布或者控制。如果没有匹配到任何规则的话，路由将不会被接受或者转发。被策略指定的路由最好不要跟路由协议指定的路由一样。指定策略会导致报文根据他们的长度或者内容经过不同的路由转发。报文转发规则的优先级是策略转发大于普通的路由转发。



这个命令对 BGP, OSPFv3, RIPng 和策略路由(PBR)有效。

## 命令语法

**match ipv6 address ACCESSLISTID**

**no match ipv6 address**

ACCESSLISTID	指定 IPV6 ACL 名
--------------	---------------

## 命令模式

Route-map 模式

## 默认

默认 `match ipv6 address` 不设置。

## 使用说明

无

## 举例说明

```
Switch# configure terminal
Switch(config)# route-map myroute permit 3
Switch(config-route-map)# match ipv6 address List1
```

## 相关命令

**match community**

**match as-path**

**set as-path**

**set community**

**match metric**

### 11.4.6 match ipv6 address prefix-list

用这个命令来匹配 ipv6 前缀列表条目；使用相应的 `no` 命令来删除这个规则。

如果匹配了前缀并且指定是 `permit` 的语法的话，路由将会被重发布或者被 `set` 语法所受控。如果满足了 `match` 条件但是制定了 `deny` 语法的话，路由将不会被重发布或者被 `set` 语法受控。如果没有满足 `match` 条件，无论指定了 `permit` 还是 `deny` 语法，路由都不会被接收或者转发。

被指定的路由不能跟路由协议相同，指定的策略让报文能够按照他们的长度及内容通过不同的路由进行转发。相对于路由表指定的路径来说，报文将会优先以配置的策略来进行转发。



这个命令对 BGP, OSPFv3, RIPng 有效。

## 命令语法

**match ipv6 address prefix-list** *LISTNAME*

**no match ipv6 address prefix-list** [ *LISTNAME* ]

LISTNAME	IPv6 前缀列表名
----------	------------

## 命令模式

Route-map 模式

## 默认

默认 `match ipv6 addressprefix-list` 不设置。

## 使用说明

无

## 举例说明

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# match ipv6 address prefix-list mylist
```

## 相关命令

**match community**

**match as-path**

**set as-path**

**set community**

**match metric**

## 11.4.7 match ipv6 next-hop

使用这个命令来指定 `match` 一个下一跳的 IPv6 地址。

使用相应的 `no` 命令来删除这个规则。

如果匹配了 `nexthop` 地址并且指定是 `permit` 的语法的话，路由将会被重发布或者被 `set` 语法所受控。如果满足了 `match` 条件但是制定了 `deny` 语法的话，路由将不会被重发布或者被 `set` 语法受控。如果没有满足 `match` 条件，无论指定了 `permit` 还是 `deny` 语法，路由都不会被接收或者转发。



这个命令对 BGP, OSPFv3, RIPng 有效。

## 命令语法

**match ipv6 next-hop** (IPv6-ADDRESS | *ACCESSSLISTID*)  
**no match ipv6 next-hop** [IPv6-ADDRESS | *ACCESSSLISTID* ]

ACCESSSLISTID	指定 IPV6 ACL 名
IPv6-ADDRESS	IPv6 prefix, e.g., 2001:db8::1

## 命令模式

Route-map 模式

## 默认

默认 **match ip next-hop** 不设置。

## 使用说明

无

## 举例说明

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# match ipv6 next-hop mylist
```

## 相关命令

**match community**  
**match as-path**  
**set as-path**  
**set community**  
**match metric**

### 11.4.8 match ipv6 next-hop prefix-list

用这个命令来匹配下一跳的前缀列表条目。

使用相应的 **no** 命令来删除这个规则。



这个命令对 BGP, OSPFv3, RIPng 有效。



## 命令语法

```
match ipv6 next-hop prefix-list LISTNAME  
no match ipv6 next-hop prefix-list [ LISTNAME ]
```

LISTNAME	IPv6 前缀列表名
----------	------------

## 命令模式

Route-map 模式

## 默认

默认 `match ipv6 next-hop prefix-list` 不设置。

## 使用说明

无

## 举例说明

```
Switch# configure terminal  
Switch(config)# route-map mymap permit 3  
Switch(config-route-map)# match ipv6 next-hop prefix-list list1
```

## 相关命令

```
match metric  
match interface  
match ipv6 next-hop
```

### 11.4.9 match local-preference

使用这个命令来指定匹配本地优先级。使用相应的 `no` 命令来删除这个规则。



这个命令对 BGP 有效。

## 命令语法

```
match local-preference LOCAL-PREFERENCE  
no match local-preference
```

LOCAL-PREFERENCE	<0-4294967295> 指定优先级
------------------	----------------------

## 命令模式

Route-map 模式

## 默认

默认 match local-preference 不设置。

## 使用说明

无

## 举例说明

```
Switch# configure terminal
Switch(config)# route-map mymap permit 3
Switch(config-route-map)# match local-preference 100
```

## 相关命令

**match community**

**match as-path**

**set as-path**

**set community**

**match ip next-hop**

### 11.4.10 match metric

使用这个命令来 match metric 值。

使用相应的 no 命令来删除这个规则。

如果指定匹配了 metric 值并且指定是 permit 的语法的话，路由将会被重发布或者被 set 语法所受控。如果满足了 match 条件但是制定了 deny 语法的话，路由将不会被重发布或者被 set 语法受控。如果没有满足 match 条件，无论指定了 permit 还是 deny 语法，路由都不会被接收或者转发。



这个命令对 BGP, OSPF, RIP 有效。

## 命令语法

**match metric** *METRICVAL*

**no match metric**

METRICVAL	<+/-metric> <0-4294967295> metric 值
-----------	-------------------------------------

## 命令模式

Route-map 模式

## 默认

默认 **match metric** 不设置。

## 使用说明

无

## 举例说明

```
Switch# configure terminal
Switch(config)# route-map myroute permit 3
Switch(config-route-map)# no match metric
```

## 相关命令

**match community**

**match as-path**

**set as-path**

**set community**

**match ip next-hop**

### 11.4.11 match origin

使用这个命令来匹配 BGP 中的起始(origin)属性。

使用相应的 **no** 命令来删除这个规则。

Origin 属性定义了路径的起始信息。EGP 参数用路由表中的 e 来表示，这表明这一条路由的起始信息是从外部网关协议(EGP)中学习到的。同样的，IGP 参数用路由表中的 i 来表示，它表示起始路径信息是通过内部网关协议(IGP)学习到的。

在路由表中，不完整的(**incomplete**)会用?来表示，这就是说，这个路由的原始路径是通过不清楚或者其他别的方式来学习到的。比如，一个静态路由被重发布到 BGP 的话，那它的原始路由就是不完整的。



这个命令只对 BGP 有效。

## 命令语法

**match origin { egp | igp | incomplete }**

**no match origin**

egp	从 EGP 学到
igp	本地 IGP
incomplete	未知源

## 命令模式

Route-map 模式

## 默认

默认 **match origin** 不设置。

## 使用说明

无

## 举例说明

```
Switch# configure terminal
Switch(config)# route-map myroute deny 34
Switch(config-route-map)# match origin egp
```

## 相关命令

无

### 11.4.12 match route-type external

使用这个命令来匹配指定的外部路由类型。

使用相应的 **no** 命令来删除这个规则。

使用 **match route-type external** 命令来匹配指定的外部路由类型。自治系统外部 LSA 即是类型 1 或者是类型 2。外部类型 1 值匹配类型 1 的外部路由，外部类型 2 只匹配类型 2 的外部路由。



这个命令仅对 OSPF 有效。

## 命令语法

**match route-type external { type-1 | type-2 }**

**no match route-type external**

type-1	匹配 OSPF 外部类型 1 metric
type-2	匹配 OSPF 外部类型 2 metric

## 命令模式

Route-map 模式

## 默认

默认 **match route-type** 不设置。

## 使用说明

无

## 举例说明

```
Switch# configure terminal
Switch(config)# route-map mymap1 permit 10
Switch(config-route-map)# match route-type external type-1
```

## 相关命令

**match tag**

### 11.4.13 match tag

使用这个命令来匹配指定的 tag。

使用相应的 **no** 命令来删除这个规则。



这个命令对 OSPF, RIP 有效。

## 命令语法

**match tag** TAG

**no match tag**

TAG	<0-4294967295> 指定 tag 值
-----	-------------------------

## 命令模式

Route-map 模式

## 默认

默认 match tag 不设置。

## 使用说明

无

## 举例说明

```
Switch# configure terminal
Switch(config)# route-map mymap1 permit 10
Switch(config-route-map)# match tag 100
```

## 相关命令

**match metric**

**match route-type external**

### 11.4.14 set ipv6 aggregator

使用这个命令来设置 route-map 和 router ID 的 AS 号。

使用相应的 no 命令来删除这个规则。

自治系统(AS)是一个网络管理机构控制下的路由器和网络群组。他们被不同的区域所分离, 被指派了一个独特的 16 位的号码。使用 set aggregator as 命令来指定这个 AS 号码。

为了使用 `set aggregator` 命令，你必须首先要有一个 `match` 规则。`Match` 和 `set` 命令设置了路由协议间重发布路由的规则。`Match` 命令制定了在满足什么样的条件下才能进行重发布，而 `Set` 命令则指定了满足条件后所执行的动作。

如果报文没有满足任何定义的条件，他们将会被正常的路由所转发。



这个命令仅对 BGP 有效。

## 命令语法

```
set ipv6 aggregator as ASNUM IPv6-ADDRESS
```

```
no set ipv6 aggregator
```

ASNUM	<1-65535> 指定集合的 AS 号
Ipv6-ADDRESS	指定集合的 IPv6 地址

## 命令模式

Route-map 模式

## 默认

默认 `set aggregator` 不设置。

## 使用说明

无

## 举例说明

```
Switch# configure terminal
```

```
Switch(config)# route-map myroute permit 3
```

```
Switch(config-route-map)# set ipv6 aggregator as 43 2001:db8::1
```

## 相关命令

无

### 11.4.15 set as-path

使用这个命令来修改自治系统(AS)的路径。

使用相应的 `no` 命令来删除这个规则。

使用 `set as-path` 命令来指定一个 AS 的路径。通过指定 AS-Path 的长度，路由器可以影响路径的最佳路径选择。在这个命令中使用 `prepend` 参数，来在已有的 AS-Path 中，再追加一个指定的 AS-path。



这个命令仅对 BGP 有效。

## 命令语法

**set as-path prepend** *ASN* [...*ASN*]

**no set as-path**

ASN	追加自治系统的 AS-path
prepend	系统会将这个号码加到现有的 AS-path 中去

## 命令模式

Route-map 模式

## 默认

默认 `set as-path` 不设置。

## 使用说明

无

## 举例说明

```
Switch# configure terminal
Switch(config)# route-map myroute permit 3
Switch(config-route-map)# set as-path prepend 8 24
```

## 相关命令

无

### 11.4.16 set atomic-aggregate

使用这个命令来设置 `atomic aggregate` 属性。

使用相应的 `no` 命令来删除这个规则。

使用该命令你首先要有个 `match` 规则，`match` 和 `set` 规则同时作用来进行路由重分布。`Match` 命令指定向其他路由协议重发布路由的规则。`Set` 命令指定在当前 `route-map` 下路由重分布的表现方式。



如果报文没有匹配到任何条件，将会被通常的路由表转发。



这个命令对 BGP 有效。

## 命令语法

**set atomic-aggregate**

**no set atomic-aggregate**

## 命令模式

Route-map 模式

## 默认

默认 set atomic-aggregator 不设置。

## 使用说明

无

## 举例说明

```
Switch# configure terminal
```

```
Switch(config)# route-map rmap1 permit 3
```

```
Switch(config-route-map)# set atomic-aggregate
```

## 相关命令

无

### 11.4.17 set comm-list delete

使用这个命令来删除从进入或者外发更新时，满足条件的 community。

使用相应的 no 命令来删除这个规则。



这个命令仅对 BGP 有效。

## 命令语法

**set comm-list { <1-199>|<100-199>|WORD } delete**

**no set comm-list**

<1-199>	标准 comminty 列表号
<100-199>	扩展 community 列表号
WORD	Community 列表名
delete	删除匹配条件的 community

## 命令模式

Route-map 模式

## 默认

默认 set comm-list delete 不设置。

## 使用说明

无

## 举例说明

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set comm-list 34 delete
```

## 相关命令

无

### 11.4.18 set community

用这个命令来设置 comminty 属性。

使用相应的 no 命令来删除这个规则。

使用这个命令来设置 community 属性和在某个特定的 community 中的组目的地址，已经，根据这些 community 来应用路由选择。



这个命令对 BGP 有效。

## 命令语法

```
set community [ AA:NN | internet | local-AS | no-advertise | no-export ]
set community none
no set community
```

AA:NN	AA:NN: 用这样的格式来描述 community 号 AA = AS 号 NN = 指定的 community 号
internet	指定 Internet 这个 community(公认的 community)
local-AS	指定不发往 local AS 以外的 AS (公认的 community)
no-advertise	指定不把这个路由对对等体宣告 (公认的 community)
no-export	指定不把这个路由对下一个 AS 宣告 (公认的 community)
none	把通过这个 route-map 的 community 属性删除

## 命令模式

Route-map 模式

## 默认

默认 set community 不设置。

## 使用说明

无

## 举例说明

下面是使用 set community 时的例子：

```
Switch# configure terminal
```

```
Switch(config)# route-map rmap1 permit 3
```

```
Switch(config-route-map)# set community no-export no-advertise
```

```
Switch# configure terminal
```

```
Switch(config)# route-map rmap1 permit 3
```

```
Switch(config-route-map)# set community no-advertise
```

```
Switch# configure terminal
```

```
Switch(config)# route-map rmap1 permit 3
```

```
Switch(config-route-map)# set community 10:01 23:34 12:14 no-export
```

## 相关命令

无

## 11.4.19 set dampening

使用这个命令来使能 **route-flap** 惩罚，并且设置它的参数。

使用相应的 **no** 命令来删除这个规则。

设置不可达的半衰期(half-life time)大于等于可达的半衰期。抑制门限值必须要比重用门限值大。



这个命令仅对 BGP 有效。

### 命令语法

**set dampening** *REACHTIME REUSE SUPPRESS MAXSUPPRESS [ UNREACHTIME ]*

**no set dampening**

REACHTIME	<1-45> 用分来表示可达的半衰期。时间衰减是当前值的一半，默认 15 分钟
REUSE	<1-20000> 指定重用门限值。当被一种的路由的惩罚值衰减到重用门限值以下时，这个路由就不再被抑制。默认重用门限是 750
SUPPRESS	<1-20000> 指定抑制门限值。当一个路由的惩罚值超过抑制门限的时候，这个路由就被抑制了。默认的抑制门限是 2000
MAXSUPPRESS	<1-255> 指定最大抑制时间。一个被惩罚的路由的最大抑制时间。默认值是半衰期的 4 倍(60 分钟)
UNREACHTIME	<1-45> 指定不可达半衰期的惩罚值，默认 15 分钟

### 命令模式

Route-map 模式

### 默认

请参考命令语法中的描述。

### 使用说明

无

### 举例说明

Switch# configure terminal

```
Switch(config)# route-map R1 permit 24
Switch(config-route-map)# set dampening 20 333 534 30
```

## 相关命令

无

### 11.4.20 set extcommunity

使用这个命令来设置一个扩展的 `community` 属性。

使用相应的 `no` 命令来删除这个规则。

使用该命令你首先要有个 `match` 规则，`match` 和 `set` 规则同时作用来进行路由重分布。`Match` 命令指定向其他路由协议重发布路由的规则。`Set` 命令指定在当前 `route-map` 下路由重分布的表现方式。

如果报文没有匹配到任何条件，将会被通常的路由表转发。



这个命令对 BGP 有效。

## 命令语法

```
set extcommunity { rt | soo } EXTCOMMNUMBER [...EXTCOMMNUMBER ]
```

```
no set extcommunity { rt | soo }
```

<code>rt</code>	指定扩展 <code>community</code> 的扩展对象
<code>soo</code>	指定扩展 <code>community</code> 的 <code>site-of-origin</code> 属性
<code>EXTCOMMNUMBER</code>	ASN:NN 或者 IP-address:nn VPN 扩展 <code>comminty</code>
ASN:NN	AS 号
IPADDRESS	以 IP 地址形式表示的 AS 号

## 命令模式

Route-map 模式

## 默认

默认 `set extcommunity` 不设置。

## 使用说明

无

## 举例说明

```
Switch# configure terminal
Switch (config)# route-map rmap1 permit 3
Switch (config-route-map)# set extcommunity rt 06:01
Switch# configure terminal
Switch (config)# route-map rmap1 permit 3
Switch (config-route-map)# set extcommunity rt 0.0.0.6:01
Switch# configure terminal
Switch (config)# route-map rmap1 permit 3
Switch (config-route-map)# set extcommunity soo 06:01
Switch# configure terminal
Switch (config-route-map)# route-map rmap1 permit 3
Switch (config-route-map)# set extcommunity soo 0.0.0.6:01
```

## 相关命令

无

### 11.4.21 set ipv6 next-hop

使用这个命令来设置指定的 ipv6 下一跳的值。

使用相应的 **no** 命令来删除这个规则。

使用该命令你首先要有个 **match** 规则，**match** 和 **set** 规则同时作用来进行路由重分布。**Match** 命令指定向其他路由协议重发布路由的规则。**Set** 命令指定在当前 **route-map** 下路由重分布的表现方式。

如果报文没有匹配到任何条件，将会被通常的路由表转发。



这个命令对 BGP, OSPFv3, RIPng 和策略路由有效。

## 命令语法

```
set ipv6 next-hop [local] IPv6-ADDRESS
```

```
no set ipv6 next-hop [local]
```

local	Link-local address
IPv6-ADDRESS	指定下一跳的 IPv6 地址

## 命令模式

Route-map 模式

## 使用说明

无

## 默认

默认 set ipv6 next-hop 不设置。

## 举例说明

```
Switch# configure terminal
Switch(config)# route-map mymap permit 3
Switch(config-route-map)# set ipv6 next-hop 2001:db8::1
```

## 相关命令

无

### 11.4.22 set ipv6 next-hop load-share

使用这个命令来设置指定的 ipv6 多个下一跳并进行负载均衡的值。

使用相应的 no 命令来删除这个规则。

使用该命令你首先要有个 match 规则，match 和 set 规则同时作用来进行路由重分布。Match 命令指定向其他路由协议重发布路由的规则。Set 命令指定在当前 route-map 下路由重分布的表现方式。

如果报文没有匹配到任何条件，将会被通常的路由表转发。



这个命令对 BGP, OSPFv3, RIPng 和策略路由有效。

## 命令语法

```
set ipv6 next-hop [local] IPv6-ADDRESS IPv6-ADDRESS [IPv6-ADDRESS] load-share
no set ipv6 next-hop [local] load-share
```

local	Link-local address
IPv6-ADDRESS	指定下一跳的 IPv6 地址

## 命令模式

Route-map 模式

## 使用说明

最多指定四个下一跳

## 默认

默认 set ipv6 next-hop 不设置。

## 举例说明

```
Switch# configure terminal
```

```
Switch(config)# route-map mymap permit 3
```

```
Switch(config-route-map)# set ipv6 next-hop 2001:db8::1 2002::2 2003::3 load-share
```

## 相关命令

无

### 11.4.23 set local-preference

使用这个命令来设置本地优先级属性。

使用相应的 no 命令来删除这个规则。

使用该命令你首先要有个 match 规则，match 和 set 规则同时作用来进行路由重分布。Match 命令指定向其他路由协议重发布路由的规则。Set 命令指定在当前 route-map 下路由重分布的表现方式。

如果报文没有匹配到任何条件，将会被通常的路由表转发



这个命令仅对 BGP 有效。

## 命令语法

```
set local-preference LOCAL-PREFERENCE
```

```
no set local-preference
```



LOCAL-  
PREFERENCE <0-4294967295> 指定优先级

## 命令模式

Route-map 模式

## 默认

默认 set local-preference 不设置。

## 使用说明

无

## 举例说明

```
Switch# configure terminal
Switch(config)# route-map mymap permit 3
Switch(config-route-map)# set local-preference 100
```

## 相关命令

无

### 11.4.24 set metric

使用这个命令来设置一个路由的 metric 值。

使用相应的 no 命令来删除这个规则。

这个命令用于设置一条路由的 metric 值，以及关于一个关于 AS 的首选路径影响的外部邻居。首选路径是一个比较有较低 metric 值的路由。一个路由器比较在同一个 AS 中，邻居路径的 metric 值。比较不同的 AS 邻居的 metric 值，使用 bgp always-compare-med 命令。



这个命令仅对 BGP，OSPF 和 RIP 有效。

## 命令语法

**set metric** *METRICVAL*

**no set metric**

METRICVAL	<+/-metric> <0-4294967295> metric 值
-----------	-------------------------------------

## 命令模式

Route-map 模式

## 默认

默认 set metric 不设置。

## 使用说明

无

## 举例说明

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set metric 600
```

## 相关命令

无

### 11.4.25 set metric-type

使用这个命令来设置目的路由协议的 metric 类型。

使用相应的 no 命令来删除这个规则。

当 route-map 匹配的时候，这个命令设置在 AS-external-LSA 中设置 Type-1 或者 Type-2 两种类型。



这个命令仅对 OSPF 有效。

## 命令语法

**set metric-type {type1 | type2}**

**no set metric-type**

type1	选择设置外部类型 1 的 metric
type2	选择设置外部类型 2 的 metric

## 命令模式

Route-map 模式

## 默认

默认 set metric-type 不设置。

## 使用说明

无

## 举例说明

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set metric-type 1
```

## 相关命令

无

### 11.4.26 set origin

使用这个命令来设置 BGP origin 代码。

使用相应的 no 命令来删除这个规则。

Origin 属性定义了路径的起始信息。EGP 参数用路由表中的 e 来表示，这表明这一条路由的起始信息是从外部网关协议(EGP)中学习到的。同样的，IGP 参数用路由表中的 i 来表示，它表示起始路径信息是通过内部网关协议(IGP)学习到的。这个路由的原始路径是通过不清楚或者其他别的方式来学习到的。比如，一个静态路由被重发布到 BGP 的话，那它的原始路由就是不完整的。



这个命令仅对 BGP 有效。

## 命令语法

**set origin { egp | igp | incomplete }**

**no set origin**

egp	指定一个远程 EGP 系统
igp	一个本地的 IGP 系统
incomplete	指定一个不明确的继承关系的系统

## 命令模式

Route-map 模式

## 默认

默认 set origin 不设置。

## 使用说明

无

## 举例说明

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set origin egp
```

## 相关命令

无

### 11.4.27 set ipv6 originator-id

使用这个命令来设置 originator ID 属性。

使用相应的 no 命令来删除这个规则。

使用该命令你首先要有个 match 规则，match 和 set 规则同时作用来进行路由重分布。Match 命令指定向其他路由协议重发布路由的规则。Set 命令指定在当前 route-map 下路由重分布的表现方式。

如果报文没有匹配到任何条件，将会被通常的路由表转发。



#### NOTE

这个命令仅对 BGP 有效。

## 命令语法

```
set ipv6 originator-id Ipv6-ADDRESS
```

```
no set ipv6 originator-id
```

IPv6-ADDRESS	指定 originator 的 IPv6 地址
--------------	-------------------------

## 命令模式

Route-map 模式

## 默认

默认 set originator-id 不设置。

## 使用说明

无

## 举例说明

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set ipv6 originator-id 2001:db8::1
```

## 相关命令

无

### 11.4.28 set tag

使用这个命令来设置一个指定的 tag 值。

使用相应的 no 命令来删除这个规则。

在这个命令中的 tag，被另外一个路由协议(重分布时的 BGP 或者其他 IGP)所标签，原因是 AS-external-LSA 在它的 LSA 中有一个 route-tag 区。并且，使用 route-map 的话，ZebOS 会使用合适的 tag 值对这个 LSA 上打上标签。有时候，这个 tag 会匹配 route-map，有时候，这个值会被其他应用程序所使用。



这个命令仅对 OSPF 和 RIP 有效。

## 命令语法

**set tag** *TAGVALUE*

**no set tag**

TAGVALUE	<0-4294967295> 目的路由协议的 tag 号
----------	------------------------------

## 命令模式

Route-map 模式

## 默认

默认 set tag 不设置。

## 使用说明

无

## 举例说明

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set tag 6
```

## 相关命令

**redistribute**  
**default-information**

### 11.4.29 set vpnv6 next-hop

使用这个命令来设置一个 VPNv6 下一跳地址。

使用相应的 no 命令来删除这个规则。

在这个命令中的 tag，被另外一个路由协议(重分布时的 BGP 或者其他 IGP)所标签，原因是 AS-external-LSA 在它的 LSA 中有一个 route-tag 区。并且，使用 route-map 的话，ZebOS 会使用合适的 tag 值对这个 LSA 上打上标签。有时候，这个 tag 会匹配 route-map，有时候，这个值会被其他应用程序所使用。



这个命令仅对 BGP 有效。

## 命令语法

**set vpnv6 next-hop IPv6-ADDRESS**  
**no set vpnv6 next-hop**

IPv6-ADDRESS	指定下一跳 IPv6 地址
--------------	---------------

## 命令模式

Route-map 模式

## 默认

默认 set vpnv6 next-hop 不设置。

## 使用说明

无

## 举例说明

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set vpnv6 next-hop 2001:db8::1
```

## 相关命令

无

### 11.4.30 set weight

使用这个命令来设置路由表的应用权重(weight)。

使用相应的 no 命令来删除这个规则。

Weight 值是用于帮助进行最优路径选择的。它在路由器本地被之地你个。当有多个路由器，他们的目的地都相同时，有比较高权重的路由器将会被优先选中。



这个命令仅对 BGP 有效。

## 命令语法

**set weight** *WEIGHT*

**no set weight**

WEIGHT	<0-4294967295> 指定权重值
--------	----------------------

## 命令模式

Route-map 模式

## 默认

默认 set weight 不设置。

## 使用说明

无

## 举例说明

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set weight 60
```

## 相关命令

match as-path

### 11.4.31 show route-map

使用这个命令来显示用户可读的 route-map 信息。

## 命令语法

```
show route-map [ NAME ]
```

NAME	route-map 名
------	-------------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch1# show route-map
route-map abc, permit, sequence 10
  Match clauses:
    ip address acl1
  Set clauses:
```



```
    local-preference 200
route-map abc, permit, sequence 20
  Match clauses:
  Set clauses:
```

## 相关命令

**route-map**

# 12 IPv6 业务命令行

## 12.1 隧道配置命令

### 12.1.1 interface

使用该命令来创建一个 Tunnel 接口。使用该命令的 no 形式删除该 Tunnel 接口。

#### 命令语法

```
interface tunnel tunnelid
```

```
no interface tunnel tunnelid
```

tunnelid	接口编号，范围为 0~1023
----------	-----------------

#### 命令模式

全局配置模式

#### 默认

无

#### 使用说明

如果要通过 IPv4 网络来连接两个隔离的 IPv6 网络，首先要创建 Tunnel 接口。配置其他属性之后，此 Tunnel 接口可用。使能 IPv6 后就可以转发 IPv6 报文。

#### 举例说明

下面的例子显示了如何创建一个 Tunnel 接口：

```
Switch# configure terminal
```

```
Switch(config)# interface tunnel 1
```

## 相关命令

```
show interface tunnel
```

### 12.1.2 tunnel mode ipv6ip

使用该命令配置隧道模式。使用该命令的 `no` 形式恢复隧道模式默认值。

## 命令语法

```
tunnel mode ipv6ip (6to4 | isatap | gre | multi-dst-gre)
```

```
no tunnel mode
```

6to4	指定 6to4 隧道模式，这种隧道地址一般带有 2002::/16 的前缀
isatap	指定 ISATAP 隧道模式，这种隧道一般用于一个站点内，其地址格式一般为::5efe:A.B.C.D
gre	当配置 tunnel 的 destination 为一个的时候，对应的 tunnel 模式
multi-dst-gre	当配置 tunnel 的 destination 为多个的时候，对应的 tunnel 模式

## 命令模式

接口模式

## 默认

无

## 使用说明

当没有指定“**6to4**”或“**isatap**”关键字的时候为手工隧道模式。用户可以根据网络拓扑和应用来选择隧道模式。手动隧道为点到点模式，6to4 隧道和 ISATAP 隧道为点到多点模式。在一个节点中，如果要创建多个自动模式隧道，那么他们的隧道源必须不一样。如果要从 6to4 隧道切换为 ISATAP 隧道，并且此时系统已经配置了 6to4 中继的路由，则该切换不允许，必须先删除相关的 6to4 中继路由。

## 举例说明

下面的例子显示了如何配置隧道模式为 6to4:

```
Switch# configure terminal
Switch(config)# interface tunnel 1
Switch(config-if)# tunnel mode ipv6ip 6to4
```

## 相关命令

tunnel source  
tunnel destination

### 12.1.3 tunnel source

使用该命令来配置隧道的源地址，使用该命令的 no 形式删除隧道的源地址。

## 命令语法

tunnel source (A.B.C.D | X:X::X:X|IFNAME)  
no tunnel source

A.B.C.D	指定隧道的源地址为 IPv4 地址格式
X:X::X:X	指定隧道的源地址为 IPv6 地址格式
IFNAME	指定隧道的源地址从接口 IPv4/IPv6 地址中获得，如果接口上有多个地址，则只取主 IP 地址。接口可以为：路由口，vlan 虚拟口，环回口

## 命令模式

接口模式

## 默认

无

## 使用说明

每个隧道必须指定一个隧道源。如果隧道源是接口方式配置的，则从接口的主 IP 地址中获取地址。

## 举例说明

下面的例子显示了如何设置隧道源：

```
Switch# configure terminal
Switch(config)# interface tunnel 1
Switch(config-if)# tunnel source 3.3.3.3
```

## 相关命令

tunnel mode ipv6ip  
tunnel destination

## 12.1.4 tunnel destination

使用该命令来配置隧道的目的地址。使用该命令的 **no** 形式删除隧道的目的地址。

### 命令语法

```
tunnel destination (A.B.C.D| X:X::X:X)
```

```
no tunnel destination
```

A.B.C.D	指定 tunnel 接口的目的 IPv4 地址
X:X::X:X	指定 tunnel 接口的目的 IPv6 地址

### 命令模式

接口模式

### 默认

无

### 使用说明

只有手工隧道才需要配置隧道目的地址。

### 举例说明

下面的例子显示了如何配置隧道的目的地址：

```
Switch# configure terminal
Switch(config)# interface tunnel 1
Switch(config-if)# tunnel destination 4.4.4.4
```

### 相关命令

```
tunnel source
```

```
tunnel mode ipv6ip
```

## 12.1.5 tunnel enable

使用该命令设置使能解封装隧道报文的接口。使用该命令的 **no** 形式恢复默认设置。

### 命令语法

```
tunnel (enable|disable)
```

enable	使能隧道报文解封装
disable	去使能隧道报文解封装

## 命令模式

接口模式

## 默认

不会对收到的隧道报文解封装。

## 使用说明

无

## 举例说明

下面的例子显示了如何设置隧道报文解封装接口：

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# tunnel enable
```

## 相关命令

interface

### 12.1.6 tunnel gre key

配置 gre key 值，用于提高 GRE 隧道的安全性。

no tunnel gre key 删除该配置

## 命令语法

tunnel gre key *key\_value*

key_value	key 值<1-4294967295>
-----------	---------------------

## 命令模式

接口模式

## 默认

无

## 使用说明

需要提高 gre tunnel 安全性的时候，可以使用设置的 gre key 对隧道封装的报文进行端到端校验。

## 举例说明

配置 gre key 值：

```
Switch(config-if)# tunnel gre key 100
```

## 相关命令

```
show running-config interface tunnel
```

## 12.1.7 tunnel dscp

使用该命令设置外层 IPv4 头的 DSCP 值。使用该命令的 no 形式恢复从内层 IPv6 头获取 DSCP 的方式。

## 命令语法

```
tunnel dscp DSCP
```

```
no tunnel dscp
```

DSCP	设置外层 IPv4 头的 DSCP 值，范围 0~63
------	-----------------------------

## 命令模式

接口模式

## 默认

默认从内层 IPv6 头获取 DSCP 值。

## 使用说明

无

## 举例说明

下面的例子显示了如何设置外层 IPv4 头的 DSCP 值为 40：

```
Switch# configure terminal
Switch(config)# interface tunnel 1
Switch(config-if)# tunnel dscp 40
```

## 相关命令

tunnel ttl

### 12.1.8 ipv6 mtu

使用该命令静态配置 tunnel 接口上的 MTU 值。使用该命令的 no 形式恢复默认值。

## 命令语法

ipv6 mtu *MTU*

no ipv6 mtu

MTU	设置 tunnel 接口的 MTU 值，范围为 1280~9500
-----	-----------------------------------

## 命令模式

接口模式

## 默认

1480

## 使用说明

系统不支持路径发现 PMTU。该命令目前只能应用在 tunnel 接口上。

## 举例说明

下面的例子显示了如何将 tunnel 接口的 MTU 值设置为 1280:

```
Switch# configure terminal
Switch(config)# interface tunnel 1
Switch(config-if)# ipv6 mtu 1280
```

## 相关命令

tunnel ttl

### 12.1.9 show interface tunnel

使用该命令来显示 tunnel 接口的信息。

## 命令语法

show interface tunnel *tunnelid*



tunnelid	接口编号，范围 0~1023
----------	----------------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面的例子显示了 tunnel 接口的信息：

```
Switch# show interface tunnel1
Interface tunnel1
  Interface current state: UP
  Hardware is Tunnel
  Index 8193 , Metric 1 , Encapsulation TUNNEL
  VRF binding: not bound
  Tunnel protocol/transport IPv6/IP, Status Valid
  Tunnel source 1.1.1.1(eth-0-1), destination 2.2.2.2
  Tunnel DSCP inherit, Tunnel TTL 64
  Tunnel transport MTU 1480 bytes
```

## 相关命令

show ipv6 interface tunnel

### 12.1.10 show resource tunnel

使用该命令来显示 tunnel 资源的使用信息。

## 命令语法

```
show resource tunnel
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面的例子显示了 **tunnel** 资源的使用信息：

```
Switch# show resource tunnel
Tunnel
Resource                               Used           Capability
=====
Peers                                   1              32
```

## 相关命令

无

## 12.2 NDP 配置

### 12.2.1 ipv6 neighbor

使用该命令配置一条静态邻居。

使用该命令的 **no** 格式删掉静态邻居。

## 命令语法

**ipv6 neighbor IPV6ADDR MAC ( IFNAME | )**

**no ipv6 neighbor IPV6ADDR ( IFNAME | )**

<b>IPV6ADDR</b>	IPv6 地址。格式为 X:X::X:X
<b>MAC</b>	MAC 地址。格式为 HHHH.HHHH.HHHH
<b>IFNAME</b>	接口名

## 命令模式

全局配置模式

## 默认配置

默认情况下，系统没有任何静态邻居表项。

## 使用说明

使用此命令配置静态邻居表项。如果 **ipv6** 地址是一个链路本地地址，必须同时指定接

口。

此命令的 `no` 格式可以删除配置的静态邻居，对动态表项不起作用。

## 举例说明

这个例子添加了一条静态邻居表项：

```
Switch# configure terminal
Switch(config)# ipv6 neighbor 2001::1 0000.0000.0001
Switch(config)# ipv6 neighbor fe80::1 0000.0000.0002 eth-0-1
```

## 相关命令

**show ipv6 neighbors**

### 12.2.2 clear ipv6 neighbors

使用该命令清除动态邻居表项。

## 命令语法

**clear ipv6 neighbors ( interface *IFNAME* | )**

**clear ipv6 neighbors IPV6ADDR ( *INTERFACE* | )**

<b>interface <i>IFNAME</i></b>	清除指定接口的邻居表项
<b>IPV6ADDR</b>	IPv6 地址。格式为 X:X::X:X。清除指定地址的邻居表项
<b><i>INTERFACE</i></b>	为链路本地地址指定出接口

## 命令模式

特权模式

## 默认配置

无

## 使用说明

使用此命令清除动态邻居表项。

可以根据接口或地址来清除。

如果地址是链路本地地址，必须同时指定出口。

## 举例说明

这个例子清除了所有动态邻居表项：

```
Switch# clear ipv6 neighbors
```

## 相关命令

```
show ipv6 neighbors
```

### 12.2.3 ipv6 hop-limit

使用该命令设置 ipv6 报文的跳数限制。

使用该命令的 no 格式恢复默认设置。

## 命令语法

```
ipv6 hop-limit HOP_LIMIT
```

```
no ipv6 hop-limit
```

<b>hop-limit HOP_LIMIT</b>
----------------------------

跳数值。范围是 1-255
---------------

## 命令模式

全局配置模式

## 默认配置

默认值是 64。

## 使用说明

该配置影响所有本设备发出的 IPv6 报文的跳数字段。

除非上层应用（例如：OSPF）规定了报文的跳数。

## 举例说明

这个例子配置了跳数限制：

```
Switch(config)# ipv6 hop-limit 255
```

## 相关命令

无

## 12.2.4 ipv6 nd ra hop-limit

使用该命令设置 RA 报文中的“Current hop limit”字段。

使用该命令的 no 格式恢复默认值。

### 命令语法

**ipv6 nd ra hop-limit** *HOP\_LIMIT*

**no ipv6 nd ra hop-limit**

<b>hop-limit</b> <i>HOP_LIMIT</i>
-----------------------------------

设置 RA 报文的“Current hop limit”。范围是 0-255
--

### 命令模式

端口配置模式

### 默认配置

默认值是 0。

### 使用说明

无

### 举例说明

这个例子配置了 RA 报文的 Current hop limit 字段：

```
Switch(config-if)# ipv6 nd ra hop-limit 255
```

### 相关命令

无

## 12.2.5 ipv6 nd dad attempts

使用该命令配置重复地址探测（DAD）次数。

使用该命令的 no 格式恢复默认值。

### 命令语法

**ipv6 nd dad attempts** *DAD\_ATTEMPTS*

**no ipv6 nd dad attempts**

<i>DAD_ATTEMPTS</i>	设置探测次数。范围是 0-600
---------------------	------------------

### 命令模式

端口配置模式

### 默认配置

默认值是 1。

### 使用说明

使用该命令配置重复地址探测（DAD）次数。

0 表示不探测。

### 举例说明

这个例子配置了重复地址探测次数：

```
Switch(config-if)# ipv6 nd dad attempts 3
```

### 相关命令

无

## 12.2.6 ipv6 nd ns-interval

使用该命令配置 NS 报文间隔。

使用该命令的 no 格式恢复默认值。

### 命令语法

**ipv6 nd ns-interval** *NS\_INTERVAL*

**no ipv6 nd ns-interval**

<i>NS_INTERVAL</i>	设置 NS 报文的间隔。范围是 1000-3600000，单位是毫秒。
--------------------	-------------------------------------

### 命令模式

端口配置模式

## 默认配置

默认值是 1000。

## 使用说明

该配置影响重复地址检测和邻居发现过程中，NS 报文的间隔。

## 举例说明

这个例子配置了 NS 报文的间隔：

```
Switch(config-if)# ipv6 nd ns-interval 2000
```

## 相关命令

无

## 12.2.7 ipv6 nd ra suppress

使用该命令配置 RA 抑制。

使用该命令的 no 格式取消抑制。

## 命令语法

```
ipv6 nd ra suppress
```

```
no ipv6 nd ra suppress
```

## 命令模式

端口配置模式

## 默认配置

默认情况下 RA 抑制是使能的。

## 使用说明

使能 RA 抑制的时候系统不会发送任何 RA 报文。即使收到 RS 也不会回复。

## 举例说明

这个例子使能了 RA 抑制：

```
Switch(config-if)# ipv6 nd ra suppress
```

这个例子去使能了 RA 抑制：

```
Switch(config-if)# no ipv6 nd ra suppress
```

## 相关命令

**ipv6 nd ra interval**

**ipv6 nd ra lifetime**

## 12.2.8 ipv6 nd ra mtu suppress

使用该命令配置 RA 报文 mtu option 抑制。

使用该命令的 no 格式取消抑制。

## 命令语法

**ipv6 nd ra mtu suppress**

**no ipv6 nd ra mtu suppress**

## 命令模式

端口配置模式

## 默认配置

默认情况下 RA 报文 mtu option 不抑制。

## 使用说明

使能 RA 报文 mtu 抑制的时候，RA 报文中不带 mtu option。

## 举例说明

这个例子使能了 RA 报文 MTU option 抑制：

```
Switch(config-if)# ipv6 nd ra mtu suppress
```

这个例子去使能了 RA 报文 MTU option 抑制：

```
Switch(config-if)# no ipv6 nd ra mtu suppress
```

## 相关命令

无



## 12.2.9 ipv6 nd ra interval

使用该命令配置 RA 报文间隔。

使用该命令的 **no** 格式恢复默认值。

### 命令语法

**ipv6 nd ra interval** *MAX* (*MIN* |)

**no ipv6 nd ra interval**

<i>MAX</i>	最大报文间隔。范围是 4-1800。单位是秒。
<i>MIN</i>	最小报文间隔。范围是 3-1350。单位是秒。

### 命令模式

端口配置模式

### 默认配置

默认情况下最大间隔是 600 秒。最小间隔是最大间隔乘以 0.33。

### 使用说明

最大值的范围是 4-1800 秒。

最小值的范围是  $4-0.74 \times \text{最大值}$

最小值如果不配，当最大值大于等于 9 的时候取  $0.33 \times \text{最大值}$ ，小于 9 的时候就取最大值。

### 举例说明

这个例子配置了 RA 报文的间隔：

```
Switch(config-if)# ipv6 nd ra interval 300
```

### 相关命令

**ipv6 nd ra suppress**

**ipv6 nd ra lifetime**

## 12.2.10 ipv6 nd ra lifetime

使用该命令配置 RA 报文的 life time。

使用该命令的 no 格式恢复默认值。

### 命令语法

**ipv6 nd ra lifetime** *LIFE\_TIME*

**no ipv6 nd ra lifetime**

<i>LIFE_TIME</i>	配置 RA 报文的 life time。范围是 0-9000。单位是秒。
------------------	--------------------------------------

### 命令模式

端口配置模式

### 默认配置

默认情况下，life time 是最大 RA 报文间隔的三倍。

### 使用说明

无

### 举例说明

这个例子配置 RA 报文的 life time:

```
Switch(config-if)# ipv6 nd ra lifetime 1000
```

### 相关命令

**ipv6 nd ra suppress**

**ipv6 nd ra interval**

## 12.2.11 ipv6 nd reachable-time

使用该命令配置邻居处于 reachable 状态的时间。

使用该命令的 no 格式恢复默认值。

### 命令语法

**ipv6 nd reachable-time** *REACHABLE\_TIME*

**no ipv6 nd reachable-time**

<i>REACHABLE_TIME</i>	配置邻居处于 Reachable 的时间。范围是 0-3600000。单位是毫秒。
-----------------------	---

## 命令模式

端口配置模式

## 默认配置

默认值是 30000

## 使用说明

配置 0 表示使用默认值 30000

Reachable 时间到期以后，表项的状态将迁移到 stale

## 举例说明

这个例子配置了 reachable 时间：

```
Switch(config-if)# ipv6 nd reachable-time 3600000
```

## 相关命令

无

## 12.2.12 ipv6 nd managed-config-flag

使用该命令配置报文的"Managed address configuration"标志位。

使用该命令的 no 格式恢复默认值。

## 命令语法

**ipv6 nd managed-config-flag**

**no ipv6 nd managed-config-flag**

## 命令模式

端口配置模式

## 默认配置

默认情况"Managed address configuration"标记不置位。

## 使用说明

无

## 举例说明

这个例子配置了"Managed address configuration"标志:

```
Switch(config-if)# ipv6 nd managed-config-flag
```

## 相关命令

**ipv6 nd other-config-flag**

### 12.2.13 ipv6 nd other-config-flag

使用该命令配置报文的"Other address configuration"标志位。

使用该命令的 no 格式恢复默认值。

## 命令语法

**ipv6 nd other-config-flag**

**no ipv6 nd other-config-flag**

## 命令模式

端口配置模式

## 默认配置

默认情况"Other address configuration"标记不置位。

## 使用说明

无

## 举例说明

这个例子配置了"Other address configuration"标志:

```
Switch(config-if)# ipv6 nd other-config-flag
```

## 相关命令

**ipv6 nd managed-config-flag**

### 12.2.14 ipv6 nd prefix

使用该命令配置 RA 报文发布的前缀信息。

使用该命令的 no 格式删除前缀信息。

## 命令语法

**ipv6 nd prefix IPv6\_PREFIX ( VALID\_TIME | infinite ) ( PREFERRED\_TIME | infinite )**  
**( { off-link | no-autoconfig } | )**

**no ipv6 nd prefix IPv6\_PREFIX**

**ipv6 nd prefix default ( VALID\_TIME | infinite ) ( PREFERRED\_TIME | infinite ) ( { off-link | no-autoconfig } | )**

**no ipv6 nd prefix default**

<b>IPv6_PREFIX</b>	设置 IPv6 路由前缀。格式是 X:X::X:X/M
<b>VALID_TIME</b>	配置 Valid lifetime。范围是 0-4294967295。单位秒。
<b>PREFERRED_TIME</b>	配置 Preferred lifetime。范围是 0-4294967295。单位秒。

## 命令模式

端口配置模式

## 默认配置

valid life 的范围是 0-4294967295。

Infinity 表示 4294967295 (0xFFFFFFFF)

默认值是 2592000 秒 (30 天)。

preferred life 的范围是 0-4294967295。Infinity 表示 4294967295 (0xFFFFFFFF)

默认值是 604800 秒 (7 天)。

## 使用说明

无

## 举例说明

这个例子配置了一个前缀：

```
Switch(config-if)# ipv6 nd prefix 2001::1/64 3000 3000
```

## 相关命令

**show ipv6 interface IFNAME prefix**

## 12.2.15 show ipv6 interface IFNAME prefix

使用该命令显示指定接口上 RA 报文发布的前缀信息。

### 命令语法

**show ipv6 interface *IFNAME* prefix**

<i>IFNAME</i>	指定需要显示的接口名
---------------	------------

### 命令模式

EXEC

### 默认配置

无

### 使用说明

无

### 举例说明

显示结果如下：

```
Switch# show ipv6 interface eth-0-1 prefix
IPv6 Prefix Advertisements eth-0-1
Codes: A - Address, P - Prefix-Advertisement
D - Default, N - Not advertised
L - On link, A - Auto-config
default [LA] Valid lifetime 2592000, preferred lifetime 604800
P 2001::/64 [LA] Valid lifetime 3000, preferred lifetime 3000
```

### 相关命令

**ipv6 nd prefix**

## 12.2.16 show ipv6 neighbors

使用该命令显示邻居表项。

### 命令语法

**show ipv6 neighbors ( *dynamic* | *static* | *interface IFNAME* | *IPV6\_ADDR* | *statistics* | )**

<i>IFNAME</i>	指定需要显示的接口名
<i>IPV6_ADDR</i>	指定需要显示的 IPv6 地址。格式为 X:X::X:X

## 命令模式

EXEC

## 默认配置

无

## 使用说明

邻居表项可以全局显示。也可以根据接口或地址来显示。

动态和静态表项可以分开显示、

## 举例说明

显示结果如下：

```
Switch# show ipv6 neighbors
IPv6 address          Age      Link-Layer Addr State Interface
2001::2                7        40f2.fd60.ac00 REACH eth-0-9
fe80::42f2:fdff:fe60:ac00 6        40f2.fd60.ac00 STALE eth-0-9
```

## 相关命令

### ipv6 neighbor

## 12.2.17 debug ipv6 nd

使用该命令打开 ND 模块的调试信息。

使用该命令的 no 格式关闭调试信息。

## 命令语法

**debug ipv6 nd ( packet | events | error | dump | info | all )**

**no debug ipv6 nd ( packet | events | error | dump | info | all )**

packet	调试 IPv6 ND 的数据包信息
events	调试 IPv6 ND 事件信息
error	调试 IPv6 ND 错误信息
dump	以十六进制调试 IPv6 ND 的数据包信息
info	调试 IPv6 ND 提示信息
all	上面提到的所有调试信息

## 命令模式

特权模式

## 默认配置

默认调试信息不打开。

## 使用说明

无

## 举例说明

这个例子打开了 ND 模块的调试信息：

```
Switch# debug ipv6 nd all
Switch# terminal monitor
```

## 相关命令

无

# 12.3 DHCPv6 Relay 命令

## 12.3.1 dhcpv6 relay

在全局配置模式下，使用 `dhcpv6 relay` 命令来启用 DHCPv6 relay 服务。使用命令相应的 `no` 形式关闭该项功能。

## 命令语法

```
dhcpv6 relay
no dhcpv6 relay
```

## 命令模式

全局配置模式

## 默认

默认情况下此功能未打开。

## 使用说明

在启用 DHCPv6 relay 服务前，必需先使用 `dhcpv6 service` 命令使能 DHCPv6 功能，DHCPv6 relay 功能要在系统使能 DHCPv6 功能后才生效。



## 举例说明

启用 dhcpv6 relay 服务:

```
Switch(config)# dhcpv6 relay
```

## 相关命令

```
service dhcpv6
```

### 12.3.2 dhcpv6-server(全局)

在全局模式下使用 dhcpv6-server 命令创建 DHCPv6 服务器组。使用命令相应的 no 形式，删除一个 DHCPv6 服务器组。

## 命令语法

```
dhcpv6-server NUMBER ADDRESS interface IFNAME
```

```
no dhcpv6-server NUMBER (ADDRESS ( interface IFNAME ) )
```

NUMBER	DHCP 服务器组的序号，范围为 1 到 16
ADDRESS	加入服务器组中的 DHCP 服务器的 IP 地址列表。一个服务器组下 DHCP 服务器个数的范围为 1 到 8
IFNAME	支持的端口名称

## 命令模式

全局配置模式

## 默认

默认情况下，系统未设置任何 DHCPv6 服务器组。

## 使用说明

该命令用于配置远程 DHCPv6 服务器。注意 dhcpv6 server 功能和 dhcpv6 snooping 功能不要在同一个 vlan 上设置。

## 举例说明

在 DHCPv6 服务器组 1 中添加 DHCPv6 服务器:

```
Switch(config)# dhcpv6-server 1 2001:1::1
```

```
Switch(config)# dhcpv6-server 1 fe80::1 interface vlan1
```

## 相关命令

```
service dhcpv6
dhcpv6-server (interface)
```

### 12.3.3 dhcpv6-server (接口)

在接口模式下，使用 `dhcpv6-server` 命令将一个接口添加到一个 DHCPv6 服务器组中去。使用命令相应的 `no` 形式，将这个接口从 DHCPv6 服务器组中删除。

## 命令语法

```
dhcpv6-server NUMBER
no dhcpv6-server
```

NUMBER	DHCPv6 服务器组的序号，范围为 1 到 16
--------	---------------------------

## 命令模式

端口配置模式

## 默认

默认情况下，接口没有加到任何 DHCPv6 服务器组。

## 使用说明

该命令用于在接口启用全局模式下配置的 DHCPv6 服务器组。

## 举例说明

```
在接口启用 DHCPv6 服务器组 1:
Switch(config-if)# dhcpv6-server 1
```

## 相关命令

```
service dhcpv6
```

### 12.3.4 dhcpv6 relay remote-id option

在全局模式下，使用 `dhcpv6 relay remote-id option` 命令启用 `remote-id` 选项。使用命令相应的 `no` 形式取消该选项的启用。

## 命令语法

```
dhcpv6 relay remote-id option
```

no dhcpv6 relay remote-id option

## 命令模式

全局配置模式

## 默认

Remote-id 选项没有被启用。

## 使用说明

无

## 举例说明

配置 DHCPv6 中继启用 remote-id 选项：

```
Switch(config)# dhcpv6 relay remote-id option
```

## 相关命令

dhcpv6 relay remote-id format

### 12.3.5 dhcpv6 relay remote-id format

在全局模式下，使用 dhcpv6 relay remote-id format 命令，配置 remote-id 的格式。使用命令相应的 no 形式恢复默认格式。

## 命令语法

```
dhcpv6 relay remote-id format { vlan | ifname | duid }
```

```
no dhcpv6 relay remote-id format
```

vlan	Vlan ID
ifname	接收客户端报文的接口名称
duid	中继的 DUID

## 命令模式

全局配置模式

## 默认

默认情况下，不对 DHCPv6 报文插入 remote-id 选项。

## 使用说明

Remote-id 的格式可以是 vlan id, 接口名称, duid 三种关键字的组合, 可以设置需要显示在 remote-id 中的关键字。

## 举例说明

配置 remote-id 的格式:

```
Switch(config)# dhcpv6 relay remote-id format vlan
```

## 相关命令

```
dhcpv6 relay remote-id option
```

### 12.3.6 dhcpv6 relay pd route

在全局模式下, 使用 dhcpv6 relay pd route 启用中继通过 prefix-delegation 学习路由。使用命令相应的 no 形式关闭该功能。

## 命令语法

```
dhcpv6 relay pd route  
no dhcpv6 relay pd route
```

## 命令模式

全局配置模式

## 默认

默认情况下, 中继不会学习路由。

## 使用说明

DHCPv6 中继可以通过 prefix-delegation 学习路由。这种路由不会影响手动配置的静态路由。

## 举例说明

使能中继学习路由:

```
Switch(config)# dhcpv6 relay pd route
```

## 相关命令

```
clear dhcpv6 relay pd route
```

## 12.3.7 dhcpv6 relay pd route distance

在全局模式下，使用 `dhcpv6 relay pd route distance` 命令配置中继学习到的路由的默认管理距离。使用命令相应的 `no` 形式恢复为默认配置。

### 命令语法

```
dhcpv6 relay pd route distance <1-255>
```

```
no dhcpv6 relay pd route distance
```

### 命令模式

全局配置模式

### 默认

默认情况下，中继学习的路由的管理距离是 254。

### 使用说明

该命令配置 DHCPv6 中继添加路由的管理距离。

### 举例说明

配置 DHCPv6 中继添加路由时使用的管理距离：

```
Switch(config)# dhcpv6 relay pd route distance 233
```

### 相关命令

```
dhcpv6 relay pd route
```

## 12.3.8 service dhcpv6

在全局模式下，使用命令 `service dhcpv6` 使能 DHCP v6 中继代理功能。使用命令相应的 `no` 形式关闭 DHCPv6 中继代理功能。

### 命令语法

```
service dhcpv6 enable
```

```
service dhcpv6 disable
```

### 命令模式

全局配置模式

### 默认

默认情况下，未使能 DHCPv6 功能。

## 使用说明

只有在用 `service dhcpv6` 命令总开关使能了 DHCPv6 服务，`DHCPv6 relay` 等 DHCPv6 功能才会生效。

## 举例说明

配置全局使能 DHCPv6 功能：

```
Switch(config)# service dhcpv6 enable
```

## 相关命令

`dhcpv6 relay`

### 12.3.9 debug dhcpv6 relay

使用此命令可以打开 DHCPv6 relay 的模块的调试功能。

在原命令之前加上关键字 “no”，关闭调试功能。

## 命令语法

```
debug dhcpv6 relay ( events | error | packet | dump | all )
```

```
no debug dhcpv6 relay ( events | error | packet | dump | all )
```

events	调试 dhcpv6 relay 事件信息
error	调试 dhcpv6 relay 错误信息
packet	调试 dhcpv6 relay 的数据包信息
dump	以十六进制调试 dhcpv6 relay 的数据包信息
all	上面提到的所有调试信息

## 命令模式

特权模式

## 默认

无

## 使用说明

使用 “terminal monitor” 打印消息

## 举例说明

使用如下命令，打开 dhcpv6 relay 的所有调试信息。

```
Switch# debug dhcpv6 relay all
```

## 相关命令

terminal monitor

show logging buffer

### 12.3.10 show dhcpv6-server

在特权模式下，使用 show dhcpv6-server 命令查看 DHCPv6 服务器组的配置信息。

## 命令语法

```
show dhcpv6-server
```

## 命令模式

特权模式

## 默认

无

## 使用说明

该命令用于显示全局模式下使用 dhcpv6-server 命令配置的所有 DHCPv6 服务器组。

## 举例说明

在特权模式下使用 show dhcpv6-server 命令：

```
Switch# show dhcpv6-server
DHCPv6 server group information:
=====
group 1 ipv6 address list:
[1] 2001:1::1
```

## 相关命令

dhcpv6-server (global)

### 12.3.11 show dhcpv6 relay interfaces

在特权模式下，使用 show dhcpv6 relay interfaces 命令显示 DHCPv6 服务器组下的接口属性。

## 命令语法

```
show dhcpv6 relay interfaces
```

## 命令模式

特权模式

## 默认

无

## 使用说明

该命令用于显示属于 DHCPv6 中继的接口信息。

## 举例说明

在特权模式下使用 `show dhcpv6 relay interfaces` 命令：

```
Switch# show dhcpv6 relay interfaces
```

```
List of DHCPv6 relay enabled interface(s):
```

```
DHCPv6 relay service status: enabled
```

```
Interface Name          DHCPv6 server group
```

```
=====
```

```
eth-0-1                 1
```

## 相关命令

```
show dhcpv6-server
```

### 12.3.12 show dhcpv6 relay pd client

在特权模式下，使用 `show dhcpv6 relay pd client` 命令显示 DHCPv6 中继通过 prefix-delegation 学到的路由信息。

## 命令语法

```
show dhcpv6 relay pd client
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无



## 举例说明

在特权模式下使用 show dhcpv6 relay pd client 命令：

```
Switch# show dhcpv6 relay pd client

DHCPv6 prefix-delegation client information:
=====
Interface : vlan2
Client DUID : 0001000117e9357b606da182030
Client IPv6 address : fe80::626d:a1ff:fe82:300
    IA ID : a18230
        IA Prefix : 2002:2:10::/64
            preferred/max lifetime : 280/300
            expired time : 2012-09-17 11:43:59
=====
```

## 相关命令

```
dhcpv6 relay pd route
dhcpv6 relay pd route distance
```

### 12.3.13 show dhcpv6 relay statistics

在特权模式下，使用 show dhcpv6 relay statistics 命令显示交换机中继的 DHCPv6 报文统计信息。

## 命令语法

```
show dhcpv6 relay statistics
```

## 命令模式

特权模式

## 默认

无

## 使用说明

该命令用于显示交换机处理的 DHCPv6 统计的详情。

## 举例说明

在特权模式下使用 show dhcpv6 relay statistics 命令：

```
Switch# show dhcpv6 relay statistics

DHCPv6 relay packet statistics:
=====
Client relayed packets: 48
Server relayed packets: 48
```

```
Client error packets: 0
Server error packets: 0
```

## 相关命令

```
clear dhcp relay statistics
```

### 12.3.14 clear dhcpv6 relay statistics

在特权模式下，使用 `clear dhcpv6 relay statistics` 命令清除交换机中继的 DHCPv6 报文统计信息。

## 命令语法

```
clear dhcpv6 relay statistics
```

## 命令模式

特权模式

## 默认

无

## 使用说明

该命令用于清除交换机处理的 DHCPv6 统计的详情。

## 举例说明

在特权模式下使用 `clear dhcpv6 relay statistics` 命令：

```
Switch# clear dhcpv6 relay statistics
```

## 相关命令

```
show dhcpv6 relay statistics
```

### 12.3.15 clear dhcpv6 relay pd route

在特权模式下，使用 `clear dhcpv6 relay pd route` 命令清除交换机中继学习到的路由。

## 命令语法

```
clear dhcpv6 relay pd route (prefix PREFIX) (interface IFNAME) (ADDRESS)
```

PREFIX	DHCPv6 服务器分配给客户端的前缀
ADDRESS	DHCPv6 客户端的 IPv6 地址

IFNAME	支持的端口名称
--------	---------

## 命令模式

特权模式

## 默认

无

## 使用说明

若该命令不带参数，则删除所有 DHCPv6 中继学到的路由。

## 举例说明

在特权模式下使用 `clear dhcpv6 relay pd route` 命令：

```
Switch# clear dhcpv6 relay pd route interface eth-0-1
```

## 相关命令

`dhcpv6 relay pd route`

`show dhcpv6 relay pd client`

# 13 IPv6 组播命令行参考

## 13.1 IPv6 组播路由命令

### 13.1.1 ipv6 multicast-routing

使用此命令启用交换机的 IPv6 多播路由功能。使用关键字 **no** 禁用此功能。

#### 命令语法

```
ipv6 multicast-routing  
no ipv6 multicast-routing
```

#### 命令模式

全局配置模式

#### 默认

开启

#### 使用说明

无

#### 举例说明

启用交换机的IPv6多播路由功能.

```
Switch(config)# ipv6 multicast-routing
```

禁用交换机的IPv6多播路由功能.

```
Switch(config)# no ipv6 multicast-routing
```

#### 相关命令

无

## 13.1.2 ipv6 multicast route-limit

使用此命令设置IPv6组播路由的最大数目。使用关键字no恢复此项设置为默认值。

### 命令语法

**ipv6 multicast route-limit** *route-number* (*threshold-number*)

**no ipv6 multicast route-limit**

<i>route-number</i>	组播路由的最大数目，范围是 1 到 2048
<i>threshold-number</i>	超过阈值时生成警告消息，这个阈值应小于或等于组播路由的最大数量

### 命令模式

全局模式

### 默认

默认 IPv6 组播路由最大数目为 2048。

默认阈值应为 IPv6 组播路由的最大数量相同。

### 使用说明

无

### 举例说明

设置IPv6组播路由的最大数目为512。

```
Switch(config)# ipv6 multicast route-limit 512
```

设置IPv6组播路由的最大数目为默认值。

```
Switch(config)# no ipv6 multicast route-limit
```

### 相关命令

无

## 13.1.3 ipv6 mroute-rpf

此命令用于命令用来配置IPv6组播静态路由。使用关键字no来删除IPv6组播静态路由表中的IPv6组播静态路由。

## 命令语法

**ipv6 mroute-rpf** *source-address/mask-length* (**static** | **ripng** | **ospfv3** | ) *rpf-nbr-address*  
*distance*

**no ipv6 mroute-rpf** *source-address/ mask-length* (**static** | **ripng** | **ospfv3** | )

<i>source-address</i>	组播源地址
<i>mask-length</i>	掩码长度
<b>static</b>	静态路由
<b>ripng</b>	RIP 协议
<b>ospfv3</b>	OSPF 协议
<i>rpf-nbr-address</i>	RPF 邻居的 IPV6 地址
<i>distance</i>	路由优先级

## 命令模式

全局模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子显示如何设置组播源 2001::1/24 的 RPF 邻居地址是 2002::3。

```
Switch(config)# ipv6 mroute-rpf 2001::1/24 2002::3
```

## 相关命令

**show ipv6 mroute-rpf**

### 13.1.4 show ipv6 mroute

使用此命令查看多播路由表。

## 命令语法

**show ipv6 mroute** (**sparse**) (**count**|**summary**)

**show ipv6 mroute *address* (sparse) (count|summary)**

**show ipv6 mroute route-limit**

<b>sparse</b>	查看稀疏模式的多播路由
<b>count</b>	查看路由和数据包的统计情况
<b>summary</b>	查看多播路由的总体情况
<i>address</i>	源 IP 地址或者组播 IP 地址；查看此地址的路由
<b>route-limit</b>	查看路由数目的最大值

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子显示组播路由表信息。

Switch# show ipv6 mroute

```
IPv6 Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
Timers: Uptime/Stat Expiry
Interface State: Interface
2001:1::1234, ff0e::1234:5678
uptime 00:00:02, stat expires 00:03:28
Owner PIM-SMv6, Flags: TF
  Incoming interface: eth-0-1
  Outgoing interface list:
    Register
    eth-0-2
```

下面例子显示组播路由表总体信息。

Switch# show ipv6 mroute summary

```
IPv6 Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
Timers: Uptime/Stat Expiry
Interface State: Interface
```

```
2001:1::1234, ff0e::1234:5678
00:01:04/00:02:26, PIM-SMv6, Flags: TF
```

## 相关命令

无

### 13.1.5 show ipv6 mif

使用此命令查看IPv6的多播接口信息。

## 命令语法

```
show ipv6 mif (IFNAME |)
```

<i>IFNAME</i>	接口名称
---------------	------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子查看所有 IPv6 多播接口信息。

```
Switch# show ipv6 mif
```

Interface	Mif Idx	Owner Module	Uptime
eth-0-1	0	PIM-SMv6	00:00:05
Register	1	PIM-SMv6	00:00:05

## 相关命令

无

### 13.1.6 show ipv6 multicast groups count

此命令用于显示IPv6组播组数目。



## 命令语法

**show ipv6 multicast groups count**

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面的例子显示当前的 IPv6 组播组数目。

```
Switch# show ipv6 multicast groups count
```

```
multicast group record count: 1
multicast source record count: 0
multicast total record count: 1
multicast max record count: 2048
```

## 相关命令

无

## 13.1.7 show ipv6 mroute-rpf

使用此命令查看IPv6多播路由的反向路径查询。

## 命令语法

**show ipv6 mroute-rpf *source-address***

<i>source-address</i>	IPv6 多播源地址
-----------------------	------------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

查看 IPv6 多播源地址为 2001:5::1 的反向路径查询。

```
Switch# show ipv6 mroute-rpf 2001:5::1
```

```
RPF information for 2001:5::1
RPF interface: eth-0-1
RPF neighbor: 2001:1::2
RPF route: 2001:5::/64
RPF type: static
RPF recursion count: 0
Doing distance-preferred lookups across tables
Distance: 0
Metric: 0
```

## 相关命令

**ipv6 mroute-rpf**

### 13.1.8 show resource mcast6

此命令用于显示IPv6组播路由资源使用情况。

## 命令语法

**show resource mcast6**

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子显示 IPv6 组播路由资源使用情况。

```
Switch# show resource mcast6
```

```
MCAST
Resource                               Used           Capability
=====
```

Mcast Entry	0	224
Mcast Member	0	1792
相关命令		
无		

## 13.2 MLD 命令

### 13.2.1 ipv6 mld access-group

此命令根据访问控制列表对加入 IPv6 组播组的主机或可以加入的 IPv6 组播组进行限制。使用关键字 **no** 取消此种限制。

#### 命令语法

**ipv6 mld access-group** *list*

**no ipv6 mld access-group**

<i>list</i>	访问控制列表名称
-------------	----------

#### 命令模式

端口配置模式

#### 默认

无

#### 使用说明

使用 IPv6 访问控制列表来控制 MLD 报文的学习。

#### 举例说明

在 VLAN1 的端口上根据访问控制列表 **acl1** 对可加入 IPv6 组播组的主机和可加入的 IPv6 组播组进行限制。

```
Switch(config-if)# interface vlan 1
```

```
Switch(config-if)# ipv6 mld access-group acl1
```

取消在 VLAN1 的端口上的限制。

```
Switch(config-if)# no ipv6 mld access-group
```

## 相关命令

**show ipv6 mld interface**

### 13.2.2 ipv6 mld immediate-leave group-list

此命令根据访问控制列表限制可快速离开的主机和主机可快速离开的IPv6组播组。使用关键字no取消此种限制。

## 命令语法

**ipv6 mld immediate-leave group-list** *list*

**no ipv6 mld immediate-leave**

<i>list</i>	访问控制列表名称
-------------	----------

## 命令模式

端口配置模式

## 默认

无

## 使用说明

假如 ACE' s 的行为是拒绝, 数据包将会被忽略; 此外, ACE' s 的行为如果允许的话, 那么数据包正常转发。

## 举例说明

在 VLAN1 端口上限制可快速离开的主机和主机可快速离开的 IPv6 组播组。

```
Switch(config-if)# interface vlan 1  
Switch(config-if)#ipv6 mld immediate-leave group-list acl1
```

在 VLAN1 端口上取消此种限制。

```
Switch(config-if)#no ipv6 mld immediate-leave group-list
```

## 相关命令

**show ipv6 mld interface**

### 13.2.3 ipv6 mld last-member-query-count

使用此命令设置当IPv6组播组的最后一个成员离开后所发送的特定组查询报文的数量；如果在发送完所有的成员查询报文后，仍然没有收到成员报告报文，则端口会退出此IPv6多播组。使用关键字no恢复成员查询报文的数量为默认值。

#### 命令语法

**ipv6 mld last-member-query-count** *count*

**no ipv6 mld last-member-query-count**

<i>count</i>	特定组查询报文的数目，范围是 2 到 7
--------------	----------------------

#### 命令模式

端口配置模式

#### 默认

2

#### 使用说明

无

#### 举例说明

设置发送成员查询报文的最大数目为 5。

```
Switch(config-if)# ipv6 mld last-member-query-count 5
```

恢复发送成员查询报文的数目为默认值。

```
Switch(config-if)# no ipv6 mld last-member-query-count
```

#### 相关命令

**show ipv6 mld interface**

**ipv6 mld last-member-query-interval**

### 13.2.4 ipv6 mld last-member-query-interval

使用此命令设置当IPv6组播组的最后一个成员离开后，发送特定组查询报文的间隔。使用关键字no恢复此间隔为默认值。

## 命令语法

**ipv6 mld last-member-query-interval** *interval*

**no ipv6 mld last-member-query-interval**

<i>interval</i>	特定组查询报文的间隔 (毫秒), 范围是 1000 到 25500
-----------------	-----------------------------------

## 命令模式

端口配置模式

## 默认

1000 毫秒

## 使用说明

无

## 举例说明

设置端口发送组成员查询报文的时间间隔是 10000ms。

```
Switch(config-if)# ipv6 mld last-member-query-interval 10000
```

恢复端口发送组成员查询报文的时间间隔默认值。

```
Switch(config-if)# no ipv6 mld last-member-query-interval
```

## 相关命令

**show ipv6 mld interface**

**ipv6 mld last-member-query-count**

### 13.2.5 ipv6 mld limit

使用此命令设置全局或端口上可加入的IPv6组播组的最大个数。使用关键字no恢复此设置为默认值。

## 命令语法

**ipv6 mld limit** *number* **except** *list*

**no ipv6 mld limit**

<i>number</i>	全局或端口上可加入的组播组的最大个数
---------------	--------------------

<i>list</i>	组播组在这个访问控制列表中时不做数目限制
-------------	----------------------

## 命令模式

全局模式和端口配置模式

## 默认

4096

## 使用说明

默认情况下，端口可加入的组播组的最大数目是 4096。

在全局配置模式下，设置所有端口可加入的 IPv6 组播组的最大数目。

在端口配置模式下，设置此端口可加入的 IPv6 组播组的最大数目。

## 举例说明

设置所有端口可加入的 IPv6 组播组的最大个数为 1000。

```
Switch(config)# ipv6 mld limit 1000
```

设置所有端口可加入的 IPv6 组播组的最大个数为默认值。

```
Switch(config)# no ipv6 mld limit
```

## 相关命令

**show ipv6 mld interface**

### 13.2.6 ipv6 mld mroute-proxy

使用此命令设置本端口的MLD代理的上行端口。

## 命令语法

**ipv6 mld mroute-proxy *IFNAME***

**no ipv6 mld mroute-proxy *IFNAME***

<i>IFNAME</i>	端口名称，指定的上行端口
---------------	--------------

## 命令模式

端口配置模式

## 默认

无

## 使用说明

一个端口只能设置一个上行代理端口。多次设置时，后面的设置会覆盖前面的设置。

## 举例说明

设置本端口的上行代理端口为 eth-0-1

```
Switch(config-if)# ipv6 mld mroute-proxy eth-0-1
```

删除本端口的上行代理端口

```
Switch(config-if)# no ipv6 mld mroute-proxy
```

## 相关命令

**ipv6 mld proxy-service**

### 13.2.7 ipv6 mld proxy-service

使用此命令启用端口的MLD代理服务。使用关键字no关闭此服务。

## 命令语法

**ipv6 mld proxy-service**

**no ipv6 mld proxy-service**

## 命令模式

端口配置模式

## 默认

无

## 使用说明

此命令与 ipv6 mld mroute-proxy 配合使用，用来设定交换机的 MLD 代理上联口。

## 举例说明

启用此端口的 MLD 代理服务的上联口。

```
Switch(config-if)# ipv6 mld proxy-service
```

关闭此端口作为 MLD 代理服务的上联口。

```
Switch(config-if)# no ipv6 mld proxy-service
```



## 相关命令

**ipv6 mld mroute-proxy**

### 13.2.8 ipv6 mld querier-timeout

使用此命令设置Querier的超时时间。使用关键字no恢复此超时时间为默认值。

## 命令语法

**ipv6 mld querier-timeout** *intval*

**no ipv6 mld querier-timeout**

<i>intval</i>	超时时间，以秒为单位，范围是 60 到 300 秒
---------------	---------------------------

## 命令模式

端口配置模式

## 默认

255 秒

## 使用说明

无

## 举例说明

设置 Querier 的超时时间为 100 秒。

```
Switch(config-if)# ipv6 mld querier-timeout 100
```

恢复 Querier 的超时时间为默认值。

```
Switch(config-if) #no ipv6 mld querier-timeout
```

## 相关命令

**ipv6 mld query-interval**

**ipv6 mld query-max-response-time**

### 13.2.9 ipv6 mld query-interval

使用此命令设置端口发送Querier查询报文的时间间隔。使用关键字no恢复此时间间隔为默认值。

## 命令语法

**ipv6 mld query-interval** *intval*

**no ipv6 mld query-interval**

<i>intval</i>	端口发送 Querier 查询报文的时间间隔，以秒为单位，范围是 2 到 18000 秒
---------------	--

## 命令模式

端口配置模式

## 默认

125 秒

## 使用说明

无

## 举例说明

设置发送 Querier 查询报文的时间间隔为 300 秒。

```
Switch(config-if)# ipv6 mld query-interval 300
```

恢复此时间间隔为默认值。

```
Switch(config-if)# no ipv6 mld query-interval
```

## 相关命令

**ipv6 mld querier-timeout**

**ipv6 mld query-max-response-time**

### 13.2.10 ipv6 mld query-max-response-time

使用此命令设置查询报文的最大响应时间；要求成员在此时间范围内必须响应一个报告消息。使用关键字 **no** 恢复此最大响应时间为默认值。

## 命令语法

**ipv6 mld query-max-response-time** *intval*

**no ipv6 query-max-response-time**

<i>intval</i>	查询报文的最大响应时间，以秒为单位，范围是 1 到 25 秒
---------------	--------------------------------

## 命令模式

端口配置模式

## 默认

10 秒

## 使用说明

无

## 举例说明

设置查询报文的最大响应时间为 20 秒。

```
Switch(config-if)# ipv6 mld query-max-response-time 20
```

恢复此最大响应时间为默认值。

```
Switch(config-if)# no ipv6 mld query-max-response-time
```

## 相关命令

**ipv6 mld querier-timeout**

**ipv6 mld query-interval**

### 13.2.11 ipv6 mld robustness-variable

使用此命令设置MLD查询器的健壮系数。使用关键字no恢复此项设置为默认值。

## 命令语法

**ipv6 mld robustness-variable *value***

**no ipv6 robustness-variable**

<i>value</i>	设定 MLD 报文的健壮程度，范围是 2 到 7
--------------	--------------------------

## 命令模式

端口配置模式

## 默认

2

## 使用说明

无

## 举例说明

设置 MLD 查询器的健壮系数为 6。

```
Switch(config-if)# ipv6 mld robustness-variable 6
```

恢复此设置到默认值。

```
Switch(config-if)# no ipv6 mld robustness-variable
```

## 相关命令

```
show ipv6 mld interface
```

### 13.2.12 ipv6 mld version

使用此命令设定端口使用的MLD协议的版本。使用关键字no恢复端口所使用的版本为默认值。

## 命令语法

```
ipv6 mld version number
```

```
no ipv6 version
```

<i>number</i>	端口所使用的 MLD 协议版本，范围是 1 到 2
---------------	---------------------------

## 命令模式

端口配置模式

## 默认

1

## 使用说明

无

## 举例说明

设定端口使用的 MLD 协议的版本为 version 2。

```
Switch(config-if)# ipv6 mld version 2
```

设定端口使用的 MLD 协议的版本为默认值。

```
Switch(config-if)# no ipv6 mld version
```

## 相关命令

```
show ipv6 mld interface
```

### 13.2.13 ipv6 mld static-group

此命令用来设置或删除端口上的静态组播组。

## 命令语法

```
ipv6 mld static-group group-address ( source source-address | )
```

```
no ipv6 mld static-group group-address ( source source-address | )
```

<i>group-address</i>	组播组地址
<b>source</b> <i>source-address</i>	组播源地址

## 命令模式

端口配置模式

## 默认

无

## 使用说明

无

## 举例说明

下面的例子说明如何在接口上配置静态组播组。

```
Switch # configure terminal
```

```
Switch (config)# interface eth-0-1
```

```
Switch (config-if)# ipv6 mld static-group ff0e::1234
```

```
Switch (config-if)# ipv6 mld static-group ff0e::1234 source 2001::2
```

下面的例子说明如何删除接口上配置的静态组播组。

```
Switch # configure terminal
```

```
Switch (config)# interface eth-0-1
```

```
Switch (config-if)# no ipv6 mld static-group ff02::1234
```

## 相关命令

**show ipv6 mld groups**

### 13.2.14 ipv6 mld ssm-map enable

此命令用来使能MLD ssm-mapping功能。使用关键字no禁用此功能。

## 命令语法

**ipv6 mld ssm-map enable**

**no ipv6 mld ssm-map enable**

## 命令模式

全局模式

## 默认

关闭

## 使用说明

无

## 举例说明

使能 MLD ssm-mapping 功能。

```
Switch(config)# ipv6 mld ssm-map enable
```

关闭 MLD ssm-mapping 功能。

```
Switch(config)# no ipv6 mld ssm-map enable
```

## 相关命令

无

### 13.2.15 ipv6 mld ssm-map static

此命令用来设置MLD ssm-mapping的规则。使用关键字no禁用此功能。

## 命令语法

```
ipv6 mld ssm-map static list source-address
no ipv6 mld ssm-map static list source-address
```

<i>list</i>	访问控制列表，指定组播组范围
<i>source-address</i>	组播源地址

## 命令模式

全局模式

## 默认

关闭

## 使用说明

无

## 举例说明

设置在 ipacl 中的 group 映射的 source 地址为 2001::2

```
Switch(config)# ipv6 mld ssm-map static ipacl 2001::2
```

取消在 ipacl 中的 group 的映射的 source 地址为 2001::2

```
Switch(config)# no ipv6 mld ssm-map static ipacl 2001::2
```

## 相关命令

无

### 13.2.16 clear ipv6 mld

此命令清除动态学习的IPv6组播组信息。

## 命令语法

```
clear ipv6 mld (* | group group-address |)
```

<i>group-address</i>	指定 IPv6 组播组地址
*	所有的 IPv6 组播组信息

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子显示如何删除所有的组播组信息。

```
Switch# clear ipv6 mld
```

```
Switch# clear ipv6 mld group *
```

下面例子显示如何删除组播组 ff02::1234。

```
Switch# clear ipv6 mld group ff02::1234
```

## 相关命令

**show ipv6 mld groups**

### 13.2.17 clear ipv6 mld interface

此命令清除指定端口上动态学习的IPv6组播组信息。

## 命令语法

```
clear ipv6 mld (group group-address | interface ) IFNAME
```

<i>group-address</i>	指定 IPv6 组播组地址
<i>IFNAME</i>	指定接口名称

## 命令模式

特权模式

## 默认

无



## 使用说明

无

## 举例说明

下面例子显示如何清除端口 eth-0-1 上动态 IPv6 组播组信息。

```
Switch# clear ipv6 mld group interface eth-0-1
```

## 相关命令

**show ipv6 mld groups**

### 13.2.18 show ipv6 mld groups

此命令用于显示IPv6组播组信息。

## 命令语法

**show ipv6 mld groups** *group-address* (**detail** |)

<i>group-address</i>	指定 IPv6 组播组地址
<b>detail</b>	IPv6 组播组详细信息

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子显示组播组的详细信息。

```
Switch# show ipv6 mld groups detail
```

```
MLD Connected Group Membership Details for eth-0-2
Interface:      eth-0-2
Group:         ff0e::1234:5678
Uptime:        00:00:10
Group mode:    Exclude (Expires: 00:04:10)
```

```
Last reporter: fe80:1111:1111:1111:1111:1111:1111:1111
Source list is empty
```

## 相关命令

无

### 13.2.19 show ipv6 mld groups interface

此命令用于显示端口的IPv6组播组信息。

## 命令语法

```
show ipv6 mld groups IFNAME (group-address | ) (detail |)
```

<i>group-address</i>	指定 IPv6 组播组地址
<b>detail</b>	IPv6 组播组详细信息
<i>IFNAME</i>	接口名称

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子显示接口 eth-0-1 上的组播组信息。

```
Switch# show ipv6 mld groups eth-0-1
```

```
MLD Connected Group Membership
Group Address                    Interface    Expires
ff0e::1234:5678                  eth-0-2     00:03:01
```

## 相关命令

无

## 13.2.20 show ipv6 mld groups count

此命令用于显示组播组数目。

### 命令语法

**show ipv6 mld groups (*IFNAME* |) count**

<i>IFNAME</i>	接口名称
---------------	------

### 命令模式

特权模式

### 默认

无

### 使用说明

无

### 举例说明

下面例子显示端口 **eth-0-1** 上的组播组数目。

```
Switch# show ipv6 mld groups eth-0-1 count
Dynamic multicast groups count: 1
Static multicast groups count: 0
Total multicast groups count: 1
```

### 相关命令

无

## 13.2.21 show ipv6 mld interface

此命令用于查看组播组端口的信息。

### 命令语法

**show ipv6 mld interface (*IFNAME* |)**

<i>IFNAME</i>	接口名称
---------------	------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

查看端口 `eth-0-1` 的多播设置信息。

```
Switch# show ipv6 mld interface eth-0-1
Interface eth-0-1 (Index 1)
  MLD Active, Querier, Version 1 (default)
  Internet address is fe80::9c7c:7eff:fe94:8300
  MLD interface has 0 group-record states
  MLD activity: 0 joins, 0 leaves
  MLD query interval is 125 seconds
  MLD querier timeout is 255 seconds
  MLD max query response time is 10 seconds
  Last member query response interval is 1000 milliseconds
  Group Membership interval is 260 seconds
```

## 相关命令

无

## 13.3 MLD Snooping 命令

### 13.3.1 ipv6 mld snooping

使用此命令启用 MLD Snooping 使用关键字 `no` 关闭此项功能。

## 命令语法

```
ipv6 mld snooping (vlan vlan_id |)
```

```
no ipv6 mld snooping (vlan vlan_id |)
```

<i>vlan_id</i>	VLAN id, 范围是 1 到 4094
----------------	-----------------------

## 命令模式

全局配置模式

## 默认

去使能

## 使用说明

在全局模式下或者 VLAN 模式下启用 Mld Snooping。

默认，mld snooping 不启用。

## 举例说明

启用 MLD Snooping 功能。

```
Switch(config)# ipv6 mld snooping
```

关闭 MLD Snooping 功能。

```
Switch(config)# no ipv6 mld snooping
```

## 相关命令

```
show ipv6 mld snooping
```

### 13.3.2 ipv6 mld snooping fast-leave

使用此命令启用 MLD snooping 成员快速离开功能。使用关键字 no 关闭此功能。

## 命令语法

```
ipv6 mld snooping (vlan vlan_id | ) fast-leave
```

```
no ipv6 mld snooping (vlan vlan_id | ) fast-leave
```

<i>vlan_id</i>	VLAN id, 范围是 1 到 4094
----------------	-----------------------

## 命令模式

全局配置模式

## 默认

关闭

## 使用说明

此命令会覆盖 `immediate-leave` 的设置。

## 举例说明

启用成员快速离开功能。

```
Switch(config)# ipv6 mld snooping fast-leave
```

关闭成员快速离开功能。

```
Switch(config)# no ipv6 mld snooping fast-leave
```

## 相关命令

```
show ipv6 mld snooping global
```

### 13.3.3 ipv6 mld last-member-query-interval

使用此命令设置当仅存最后一个成员时的查询间隔。使用关键字 `no` 恢复查询间隔为默认值。

## 命令语法

```
ipv6 mld snooping (vlan vlan_id | ) last-member-query-interval interval
```

```
no ipv6 mld snooping (vlan vlan_id | ) last-member-query-interval
```

<b>vlan <i>vlan_id</i></b>	VLAN id, 范围是 1 到 4094
<b><i>interval</i></b>	查询间隔, 单位为毫秒, 范围是 1000 到 25500

## 命令模式

全局配置模式

## 默认

1000 毫秒

## 使用说明

无

## 举例说明

设置当仅存最后一个成员时的查询间隔。

```
Switch(config)# ipv6 mld snooping last-member-query-interval 2000
```

恢复查询间隔为默认值。

```
Switch(config)# no ipv6 mld snooping last-member-query-interval
```

## 相关命令

**show ipv6 mld snooping**

**show ipv6 mld snooping vlan**

### 13.3.4 ipv6 mld snooping global source-address

使用此命令设置MLD snooping查询器源地址。

## 命令语法

**ipv6 mld snooping global source-address** *address*

**no ipv6 mld snooping global source-address**

<i>address</i>	查询器源 IP 地址
----------------	------------

## 命令模式

全局配置模式

## 默认

0.0.0.0

## 使用说明

VLAN 上没有配置查询器源地址时使用全局的查询器地址，VLAN 上配置了查询器地址后使用 VLAN 上配置的查询器地址。

## 举例说明

全局模式下配置查询器源 IP 地址 2001::2。

```
Switch(config)# ipv6 mld snooping global source-address 2001::2
```

恢复全局模式的查询器地址。

```
Switch(config)# no ipv6 mld snooping global source-address
```

## 相关命令

**show ipv6 mld snooping querier**

### 13.3.5 ipv6 mld snooping max-member-num

使用此命令设置MLD snooping最大成员数目。使用关键字no恢复此数目为默认值。

#### 命令语法

**ipv6 mld snooping (vlan *vlan\_id* | ) max-member-num *number***

**no ipv6 mld snooping (vlan *vlan\_id* | ) max-member-num**

<b>vlan <i>vlan_id</i></b>	VLAN id, 范围是 1 到 4094
<b><i>number</i></b>	最大成员数目, 范围是 1 到 4096

#### 命令模式

全局配置模式

#### 默认

4096

#### 使用说明

无

#### 举例说明

设置 MLD snooping 最大成员数目为 1024 。

```
Switch(config)# ipv6 mld snooping max-member-num 1024
```

恢复 MLD snooping 最大成员数目为默认值。

```
Switch(config)# no ipv6 mld snooping max-member-num
```

#### 相关命令

**show ipv6 mld snooping global**

**show ipv6 mld snooping vlan**

### 13.3.6 ipv6 mld snooping query-interval

使用此命令设置成员查询的间隔。使用关键字no恢复此间隔为默认值。

#### 命令语法

**ipv6 mld snooping (vlan *vlan\_id* | ) query-interval *interval***



**no ipv6 mld snooping (vlan *vlan\_id* | ) query-interval**

<b>vlan <i>vlan_id</i></b>	VLAN id, 范围是 1 到 4094
<b><i>interval</i></b>	成员查询间隔, 以秒为单位, 范围是 2 到 18000

**命令模式**

全局配置模式

**默认**

125 秒

**使用说明**

查询的间隔时间不能少于 MLD snooping 查询最大的响应时间。

**举例说明**

设置成员查询间隔为 64 秒。

```
Switch(config)# ipv6 mld snooping query-interval 64
```

恢复成员查询间隔为默认值。

```
Switch(config)# no ipv6 mld snooping query-interval
```

**相关命令**

```
show ipv6 mld snooping querier
```

```
show ipv6 mld snooping querier vlan
```

**13.3.7 ipv6 mld snooping query-max-response-time**

使用此命令设置等待查询应答报文的超时时间。使用关键字no恢复此超时时间为默认值。

**命令语法**

```
ipv6 mld snooping (vlan vlan_id | ) query-max-response-time time
```

```
no ipv6 mld snooping (vlan vlan_id | ) query-max-response-time
```

<b><i>vlan_id</i></b>	VLAN id, 范围是 1 到 4094
<b><i>time</i></b>	等待查询应答报文的超时时间, 以秒为单位, 范围是 1 到 25

## 命令模式

全局配置模式

## 默认

10 秒

## 使用说明

查询应答时间不能少于 MLD snooping 查询间隔。

## 举例说明

设置等待查询应答报文的超时时间为 15 秒。

```
Switch(config)# ipv6 mld snooping query-max-response-time 15
```

恢复此超时时间。

```
Switch(config)# no ipv6 mld snooping query-max-response-time
```

## 相关命令

```
show ipv6 mld snooping querier
```

```
show ipv6 mld snooping querier vlan
```

### 13.3.8 ipv6 mld snooping report-suppression

使用此命令设置端口对MLDv1/v2的成员报告报文进行抑制。使用关键字no取消对对MLDv1/v2的成员报告报文的抑制。

## 命令语法

```
ipv6 mld snooping (vlan vlan_id | ) report-suppression
```

```
no ipv6 mld snooping (vlan vlan_id | ) report-suppression
```

<i>vlan_id</i>	VLAN id, 范围是 1 到 4094
----------------	-----------------------

## 命令模式

全局配置模式

## 默认

启用

## 使用说明

MLD snooping 工作在 v2 模式时，成员报告报文不进行抑制。

## 举例说明

对 MLDv1/MLDv2 的成员报告报文进行抑制。

```
Switch(config)# ipv6 mld snooping report-suppression
```

取消对 MLDv1/MLDv2 的成员报告报文的抑制

```
Switch(config)# no ipv6 mld snooping report-suppression
```

## 相关命令

```
show ipv6 mld snooping
```

```
show ipv6 mld snooping vlan
```

## 13.3.9 ipv6 mld snooping version

使用此命令指定运行的MLD版本。使用关键字no恢复运行的MLD版本为默认值

## 命令语法

```
ipv6 mld snooping (vlan vlan_id | ) version version
```

```
no ipv6 mld snooping (vlan vlan_id | ) version
```

<i>vlan_id</i>	VLAN id, 范围是 1 到 4094
<i>version</i>	MLD 版本, 范围是 1 到 2

## 命令模式

全局配置模式

## 默认

1

## 使用说明

无

## 举例说明

指定全局 MLD snooping 运行 MLDv2 模式下。

```
Switch(config)# ipv6 mld snooping version 2
```

## 相关命令

```
show ipv6 mld snooping
```

```
show ipv6 mld snooping vlan
```

### 13.3.10 ipv6 mld snooping discard-unknown

使用此命令丢弃未知的IPv6组播流量。使用no命令恢复默认值。

## 命令语法

```
ipv6 mld snooping (vlan vlan_id | ) discard-unknown
```

```
no ipv6 mld snooping (vlan vlan_id | ) discard-unknown
```

<b>vlan <i>vlan_id</i></b>	VLAN id, 范围是 1 到 4094
----------------------------	-----------------------

## 命令模式

全局配置模式

## 默认

未知组播流量在 VLAN 内泛洪。

## 使用说明

无

## 举例说明

在全局模式下配置交换机丢弃未知组播流量

```
Switch(config)# ipv6 mld snooping discard-unknown
```

## 相关命令

```
show ipv6 mld snooping
```

```
show ipv6 mld snooping vlan
```

### 13.3.11 ipv6 mld snooping querier tcn

使用此命令设置MLD snooping的TCN 相关参数。

#### 命令语法

**ipv6 mld snooping querier tcn (query-count *count* | query-interval *interval*)**

**no ipv6 mld snooping querier tcn (query-count | query-interval)**

<b>query-count</b> <i>count</i>	MLD snooping 查询 TCN 查询次数，范围是 1 到 10
<b>query-interval</b> <i>interval</i>	MLD snooping 查询 TCN 查询间隔，范围是 1 到 255

#### 命令模式

全局配置模式

#### 默认

使能

#### 使用说明

Mld snooping tcn 查询次数必须配置，默认值为 2，范围取值 1-10。

Mld snooping tcn 查询间隔必须配置，默认值 10 秒，范围 1-255 秒。

#### 举例说明

设置 MLD Snooping Tcn 的查询次数为 2 次。

```
Switch(config)# ipv6 mld snooping querier tcn query-count 2
```

#### 相关命令

**show ipv6 mld snooping vlan**

### 13.3.12 ipv6 mld snooping vlan access-group

此命令用于设置允许加入的组播组范围。

#### 命令语法

**ipv6 mld snooping vlan *vlan\_id* access-group *acl***

**no ipv6 mld snooping vlan *vlan\_id* access-group**

<i>vlan_id</i>	VLAN id, 范围是 1 到 4094
<i>acl</i>	访问控制列表名称

## 命令模式

全局配置模式

## 默认

无

## 使用说明

无

## 举例说明

在 VLAN 上设置运行加入的组播组范围是 *acl* 中的组播组范围。

```
Switch(config)# ipv6 mld snooping vlan 10 access-group acl
```

## 相关命令

**show ipv6 mld snooping vlan**

### 13.3.13 ipv6 mld vlan mrouter interface

此命令用于静态配置VLAN的IPv6组播路由端口。

## 命令语法

**ipv6 mld snooping vlan *vlan\_id* mrouter interface *IFNAME***

**no ipv6 mld snooping vlan *vlan\_id* mrouter interface *IFNAME***

<i>vlan_id</i>	VLAN id, 范围是 1 到 4094
<i>IFNAME</i>	端口名称

## 命令模式

全局配置模式

## 默认

无

## 使用说明

指定的组播路由端口必须属于指定的 VLAN。

## 举例说明

将 eth-0-1 设置成 VLAN10 的组播路由端口。

```
Switch(config)# ipv6 mld snooping vlan 10 mrouter interface eth-0-1
```

## 相关命令

**show ipv6 mld snooping vlan**

### 13.3.14 ipv6 mld vlan mrouter-aging-interval

此命令用于设置动态组播路由端口老化的时间间隔。

## 命令语法

**ipv6 mld snooping vlan *vlan\_id* mrouter-aging-interval *interval***

**no ipv6 mld snooping vlan *vlan\_id* mrouter-aging-interval**

<i>vlan_id</i>	VLAN id, 范围是 1 到 4094
<i>interval</i>	老化时间间隔, 单位是秒, 范围是 1 到 65535

## 命令模式

全局配置模式

## 默认

255 秒

## 使用说明

无

## 举例说明

设置 VLAN 上的动态 IPv6 组播路由端口老化间隔是 100 秒。

```
Switch(config)# ipv6 mld snooping vlan 10 mrouter-aging-interval 100
```

## 相关命令

**show ipv6 mld snooping vlan**

### 13.3.15 ipv6 mld snooping vlan querier

此命令用于在VLAN上使能IPv6组播查询器功能。

## 命令语法

**ipv6 mld snooping vlan *vlan\_id* querier**

**no ipv6 mld snooping vlan *vlan\_id* querier**

<i>vlan_id</i>	VLAN id, 范围是 1 到 4094
----------------	-----------------------

## 命令模式

全局配置模式

## 默认

关闭

## 使用说明

无

## 举例说明

在 VLAN10 上使能 IPv6 组播查询器功能。

```
Switch(config)# ipv6 mld snooping vlan 10 querier
```

## 相关命令

**show ipv6 mld snooping querier vlan**

### 13.3.16 ipv6 mld snooping vlan querier address

此命令用于设置VLAN上IPv6组播查询器的源地址。

## 命令语法

**ipv6 mld snooping vlan *vlan\_id* querier address *address***

**no ipv6 mld snooping vlan *vlan\_id* querier address *address***



<i>vlan_id</i>	VLAN id, 范围是 1 到 4094
<i>address</i>	IPv6 组播查询器源地址

## 命令模式

全局配置模式

## 默认

无

## 使用说明

VLAN 上配置的 IPv6 组播查询器源地址将覆盖全局的 IPv6 组播查询器地址。

## 举例说明

设置 VLAN10 上 IPv6 组播查询器的源地址是 2001::2。

```
Switch(config)# ipv6 mld snooping vlan 10 querier address 2001::2
```

## 相关命令

```
show ipv6 mld snooping querier vlan
```

### 13.3.17 ipv6 mld snooping vlan querier-timeout

此命令用于设置 VLAN 上查询器老化时间。

## 命令语法

```
ipv6 mld snooping vlan vlan_id querier-timeout interval
```

```
no ipv6 mld snooping vlan vlan_id querier-timeout
```

<i>vlan_id</i>	VLAN id, 范围是 1 到 4094
<i>interval</i>	查询器老化时间间隔, 单位是秒, 范围是 60 到 300 秒

## 命令模式

全局配置模式

## 默认

255 秒

## 使用说明

无

## 举例说明

设置 VLAN10 查询器老化间隔为 100 秒

```
Switch(config)# ipv6 mld snooping vlan 10 querier-timeout 100
```

## 相关命令

```
show ipv6 mld snooping querier vlan
```

### 13.3.18 ipv6 mld snooping vlan static-group

此命令用于设置VLAN的成员端口加入IPv6组播组或组播源组。

## 命令语法

```
ipv6 mld snooping vlan vlan_id static-group group-address (source source-address |)  
interface IFNAME
```

```
no ipv6 mld snooping vlan vlan_id static-group group-address (source source-address |)  
interface IFNAME
```

<i>vlan_id</i>	VLAN id, 范围是 1 到 4094
<i>group-address</i>	组播组地址
<b>source</b> <i>source-address</i>	组播源地址
<i>IFNAME</i>	VLAN 的成员端口名称

## 命令模式

全局配置模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子显示如何将 VLAN10 的成员端口 eth-0-11 加入组播组 ff0e::1234。

```
Switch(config)# ipv6 mld snooping vlan 10 static-group ff0e::1234 interface eth-0-11
```

## 相关命令

**show ipv6 mld snooping group**

### 13.3.19 clear ipv6 mld snooping group

此命令用于删除所有的MLD snooping组信息。

## 命令语法

```
clear ipv6 mld snooping (group * )
```

## 命令模式

特权模式

## 默认

无

## 使用说明

此命令用来删除动态学习到的 IPv6 组播组信息。

## 举例说明

下面例子显示如何删除所有的 IPv6 组播组信息。

```
Switch# clear ipv6 mld snooping
```

## 相关命令

无

### 13.3.20 clear ipv6 mld snooping vlan group

此命令用于删除指定VLAN上的IPv6组播组信息。

## 命令语法

```
clear ipv6 mld snooping vlan vlan_id
```

<i>vlan_id</i>	VLAN id, 范围是 1 到 4094
----------------	-----------------------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子显示如何删除 VLAN10 上的 IPv6 组播组信息

```
Switch# clear ipv6 mld snooping vlan 10
```

## 相关命令

无

### 13.3.21 show ipv6 mld snooping global

使用此命令查看所有关于MLD Snooping的全局配置。

## 命令语法

```
show ipv6 mld snooping global
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

查看所有关于 MLD Snooping 的全局配置。

```
Switch# show ipv6 mld snooping global
```

```
Global Mld Snooping Configuration
-----
Mld Snooping                               :Enabled
Mld Snooping Fast-Leave                     :Disabled
Mld Snooping Version                       :1
Mld Snooping Max-Member-Number            :4096
Mld Snooping Unknown Multicast Behavior   :Flood
Mld Snooping Report-Suppression           :Enabled
```

## 相关命令

无

### 13.3.22 show ipv6 mld snooping groups

此命令用于显示MLD snooping组播组信息。

## 命令语法

```
show ipv6 mld snooping groups
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

显示 MLD snooping 组播组信息。

```
Switch# show ipv6 mld snooping groups
```

VLAN	Interface	Group Address	Uptime	Expire-time
1	eth-0-3	ff0e:2111:1111:1111:1111:1111:1234:5678	00:00:04	00:04:16

## 相关命令

无

### 13.3.23 show ipv6 mld snooping groups vlan

此命令用于指定VLAN上的组播组信息。

## 命令语法

**show ipv6 mld snooping groups vlan *vlan\_id* (*group\_address* |)**

<i>vlan_id</i>	VLAN id, 范围是 1 到 4094
<i>group_addres</i>	组播组信息

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子显示 VLAN1 上的组播组信息。

```
Switch# show ipv6 mld snooping groups vlan 1
```

```
MLD Snooping groups for vlan1
Interface:      eth-0-3
Group:         ff0e:2111:1111:1111:1111:1234:5678
Uptime:        00:00:42
Group mode:    Exclude (Expires: 00:03:38)
Last reporter: fe80:1111:1111:1111:1111:1111:1111
Source list is empty
```

## 相关命令

无

### 13.3.24 show ipv6 mld snooping groups count

此命令用于显示MLD snooping组播组数目。

## 命令语法

**show ipv6 mld snooping groups (vlan *vlan\_id* |) count**

<b>vlan <i>vlan_id</i></b>	VLAN id, 范围是 1 到 4094
----------------------------	-----------------------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子 VLAN1 上组播组数目。

```
Switch# show ipv6 mld snooping groups vlan 1 count
```

```
Dynamic multicast groups count: 1
Static multicast groups count: 0
Total multicast groups count: 1
```

## 相关命令

无

### 13.3.25 show ipv6 mld snooping querier

此命令用于显示MLD snooping查询器相关信息。

## 命令语法

```
show ipv6 mld snooping querier (vlan vlan_id |)
```

<b>vlan <i>vlan_id</i></b>	VLAN id, 范围是 1 到 4094
----------------------------	-----------------------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子显示 VLAN1 上查询器信息。

```
Switch# show ipv6 mld snooping querier vlan 1

Global Mld Snooping Querier Configuration
-----
Version                               :1
Last-Member-Query-Interval (msec)    :1000
Max-Query-Response-Time (sec)       :10
Query-Interval (sec)                 :125
Global Source-Address                 :::
TCN Query Count                       :2
TCN Query Interval (sec)              :10
Vlan 1:  MLD snooping querier status
-----

Elected querier is : ::
-----

Admin state                           :Disabled
Admin version                          :1
Operational state                      :Non-Querier
Querier operational address            :::
Querier configure address              :N/A
Last-Member-Query-Interval (msec)    :1000
Max-Query-Response-Time (sec)       :10
Query-Interval (sec)                 :125
Querier-Timeout (sec)                 :255
```

## 相关命令

无

### 13.3.26 show ipv6 mld snooping mrouter

此命令用于显示IPv6组播路由端口信息。

## 命令语法

```
show ipv6 mld snooping mrouter (vlan vlan_id |)
```

<b>vlan <i>vlan_id</i></b>	VLAN id, 范围是 1 到 4094
----------------------------	-----------------------

## 命令模式

特权模式



## 默认

无

## 使用说明

无

## 举例说明

下面例子显示 VLAN1 上的 IPv6 组播路由端口信息。

```
Switch# show ipv6 mld snooping mrouter vlan 1
```

VLAN	Interface	Mode	Uptime	Expires-time
2	eth-0-1	static	-	-

## 相关命令

无

### 13.3.27 show ipv6 mld snooping vlan

此命令用于 MLD snooping 的配置信息。

## 命令语法

```
show ipv6 mld snooping (vlan vlan_id |)
```

<b>vlan <i>vlan_id</i></b>	VLAN id, 范围是 1 到 4094
----------------------------	-----------------------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子显示 VLAN1 上 MLD snooping 的信息。

```
Switch# show ipv6 mld snooping vlan 1
```

```

Global Mld Snooping Configuration
-----
Mld Snooping                               :Enabled
Mld Snooping Fast-Leave                     :Disabled
Mld Snooping Version                       :1
Mld Snooping Max-Member-Number            :4096
Mld Snooping Unknown Multicast Behavior   :Flood
Mld Snooping Report-Suppression           :Enabled
Vlan 2
-----
Mld Snooping                               :Enabled
Mld Snooping Fast-Leave                     :Disabled
Mld Snooping Report-Suppression           :Enabled
Mld Snooping Version                       :1
Mld Snooping Max-Member-Number            :4096
Mld Snooping Unknown Multicast Behavior   :Flood
Mld Snooping Group Access-list            :N/A
Mld Snooping Mrouter Port                  :eth-0-1(static)
Mld Snooping Mrouter Port Aging Interval(sec) :255

```

## 相关命令

无

### 13.3.28 show resource l2mcast

此命令用于二层组播的资源使用情况。

## 命令语法

```
show resource l2mcast
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子显示二层组播资源使用情况。

```
Switch# show resource l2mcast
```

```

L2MCAST
Resource                               Used           Capability
=====

```

L2 Mcast Entry	1	1024
L2 Mcast Member	2	8192

## 相关命令

无

## 13.4 PIMv6 命令

### 13.4.1 ipv6 pim accept-register

此命令根据访问控制列表限制 RP 可接受的 PIM 注册报文。使用关键字 **no** 关闭此功能。

## 命令语法

**ipv6 pim accept-register list list**

**no ipv6 pim accept-register**

<i>list</i>	访问控制列表
-------------	--------

## 命令模式

全局配置模式

## 默认

无

## 使用说明

此功能用来防止未经认证的用户注册到交换机；当其用此功能后，如果一个未经认证的主机发送一个 PIMv6 注册报文给交换机，此交换机会立即发送一个 Stop 报文回去阻止其继续发送报文注册。此命令可以有效的让网络中众多 RP 负载分担，通过 ACL 的设置控制不同的组播组。

## 举例说明

下面例子讲述了如何根据访问控制列表 **acl1** 限制 RP 可接受的 PIMv6 注册报文。

```
Switch(config)# ipv6 pim accept-register list acl1
```

## 相关命令

无

## 13.4.2 ipv6 pim anycast-rp

使用此命令设置任播汇聚路由器地址及其成员。使用关键字no删除指定成员。

### 命令语法

```
ipv6 pim anycast-rp anycast_rp_address anycast_member_address
no ipv6 pim anycast-rp anycast_rp_address (anycast_member_address |)
```

<i>anycast_rp_address</i>	RP 地址
<i>anycast_member_address</i>	组成员地址

### 命令模式

全局配置模式

### 默认

无

### 使用说明

如果要配置，则应在所有路由器上配置，所有路由器必须使用相同的 RP 地址，当静态配置的 RP 失效时，路由器不可能切换到其它的备用 RP(除非使用 Anycast-RP，在 RP 之间运行)。

### 举例说明

设置任播汇聚路由器地址及其组成员。

```
Switch(config)# ipv6 pim anycast-rp 2001::1 2001::11
```

```
Switch(config)# no ipv6 pim anycast-rp 2001::1 2001::11
```

### 相关命令

无

## 13.4.3 ipv6 pim bsr-candidate

使用此命令设置本交换机作为候选的自举交换机，使用关键字no取消此项设置。

### 命令语法

```
ipv6 pim bsr-candidate IFNAME (hash-mask (priority))
no ipv6 pim bsr-candidate
```

<i>IFNAME</i>	端口名称
<i>hash-mask</i>	RP 选举时候 HASH 的掩码长度，范围是 0 到 32
<i>priority</i>	候选 BSR 路由器的优先级，范围是 0 到 255

## 命令模式

全局配置模式

## 默认

无

## 使用说明

无

## 举例说明

设置此交换机作为 BSR，设置端口 eth-0-1 的地址作为 BSR 的地址

```
Switch(config)# ipv6 pim bsr-candidate eth-0-1
```

## 相关命令

```
ipv6 pim bsr-border
```

### 13.4.4 ipv6 pim bsr-border

使用此命令设置此交换机作为PIMv6域的边界，BSR报文不再被转发出去。

## 命令语法

```
ipv6 pim bsr-border
```

```
no ipv6 pim bsr-border
```

## 命令模式

端口配置模式

## 默认

不使能

## 使用说明

无

## 举例说明

设置此交换机作为 PIMv6 域的边界。

```
Switch(config-if)# ipv6 pim bsr-border
```

## 相关命令

**ipv6 pim bsr-candidate**

### 13.4.5 ipv6 pim dr-priority

使用此命令设定竞选指定路由器的优先权值，使用关键字no恢复优先权值为默认值。

## 命令语法

**ipv6 pim dr-priority** *priority*

**no ipv6 pim dr-priority**

<i>priority</i>	设定的指定路由器的优先权值，范围是 0 到 4294967294
-----------------	----------------------------------

## 命令模式

端口配置模式

## 默认

1

## 使用说明

端口的优先权默认为 1，如果一个路由器在它的 Hello 报文中没有宣布它的优先权值，此路由器将被认为具有最大的优先权值，因此将被选举为 DR。如果有不止一个的路由器在它的 HELLO 报文中没有宣布它的优先权值，则具有最高 IP 地址的将被选为 DR。

## 举例说明

设定竞选指定路由器的优先权值是 1000。

```
Switch(config-if)# ipv6 pim dr-priority 1000
```

## 相关命令

无

## 13.4.6 ipv6 pim exclude-genid

使用此命令设置此端口发出的Hello报文不包括GenerationID选项。使用关键字no恢复此项设置为默认状态。

### 命令语法

**ipv6 pim exclude-genid**

**no ipv6 pim exclude-genid**

### 命令模式

端口配置模式

### 默认

不使能

### 使用说明

GenerationID 是 PIM 邻居的一个标识 ID，在 PIM Hello 中携带，本端设备会记录对端发送的 hello 报文中携带的 GenerationID，本端设备每次收到对端的 PIM Hello 会去 check 一下这个 ID 是否有变化，如果有变化，则认为邻居状态发生改变，重新走状态机。

### 举例说明

设置 RP 发送的 Hello 报文中无 GenerationID 的报文。

```
Switch(config-if)# ipv6 pim exclude-genid
```

### 相关命令

无

## 13.4.7 ipv6 pim hello-interval

使用此命令设定端口发送Hello报文的时间间隔，使用关键字no恢复时间间隔为默认值。

### 命令语法

**ipv6 pim hello-interval *interval***

**no ipv6 pim hello-interval**

<i>interval</i>	>发送 Hello 报文的时间间隔，以秒为单位，范围是 1 到 65535
-----------------	---------------------------------------

## 命令模式

端口配置模式

## 默认

30 秒

## 使用说明

无

## 举例说明

设定发送 Hello 报文的时间间隔是 100 秒。

```
Switch(config-if)# ipv6 pim hello-interval 100
```

## 相关命令

无

### 13.4.8 ipv6 pim ignore-rp-set-priority

设置忽略关于 RP（Rendezvous Router，汇聚路由器）的优先权。使用关键字 **no** 对 RP 优先权不进行忽略。

## 命令语法

```
ipv6 pim ignore-rp-set-priority  
no ipv6 pim ignore-rp-set-priority
```

## 命令模式

全局配置模式

## 默认

默认情况下，对 RP 优先权不进行忽略。

## 使用说明

无

## 举例说明

忽略关于 RP 优先权的设置值。

```
Switch(config)# ipv6 pim ignore-rp-set-priority
```



## 相关命令

无

### 13.4.9 ipv6 pim jp-timer

设置端口发送加入/修剪报文的时间间隔。使用关键字no恢复此时间间隔为默认值。

## 命令语法

**ipv6 pim jp-timer** *timer*

**no ipv6 pim jp-timer**

<i>timer</i>	端口发送加入/修剪报文的时间间隔，以秒为单位，范围是 1 到 65535
--------------	--------------------------------------

## 命令模式

全局配置模式

## 默认

60 秒

## 使用说明

无

## 举例说明

设置端口发送加入/修剪报文的时间间隔为 100 秒。

```
Switch(config)# ipv6 pim jp-timer 100
```

## 相关命令

无

### 13.4.10 ipv6 pim neighbor-filter

此命令根据访问控制列表限制与此设备建立邻居关系的节点。使用关键字no 取消此项限制。

## 命令语法

**ipv6 pim neighbor-filter** *list*

**no ipv6 pim neighbor-filter**

<i>list</i>	访问控制列表
-------------	--------

## 命令模式

端口配置模式

## 默认

无

## 使用说明

在 PIMv6 协议中，节点之间会互相发送 PIMv6 Hello 报文来与对方建立邻居关系；此命令可以根据访问控制列表来限制与此设备建立邻居关系的节点。

## 举例说明

根据访问控制列表 `acl1` 限制与此设备建立邻居关系的节点。

```
Switch(config-if)# ipv6 pim neighbor-filter acl1
```

## 相关命令

无

### 13.4.11 ipv6 pim register-rate-limit

使用此命令设置 DR 发往 RP 的 PIM 注册报文的最大速度。使用关键字 `no` 恢复此项设置为默认值。

## 命令语法

**ipv6 pim register-rate-limit *limit***

**no ipv6 pim register-rate-limit**

<i>limit</i>	DR 发往 RP 的 PIM 注册报文的最大速度，范围是 1 到 65535
--------------	--

## 命令模式

全局配置模式

## 默认

默认情况下，对 DR 发往 RP 的 PIM 注册报文的速度不进行限制。如果设定了此项，则超过此速度的 PIM 注册报文在 RP 处会被丢弃。

## 使用说明

无

## 举例说明

设置 DR 发往 RP 的 PIM 注册报文的最大速度为每秒 100 个。

```
Switch(config)# ipv6 pim register-rate-limit 100
```

## 相关命令

**ipv6 pim register-rp-reachability**

**ipv6 pim register-source**

**ipv6 pim register-suppression**

### 13.4.12 ipv6 pim register-source

此命令设置DR发往RP的注册报文的源IP地址，使用关键字no恢复注册报文的源IP地址为默认值

## 命令语法

**ipv6 pim register-source** *IFNAME*

**no ipv6 pim register-source**

<i>IFNAME</i>	接口名称
---------------	------

## 命令模式

全局配置模式

## 默认

无

## 使用说明

使用此端口的 IPv6 地址为注册报文的源 IPv6 地址，默认情况下，源 IPv6 地址为 DR 的 interface IPv6 地址。

## 举例说明

设置注册报文的源 IP 地址为 eth-0-1 端口的 IP 地址。

```
Switch(config)# ipv6 pim register-source eth-0-1
```

## 相关命令

**ipv6 pim register-rate-limit**

**ipv6 pim register-rp-reachability**

**ipv6 pim register-suppression**

### 13.4.13 ipv6 pim register-rp-reachability

此命令设置对 RP（Rendezvous Router，汇聚路由器）可到达性的检测。

## 命令语法

**ipv6 pim register-rp-reachability**

**no ipv6 pim register-rp-reachability**

## 命令模式

全局配置模式

## 默认

不使能

## 使用说明

无

## 举例说明

设置对 RP（Rendezvous Router，汇聚路由器）可到达性的检测。

```
Switch(config)# ipv6 pim register-rp-reachability
```

## 相关命令

**ipv6 pim register-rate-limit**

**ipv6 pim register-source**

**ipv6 pim register-suppression**

## 13.4.14 ipv6 pim register-suppression

当RP给DR发送Stop报文后，DR会停止发送PIMv6注册报文一段时间。此命令可以设置DR停止发送PIMv6注册报文的时间长短。使用关键字no恢复此时间段的设置为默认值。

### 命令语法

**ipv6 pim register-suppression** *time*

**no ipv6 pim register-suppression**

<i>time</i>	限制时间的长短，以秒为单位，范围是 11 到 65535
-------------	------------------------------

### 命令模式

全局配置模式

### 默认

60 秒

### 使用说明

无

### 举例说明

设置当 DR 接受到 Stop 报文后停止发送注册报文的时间间隔为 100 秒。

```
Switch(config)# ipv6 pim register-suppression 100
```

### 相关命令

**ipv6 pim register-rate-limit**

**ipv6 pim register-rp-reachability**

**ipv6 pim register-source**

## 13.4.15 ipv6 pim rp-address

使用此命令为设置静态RP地址，使用关键字no删除RP。

### 命令语法

**ipv6 pim rp-address** *address* ( *list* | **override** | )

**no ipv6 pim rp-address** *address* ( *list* | )

<i>address</i>	RP 地址
<i>list</i>	访问控制列表
<b>override</b>	覆盖动态学习的 RP 的映射

## 命令模式

全局配置模式

## 默认

无

## 使用说明

无

## 举例说明

设置 RP 地址为 2001::2。

```
Switch(config)# ipv6 pim rp-address 2001::2
```

## 相关命令

**ipv6 pim rp-candidate**

**ipv6 pim rp-register-kat**

### 13.4.16 ipv6 pim rp-candidate

使用此命令设置本交换机作为候选的RP，使用关键字no取消此设置。

## 命令语法

**ipv6 pim rp-candidate** *IFNAME* ({**priority** *priority* |**interval** *interval* |**group-list** *list*})

**no ipv6 pim rp-candidate** (*IFNAME* )

<i>IFNAME</i>	此端口的 IP 地址会作为候选的 RP 在网络上被广播
<b>priority</b> <i>priority</i>	发送宣告报文的时间间隔，单位是秒，范围是 1 到 16183
<b>interval</b> <i>interval</i>	候选 RP 的优先权，范围是 0 到 255
<b>group-list</b> <i>list</i>	访问控制列表限制可注册到此 RP 的组播组

## 命令模式

全局配置模式

## 默认

无

## 使用说明

无

## 举例说明

设置本交换机的 eth-0-1 端口的 IPv6 地址为候选的 RP 地址。

```
Switch(config)# ipv6 pim rp-candidate eth-0-1
```

## 相关命令

**ipv6 pim rp-address**

### 13.4.17 ipv6 pim rp-register-kat

使用此命令设置DR发往RP的PIM注册报文的存活时间。使用关键字no恢复此存活时间为默认值。

## 命令语法

**ipv6 pim rp-register-kat** *time*

**no ipv6 pim rp-register-kat**

<i>time</i>	DR 发往 RP 的 PIM 注册报文的存活时间，以秒为单位，范围是 1 到 65535
-------------	--

## 命令模式

全局配置模式

## 默认

185 秒

## 使用说明

DR 发往 RP 的 PIMv6 注册报文在 RP 上会生成一个(S,G)条目，此条目会在 RP 上存在一段时间，超过此时间后，交换机会删除相应条目；此命令可以设置当 RP 发送 Stop 报文后该条目在 RP 上存活的时间。

## 举例说明

设置 DR 发往 RP 的 PIMv6 注册报文的存活时间为 100 秒。

```
Switch(config)# ipv6 pim rp-register-kat 100
```

## 相关命令

**ipv6 pim rp-address**

**ipv6 pim rp-candidate**

### 13.4.18 ipv6 pim spt-switch-threshold infinity

使用此功能设置永远都不切换到最短路径树，使用关键字no取消此项设置。

## 命令语法

**ipv6 pim spt-switch-threshold infinity (group-list list|)**

**no ipv6 pim spt-switch-threshold infinity (group-list list|)**

<b>group-list list</b>	IPv6 组播组地址范围
------------------------	--------------

## 命令模式

全局配置模式

## 默认

默认 DR 收到第一个 IPv6 组播流后立即切换为最短路径树。

## 使用说明

无

## 举例说明

设置永远都不切换到最短路径树。

```
Switch(config)# ipv6 pim spt-switch-threshold infinity
```



## 相关命令

**show ipv6 pim sparse-mode spt-threshold**

### 13.4.19 ipv6 pim cisco-register-checksum

使用此功能设置DR发送注册报文时使用CISCO Register Checksum，使用关键字no取消此项设置。

## 命令语法

**ipv6 pim cisco-register-checksum (group-list list)**

**no ipv6 pim cisco-register-checksum (group-list list|)**

<b>group-list list</b>	IPv6 组播组地址范围
------------------------	--------------

## 命令模式

全局配置模式

## 默认

无

## 使用说明

默认是 RFC 规定的 register checksum，如果配置了访问控制列表，只有通过验证的报文才能以 CISCO Register Checksum 的方式发送。

## 举例说明

设置 DR 发送注册报文时使用 CISCO Register Checksum。

```
Switch(config)# ipv6 pim cisco-register-checksum
```

## 相关命令

无

### 13.4.20 ipv6 pim sparse-mode

使用此命令在此端口启用PIMv6-SM协议，使用关键字no在此端口关闭PIMv6-SM协议。

## 命令语法

**ipv6 pim sparse-mode (passive|)**

**no ipv6 pim sparse-mode (passive|)**

<b>passive</b>	被动模式
----------------	------

**命令模式**

端口配置模式

**默认**

不使能

**使用说明**

默认情况下，端口没有启用 PIMv6-SM 协议；工作在被动模式的端口不会发送 PIMv6 Hello 报文。

**举例说明**

在此端口启用 PIMv6 协议。

```
Switch(config-if)# ipv6 pim sparse-mode
```

**相关命令**

无

**13.4.21 ipv6 pim unicast-bsm**

默认情况下，端口会向整个 PIMv6 域发送 BSM 报文；此命令可以限制交换机只向它的邻居发送 BSM 报文。使用关键字 **no** 恢复此项设置为默认值。

**命令语法**

```
ipv6 pim unicast-bsm
```

```
no ipv6 pim unicast-bsm
```

**命令模式**

端口配置模式

**默认**

不使能

## 使用说明

每个端口只能创建一条统计。

## 举例说明

设置端口向它的邻居发送单播的 BSM 报文。

```
Switch(config-if)# ipv6 pim unicast-bsm
```

## 相关命令

无

### 13.4.22 ipv6 pim ssm

使用这个命令来使能PIMv6-SSM和指定SSM组范围。默认范围是FF3X::/32。使用关键字no来关闭PIMv6-SSM。

## 命令语法

```
ipv6 pim ssm [default | range list]
```

```
no ipv6 pim ssm
```

<b>default</b>	使用默认的 SSM IPv6 组播组范围
<b>range list</b>	使用访问控制列表中的组播组范围作为 SSM IPv6 组播组范围

## 命令模式

全局配置模式

## 默认

不使能

## 使用说明

无

## 举例说明

下面的例子用来演示使能 PIMv6-SSM,并将 SSM 组范围设置为默认范围。

```
Switch(config-if)# ipv6 pim ssm default
```

## 相关命令

无

### 13.4.23 show ipv6 pim sparse-mode bsr-router

使用此命令查看自举路由器信息。

## 命令语法

```
show ipv6 pim sparse-mode bsr-router
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

查看自举路由器信息。

```
Switch# show ipv6 pim sparse-mode bsr-router
```

```
PIM6v2 Bootstrap information
This system is the Bootstrap Router (BSR)
  BSR address: 2001:2::1 (?)
  Uptime:      00:00:08, BSR Priority: 64, Hash mask length: 126
  Next bootstrap message in 00:00:52
  Role: Candidate BSR
  State: Elected BSR
```

## 相关命令

无

### 13.4.24 show ipv6 pim sparse-mode interface

使用此命令查看稀疏模式下的端口信息。

## 命令语法

```
show ipv6 pim sparse-mode interface [detail]
```

<b>detail</b>	查看详细信息
---------------	--------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

查看稀疏模式下的端口信息。

Switch# show ipv6 pim sparse-mode interface detail

```
eth-0-1 (vif 0):
  Address fe80::9c7c:7eff:fe94:8300, DR fe80::9c7c:7eff:fe94:8300
  Hello period 30 seconds, Next Hello in 3 seconds
  Triggered Hello period 5 seconds
  Secondary addresses:
    2001:1::1
  Neighbors:
```

## 相关命令

无

### 13.4.25 show ipv6 pim sparse-mode local-member

使用此命令查看稀疏模式下的本地成员信息。

## 命令语法

**show ipv6 pim sparse-mode local-member** (*IFNAME* | )

<i>IFNAME</i>	端口名称
---------------	------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

查看稀疏模式下的本地成员信息。

```
Switch# show ipv6 pim sparse-mode local-members
```

```
PIM Local membership information
eth-0-2:
*, ff0e::1234:5678
   info: Include
```

## 相关命令

无

### 13.4.26 show ipv6 pim sparse-mode mroute

使用此命令查看SM模式下的多播路由。

## 命令语法

```
show ipv6 pim sparse-mode mroute (source_address | group_address |) (detail |)
```

<i>source_address</i>	IPv6 多播路由源地址
<i>group_address</i>	IPv6 多播路由目的地址
<b>detail</b>	详细信息

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

查看稀疏模式下的 IPv6 多播路由。

```
Switch# show ipv6 pim sparse-mode mroute detail
```

```
IPv6 Multicast Routing Table
(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 0
(S,G,rpt) Entries: 0
FCR Entries: 0
*, ff0e::1234:5678
Type: (*,G)
Uptime: 00:01:49
  RP: ::, RPF nbr: None, RPF idx: None
  Upstream:
    State: JOINED, SPT Switch: Enabled, JT: off
    Macro state: Join Desired,
  Downstream:
    eth-0-2:
      State: NO INFO, ET: off, PPT: off
      Assert State: NO INFO, AT: off
      Winner: ::, Metric: 4294967295, Pref: 4294967295, RPT bit: on
      Macro state: Could Assert, Assert Track
  Local Olist:
    eth-0-2
```

## 相关命令

无

### 13.4.27 show ipv6 pim sparse-mode neighbor

使用此命令查看稀疏模式下的邻居信息。

## 命令语法

```
show ipv6 pim sparse-mode neighbor ((IFNAME (address | )) | detail | )
```

<i>IFNAME</i>	端口名称
<i>address</i>	邻居地址
<b>detail</b>	详细信息

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

查看稀疏模式下的邻居信息

```
Switch# show ipv6 pim sparse-mode neighbor
```

Neighbor Address	Interface	Uptime/Expires	DR Pri/Mode
fe80::9c7c:7eff:fe94:8300	eth-0-9	00:00:40/00:01:44	1 / DR

## 相关命令

无

## 13.4.28 show ipv6 pim sparse-mode rp mapping

使用此命令查看IPv6多播组与RP的对应关系。

## 命令语法

```
show ipv6 pim sparse-mode rp mapping
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

查看 IPv6 多播组与 RP 的对应关系。

```
Switch# show ipv6 pim sparse-mode rp mapping
```

```
PIM Group-to-RP Mappings
Group(s): ff00::/8
  RP: 2001:1::1
    Info source: 2001:1::1, via bootstrap, priority 192
    Uptime: 00:00:25, expires: 00:02:05
```



Embedded RP Groups:

## 相关命令

无

### 13.4.29 show ipv6 pim sparse-mode rp-hash

使用此命令查看指定IPv6多播组的RP信息。

## 命令语法

**show ipv6 pim sparse-mode rp-hash** *group\_address*

<i>group_address</i>	组播组地址
----------------------	-------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

查看多播组 ff02::1234 的 RP。

```
Switch# show ipv6 pim sparse-mode rp-hash 224.0.0.10
```

```
RP: 2001:1::1
```

```
Info source: 2001:1::1, via bootstrap
```

## 相关命令

无

### 13.4.30 show ipv6 pim sparse-mode spt-threshold

使用此命令查看从共享树切换为最短路径树的阈值。

## 命令语法

**show ipv6 pim sparse-mode spt-threshold**

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

查看从共享树切换为最短路径树的阈值。

```
Switch# show ipv6 pim sparse-mode spt-threshold
```

```
IPv6 PIM sparse-mode immediately switches over to SPT upon receiving the first traffic
```

## 相关命令

无

# 13.5 MVR6 命令

## 13.5.1 mvr6

此命令用来使能和去使能 MVR6。

## 命令语法

```
mvr6
```

```
no mvr6
```

## 命令模式

全局配置模式

## 默认

不使能

## 使用说明

在交换机上使能 MVR6，在使能 MVR6 前，组播路由功能需要关闭。

## 举例说明

在交换机上使能 MVR6。

```
Switch(config)# no ipv6 multicast-routing
```

```
Switch(config)# mvr6
```

## 相关命令

无

### 13.5.2 mvr6 vlan

此命令用来指定MVR6的源VLAN。

## 命令语法

```
mvr6 vlan vlan vlan_id
```

```
no mvr6 vlan
```

<i>vlan_id</i>	VLAN id, 范围是 1 到 4094
----------------	-----------------------

## 命令模式

全局配置模式

## 默认

无

## 使用说明

在指定 MVR6 的源 VLAN 前，该 VLAN 的 `vlan interface` 需要先创建起来。

## 举例说明

下面的例子用来说明如何配置 MVR6 的源 VLAN。

```
Switch(config)# vlan database
```

```
Switch (config-vlan)# vlan 2
```

```
Switch (config)# interface vlan 2
```

```
Switch (config-if)# exit
```

```
Switch(config)# mvr6 vlan 2
```

## 相关命令

无

### 13.5.3 mvr6 group

此命令用来设置MVR6全局group。

## 命令语法

**mvr6 group** *address* (*count* | )

**no mvr6 group** *address* (*count* | )

<i>address</i>	组播组地址
<i>count</i>	要配置的组播组数目, 范围是 1~64

## 命令模式

全局配置模式

## 默认

无

## 使用说明

此命令用来设置 MVR6 全局 group。

## 举例说明

下面例子显示如何在端口上创建一条统计

下面的例子说明如何来创建 50 个静态 group, 范围是 ff0e::1~ff0e::50。

```
Switch(config)# mvr6 group ff0e::1 50
```

## 相关命令

无

### 13.5.4 mvr6 source-address

此命令用来设置或删除MVR6源地址。

## 命令语法

**mvr6 source-address** *address*

**no mvr6 source-address**

<i>address</i>	MVR6 上报组播报文的源地址
----------------	-----------------

**命令模式**

全局配置模式

**默认**

无

**使用说明**

无

**举例说明**

设置 MVR6 源地址为 2001::2

Switch(config)# mvr6 source-address 2001::2

**相关命令**

无

### 13.5.5 mvr6 type

此命令用来设置交换机端口作为MVR6的源端口或者接收端口。

**命令语法****mvr6 type (source | receiver vlan *vlan\_id*)****no mvr6 type (receiver vlan *vlan\_id* |)**

<b>source</b>	MVR6 源端口
<b>receiver</b>	MVR6 接收端口
<b>vlan <i>vlan_id</i></b>	VLAN id, 范围是 1 到 4094

**命令模式**

端口配置模式

## 默认

无

## 使用说明

在配置某个端口作为 MVR6 的源端口或接收端口时，源端口必须在 MVR6 源 VLAN 中，接收端口必须不在 MVR6 的源 VLAN 中。

## 举例说明

下面的例子将 eth-0-1 配置成 MVR6 的源端口，eth-0-2 配置成 VLAN2 中的接收端口。

```
Switch(config)# interface eth-0-1
Switch(config-if)# mvr6 type source
Switch(config)# interface eth-0-2
Switch(config-if)# mvr6 type receiver vlan 2
```

## 相关命令

无

### 13.5.6 show mvr6

此命令用来显示MVR6相关的信息。

## 命令语法

```
show mvr6
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子显示 MVR6 相关的信息。

```
Switch# show mvr6

MVR6 Running: TRUE
MVR6 Multicast VLAN: 2
```

```
MVR6 Source-address: fe80::1
MVR6 Max Multicast Groups: 1024
MVR6 Hw Rt Limit: 224
MVR6 Current Multicast Groups: 3
```

## 相关命令

无

### 13.5.7 show mvr6 interface

此命令用来显示MVR6端口相关的信息。

## 命令语法

```
show mvr6 interface
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子显示 MVR6 端口相关的信息。

```
Switch# show mvr6 interface
```

Port	Type	VLAN	Status
eth-0-2	source	10	ACTIVE
eth-0-1	receiver	11	ACTIVE

## 相关命令

无

### 13.5.8 show mvr6 group

此命令用来显示从MVR6接收端口上学习到组播组信息。

## 命令语法

```
show mvr6 group vlan vlan_id (group_address | )
```

<b>vlan</b> <i>vlan_id</i>	VLAN id, 范围是 1 到 4094
<i>group_address</i>	组播组地址

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子显示如何从 MVR6 接收端口上学习到组播组信息。

```
Switch# show mvr6 groups
```

```
VLAN  Interface  Group Address                               Uptime      Expire-time
1     eth-0-3    ff0e:2111:1111:1111:1111:1234:5678      00:00:11    00:04:10
```

## 相关命令

无

### 13.5.9 show mvr6 group static

此命令用来显示MVR6全局配置的静态组播组信息。

## 命令语法

```
show mvr6 group static global
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无



## 举例说明

下面例子显示 MVR6 全局配置的静态组播组信息。

```
Switch# show mvr6 groups static global
```

```
MVR6 Static Global Group:
ff0e::1234
ff0e::1235
ff0e::1236
ff0e:2111:1111:1111:1111:1111:1234:5678
```

## 相关命令

无

### 13.5.10 show resource mvr6

此命令用于显示MVR6的资源使用情况。

## 命令语法

```
show resource mvr6
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面例子显示 MVR6 的资源使用情况。

```
Switch# show resource mvr6
MVR
Resource                               Used      Capability
=====
MVR Entry                               4         224
L2 Mcast Member                         1         1792
```

## 相关命令

无

# 14 VPN 命令行参考

## 14.1 VRF 命令

### 14.1.1 ip vrf

使用该命令来配置 VPN 的路由转发表，使用该命令的 no 形式删除路由转发表。

#### 命令语法

**ip vrf** *VRF-NAME*

**no ip vrf** *VRF-NAME*

<i>VRF-NAME</i>	路由转发实例名
-----------------	---------

#### 命令模式

全局配置模式

#### 默认

无

#### 使用说明

无

#### 举例说明

```
Switch(config)# ip vrf ComA
Switch(config-vrf)# route-target both 100:2
Switch(config-vrf)# route-target import 200:1
```

#### 相关命令

**ip vrf forwarding**

## 14.1.2 为租户绑定 VXLAN 路由的 VNI

使用此命令为租户绑定 VXLAN 路由的 VNI，即将 VNI 配置为 L3VNI。

### 命令语法

**vni vni l3**

**no vni vni l3**

vni	Range <1-16777215>.
-----	---------------------

### 命令模式

VRF 模式

### 默认

无

### 使用说明

将 L2VNI 与 VRF 绑定，配置为 L3VNI。

### 举例说明

```
Switch(config)# ip vrf test
Switch(config-vrf)# vni-bind 50000
```

## 14.1.3 show ip vrf

使用该命令来显示 VRF 以及相关的接口。

### 命令语法

**show ip vrf (bgp (brief | detail) | interfaces | ospf | rip | VRF-NAME)**

<b>bgp</b>	显示 BGP 协议里 VRF 相关的接口信息
<b>interfaces</b>	显示所有的 VRF 相关的接口信息
<b>ospf</b>	显示 OSPF 协议里 VRF 相关的接口信息
<b>rip</b>	显示 RIP 协议里 VRF 相关的接口信息
<b>VRF-NAME</b>	VPN 路由转发实例名

<b>brief</b>	显示 BGP 协议里 VRF 的摘要信息
<b>detail</b>	显示 BGP 协议里 VRF 的详细信息

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch# show ip vrf
```

## 相关命令

无

## 14.1.4 ip vrf forwarding

使用该命令将某个 3 层接口加入 VPN 转发实例。使用该命令的 no 形式将 VRF 和 3 层接口解除绑定。

## 命令语法

**ip vrf forwarding** *VRF-NAME*

**no ip vrf forwarding** *VRF-NAME*

<i>VRF-NAME</i>	VPN 路由转发实例名
-----------------	-------------

## 命令模式

接口模式

## 默认

无

## 使用说明

使用该命令将会删除接口上原来的 IP 地址，您必须重新配置 IP 地址。

## 举例说明

```
Switch# configure terminal
Switch(config)# ip vrf ComA
Switch(config-vrf)# exit
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip vrf forwarding ComA
```

## 相关命令

**ip vrf**

**ip route vrf**

### 14.1.5 ip route vrf

使用该命令在 VRF 下创建静态路由，使用该命令的 **no** 形式删除该路由。

## 命令语法

**ip route vrf** *VRF-NAME* *DST\_NET* *NH\_ADDR*

**no ip route vrf** *VRF-NAME* *DST\_NET* *NH\_ADDR*

<i>VRF-NAME</i>	VPN 路由转发实例名
<i>DST_NET</i>	目的网段，目的网段的 IP 地址必须是如下格式：IP 地址加掩码长度(A.B.C.D/M) 或者 IP 地址加网络掩码 (A.B.C.D A.B.C.D)
<i>NH_ADDR</i>	下一跳的 IP 地址，地址格式为 A.B.C.D

## 命令模式

全局配置模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch(config)# ip route vrf VPN-NAME 2.2.2.0/24 1.1.1.2
```

## 相关命令

**show ip route vrf**

### 14.1.6 arp vrf

使用该命令在 VRF 下增加一条静态的 ARP 条目，使用该命令的 no 形式删除这条 ARP。

## 命令语法

**arp vrf** *VRF\_NAME* *A.B.C.D* *MAC*

**no arp vrf** *VRF\_NAME* *A.B.C.D*

<i>VRF-NAME</i>	VPN 路由转发实例名
<i>A.B.C.D</i>	主机 IP 地址
<i>MAC</i>	以 HHHH.HHHH.HHHH 格式表示的 MAC 地址

## 命令模式

全局配置模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch# configure terminal
Switch(config)# arp vrf vpn3 1.1.1.1 0000.1111.2222
```

## 相关命令

**show ip arp vrf** *VRF-NAME*

**clear ip arp vrf** *VRF-NAME* *A.B.C.D*

## 14.1.7 show ip arp vrf

使用该命令显示某个 VRF 下的 ARP 条目。

### 命令语法

**show ip arp vrf** *VRF-NAME*

<i>VRF-NAME</i>	VPN 路由转发实例名
-----------------	-------------

### 命令模式

特权模式

### 默认

无

### 使用说明

无

### 举例说明

这个例子显示了在 VRF ComA 下的所有 ARP 条目。

```
SwitH# show ip arp vrf ComA
Protocol    Address          Age (min)  Hardware Addr  Interface
Internet    1.1.1.1          -          0000.1111.2222
```

### 相关命令

**arp vrf**

## 14.1.8 clear ip arp vrf

使用该命令清除 VRF 下指定的动态 ARP 条目。

### 命令语法

**clear ip arp vrf** *VRF-NAME A.B.C.D*

<i>VRF-NAME</i>	VPN 路由转发实例名
<i>A.B.C.D</i>	动态学习到的主机 IP 地址

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

该命令显示了如何清除在 VRF 下学习到的 1.1.1.1 这条 ARP。

```
Switch# clear ip arp vrf ComA 1.1.1.1
```

## 相关命令

**arp vrf**

### 14.1.9 ping vrf

使用该命令在 VRF 下检测主机的可达性。

## 命令语法

**ping vrf** *VRF-NAME* *WORD*

<i>VRF-NAME</i>	VPN 路由转发实例名
<i>WORD</i>	目的 IP 地址或主机名

## 命令模式

特权模式

## 默认

无

## 使用说明

无



## 举例说明

```
Switch# ping vrf vpn 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
64 bytes from 1.1.1.1: icmp_seq=0 ttl=64 time=0.114 ms
64 bytes from 1.1.1.1: icmp_seq=1 ttl=64 time=0.087 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=64 time=0.087 ms
64 bytes from 1.1.1.1: icmp_seq=3 ttl=64 time=0.097 ms
64 bytes from 1.1.1.1: icmp_seq=4 ttl=64 time=0.133 ms
--- 1.1.1.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4041ms
rtt min/avg/max/mdev = 0.087/0.103/0.133/0.020 ms, pipe 2
```

## 相关命令

无

### 14.1.10 traceroute vrf

使用该命令在 VRF 下查看报文从当前设备到目的地所经过的路径。

## 命令语法

**traceroute vrf** *VRF-NAME* *WORD*

<i>VRF-NAME</i>	VPN 路由转发实例名
<i>WORD</i>	要跟踪的目的 IP 地址或主机名

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch# traceroute vrf vpn 1.1.1.1
traceroute to 1.1.1.1 (1.1.1.1), 30 hops max, 38 byte packets
 1  1.1.1.1 (1.1.1.1)  0.222 ms  0.169 ms  0.169 ms
```

## 相关命令

无

### 14.1.11 telnet vrf

使用该命令使用户可以方便地从当前以太网交换机登录到其它以太网交换机进行远程管理。

## 命令语法

**telnet vrf** *VRF-NAME* *WORD*

<i>VRF-NAME</i>	VPN 路由转发实例名
<i>WORD</i>	远端交换机的主机名或 IP 地址

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch# telnet vrf vpn 9.9.9.2
Trying 9.9.9.2...
Connected to 9.9.9.2.
Escape character is '^]'.
Fedora Core release 4 (Stentz)
Kernel 2.6.32.23 on an i686
login: root
Password:
```

## 相关命令

无

### 14.1.12 rd

使用该命令来设置 RD。

## 命令语法

**rd** *RD-VALUE*

<i>RD-VALUE</i>	RD 的值，格式为 <i>ASN:nn</i> 或 <i>IP-address:nn</i>
-----------------	--

## 命令模式

VRF 模式

## 默认

无

## 使用说明

RD 的作用是为了防止一台 PE 接收到远端 PE 发来的不同 VRF 的相同路由时不知所措，而加在路由前面的特殊信息。在 PE 发布路由时加上，在远端 PE 接收到路由后放在本地路由表中，用来与后来接收到的路由进行比较。

## 举例说明

```
Switch(config-vrf)# rd 1.1.1.1:1
```

## 相关命令

无

### 14.1.13 route-target

使用该命令来设置 RT。

## 命令语法

**route-target** ( **both** | **export** | **import** ) *RT-VALUE*

<b>both</b>	入方向和出方向
<b>export</b>	出方向
<b>import</b>	入方向
<i>RT-VALUE</i>	RT 的值，格式为 <i>ASN:nn</i> 或 <i>IP-address:nn</i>

## 命令模式

VRF 模式

## 默认

无

## 使用说明

RT 表明了一个 VRF 的路由喜好，通过他可以实现不同 VRF 之间的路由互通。他的本质就是 BGP 的 community 属性。

## 举例说明

```
Switch(config-vrf)# route-target import 100:1
```

## 相关命令

无

### 14.1.14 import map

该命令用来对当前 VPN 实例应用入方向路由策略。

## 命令语法

**import map** *WORD*

<i>WORD</i>	路由策略名
-------------	-------

## 命令模式

VRF 模式

## 默认

无

## 使用说明

当要求比采用扩展团体属性方式更精确地控制引入 VPN 实例路由时，可以采用入方向路由策略，缺省情况下根据路由的 VPN-target 扩展团体属性过滤引入的路由。入方向路由策略可能会拒绝从输入列表中的团体里选定的路由。

缺省情况下，允许所有 VPN Target 属性匹配的路由通过。

## 举例说明

```
Switch(config-vrf)# import map 100
```

## 相关命令

**export map**

### 14.1.15 export map

该命令用来对当前 VPN 实例应用出方向路由策略。

## 命令语法

**export map** *WORD*

<i>WORD</i>	路由策略名
-------------	-------

## 命令模式

VRF 模式

## 默认

无

## 使用说明

当要求比采用扩展团体属性方式更精确地控制发布的 VPN 实例路由时，可以使用出方向路由策略。此路由策略可能会过滤掉发布路由中选定的路由。缺省情况下，允许所有 VPN Target 属性匹配的路由通过。

## 举例说明

```
Switch(config-vrf)# export map 100
```

## 相关命令

**import map**

### 14.1.16 router-id

使用该命令设置路由器标志符。

## 命令语法

**router-id** *A.B.C.D*

<i>A.B.C.D</i>	以 IP 地址表示的路由器标志符
----------------	------------------

## 命令模式

VRF 模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch(config-vrf)# router-id 1.1.1.1
```

## 相关命令

**show ip vrf**

### 14.1.17 description

使用该命令给 VRF 增加描述。

## 命令语法

**description** *LINE*

<i>LINE</i>	VRF 描述，字符串长度不能超过 40，并且字符必须是 a-z，A-Z 或者 0-9
-------------	--

## 命令模式

VRF 模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch(config-vrf)# description VrfName1
```

## 相关命令

```
show ip vrf
```

# 14.2 IPv4 GRE 隧道配置命令

## 14.2.1 interface

使用该命令来创建一个 Tunnel 接口。使用该命令的 no 形式删除该 Tunnel 接口。

## 命令语法

```
interface tunnel tunnelid  
no interface tunnel tunnelid
```

<i>tunnelid</i>	接口编号，范围为 0~1023
-----------------	-----------------

## 命令模式

全局配置模式

## 默认

无

## 使用说明

如果要通过 IPv4 网络来连接两个隔离的 IPv4 网络，首先要创建 Tunnel 接口。配置其他属性之后，此 Tunnel 接口可用。使能后就可以转发封装后的 IPv4 报文。

注意，创建的 interface 没有配置 mode 之前，是不能进行有关接口上的任何操作的，此时接口不具备任何功能，只是单纯的创建 interface 结构体。

## 举例说明

下面的例子显示了如何创建一个 Tunnel 接口：

```
Switch# configure terminal  
Switch(config)# interface tunnel 1
```

## 相关命令

**show interface tunnel**

### 14.2.2 tunnel mode gre

使用该命令配置隧道模式。使用该命令的 **no** 形式恢复隧道模式默认值。

## 命令语法

**tunnel mode gre**

**no tunnel mode**

<b>gre</b>	当配置 tunnel 的模式为 GRE，即通用路由封装协议，目前暂时只支持 IPv4 gre tunnel，即针对 IPv 4 报文进行封装，且封装后的报文依然为 IPv4。
------------	---

## 命令模式

接口模式

## 默认

无

## 使用说明

当配置 tunnel 的模式为 GRE 时，必须要手动配置 tunnel source 和 tunnel destination，不支持自动隧道。只有先配好 mode，才能继续配置 tunnel 的上其他参数。

## 举例说明

下面的例子显示了如何配置隧道模式为 gre:

```
Switch# configure terminal
Switch(config)# interface tunnel 1
Switch(config-if)# tunnel mode gre
```

## 相关命令

**tunnel source**

**tunnel destination**

### 14.2.3 tunnel source

使用该命令来配置隧道的源地址，使用该命令的 **no** 形式删除隧道的源地址。



## 命令语法

**tunnel source (A.B.C.D | IFNAME)**

**no tunnel source**

<b>A.B.C.D</b>	指定隧道的源地址为 IPv4 地址格式
<b>IFNAME</b>	指定隧道的源地址从接口 IPv4 地址中获得，如果接口上有多个地址，则只取主 IP 地址。接口可以为：路由口，vlan 虚拟口，环回口

## 命令模式

接口模式

## 默认

无

## 使用说明

每个隧道必须指定一个隧道源。如果隧道源是接口方式配置的，则从接口的主 IP 地址中获取地址。

## 举例说明

下面的例子显示了如何设置隧道源：

```
Switch# configure terminal
Switch(config)# interface tunnel 1
Switch(config-if)# tunnel source 3.3.3.3
```

## 相关命令

**tunnel mode gre**

**tunnel destination**

### 14.2.4 tunnel destination

使用该命令来配置隧道的目的地址。使用该命令的 no 形式删除隧道的目的地址。

## 命令语法

**tunnel destination A.B.C.D**

**no tunnel destination**

<b>A.B.C.D</b>	指定 tunnel 接口的目的 IPv4 地址
----------------	-------------------------

## 命令模式

接口模式

## 默认

无

## 使用说明

只有手工隧道才需要配置隧道目的地址。

## 举例说明

下面的例子显示了如何配置隧道的目的地址：

```
Switch# configure terminal
Switch(config)# interface tunnel 1
Switch(config-if)# tunnel destination 4.4.4.4
```

## 相关命令

**tunnel source**

**tunnel mode ipv6ip**

### 14.2.5 tunnel enable

使用该命令设置使能解封装隧道报文的接口。使用该命令的 **no** 形式恢复默认设置。

## 命令语法

**tunnel (enable|disable)**

<b>enable</b>	使能隧道报文解封装
<b>disable</b>	去使能隧道报文解封装

## 命令模式

接口模式

## 默认

不会对收到的隧道报文解封装。

## 使用说明

无

## 举例说明

下面的例子显示了如何设置隧道报文解封装接口：

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# tunnel enable
```

## 相关命令

**interface**

### 14.2.6 tunnel gre key

配置 gre tunnel 的 key

no tunnel gre key 删除该配置。

## 命令语法

tunnel gre key *key\_value*

<i>key_value</i>	<1- 4294967295>
------------------	-----------------

## 命令模式

接口模式

## 默认

无

## 使用说明

配置 gre key 为了与对端 tunnel 进行报文认证，是 gre tunnel 的一个重要功能，只有对 key 相匹配的报文才进行解封装后转发，提高 gre 隧道的安全性，可以使用设置的 gre key 对隧道封装的报文进行端到端校验。只有在 tunnel mode 为 gre 模式的时候才能配置 gre key，目前 gre key 可以支持 32bit，但是不支持配置 0。

## 举例说明

配置 tunnel 的 gre key

```
Switch(config-if)# tunnel gre key 666
```

## 相关命令

**tunnel source**

**no tunnel gre key**

## 14.2.7 tunnel dscp

使用该命令设置外层 IPv4 头的 DSCP 值。使用该命令的 **no** 形式恢复从内层 IPv4 头获取 DSCP 的方式。

### 命令语法

**tunnel dscp** *DSCP*

**no tunnel dscp**

<i>DSCP</i>	设置外层 IPv4 头的 DSCP 值，范围 0~63
-------------	-----------------------------

### 命令模式

接口模式

### 默认

默认从内层 IPv4 头获取 DSCP 值。

### 使用说明

无

### 举例说明

下面的例子显示了如何设置外层 IPv4 头的 DSCP 值为 40:

```
Switch# configure terminal
Switch(config)# interface tunnel 1
Switch(config-if)# tunnel dscp 40
```

### 相关命令

## 14.2.8 keepalive

使用该命令使能 **keepalive** 功能，用来检测对端 **gre tunnel** 是否处于有效 **up** 状态以及 **tunnel** 之间的链路是否通或者可达。

### 命令语法

**keepalive** *period\_value* *retry\_value*

**no keepalive**

<i>period_value</i>	keepalive 发包的间隔时间 <1-32767>
<i>retry_value</i>	keepalive 发包的超时次数 <1-255>

## 命令模式

接口模式

## 默认

*period\_value*: 10s

*retry\_value*: 3

## 使用说明

keepalive 只支持在 gre tunnel 上使能，不支持其他类型的 tunnel。当使能 keepalive 后，只有当 tunnel 接口上配有 tunnel source 和 tunnel destination 时，才会发 keepalive 报文出来。

## 举例说明

下面的例子显示了如何使能 gre tunnel 接口的 keepalive 功能：

```
Switch# configure terminal
Switch(config)# interface tunnel 1
Switch(config-if)# keepalive 10 5
```

## 相关命令

**no keepalive**

## 14.2.9 show interface tunnel

使用该命令来显示 tunnel 接口的信息。

## 命令语法

**show interface tunnel** *tunnelid*

<i>tunnelid</i>	接口编号，范围 0~1023
-----------------	----------------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面的例子显示了 **tunnel** 接口的信息：

```
Switch# show interface tunnel 1
Interface tunnell
  Interface current state: UP
  Hardware is Tunnel
  Index 8193 , Metric 1 , Encapsulation TUNNEL
  VRF binding: not bound
  Internet primary address:
    1.1.1.1/24 pointopoint 1.1.1.255
  Tunnel protocol/transport GRE/IP, Status Valid
  Tunnel source 192.192.168.1(eth-0-10), destination 10.10.10.10
  Tunnel DSCP inherit, Tunnel TTL 255
  Tunnel transport MTU 1476 bytes
  Tunnel GRE key enable: 100
  Tunnel GRE keepalive enable, Send period: 5, Retry times: 3
  0 packets input, 0 bytes
  0 packets output, 0 bytes
```

## 相关命令

**show resource tunnel**

### 14.2.10 show resource tunnel

使用该命令来显示 **tunnel** 资源的使用信息。

## 命令语法

**show resource tunnel**

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面的例子显示了 **tunnel** 资源的使用信息：

```
Switch# show resource tunnel
Tunnel
Resource                               Used           Capability
=====
Peers                                   3              8
```

## 相关命令

### 14.2.11 show tunnel keepalive statistics

使用该命令来显示 gre tunnel keepalive 报文的统计信息

## 命令语法

**show tunnel keepalive statistics** (*interface tunnel id*)

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面的例子显示了 gre tunnel 使能 keepalive 后的统计信息：

```
Switch# show tunnel keepalive statistics
Name          Status   Keepalive  Out_ka_pkt  In_ka_pkt  TunnelUp  TunnelDown
-----
tunnel1       Up       Enable    9347        9347        0          0
tunnel2       Up       Disable   0           0           0          0
```

## 相关命令

clear tunnel keepalive statistics

### 14.2.12 clear tunnel keepalive statistics

使用该命令可以清空 gre tunnel 上 keepalive 的统计信息

## 命令语法

```
clear tunnel keepalive statistics(all |interface tunnel id)
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面的例子清空 gre tunnel 使能 keepalive 后的统计信息：

```
Switch# clear tunnel keepalive statistics all
```

## 相关命令

```
show tunnel keepalive statistics
```

### 14.2.13 clear tunnel statistics

使用该命令可以清空 gre tunnel 上 output 和 input 方向的统计信息

## 命令语法

```
clear tunnel statistics (all |interface tunnel id)
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面的例子清空 gre tunnel encap 和 decap 的统计信息：

```
Switch# clear tunnel statistics all
```



## 相关命令

show interface tunnel id

---

# 15 可靠性命令行参考

---

## 15.1 BHM 命令

### 15.1.1 sysmon enable

使用此命令使能系统监控功能，使用此命令的 no 形式关闭监控功能。

#### 命令语法

```
sysmon enable
no sysmon enable
```

#### 命令模式

全局配置模式

#### 默认

系统监控功能打开

#### 用法

无

#### 举例说明

下面的例子显示如何使能系统监控功能：

```
Switch# configure terminal
Switch(config)# sysmon enable
```

#### 相关命令

```
show sysmon
```

### 15.1.2 show sysmon

使用此命令查看系统监控功能的状态。

## 命令语法

**show sysmon**

## 命令模式

特权模式

## 默认

无

## 用法

无

## 举例说明

下面的例子显示如何查看系统监控功能的状态：

```
Switch# show sysmon
System monitor enable.
```

## 相关命令

**sysmon enable**

### 15.1.3 heart-beat-monitor enable

使用此命令使能 bhm 功能，使用此命令的 no 形式关闭 bhm 功能。

## 命令语法

**heart-beat-monitor enable**

**no heart-beat-monitor enable**

## 命令模式

全局配置模式

## 默认

使能 bhm 功能

## 用法

无

## 举例说明

下面的例子显示了如何使能 bhm 功能：

```
Switch# configure terminal
Switch(config)# heart-beat-monitor enable
```

## 相关命令

**show heart-beat-monitor**

### 15.1.4 heart-beat-monitor reactivate

使用此命令指定当某个 PM 无响应时系统采取的措施，使用此命令的 no 命令恢复默认配置。

## 命令语法

**heart-beat-monitor reactivate (reload system | shutdown port [warning])**

reload system	重启系统
shutdown port	关闭所有的端口
warning	在终端打印警告信息

## 命令模式

全局配置模式

## 默认

默认使能 bhm 的重启系统

## 用法

无

## 举例说明

如下例子显示如何配置系统在程序无响应时采取的措施：

```
Switch# configure terminal
Switch(config)# heart-beat-monitor reactivate reload system
```

## 相关命令

**show heart-beat-monitor**

### 15.1.5 show heart-beat-monitor

使用此命令查看程序监控状态。

## 命令语法

**Show heart-beat-monitor**

## 命令模式

特权模式

## 默认

无

## 用法

无

## 举例说明

如下例子显示查看程序监控状态：

```
Switch# show heart-beat-monitor
heart-beat-monitor enable.
heart-beat-monitor reactivation: restart system.
```

## 相关命令

**heart-beat-monitor enable**

**heart-beat-monitor reactivate**

## 15.1.6 cpu-limit percent

CPU limit 是一个限制进程使用 CPU 的功能。使用此命令指定特定进程最大能使用的 CPU 利用率，使用此命令的 no 命令恢复默认配置。利用率的精准度误差小于 5%。

## 命令语法

**cpu-limit (ospf|rip|mstp|bgp|pim|ldp|ssm|pdm|ospf6|ripng|pim6|nsm|hsrv|dhcpd|snmp)  
percent <1-100>**

ospf	OSPF 模块
rip	RIP 模块
mstp	MSTP 模块
bgp	BGP 模块
pim	PIM 模块
ldp	LDP 模块
ssm	Synce 模块

pdm	PIM DM 模块
ospf6	OSPFv6 模块
ripng	RIPNG 模块
pim6	PIM6 模块
nsm	nsm 模块
hsrv	hsrv 模块
dhcpcd	dhcpcd 模块
snmp	snmp 模块

## 命令模式

全局配置模式

## 默认

默认不使能 CPU limit。

## 用法

无

## 举例说明

如下例子显示如何配置 CPU limit:

```
Switch# configure terminal
Switch(config)# cpu-limit ospf percent 60
```

## 相关命令

# 15.2 CFM 命令

## 15.2.1 ethernet cfm enable

使用该命令全局启用 CFM 功能，使用 no 命令关闭该功能。

## 命令语法

**ethernet cfm enable**

**no ethernet cfm enable**

## 命令模式

全局配置模式

## 默认

默认关闭

## 使用说明

无

## 举例说明

以下用例展示了如何全局使能 CFM:

```
Switch# configure terminal
Switch(config)# ethernet cfm enable
Switch(config)# no ethernet cfm enable
```

## 相关命令

无

## 15.2.2 ethernet cfm domain level

使用该命令可以创建一个维护域，每个维护域对应一个等级，不同等级提供不同的功能。

## 命令语法

**ethernet cfm domain** *DOMAIN\_NAME* level *LEVEL*

**no ethernet cfm domain** *DOMAIN\_NAME*

DOMAIN_NAME	维护域名字
LEVEL	维护域等级，取值范围 0-7

## 命令模式

全局配置模式

## 默认

无

## 使用说明

维护域取值范围 0-7，定义如下：

0~2 (运营商等级)

3~4 (提供商等级)

5~7 (客户等级)

## 举例说明

以下用例展示了如何创建和删除 MD：

```
Switch# configure terminal
Switch(config)# ethernet cfm domain test level 5
Switch(config-ether-cfm)# exit
Switch(config)# no ethernet cfm domain test
```

## 相关命令

无

### 15.2.3 service

使用该命令创建一个服务。

## 命令语法

**service** *CSI\_ID* (**vlan** *VLAN\_ID*)

**no service** *CSI\_ID*

<b>CSI_ID</b>	服务名
<b>vlan VLAN_ID</b>	Vlan 标识，取值范围 1-4094

## 命令模式

CFM 配置模式

## 默认

无

## 使用说明

无



## 举例说明

以下用例展示了如何创建和删除 MA:

```
Switch# configure terminal
Switch(config)# ethernet cfm domain test level 5
Switch(config-ether-cfm)# service cst vlan 30
Switch(config-ether-cfm)# no service cst
```

## 相关命令

**ethernet cfm domain** *DOMAIN\_NAME* level *LEVEL*

### 15.2.4 ethernet cfm mep

使用该命令创建维护域端点 MEP。在同一个服务内，每一个 MEP 和远端 MEP 必须有一个唯一的标识。如果在同一台交换机上配置相同标识的 MEP，设备会提示重复，不允许配置。

## 命令语法

**ethernet cfm mep** (**down|up**) **mpid** *MEPID* **domain** *DOMAIN\_NAME* (**vlan** *VLAN\_ID* | **interval** (1 | 2 | 3 | 4 | 5 | 6 | 7))

**no ethernet cfm mep** (**down|up**) **mpid** *MEPID* **domain** *DOMAIN\_NAME* (**vlan** *VLAN\_ID* |)

down	Down 维护域端节点
up	Up 维护域端节点
MEPID	MEP 标识，取值范围 1-8191
DOMAIN_NAME	维护域名字
<b>vlan</b> <i>VLAN_ID</i>	Vlan 标识，取值范围 1-4094
1	CCM 发送周期为 3.3 毫秒
2	CCM 发送周期为 10 毫秒
3	CCM 发送周期为 100 毫秒
4	CCM 发送周期为 1 秒
5	CCM 发送周期为 10 秒
6	CCM 发送周期为 1 分钟
7	CCM 发送周期为 10 分钟

## 命令模式

端口配置模式

## 默认

无

## 使用说明

无

## 举例说明

以下用例展示了如何创建 MEP:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ethernet cfm mep down mpid 1 domain md1 vlan 2 interval 1
```

## 相关命令

`ethernet cfm domain DOMAIN_NAME level LEVEL`

`service CSI_ID (vlan VLAN_ID)`

## 15.2.5 ethernet cfm mep crosscheck mpid

使用该命令配置远端 MEP。在同一个服务内，每一个 MEP 和远端 MEP 必须有一个唯一的标识。如果在同一台交换机上配置相同标识的 MEP，设备会提示重复，不允许配置。

## 命令语法

`ethernet cfm mep crosscheck mpid MEPID domain DOMAIN_NAME (vlan VLAN_ID |) (mac MAC)`

`no ethernet cfm mep crosscheck mpid MEPID domain DOMAIN_NAME (vlan VLAN_ID |)`

MEPID	MEP 标识，取值范围 1-8191
DOMAIN_NAME	维护域名字
vlan VLAN_ID	Vlan 标识，取值范围 1-4094
MAC	远端 MEP 的 mac 地址

## 命令模式

端口配置模式

## 默认

无

## 使用说明

无

## 举例说明

以下用例展示了如何创建远端 MEP:

```
Switch# configure terminal
Switch(config)# ethernet cfm domain test level 5
Switch(config-ether-cfm)# service cst vlan 30
Switch(config-ether-cfm)# exit
Switch(config)# interface eth-0-9
Switch(config-if)# ethernet cfm mep crosscheck mpid 8000 domain test vlan 30 mac
0.0.1
```

## 相关命令

`ethernet cfm domain DOMAIN_NAME level LEVEL`

`service CSI_ID (vlan VLAN_ID)`

## 15.2.6 ethernet cfm mip

使用该命令配置维护域中间节点。

## 命令语法

`ethernet cfm mip level LEVEL vlan VLAN_ID`

`no ethernet cfm mip level LEVEL vlan VLAN_ID`

LEVEL	维护域等级，取值范围 1-7
VLAN_ID	Vlan 标识，取值范围 1-4094

## 命令模式

端口配置模式

## 默认

无

## 使用说明

无

## 举例说明

以下用例展示了如何创建 MIP:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ethernet cfm mip level 5 vlan 2
```

## 相关命令

ethernet cfm domain *DOMAIN\_NAME* level *LEVE*  
**service** *CSI\_ID* (vlan *VLAN\_ID*)

## 15.2.7 ethernet cfm cc enable domain

使用该命令启动维护域内某个服务的连续性检查功能。

## 命令语法

ethernet cfm cc enable domain *DOMAIN\_NAME* (vlan *VLAN\_ID*)  
 no ethernet cfm cc enable domain *DOMAIN\_NAME* (vlan *VLAN\_ID*)

<b>DOMAIN_NAME</b>	维护域名字
<b>vlan VLAN_ID</b>	Vlan 标识, 取值范围 1-4094

## 命令模式

全局配置模式

## 默认

无

## 使用说明

无

## 举例说明

以下用例展示了如何启用连续性检查:

```
Switch# configure terminal
Switch(config)# ethernet cfm cc enable domain test vlan 2
```

## 相关命令

ethernet cfm domain *DOMAIN\_NAME* level *LEVEL*

**service** *CSI\_ID* (**vlan** *VLAN\_ID*)

## 15.2.8 ethernet cfm cc domain priority

使用该命令配置某个服务的连续性检查报文中 VLAN 的优先权值。

### 命令语法

**ethernet cfm cc domain** *DOMAIN\_NAME* (**vlan** *VLAN\_ID*) **priority** *VLAN\_PRIORITY*

no ethernet cfm cc domain *DOMAIN\_NAME* (**vlan** *VLAN\_ID*) priority

DOMAIN_NAME	维护域名字
<b>vlan</b> VLAN_ID	Vlan 标识, 取值范围 1-4094
VLAN_PRIORITY	Vlan 优先级, 取值范围 0-7

### 命令模式

全局配置模式

### 默认

无

### 使用说明

无

### 举例说明

以下用例展示了如何设置连续性检查报文中的 VLAN 优先权值:

```
Switch# configure terminal
Switch(config)# ethernet cfm cc domain test vlan 2 priority 3
```

### 相关命令

ethernet cfm domain *DOMAIN\_NAME* level *LEVEL*

**service** *CSI\_ID* (**vlan** *VLAN\_ID*)

ethernet cfm cc enable domain *DOMAIN\_NAME* (**vlan** *VLAN\_ID*)

## 15.2.9 ethernet cfm loopback

使用该命令发起以太网环回消息 LBM 到远端 MEP 以验证远端 MEP 是否可达。

## 命令语法

**ethernet cfm loopback (multicast | unicast rmepid RMEPID) mepid MEPID (domain DOMAIN\_NAME | level LEVEL) (vlan VLAN\_ID) (repeat COUNT)(timeout TIMEOUT)(priority PRIORITY)**

<b>multicast</b>	发给组播报文
<b>unicast</b>	发送单播报文
<b>rmepid</b>	远端 MEP
<b>RMEPID</b>	远端 MEP 标识, 取值范围 1-8191
<b>MEPID</b>	MEP 标识, 取值范围 1-8191
<b>domain DOMAIN_NAME</b>	维护域名字
<b>level LEVEL</b>	维护域等级, 取值范围 0-7
<b>vlan VLAN_ID</b>	Vlan 标识, 取值范围 1-4094
<b>repeat COUNT</b>	发送 LB 报文次数, 取值范围 1-255
<b>timeout TIMEOUT</b>	LB 报文超时时间, 取值范围 1-65535, 默认 5 秒
<b>priority PRIORITY</b>	LB 报文中的 vlan 优先级, 取值范围 0-7

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

以下用例展示了如何发起以太网回环:

```
Switch# ethernet cfm loopback multicast mepid 1 domain test vlan 2 repeat 3 timeout 5 priority 7
```

## 相关命令

**ethernet cfm mep (down|up) mpid *MEPID* domain *DOMAIN\_NAME* (vlan *VLAN\_ID* ) interval (1 | 2 | 3 | 4 | 5 | 6 | 7)**

ethernet cfm mep crosscheck mpid *MEPID* (vlan *VLAN\_ID* |) mac *MAC*

### 15.2.10 ethernet cfm loopback mac

发送以太网环回消息 LBM 到远端 MEP 或 MIP，验证 MEP 或 MIP 的可达性。

## 命令语法

**ethernet cfm loopback mac *MACADDRESS* unicast mepid *MEPID* (domain *DOMAIN\_NAME* | level *LEVEL*) (vlan *VLAN\_ID*) (repeat *COUNT*)(timeout *TIMEOUT*)(priority *PRIORITY*)**

<b>MACADDRESS</b>	远端 MEP 的 mac 地址
<b>MEPID</b>	MEP 标识，取值范围 1-8191
<b>domain DOMAIN_NAME</b>	维护域名称
<b>level LEVEL</b>	维护域等级，取值范围 0-7
<b>vlan VLAN_ID</b>	Vlan 标识，取值范围 1-4094
<b>repeat COUNT</b>	发送 LB 报文次数，取值范围 1-255
<b>timeout TIMEOUT</b>	LB 报文超时时间，取值范围 1-65535，默认 5 秒
<b>priority PRIORITY</b>	LB 报文中的 vlan 优先级，取值范围 0-7

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

以下用例展示了如何发起以太网回环：

```
Switch# ethernet cfm loopback mac 0.0.1 unicast mepid 1 domain test vlan 2 repeat 3
timeout 5 priority 7
```

## 相关命令

**ethernet cfm mep (down|up) mpid** *MEPID* **domain** *DOMAIN\_NAME* (**vlan** *VLAN\_ID* |) **interval** (*1* | *2* | *3* | *4* | *5* | *6* | *7*)

ethernet cfm mep crosscheck mpid *MEPID* (vlan *VLAN\_ID* |) mac *MAC*

### 15.2.11 ethernet cfm errors enable domain

使用该命令配置保存上报的 CCM 的错误信息，默认保存。

## 命令语法

ethernet cfm errors enable domain *DOMAIN\_NAME* (vlan *VLAN\_ID* |)

no ethernet cfm errors enable domain *DOMAIN\_NAME* (vlan *VLAN\_ID* |)

DOMAIN_NAME	维护域名字
vlan VLAN_ID	Vlan 标识，取值范围 1-4094

## 命令模式

全局配置模式

## 默认

无

## 使用说明

对于每一个 MEP，最多保存最近的五条错误信息

## 举例说明

以下用例展示了如何开启错误缓存功能：

```
Switch# configure terminal
Switch(config)# ethernet cfm errors enable domain test vlan 2
```

## 相关命令

无



## 15.2.12 clear ethernet cfm errors

使用该命令清空维护域中的错误信息。

### 命令语法

```
clear ethernet cfm errors (domain DOMAIN_NAME | level LEVEL)
```

<b>domain</b> DOMAIN_NAME	维护域名字
<b>level</b> LEVEL	维护域等级，取值范围 0-7

### 命令模式

特权模式

### 默认

无

### 使用说明

无

### 举例说明

以下用例展示了如何清空错误信息：

```
Switch# clear ethernet cfm errors domain test
```

### 相关命令

无

## 15.2.13 ethernet cfm ais status enable

使用该命令启动或关闭告警指示信号 ais 功能和配置相关参数。

### 命令语法

```
ethernet cfm ais status enable (all | loc | mismerge | unexpected-mep | unexpected-meg-level |  
unexpected-period) domain DOMAIN_NAME (vlan VLAN_ID)
```

```
level LEVEL (unicast RMEP_MAC | multicast) (cvlan VLAN_LIST)
```

```
no ethernet cfm ais status enable (all | loc | mismerge | unexpected-mep | unexpected-meg-  
level | unexpected-period) domain DOMAIN_NAME (vlan VLAN_ID)
```

**level LEVEL (unicast RMEP\_MAC | multicast)**

all	对所有 error 产生 ais 报文
loc	对 CCM 报文丢失产生 ais 报文
mismmerge	当 MD 或 MA 不匹配时，产生 ais 报文
unexpected-mep	当 MEP 的 ID 不匹配时，产生 ais 报文
unexpected-meg-level	当报文的 level 不匹配时，产生 ais 报文
unexpected-period	当报文的发送周期不匹配时，产生 ais 报文
DOMAIN_NAME	维护域名字
vlan VLAN_ID	Vlan 标识，取值范围 1-4094
LEVEL	发送 ais 报文的维护域等级，取值范围 1-7
unicast	发送单播报文
RMEP_MAC	远端 MEP 的 mac 地址
multicast	发送组播报文
cvlan VLAN_LIST	配置 ais 报文 cvlan 的取值范围 1-4094

**命令模式**

端口配置模式

**默认**

无

**使用说明**

无

**举例说明**

以下用例展示了如何配置 AIS:

```
Switch# configure terminal
Switch(config)# ethernet cfm ais status enable all domain test vlan 2 level 5
multicast
```

**相关命令**

无

## 15.2.14 ethernet cfm ais suppress alarm enable domain

使用该命令配置 ais 抑制告警。当启用该功能且已进入 AIS 状态时，LOC 错误信息将不会再上报。

### 命令语法

```
ethernet cfm ais suppress alarm enable domain DOMAIN_NAME (vlan VLAN_ID)
```

```
no ethernet cfm ais suppress alarm enable domain DOMAIN_NAME (vlan VLAN_ID)
```

DOMAIN_NAME	维护域名字
vlan VLAN_ID	Vlan 标识，取值范围 1-4094

### 命令模式

全局配置模式

### 默认

无

### 使用说明

无

### 举例说明

以下用例展示了如何配置 AIS 抑制告警：

```
Switch# configure terminal
Switch(config)# ethernet cfm ais suppress alarm enable domain test vlan 2
```

### 相关命令

无

## 15.2.15 ethernet cfm server-ais status enable level

使用该命令配置 ais 服务器和相关参数。

### 命令语法

```
ethernet cfm server-ais status enable level LEVEL (interval (1|60))
```

```
no ethernet cfm server-ais status enable
```

LEVEL	发送 ais 报文的维护域等级，取值范围 1-7
interval (1 60)	Ais 报文的发送周期，发送 ais 报文的时间间隔为 1 秒或 60 秒，默认值为 1 秒

## 命令模式

端口配置模式

## 默认

无

## 使用说明

无

## 举例说明

以下用例展示了如何配置 AIS 服务器：

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ethernet cfm server-ais status enable level 5 interval 60
```

## 相关命令

无

### 15.2.16 show ethernet cfm domain

使用该命令显示维护域和服务的相关信息。

## 命令语法

```
show ethernet cfm domain DOMAIN_NAME
```

DOMAIN_NAME	维护域名字
-------------	-------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

以下用例展示了如何显示维护域的相关信息：

```
Switch# show ethernet cfm domain test
```

## 相关命令

无

### 15.2.17 show ethernet cfm maintenance-points

使用该命令显示相关的 MEP, 远端 MEP 和 MIP 的相关信息。

## 命令语法

```
show ethernet cfm maintenance-points
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

以下用例展示了如何显示 MEP, 远端 MEP 和 MIP 的信息：

```
Switch# show ethernet cfm maintenance-points
```

## 相关命令

无

### 15.2.18 show ethernet cfm maintenance-points local

使用该命令显示本地 MEP 和 MIP 的相关信息。

## 命令语法

```
show ethernet cfm maintenance-points local (mep|mip) (interface IFNAME | domain
DOMAIN_NAME | level LEVEL)
```

mep	维护域端节点
mip	维护域中间节点
interface <i>IFNAME</i>	端口名
<b>domain</b> <i>DOMAIN_NAME</i>	维护域名字
<b>level</b> <i>LEVEL</i>	维护域等级，取值范围 0-7

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

以下用例展示了如何显示 MEP 和 MIP 的信息：

```
Switch# show ethernet cfm maintenance-points local mep interface eth-0-1
```

## 相关命令

无

### 15.2.19 show ethernet cfm maintenance-points remote

使用该命令显示远端 MEP 的相关信息。

## 命令语法

```
show ethernet cfm maintenance-points remote (mpid MEPID | mac MAC) (domain
DOMAIN_NAME | level LEVEL) (vlan VLAN_ID)
```

<b>mpid</b> MEPID	远端 MEP 标识, 取值范围 1-8191
<b>mac</b> MAC	远端 MEP 的 mac 地址
<b>domain</b> DOMAIN_NAME	维护域名字
<b>level</b> LEVEL	维护域等级, 取值范围 0-7
<b>vlan</b> VLAN_ID	Vlan 标识, 取值范围 1-4094

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

以下用例展示了如何显示远端 MEP 的相关信息:

```
Switch# show ethernet cfm maintenance-points remote mpid 1 domain test
```

## 相关命令

无

## 15.2.20 show ethernet cfm cc config

使用该命令显示连续性检查的配置。

## 命令语法

```
show ethernet cfm cc config
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

以下用例展示了如何显示连续性检查的配置：

```
Switch# show ethernet cfm cc config
```

## 相关命令

无

### 15.2.21 show ethernet cfm errors

使用该命令显示 CFM 的错误信息。

## 命令语法

```
show ethernet cfm errors (domain DOMAIN_NAME | level LEVEL)
```

<b>domain</b> DOMAIN_NAME	维护域名字
<b>level</b> LEVEL	维护域等级，取值范围 0-7

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

以下用例展示了如何显示错误信息：

```
Switch# show ethernet cfm errors
```

## 相关命令

无



## 15.2.22 show ethernet cfm ais mep

使用该命令显示 MEP 的 ais 相关信息。

### 命令语法

show ethernet cfm ais mep *MEPID* domain *DOMAIN\_NAME* (vlan *VLAN\_ID*)

<b>MEPID</b>	MEP 标识, 取值范围 1-8191
<b>DOMAIN_NAME</b>	维护域名字
<b>vlan VLAN_ID</b>	Vlan 标识, 取值范围 1-4094

### 命令模式

特权模式

### 默认

无

### 使用说明

无

### 举例说明

以下用例展示了如何显示 AIS 的相关信息:

```
Switch# show ethernet cfm ais mep 1 domain test vlan 2
```

### 相关命令

无

## 15.2.23 show ethernet cfm

该用该命令显示 CFM 的全局信息

### 命令语法

show ethernet cfm

### 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

以下用例展示了如何显示 CFM 的全局信息：

```
Switch# show ethernet cfm
```

## 相关命令

无

### 15.2.24 ethernet cfm linktrace rmepid

使用该命令发送链路跟踪 LTM 报文到远端 MEP, 用于发现到达远端 MEP 的路径。

## 命令语法

ethernet cfm linktrace rmepid *RMEPID* (domain *DOMAIN\_NAME* | level *LEVEL*) (vlan *VLAN\_ID*) (ttl *TTL* | timeout *TIMEOUT* | priority *PRIORITY* | ltm-egress-identifier-tlv | sender-id-tlv | organization-specific-tlv )

<b>RMEPID</b>	远端 MEP 标识, 取值范围 1-8191
<b>MEPID</b>	MEP 标识, 取值范围 1-8191
<b>domain DOMAIN_NAME</b>	维护域名字
<b>level LEVEL</b>	维护域等级, 取值范围 0-7
<b>vlan VLAN_ID</b>	Vlan 标识, 取值范围 1-4094
<b>ttl TTL</b>	最大跳数, 取值范围 1-255, 默认值为 64
<b>timeout TIMEOUT</b>	超时时间, 取值范围 1-65535, 默认值为 5
<b>priority PRIORITY</b>	Vlan 优先级, 取值范围 0-7, 默认值为 7
<b>ltm-egress-identifier-tlv</b>	是否携带 LTM egress identifier TLV
<b>sender-id-tlv</b>	是否携带 Sender ID TLV
<b>organization-specific-tlv</b>	是否携带 Organization Specific TLV

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

以下用例展示了如何发起链路追踪：

```
Switch# ethernet cfm linktrace rmepid 1 mepid 2 domain test vlan 2 ttl 255 timeout
5 priority 7
```

## 相关命令

**ethernet cfm mep (down|up) mpid MEPID domain DOMAIN\_NAME (vlan VLAN\_ID | interval (1 | 2 | 3 | 4 | 5 | 6 | 7))**

ethernet cfm mep crosscheck mpid MEPID (vlan VLAN\_ID | (mac MAC))

## 15.2.25 ethernet cfm linktrace mac

使用该命令向远端 MEP 或 MIP 的 mac 地址发送 LTM 报文，用于发现到达远端 MEP 或 MIP 的路径。

## 命令语法

**ethernet cfm linktrace mac MACADDRESS mepid MEPID (domain DOMAIN\_NAME | level LEVEL) (vlan VLAN\_ID) (ttl TTL | timeout TIMEOUT) priority PRIORITY)**

MACADDRESS	远端 MEP 的 mac 地址
MEPID	MEP 标识，取值范围 1-8191
<b>domain</b> DOMAIN_NAME	维护域名字
<b>level</b> LEVEL	维护域等级，取值范围 0-7
VLAN_ID	Vlan 标识，取值范围 1-4094
<b>ttl</b> TTL	最大跳数，取值范围 1-255，默认值为 64
<b>timeout</b> TIMEOUT	超时时间，取值范围 1-65535，默认值为 5

<b>priority PRIORITY</b>	Vlan 优先级，取值范围 0-7，默认值为 7
--------------------------	--------------------------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

以下用例展示了如何发起链路追踪：

```
Switch# ethernet cfm linktrace mac 7234.ef5a.2806 mepid 1 domain test vlan 2 ttl
255 timeout 5 priority 7
```

## 相关命令

**ethernet cfm mep (down|up) mpid MEPID domain DOMAIN\_NAME (vlan VLAN\_ID | interval (1 | 2 | 3 | 4 | 5 | 6 | 7))**

ethernet cfm mep crosscheck mpid MEPID (vlan VLAN\_ID |) (mac MAC)

## 15.2.26 ethernet cfm linktrace cache enable

使用该命令缓存 LT 的信息，默认不缓存。

## 命令语法

ethernet cfm linktrace cache enable

no ethernet cfm linktrace cache enable

## 命令模式

全局配置模式

## 默认

不缓存

## 使用说明

无

## 举例说明

以下用例展示了如何缓存链路追踪的信息：

```
Switch# configure terminal
Switch(config)# ethernet cfm linktrace cache enable
```

## 相关命令

无

### 15.2.27 ethernet cfm linktrace cache size

使用该命令配置 LT 缓存区的大小。

## 命令语法

```
ethernet cfm linktrace cache size ENTRIES
no ethernet cfm linktrace cache size
```

ENTRIES	缓存区的大小，取值范围 1-65535，默认 100
---------	----------------------------

## 命令模式

全局配置模式

## 默认

100

## 使用说明

无

## 举例说明

以下用例展示了如何配置链路追踪信息缓存区的大小：

```
Switch# configure terminal
Switch(config)# ethernet cfm linktrace cache size 200
```

## 相关命令

无

### 15.2.28 ethernet cfm linktrace cache holdtime

使用该命令配置 LT 缓存区保持时间。

## 命令语法

ethernet cfm linktrace cache holdtime *MINUTES*

MINUTES	缓存时间，取值范围 1-65535 分钟，默认值为 60 分钟
---------	---------------------------------

## 命令模式

全局配置模式

## 默认

60 分钟

## 使用说明

无

## 举例说明

以下用例展示了如何配置链路追踪信息缓存的时间：

```
Switch# configure terminal
Switch(config)# ethernet cfm linktrace cache holdtime 90
```

## 相关命令

无

## 15.2.29 show ethernet cfm linktrace cache

使用该命令显示 LT 缓存区条目

## 命令语法

show ethernet cfm linktrace cache

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

以下用例展示了如何显示链路追踪缓存区的信息：

```
Switch# show ethernet cfm linktrace cache
```

## 相关命令

无

### 15.2.30 clear ethernet cfm linktrace cache

使用该命令清空 LT 的缓存区。

## 命令语法

```
clear ethernet cfm linktrace cache
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

以下用例展示了如何清除链路追踪缓存区的信息：

```
Switch# clear ethernet cfm linktrace cache
```

## 相关命令

无

### 15.2.31 ethernet cfm mip ccm-database size

使用该命令配置 MIP 转发表的数据库大小。

## 命令语法

```
ethernet cfm mip ccm-database size ENTRIES  
no ethernet cfm mip ccm-database size
```

ENTRIES	缓存区的大小，取值范围 1-65535，默认 100 条
---------	------------------------------

**命令模式**

全局配置模式

**默认**

100 条

**使用说明**

无

**举例说明**

以下用例展示了如何配置 MIP 转发表的大小：

```
Switch# configure terminal
Switch(config)# ethernet cfm mip ccm-database size 200
```

**相关命令**

无

### 15.2.32 ethernet cfm mip ccm-database holdtime

使用该命令配置 MIP 转发表的数据库保持时间。

**命令语法**

```
ethernet cfm mip ccm-database holdtime MINUTES
no ethernet cfm mip ccm-database holdtime
```

MINUTES	MIP 转发表保持时间，取值范围 60-65535 分钟，默认为 60 分钟
---------	--

**命令模式**

全局配置模式

**默认**

60 分钟



## 使用说明

无

## 举例说明

以下用例展示了如何配置 MIP 转发表保持的时间：

```
Switch# configure terminal
Switch(config)# ethernet cfm mip ccm-database holdtime 90
```

## 相关命令

无

### 15.2.33 show ethernet cfm mip ccm-database

使用该命令显示 MIP 转发表。

## 命令语法

```
show ethernet cfm mip ccm-database
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

以下用例展示了如何显示 MIP 转发表的信息：

```
Switch# show ethernet cfm mip ccm-database
```

## 相关命令

无

### 15.2.34 clear ethernet cfm mip ccm-database

使用该命令清空 MIP 转发表。

## 命令语法

```
clear ethernet cfm mip ccm-database
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

以下用例展示了如何清除 MIP 转发表：

```
Switch# clear ethernet cfm mip ccm-database
```

## 相关命令

无

## 15.2.35 ethernet cfm sf-reason

使用该命令可配置信号失败的原因，这些原因将触发 g8031/g8032 切换。

## 命令语法

```
ethernet cfm sf-reason (all | {loc | rdi-rx | ais-defect} | none)
```

```
no Ethernet cfm sf-reason
```

all	配置所有原因都触发 g8031/g8032 切换
loc	配置仅 CCM 报文丢失触发 g8031/g8032 切换
rdi-rx	配置仅远端 MEP 的 RDI 为 0 时触发 g8031/g8032 切换
ais-defect	配置仅 MEP 进入 ais 状态时触发 g8031/g8032 切换
none	无任何原因会触发 g8031/g8032 切换

## 命令模式

全局配置模式

## 默认

Loc 会触发 g8031/g8032 切换

## 使用说明

无

## 举例说明

以下用例展示了如何配置显示信息失败的原因:

```
Switch# configure terminal
Switch(config)# ethernet cfm sf-reason all
```

## 相关命令

无

## 15.2.36 ethernet cfm mode

使用该命令配置 CFM 的全局模式，使用 no 命令将 CFM 的模式恢复成 802.1ag。

## 命令语法

ethernet cfm mode (dot1ag|y1731)

no ethernet cfm mode

dot1ag	IEEE 802.1ag-2007
y1731	ITU-T Y.1731

## 命令模式

全局配置模式

## 默认

IEEE 802.1ag-2007

## 使用说明

无

## 举例说明

以下用例展示了如何配置 CFM 的模式:

```
Switch# configure terminal
Switch(config)# ethernet cfm mode dot1ag
Switch(config)# no ethernet cfm mode
```

## 相关命令

无

### 15.2.37 ethernet cfm lm enable dual-ended

使用该命令使能双端的帧丢失测量。

## 命令语法

**ethernet cfm lm enable dual-ended** (domain *DOMAIN\_NAME* | level *LEVEL*) (vlan *VLAN\_ID* |) **mepid** *MEPID* (all-cos | per-cos | cos *COS\_VALUE*) (stats-interval *INTERVAL\_VALUE*) (cache-size *CACHE\_VALUE*)

no ethernet cfm lm enable dual-ended (domain *DOMAIN\_NAME* | level *LEVEL*) (vlan *VLAN\_ID* |) mepid *MEPID*

DOMAIN_NAME	维护域名字
LEVEL	维护域等级，取值范围 0-7
VLAN_ID	Vlan 标识，取值范围 1-4094
MEPID	MEP 标识，取值范围 1-8191
all-cos	将带不同 cos 的所有报文一起统计
per-cos	将带不同 cos 的所有报文分别统计
cos <i>COS_VALUE</i>	.统计带有特定 cos 的报文
stats-interval INTERVAL_VALUE	每隔一个统计周期，系统会读取计数值，计算近端和远端的丢包和丢包率统计周期取值范围是 1 秒到 10 秒，默认 1 秒
cache-size CACHE_VALUE	缓存统计结果的条数，取值范围是 1 到 512，默认值为 128

## 命令模式

全局配置模式

## 默认

无

## 使用说明

无

## 举例说明

以下用例展示了如何使能双端的帧丢失测量:

```
Switch# configure terminal
Switch(config)# ethernet cfm lm enable dual-ended domain md1 vlan 2 mepid 1 all-cos
stats-interval 1 cache-count 256
```

## 相关命令

无

### 15.2.38 ethernet cfm lm enable single-ended

使用该命令使能单端的帧丢失测量。

## 命令语法

ethernet cfm lm enable single-ended (domain *DOMAIN\_NAME* | level *LEVEL*) (vlan *VLAN\_ID* |) mepid *MEPID* (all-cos | per-cos | cos *COS\_VALUE*)

no ethernet cfm lm enable single-ended (domain *DOMAIN\_NAME* | level *LEVEL*) (vlan *VLAN\_ID* |) mepid *MEPID*

DOMAIN_NAME	维护域名字
LEVEL	维护域等级, 取值范围 0-7
VLAN_ID	Vlan 标识, 取值范围 1-4094
MEPID	MEP 标识, 取值范围 1-8191
all-cos	将带不同 cos 的所有报文一起统计
per-cos	将带不同 cos 的所有报文分别统计
cos COS_VALUE	.统计带有特定 cos 的报文

## 命令模式

全局配置模式

## 默认

无

## 使用说明

无

## 举例说明

以下用例展示了如何使能单端的帧丢失测量:

```
Switch# configure terminal
Switch(config)# ethernet cfm lm enable single-ended domain mdl vlan 2 mepid 1 all-
cos
```

## 相关命令

无

### 15.2.39 ethernet cfm lm single-ended

使用该命令发送单端帧丢失测量消息。

## 命令语法

```
ethernet cfm lm single-ended (domain DOMAIN_NAME | level LEVEL) (vlan VLAN_ID |)
rmepid RMEPID mepid MEPID (count COUNT) (interval (1|2|3|))
```

DOMAIN_NAME	维护域名字
LEVEL	维护域等级, 取值范围 0-7
VLAN_ID	Vlan 标识, 取值范围 1-4094
RMEPID	远端 MEP 标识, 取值范围 1-8191
MEPID	MEP 标识, 取值范围 1-8191
count COUNT	发送报文数目, 取值范围是 1 到 60, 默认值为 1
interval	LMM 报文发送间隔, 默认值是 1 秒
1	LMM 报文发送间隔为 100 毫秒
2	LMM 报文发送间隔为 1 秒
3	LMM 报文发送间隔为 10 秒

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

以下用例展示了如何发送单端帧丢失测量消息:

```
Switch# ethernet cfm lm single-ended domain mdl vlan 2 rmepid 2 mepid 1 count 10
interval 1
```

## 相关命令

无

### 15.2.40 show ethernet cfm lm

使用该命令可以显示双端帧丢失测量的结果。

## 命令语法

**show ethernet cfm lm domain** *DOMAIN\_NAME* (**vlan** *VLAN\_ID*) **mepid** *MEPID* (**cos** *COS\_VALUE*)

DOMAIN_NAME	维护域名字
VLAN_ID	Vlan 标识, 取值范围 1-4094
MEPID	MEP 标识, 取值范围 1-8191
cos COS_VALUE	显示指定 cos 的测量结果, 取值范围是 0-7, 默认值为 0

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

以下用例展示了如何显示双端帧丢失测量的结果:

```
Switch# show ethernet cfm lm domain mdl vlan 2 mepid 3
DOMAIN      : mdl
VLAN        : 2
MEPID       : 1
Start Time  : 2013/07/15 9:00:09
End Time    : 2013/07/15 9:00:09
```

Notes : 1. When the difference of Tx is less than the difference of Rx,  
the node is invalid, loss and loss ratio should be "-";  
2. When loc is reported for mep, the loss should be "-" and loss  
ratio should be 100%;  
3. When calculate average loss and loss ratio, invalid or loc nodes  
will be excluded;  
Latest dual-ended loss statistics:

-----

Index Cos Local-loss Local-loss ratio Remote-loss Remote-loss ratio Time

Index	Cos	Local-loss	Local-loss ratio	Remote-loss	Remote-loss ratio	Time
1	all	4	050.0000%	4	050.0000%	09:00:09
2	all	-	-	-	-	09:00:09
3	all	0	000.0000%	100	100.0000%	09:00:09
4	all	0	000.0000%	99	099.0000%	09:00:09
5	all	0	000.0000%	90	090.0000%	09:00:09
6	all	0	000.0000%	1	001.0000%	09:00:09
7	all	0	000.0000%	0	000.0000%	09:00:09
8	all	-	-	-	-	09:00:09
9	all	0	000.0000%	4294967039	099.9999%	09:00:09
10	all	0	000.0000%	510	099.8043%	09:00:09
11	all	-	100.0000%	-	100.0000%	09:00:09
12	all	0	000.0000%	0	000.0000%	09:00:09
13	all	4	050.0000%	4	050.0000%	09:00:09
14	all	4	050.0000%	4	050.0000%	09:00:09

-----

Maximum Local-loss : 4            Maximum Local-loss Ratio : 100.0000%  
 Minimum Local-loss : 0            Minimum Local-loss Ratio : 000.0000%  
 Average Local-loss : 1            Average Local-loss Ratio : 013.6363%  
 Maximum Remote-loss : 4294967039    Maximum Remote-loss Ratio : 100.0000%  
 Minimum Remote-loss : 0            Minimum Remote-loss Ratio : 000.0000%  
 Average Remote-loss : 390451622    Average Remote-loss Ratio : 058.1640%

## 相关命令

无

### 15.2.41 ethernet cfm sd-reason

使用该命令配置信号缺陷原因（SD-Reason）。当双端帧丢包率超过门限，会打印日志。

## 命令语法

**ethernet cfm sd-reason (domain DOMAIN\_NAME | level LEVEL) (vlan VLAN\_ID |) mepid MEPID ratio RATIO\_VALUE**

**no ethernet cfm sd-reason (domain DOMAIN\_NAME | level LEVEL) (vlan VLAN\_ID |) mepid MEPID**

DOMAIN_NAME	维护域名字
-------------	-------



LEVEL	维护域等级，取值范围 0-7
VLAN_ID	Vlan 标识，取值范围 1-4094
MEPID	MEP 标识，取值范围 1-8191
RATIO_VALUE	双端帧丢包率门限取值范围是 1-1000，单位是千分之一

## 命令模式

全局配置模式

## 默认

无

## 使用说明

无

## 举例说明

以下用例展示了如何配置信号缺陷原因:

```
Switch# configure terminal
Switch(config)# ethernet cfm sd-reason domain md1 vlan 2 mepid 1 ratio 100
```

## 相关命令

无

### 15.2.42 ethernet cfm (1dm | dmm)

使用该命令可以发送 1dm 或 dmm 帧时延测量消息，并接收远端的回复，计算帧时延。

## 命令语法

```
ethernet cfm (1dm|dmm) rmepid RMEPID mepid MEPID count COUNT (domain
DOMAIN_NAME | level LEVEL) (vlan VLAN_ID |) (priority PRIORITY |interval (1|2|3|))
(frame_size SIZE|)
```

RMEPID	远端 MEP 标识，取值范围 1-8191
MEPID	MEP 标识，取值范围 1-8191
COUNT	发送报文数，取值范围是 1-60
DOMAIN_NAME	维护域名字

VLAN_ID	Vlan 标识, 取值范围 1-4094
LEVEL	维护域等级, 取值范围 0-7
priority PRIORITY	Vlan 的优先级, 取值范围是 0-7, 默认值为 7
interval	发送 DM 的时间间隔, 默认是 1 秒
1	发送 DM 的时间间隔为 100 毫秒
2	发送 DM 的时间间隔为 1 秒
3	发送 DM 的时间间隔为 10 秒
frame_size SIZE	报文的大小, 取值范围是 64 字节-9600 字节, 默认是 64 字节

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

以下用例展示了发送 DMM 消息:

```
Switch# configure terminal
Switch(config)# ethernet cfm dmm mepid 1 rmepid 2 duration 5 domain mdl vlan 2
priority 3 interval 1
```

## 相关命令

无

### 15.2.43 ethernet cfm delaymeasurement cache enable

使用该命令配置缓存延时测量的结果, 默认是使能的。

## 命令语法

```
ethernet cfm delaymeasurement cache enable
no ethernet cfm delaymeasurement cache enable
```

## 命令模式

全局配置模式

## 默认

使能

## 使用说明

无

## 举例说明

以下用例展示了如何配置缓存帧时延测量的结果:

```
Switch# configure terminal
Switch(config)# ethernet cfm delaymeasurement cache enable
```

## 相关命令

无

### 15.2.44 ethernet cfm delaymeasurement cache size

使用该命令配置帧时延测量缓存区的大小。

## 命令语法

```
ethernet cfm delaymeasurement cache size ENTRIES
no Ethernet cfm delaymeasurement cache size
```

ENTRIES	缓存条目数，取值范围是 1-65535，默认值为 1000
---------	-------------------------------

## 命令模式

全局配置模式

## 默认

1000

## 使用说明

无

## 举例说明

以下用例展示了如何配置帧时延测量缓存区的大小:

```
Switch# configure terminal
Switch(config)# ethernet cfm delaymeasurement cache size 100
```

## 相关命令

无

### 15.2.45 show ethernet cfm delaymeasurement cache

使用该命令可以显示帧时延测量的结果。

## 命令语法

```
show ethernet cfm delaymeasurement cache
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

以下用例展示了如何显示帧时延测量的结果:

```
Switch# show ethernet cfm delaymeasurement cache
```

## 相关命令

无

### 15.2.46 clear ethernet cfm delaymeasurement cache

使用该命令可以清空帧时延测量缓存区。

## 命令语法

```
clear ethernet cfm delaymeasurement cache
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

以下用例展示了如何清空帧时延测量缓存区:

```
Switch# clear ethernet cfm delaymeasurement cache
```

## 相关命令

无

### 15.2.47 ethernet cfm csf

使用该命令在客户 MEP 和服务器 MEP 间配置 客户信号失败（CSF）关系。

## 命令语法

**ethernet cfm csf client domain** *CLI\_DOMAIN\_NAME* (**vlan** *CLI\_VLAN\_ID* |) **mepid** *CLI\_MEPID* **server domain** *SRV\_DOMAIN\_NAME* (**vlan** *SRV\_VLAN\_ID* |) **mepid** *SRV\_MEPID* (**tx-interval** (1|60))

**no ethernet cfm csf client domain** *CLI\_DOMAIN\_NAME* (**vlan** *CLI\_VLAN\_ID* |) **mepid** *CLI\_MEPID* **server domain** *SRV\_DOMAIN\_NAME* (**vlan** *SRV\_VLAN\_ID* |) **mepid** *SRV\_MEPID*

CLI_DOMAIN_NAME	客户维护域名字
<b>vlan</b> CLI_VLAN_ID	客户 Vlan 标识, 取值范围 1-4094
CLI_MEPID	客户 MEP 标识, 取值范围 1-8191
SRV_DOMAIN_NAME	服务器维护域名字
<b>vlan</b> SRV_VLAN_ID	服务器 Vlan 标识, 取值范围 1-4094
SRV_MEPID	服务器 MEP 标识, 取值范围 1-8191
tx-interval (1 60)	发送 CSF 报文的时间间隔, 取值范围是 1、60 秒, 默认是 60 秒

## 命令模式

全局配置模式

## 默认

无

## 使用说明

无

## 举例说明

以下用例展示了如何配置 CSF 关系:

```
Switch# configure terminal
Switch(config)# ethernet cfm csf client domain cust vlan 30 mepid 88 server domain
provid vlan 20 mepid 666 tx-interval 1
```

## 相关命令

无

## 15.2.48 show ethernet cfm csf

使用该命令显示 CSF 的关系和状态。

## 命令语法

```
show ethernet cfm csf
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

以下用例展示了如何显示 CSF:

```
Switch# show ethernet cfm csf
En-CSF Enable, Y(Yes)/N(No)
CTR-Client Trigger reason, L(los)/F(fdi)/R(rdi)/N(null)
ECC-Enter CSF Condition, Y(Yes)/N(No)
SRR-Server Rx Reason, L(los)/F(fdi)/R(rdi)/D(dci)/N(null)
Tx-I, Transmit Interval
Rx-I, The period which is gotten from LCK packets
Client Mep                               Server Mep
```

```

MEPID Cli-Domain  VLAN  CTR  ECC MPID Srv-Domain  VLAN SRR  Tx-I Rx-I
1003 md1234567890 3001 L/F/R  Y   1004  md1234567890 2001 L/F/R 1    1

```

## 相关命令

无

### 15.2.49 ethernet cfm lck enable

使用该命令锁定 MEP，使数据报文无法通过。

## 命令语法

```

ethernet cfm lck enable mep MEPID domain DOMAIN_NAME (vlan VLAN_ID |) tx-level
TX_LEVEL ({tx-interval (1|60)| cvlan VLAN_LIST}|)

```

```

no ethernet cfm lck enable mep MEPID domain DOMAIN_NAME (vlan VLAN_ID |)

```

DOMAIN_NAME	维护域名字
vlan VLAN_ID	Vlan 标识，取值范围 1-4094
MEPID	MEP 标识，取值范围 1-8191
TX_LEVEL	指定 LCK 报文向哪个 level 发送
tx-interval (1 60)	发送 LCK 报文的周期，取值范围是 1-60 秒，默认是 60 秒
cvlan VLAN_LIST	配置 LCK 报文 cvlan 的取值范围 1-4094

## 命令模式

端口配置模式

## 默认

无

## 使用说明

无

## 举例说明

以下用例展示了如何锁定 MEP:

```

Switch# configure terminal
Switch(config)# ethernet cfm lck enable mep 1 domain md1 tx-level 2 interval 1
cvlan 1

```

## 相关命令

无

### 15.2.50 show ethernet cfm lck

使用该命令显示 LCK 的信息。

## 命令语法

```
show ethernet cfm lck
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

以下用例展示了如何显示 LCK 的信息:

```
Switch# show ethernet cfm lck
En-LCK Enable, Y(Yes)/N(No)
Rx-LC, Receive LCK packets and enter LCK condition, Y(Yes)/N(No)
Rx-I, The period which is gotten from LCK packets
Tx-Domain, frames with ETH-LCK information are sent to this Domain
Tx-I, Transmit Interval
MPID Domain          VLAN En Rx-LC Rx-I Tx-Domain      Tx-I
1001 md1234567890 3001 Y N          N/A md1234567891 1
```

## 相关命令

无

### 15.2.51 show ethernet cfm lm brief

使用该命令显示所有使能了 LM 的 mep 信息。

## 命令语法

```
show ethernet cfm lm brief
```

## 命令模式

特权模式



默认

无

使用说明

无

举例说明

以下用例展示了如何显示使能了 LM 的 mep 信息:

```
Switch# show ethernet cfm lm
-----
MPID Domain      VLAN LM-En
-----
1    mdl          2    dual-lm-enabled
5    mdl          2    single-lm-enabled
```

相关命令

无

### 15.2.52 ethernet cfm tst transmission enable

使用该命令使能以太网测试信号(ETH-Test)发送功能。

命令语法

ethernet cfm tst transmission enable session *SESSION\_ID* domain *DOMAIN\_NAME* (vlan *VLAN\_ID* |) mep *MEPID* tx-mode (fixed pkt-num *NUMBER* |continuous) ({pattern-type (repeat *VALUE* | random | increment-byte | decrement-byte) |packet-size *PACKET\_SIZE* | dest-mac (multicast | *MACADDRESS*)}|)

no ethernet cfm tst transmission enable session *SESSION\_ID* domain *DOMAIN\_NAME* (vlan *VLAN\_ID* |) mepid *MEPID*

SESSION_ID	测试用会话 ID
DOMAIN_NAME	客户维护域名字
vlan VLAN_ID	客户 Vlan 标识, 取值范围 1-4094
MEPID	客户 MEP 标识, 取值范围 1-8191
NUMBER	发送报文个数, 取值范围 从 1 到 65535
VALUE	报文填充模式为重复固定值时, 该固定值取值范围从 0 到 0xFFFFFFFF
PACKET_SIZE	发送报文的大小, 取值范围 从 64 字节到 16027 字节, 默认 512 字节
multicast	tst 报文的地址为组播地址, 默认是组播地址

MACADDRESS	tst 报文的目的地地址为单播地址
------------	-------------------

## 命令模式

全局配置模式

## 默认

无

## 使用说明

无

## 举例说明

下面举例说明如何使能 tst:

```
Switch# configure terminal
Switch(config)# ethernet cfm tst transmission enable session 1 domain md1 vlan 2
mep 1 tx-mode continuous pattern-type random packet-size 1518
```

## 相关命令

无

### 15.2.53 ethernet cfm tst start/stop

使用该命令启动或停止发送 test 报文。

## 命令语法

**ethernet cfm tst start session *SESSION\_ID* rate *RATE* time (cos *COS\_VALUE*)(second *SECOND* |1m|15m|2h|24h) (tx\_port *TX\_PORT*)**

ethernet cfm tst stop

SESSION_ID	测试用会话 ID
RATE	发送速率，取值范围是 1mbps 到 10G
cos COS_VALUE	Vlan 优先级，取值范围 0-7，默认值为 7
SECOND	发送时长为从 1 秒钟到 60 秒钟
15m	发送时长为 15 分钟
2h	发送时长为 2 小时
24h	发送时长为 24 小时

TX_PORT	发送 TST 报文的端口，仅对 up mep 有效
---------	---------------------------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

以下用例展示如何启动发送 test 报文:

```
Switch(config)# ethernet cfm tst start session 2 rate 10 time second 1
```

## 相关命令

无

## 15.2.54 ethernet cfm tst reception enable

使用该命令使能接收 test 报文.

## 命令语法

```
ethernet cfm tst reception enable session SESSION_ID domain DOMAIN_NAME (vlan VLAN_ID |) mepid MEPID
```

```
no ethernet cfm tst reception enable session SESSION_ID domain DOMAIN_NAME (vlan VLAN_ID |) mepid MEPID
```

session	测试用会话 ID
DOMAIN_NAME	客户维护域名字
vlan VLAN_ID	客户 Vlan 标识，取值范围 1-4094
MEPID	客户 MEP 标识，取值范围 1-8191

## 命令模式

全局配置模式

## 默认

无

## 使用说明

Test 发送和接收只可以使能在同一个 MEP 上。

## 举例说明

以下用例展示如何使能接收 test 报文:

```
Switch# configure terminal
Switch(config)# ethernet cfm tst reception enable session 1 domain md1 vlan 2 mep 1
```

## 相关命令

无

## 15.2.55 show ethernet cfm tst

使用该命令显示 test 的信息

## 命令语法

```
show ethernet cfm tst
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

以下用例展示如何显示 test 的信息:

发送侧显示信息如下:

```
Switch# show ethernet cfm tst
DOMAIN          : md1
VLAN            : 2
MEPID           : 1
Transmission    : Enabled
Reception       : Disabled
Status          : Non-Running
```

```
Start Time      : 03:22:35
Predict End Time : 03:23:05
Actual End Time  : 03:23:05
Packet Type     : TST
Rate            : 1000 mbps
Packet Size     : 64 bytes
Tx Number       : 28
Tx Bytes        : 1792
Rx Number       : 0
Rx Bytes        : 0
```

接收侧显示信息如下:

```
Switch# show ethernet cfm tst
DOMAIN          : mdl
VLAN            : 2
MEPID          : 2
Transmission    : Disabled
Reception       : Enabled
Status          : Non-Running
Start Time      : null
End Time        : null
Packet Type     : null
Rate            : null
Packet Size     : null
Tx Number       : 0
Tx Bytes        : 0
Rx Number       : 28
Rx Bytes        : 1792
```

## 相关命令

无

## 15.2.56 clear ethernet cfm tst counters

使用该命令清空 test 计数器。

## 命令语法

```
clear ethernet cfm tst counters
```

## 命令模式

特权模式

## 默认

无

## 使用说明

当正在发送 test 报文时，不允许去清 test 的计数器。

## 举例说明

以下用例展示清空 test 计数器:

```
Switch# clear ethernet cfm tst counters
```

## 相关命令

无

## 15.3 CPU Traffic Limit 命令

### 15.3.1 cpu-traffic-limit total rate

使用此命令配置所有进入 CPU 的流的总限速，使用此命令的 **no** 形式恢复到默认值。

## 命令语法

```
cpu-traffic-limit total rate RATE-RANGE
```

```
no cpu-traffic-limit total rate
```

<b>RATE-RANGE</b>	进入 CPU 的流的总限速，单位 pps，范围<0-1000000>
-------------------	------------------------------------

## 命令模式

全局配置模式

## 默认

2048 pps

## 使用说明

无。

## 举例说明

如下的例子显示如何配置进入 CPU 的流的总限速:

```
Switch(config)# cpu-traffic-limit total rate 3000
```

## 相关命令

```
show cpu traffic-limit
```

## 15.3.2 cpu-traffic-limit reason rate

使用此命令配置进入 CPU 的各个 reason 的限速，使用此命令的 no 形式恢复到默认值。

### 命令语法

```
cpu-traffic-limit reason {bpdu | slow-protocol | eapol | erps | smart-link | arp | dhcp | rip | ldp | ospf | pim | vrrp | ipda | icmp-redirect | mcast-rpf-fail | macsa-mismatch | port-security-discard | vlan-security-discard | ip-mtu-fail | ip-option | ucast-ip-ttl-fail | mpls-ttl-fail | igmp | sflow-ingress | fwd-to-cpu | udld | mld | dot1x-mac-bypass | bfd-learning } rate RATE-RANGE
```

```
no cpu-traffic-limit reason {bpdu | slow-protocol | eapol | erps | smart-link | arp | dhcp | rip | ldp | ospf | pim | vrrp | ipda | icmp-redirect | mcast-rpf-fail | macsa-mismatch | port-security-discard | vlan-security-discard | ip-mtu-fail | ip-option | ucast-ip-ttl-fail | mpls-ttl-fail | igmp | sflow-ingress | sflow-egress | fwd-to-cpu | udld | mld | dot1x-mac-bypass | bfd-learning } rate
```

bpdu	BPDU 协议报文(包括 STP, RSTP, MSTP)
slow-protocol	Slow 协议报文.(包括 EFM, LACP, SYNCE)
eapol	Dot1x 协议报文
erps	ERPS 协议报文
arp	ARP 协议报文
dhcp	DHCP 协议报文
rip	RIP 协议报文
bgp	BGP 协议报文
ldp	LDP 协议报文
ospf	OSPF 协议报文
pim	PIM 协议报文
vrrp	VRRP 协议报文
ipda	IPDA 协议报文
icmp-redirect	ICMP 重定向
learning-full	MAC 学习缓存已满
mcast_rpf_fail	组播报文 RPF 检查失败
macsa-mismatch	与一个端口 security entry 不匹配时的学习报文
port-security-discard	端口 security entry 学满时的学习报文
vlan-security-discard	VLAN 内学习的 MAC 达到限制是的学习报文

ip-mtu-fail	需要分片的报文
Ip-option	带有可选字段的 IP 报文
ucast-ttl-fail	TTL 失效的单播 IP 报文
mpls-ttl-fail	TTL 失效 MPLS 报文
Igmp	IGMP 或者 IGMP Snooping 报文
sflow-ingress	在入口方向 Sflow 的采样报文
sflow-egress	在出口方向 Sflow 的采样报文
fwd-to-cpu	转发到 CPU 的报文
mld	MLD 或者 MLD Snooping 报文
dot1x-mac-bypass	Dot1x 旁路认证报文
bfd-learning	Bfd 学习报文
RATE-RANGE	进入 CPU 的各个 Reason 的限速值，单位 kbps，范围 <0-1000000>

## 命令模式

全局配置模式

### 默认

Reason	Rate(pps)	Reason	Rate(pps)
bpdu	64	icmp-redirect	128
slow-protocol	128	mcast-rpf-fail	128
eapol	128	macsa-mismatch	128
erps	128	port-security-discard	128
smart-link	128	vlan-security-discard	128
arp	640	udld	128
dhcp	128	ip-mtu-fail	64
rip	64	fwd-to-cpu	64
ldp	512	ip-option	512
ospf	256	ucast-ttl-fail	64
pim	128	mpls-ttl-fail	64
vrrp	512	igmp	128



Reason	Rate(pps)	Reason	Rate(pps)
ipda	1024	sflow-ingress	128
sflow-egress	128	mld	128
dot1x-mac-bypass	64	bfd-learning	128

## 使用说明

无。

## 举例说明

如下的例子显示了如何配置 reason bpdu 的限速值为 300kbps:

```
Switch(config)# cpu-traffic-limit reason bpdu rate 300
```

## 相关命令

```
show cpu traffic-limit
```

### 15.3.3 cpu-traffic-limit reason class

使用此命令配置各个进入 CPU 的 reason 的调度优先级类。使用此命令的 no 形式恢复到默认值。

## 命令语法

```
cpu-traffic-limit reason {bpdu | slow-protocol | eapol | erps | smart-link | arp | dhcp | rip | ldp | ospf | pim | vrrp | ipda | icmp-redirect | mcast-rpf-fail | macsa-mismatch | port-security-discard | vlan-security-discard | mtu-dontfrag | mtu-frag | ip-option | ucast -ttl-fail | mpls-ttl-fail | igmp | sflow-ingress | udld|mld| dot1x-mac-bypass | bfd-learning } class CLASS-RANGE
```

```
no cpu-traffic-limit reason {bpdu | slow-protocol | eapol | erps | smart-link | arp | dhcp | rip | ldp | ospf | pim | vrrp | ipda | icmp-redirect | mcast-rpf-fail | macsa-mismatch | port-security-discard | vlan-security-discard | mtu-dontfrag | mtu-frag | ip-option | ucast -ttl-fail | mpls-ttl-fail | igmp | sflow-ingress | sflow-egress| udld|mld| dot1x-mac-bypass | bfd-learning } class
```

CLASS-RANGE	调度优先级类，3 表示调度优先级最高，范围<0-3>
-------------	----------------------------

## 命令模式

全局配置模式

## 默认

Reason	class	Reason	class
bpdu	3	icmp-redirect	0
slow-protocol	1	mcast-rpf-fail	1
eapol	0	macsa-mismatch	0
erps	2	port-security-discard	0
smart-link	2	vlan-security-discard	0
arp	1	udld	3
dhcp	0	mtu-dontfrag	0
rip	1	mtu-frag	0
ldp	1	sflow-ingress	0
ospf	1	ip-option	0
pim	1	ucast-ttl-fail	0
vrrp	1	mpls-ttl-fail	0
ipda	0	igmp	2
mld	2	sflow-egress	0
dot1x-mac-bypass	2	fwd-to-cpu	0
bfd-learning	1		

## 使用说明

Reason 调度优先级越高，这种报文在调度时会优先被送入 CPU。调度器采用的是严格优先级调度策略，只有当高优先级的流调度完才会调度低优先级的里。

## 举例说明

如下例子显示了如何配置 bpdu 的调度优先级类：

```
Switch(config)# cpu-traffic-limit reason bpdu class 3
```

## 相关命令

```
show cpu traffic-limit
```

### 15.3.4 show cpu traffic-limit

使用此命令查看 cpu traffic limit 的配置。

## 命令语法

```
show cpu traffic-limit
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

如下例子显示了 `cpu traffic limit` 的默认配置：

```
Switch# show cpu traffic-limit
reason                rate (pps)  class
dot1x-mac-bypass     64          2
bpdu                  64          3
slow-protocol        128         1
eapol                 128         0
erps                  128         2
smart-link           128         2
udld                  128         3
loopback-detection   64          3
arp                   256         1
dhcp                  128         0
rip                   64          1
ldp                   512         1
ospf                  256         1
pim                   128         1
vrrp                  512         1
ipda                  1024        0
icmp-redirect        128         0
mcast-rpf-fail       128         1
macsa-mismatch       128         0
port-security-discard 128         0
vlan-security-discard 128         0
mtu-dontfrag         64          0
mtu-frag             64          0
ip-mtu-fail          64          0
bfd-learning         128         1
ip-option            512         0
ucast-ttl-fail       64          0
mpls-ttl-fail        64          0
igmp                 128         2
sflow-ingress        128         0
sflow-egress         128         0
fwd-to-cpu           64          0
```

```
l2protocol-tunnel          1024          0
Total rate:                2048 (pps)
```

## 相关命令

```
cpu-traffic-limit total rate
cpu-traffic-limit reason rate
cpu-traffic-limit reason class
```

## 15.4 CPU Traffic Statistics 命令

### 15.4.1 cpu-traffic-statistics time

使用此命令配置上 CPU 报文或者 CPU 发出报文统计的间隔时间。

## 命令语法

```
cpu-traffic-statistics time RATE-TIME
```

RATE- TIME	统计报文的间隔时间，单位 s，范围<1-10>
------------	-------------------------

## 命令模式

全局配置模式

## 默认

5 s

## 使用说明

无。

## 举例说明

如下的例子显示如何配置上 CPU 报文统计间隔时间：

```
Switch(config)# cpu-traffic-statistics time 2
```

## 相关命令

```
no cpu-traffic-statistics time
```

### 15.4.2 no cpu-traffic-statistics time

使用此命令恢复上 CPU 报文或者 CPU 发出报文统计的间隔时间。

## 命令语法

```
no cpu-traffic-statistics time
```

## 命令模式

全局配置模式

## 默认

无

## 使用说明

无

## 举例说明

如下的例子显示如何恢复上 CPU 报文统计间隔时间：

```
Switch(config)# no cpu-traffic-statistics time
```

## 相关命令

无

### 15.4.3 show cpu traffic- statistics receive

使用此命令配置显示上 CPU 报文数的统计。

## 命令语法

```
show cpu traffic-statistics receive (bpdu|slow-protocol|eapol|erps|smart-link|arp|dhcp|rip|ldp|ospf|pim|bgp|vrrp|ipda|icmp-redirect|mcast-rpf-fail|macsa-mismatch|port-security-discard|vlan-security-discard|ip-mtu-fail|ip-option|ucast-ttl-fail|sflow-ingress|sflow-egress|igmp|udld|dot1x-mac-bypass|l2protocol-tunnel|mirror-to-cpu|tunnel-gre-keepalive|loopback-detection|rsvp|bfd-learning|mpls-ttl-fail|fwd-to-cpu|ptp)
```

bpdu	BPDU 协议报文(包括 STP, RSTP, MSTP)
slow-protolcol	Slow 协议报文.(包括 EFM, LACP, SYNCE)
eapol	Dot1x 协议报文
erps	ERPS 协议报文
arp	ARP 协议报文
dhcp	DHCP 协议报文
rip	RIP 协议报文

bgp	BGP 协议报文
ldp	LDP 协议报文
ospf	OSPF 协议报文
pim	PIM 协议报文
vrrp	VRRP 协议报文
ipda	IPDA 协议报文
icmp-redirect	ICMP 重定向
learning-full	MAC 学习缓存已满
mcast_rpf_fail	组播报文 RPF 检查失败
macsa-mismatch	与一个端口 security entry 不匹配时的学习报文
port-security-discard	端口 security entry 学满时的学习报文
vlan-security-discard	VLAN 内学习的 MAC 达到限制是的学习报文
ip-mtu-fail	需要分片的报文
Ip-option	带有可选字段的 IP 报文
ucast-ttl-fail	TTL 失效的单播 IP 报文
mpls-ttl-fail	TTL 失效 MPLS 报文
Igmp	IGMP 或者 IGMP Snooping 报文
sflow-ingress	在入口方向 Sflow 的采样报文
sflow-egress	在出口方向 Sflow 的采样报文
fwd-to-cpu	转发到 CPU 的报文
mld	MLD 或者 MLD Snooping 报文
dot1x-mac-bypass	Dot1x 旁路认证报文
bfd-learning	Bfd 学习报文

## 命令模式

特权模式

## 默认

无。

## 使用说明

不指定报文类型时，默认查看上 CPU 的报文数不为 0 的报文。

## 举例说明

如下的例子显示了如何查看 BPDU 报文上 CPU 的统计：

```
Switch# show cpu traffic-statistics receive bpdu
statistics rate time is 5 second(s)
reason          count (packets)   rate (pps)
-----
bpdu             0                  0
```

## 相关命令

show cpu traffic-statistics receive all

### 15.4.4 show cpu traffic-statistics receive all

使用此命令配置显示所有上 CPU 报文数的统计。

## 命令语法

show cpu traffic-statistics receive all

## 命令模式

特权模式

## 默认

无。

## 使用说明

无。

## 举例说明

如下例子显示了如何显示所有上 CPU 报文数的统计：

```
Switch# show cpu traffic-statistics receive all
statistics rate time is 5 second(s)
reason          count (packets)   rate (pps)
-----
dot1x-mac-bypass  0                  0
bpdu             0                  0
slow-protocol    0                  0
eapol            0                  0
erps              0                  0
smart-link       0                  0
udld              0                  0
loopback-detection 0                  0
arp               0                  0
```

---

dhcp	0	0
rip	0	0
ldp	0	0
ospf	0	0
pim	0	0
bgp	0	0
vrrp	0	0
rsvp	0	0
ipda	0	0
icmp-redirect	0	0
mcast-rpf-fail	0	0
macsa-mismatch	0	0
port-security-discard	0	0
vlan-security-discard	0	0
ip-mtu-fail	0	0
bfd-learning	0	0
ptp	0	0
ip-option	0	0
tunnel-gre-keepalive	0	0
ucast-ttl-fail	0	0
mpls-ttl-fail	0	0
igmp	0	0
sflow-ingress	0	0
sflow-egress	0	0
fwd-to-cpu	0	0
l2protocol-tunnel	0	0
mirror-to-cpu	0	0
mpls-tp-pwoam	0	0
other	0	0
Total	0	0

## 相关命令

无。

## 15.4.5 show cpu traffic-statistics transmit

使用此命令配置显示所有 CPU 发出报文数的统计。

## 命令语法

```
show cpu-traffic -statistic transmit
```

## 命令模式

特权模式

## 默认

无



## 使用说明

CPU 发出报文统计不区分类型。

## 举例说明

如下例子显示所有 CPU 发出报文数的统计：

```
Switch# show cpu traffic-statistics transmit
statistics rate time is 5 second(s)
              count (packets)   rate (pps)
Total                0           0
```

## 相关命令

无。

# 15.5 UDLD 命令

## 15.5.1 udld enable

使用此命令全局使能或者关闭 UDLD 功能。

## 命令语法

```
udld enable
no udld enable
```

## 命令模式

全局配置模式

## 默认

关闭

## 使用说明

无

## 举例说明

以下例子全局使能了 UDLD 功能：

```
Switch(config)# udld enable
```

## 相关命令

```
show udld
```

## 15.5.2 uddl port

使用此命令在指定接口上使能或者关闭 UDLD 功能。

### 命令语法

**udld port (aggressive)**

**no uddl port**

aggressive	UDLD 激进模式
------------	-----------

### 命令模式

端口配置模式

### 默认

关闭

### 使用说明

无

### 举例说明

以下例子在端口 eth-0-9 上使能了 UDLD 功能：

```
Switch(config)# interface eth-0-9
Switch(config)# uddl port
```

### 相关命令

show uddl

## 15.5.3 uddl message interval

使用此命令设置 UDLD 消息间隔。使用 no 命令来恢复默认值。

### 命令语法

**udld message interval *INTERVAL***

**no uddl message interval**

INTERVAL	UDLD 消息间隔（秒），范围是 1~90
----------	-----------------------

## 命令模式

全局配置模式

## 默认

15 秒

## 使用说明

无

## 举例说明

以下例子将 UDLD 消息间隔设置为 5 秒：

```
Switch(config)# udld message interval 5
```

## 相关命令

show udld

### 15.5.4 udld reset

使用此命令重置被 UDLD 禁用的接口。

## 命令语法

**udld reset**

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

以下例子重置被 UDLD 禁用的接口：

```
Switch# udld reset
```

## 相关命令

无

## 15.5.5 show udld

使用此命令显示接口的 UDLD 信息。

### 命令语法

**show udld** (*IFNAME*)

IFNAME	端口名
--------	-----

### 命令模式

特权模式

### 默认

无

### 使用说明

无

### 举例说明

以下例子显示了端口 eth-0-1 的 UDLD 信息：

```
Switch# show udld eth-0-1
Interface eth-0-1
---
UDLD mode      : aggressive mode
Operational state : Bidirectional
Message interval : 15
Time out interval : 3
Neighbor 1
---
Device ID      : 001e.0808.0360
Port ID       : eth-0-2
Device Name    : DUT2
Message Interval : 15
Timeout Interval : 3
Link status    : Bidirectional
Expiration time : 40
```

### 相关命令

无

## 15.5.6 show udld neighbors

使用此命令显示 UDLD 邻居信息。

## 命令语法

**show udld neighbors**

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

以下例子显示了 UDLD 邻居的信息：

```
Switch# show udld neighbor
Port          Device Name      Device ID          Port ID          Neighbor State
----          -
eth-0-9       DUT2             d4f2.489f.d100   eth-0-9         bidirectional
```

## 相关命令

无

## 15.5.7 debug udld

使用此命令使能 UDLD 调试信息。

## 命令语法

**debug udld (all|packet|events)**

**no debug udld (all|packet|events)**

all	使能全部调试信息
packet	使能报文调试信息
events	使能事件调试信息

## 命令模式

特权模式

**默认**

无

**使用说明**

无

**举例说明**

以下例子使能 UDLD 的报文调试信息：

```
Switch# debug udld packet
```

**相关命令**

无

## 15.5.8 show debugging udld

使用此命令显示 UDLD 调试状态。

**命令语法**

```
show debugging udld
```

**命令模式**

特权模式

**默认**

无

**使用说明**

无

**举例说明**

以下例子显示了 UDLD 的调试功能状态：

```
Switch# show debugging udld
```

**相关命令**

无

## 15.6 Smart-Link 命令

### 15.6.1 smart-link group

此命令用来创建一个 Smart-link 组。

#### 命令语法

```
smart-link group GROUP-ID  
no smart-link group (GROUP-ID | all)
```

GROUP-ID	组 ID, 范围 1~16
all	所有的组

#### 命令模式

全局配置模式

#### 默认

无

#### 使用说明

最多 16 个组可以使用

#### 举例说明

创建一个 Smart-link 组。

```
Switch(config)# smart-link group 1
```

#### 相关命令

```
show smart-link group
```

### 15.6.2 smart-link relay enable

使用此命令允许设备转发 Smart-link 更新报文。

#### 命令语法

```
smart-link relay enable  
no smart-link relay enable
```

## 命令模式

全局配置模式

## 默认

开启

## 使用说明

默认情况下设备会在对应 vlan 中广播该报文。使用 no 命令关闭该转发功能。

## 举例说明

```
Switch(config)# no smart-link relay enable
```

## 相关命令

无

### 15.6.3 interface

使用此命令为 smart link 组设置主端口或副端口。no 命令删除主端口或副端口。

## 命令语法

```
interface (IFPHYSICAL|IFAGG) (master | slave)
```

```
no interface (master | slave | all)
```

IFPHYSICAL	物理接口,例如 eth-0-1
IFAGG	汇聚链路接口
master	主接口
slave	副接口
all	主接口和副接口

## 命令模式

组模式

## 默认

默认不指定任何端口



## 使用说明

每个 Smart-link 组都应该有两个端口（主端口和副端口）。端口类型可以是物理接口或 agg 接口。

注意：端口必须关闭 STP 后才可以加入 smart link 组。

## 举例说明

创建一个 Smart-link 组

```
Switch(config)# interface eth-0-9
Switch(config-if)# spanning-tree port disable
Switch(config-if)# exit
Switch(config)# interface eth-0-13
Switch(config-if)# spanning-tree port disable
Switch(config-if)# exit
Switch(config)# smart-link group 1
Switch(config-smlk-group)# interface eth-0-9 master
Switch(config-smlk-group)# interface eth-0-13 slave
Switch(config-smlk-group)# end
Switch# show smart-link group 1
Smart-link group 1 information:
The smart-link group was disabled.
=====
Auto-restore:
  state      time      count      Last-time
  disabled   60        0          N/A
=====
Protected instance:
Load balance instance:
=====
INTERFACE:
Role      Member      DownCount  Last-Down-Time  FlushCount  Last-Flush-Time
MASTER   eth-0-9     0          N/A              0           N/A
SLAVE    eth-0-13    0          N/A              0           N/A
```

## 相关命令

show smart-link group

### 15.6.4 protected mstp instance

此命令设置 Smart-link 组保护的 MSTP 实例。

## 命令语法

protected mstp instance *INSTANCE-ID*

no protected mstp instance (all | *INSTANCE-ID*)

INSTANCE-ID	MSTP 实例 ID。范围是 0~4094
-------------	-----------------------

all	所用的 MSTP 实例
-----	-------------

## 命令模式

组配置模式

## 默认

默认不保护任何组

## 使用说明

Smart link 只保护指定的 MSTP instance。如果 vlan 没有加入任何 MSTP instance 则会默认加入 instance 0。

注意：加入 MSTP 实例的 vlan 被删除了,那么在 Smart-link 组内被自动删除。

## 举例说明

创建 Smart-link 组内的 MSTP 实例

```
Switch(config)# smart-link group 1
Switch(config-smlk-group)# protected mstp instance 0
Switch(config-smlk-group)# protected mstp instance 10
Switch(config-smlk-group)# protected mstp instance 100
Switch(config-smlk-group)# end
Switch# show smart-link group 1
Smart-link group 1 information:
The smart-link group was disabled.
=====
Auto-restore:
  state      time      count    Last-time
  disabled   60        0        N/A
=====
Protected instance: 0 100 10
Load balance instance:
=====
INTERFACE:
Role      Member    DownCount Last-Down-Time  FlushCount Last-Flush-Time
MASTER   eth-0-9   0         N/A              0          N/A
SLAVE    eth-0-13  0         N/A              0          N/A
```

## 相关命令

show smart-link group

### 15.6.5 load-balance instance

此命令被 Smart-link 组用来实现负载均衡。

## 命令语法

load-balance instance *INSTANCE-ID*

no load-balance instance (all | *INSTANCE-ID*)

INSTANCE-ID	MSTP 实例 ID。范围是 0~4094
all	所用的 MSTP 实例

## 命令模式

组模式

## 默认

未启用

## 使用说明

负载均衡的实例的流量将走 Smart-link 组的副端口。

## 举例说明

设置实例 10 为负载均衡。

```
Switch(config)# smart-link group 1
Switch(config-smlk-group)# load-balance instance 10
```

## 相关命令

show smart-link group

### 15.6.6 restore time

此命令设置 Smart-link 组的自动切换时间。

## 命令语法

restore time *RESTORE-TIME*

no restore time

RESTORE-TIME	链路自动切换时间（秒），范围是 30~1200
--------------	-------------------------

## 命令模式

组模式

## 默认

默认恢复时间 60 秒

## 使用说明

当主接口恢复，链接不会立即切换，需要等待一段时间。这段时间就是切换时间。

## 举例说明

设置 Smart-link 组的切换时间为 30 秒

```
Switch(config)# smart-link group 1
Switch(config-smlk-group)# restore time 30
```

## 相关命令

show smart-link group

## 15.6.7 restore enable

此命令被用来启用切换时间

## 命令语法

```
restore enable
no restore enable
```

## 命令模式

组模式

## 默认

该功能默认不启用

## 使用说明

当主接口出现故障时，链接将切换到副接口。如果主接口恢复，链接不会被切换以保持流量稳定。如果启用恢复功能，链接将被切换。

注：如果配置了负载均衡实例，此功能强烈建议打开。

## 举例说明

在 Smart-link 组内启用恢复时间功能

```
Switch(config)# smart-link group 1
Switch(config-smlk-group)# restore enable
```

## 相关命令

```
show smart-link group
```

## 15.6.8 flush send

此命令配置是否发送 smart link 更新报文。

## 命令语法

```
flush send control-vlan VLAN-ID password simple PASSWORD
no flush send
```

VLAN-ID	VLAN 号，范围是 1~4094
PASSWORD	更新报文的密码，长度为 1~15

## 命令模式

组模式

## 默认

默认不发送

## 使用说明

当主（转发）链路出现故障，流量切换到副端口时发送 flush fdb 报文通知上游更新 FDB。

## 举例说明

设置 Smart-link 的发送更新报文的密码。

```
Switch(config)# smart-link group 1
Switch(config-smlk-group)# flush send control-vlan 4 password simple test
```

## 相关命令

```
show smart-link group
smart-link flush receive
```

## 15.6.9 group enable

使用此命令关闭或开启组。

### 命令语法

```
group enable
no group enable
```

### 命令模式

组模式

### 默认

无

### 使用说明

无

### 举例说明

启用 Smart-link 组

```
Switch(config)# smart-link group 1
Switch(config-smlk-group)# group enable
```

### 相关命令

```
show smart-link group
```

## 15.6.10 smart-link flush receive

此命令被用作是否接收更新报文。

### 命令语法

```
smart-link flush receive control-vlan VLAN-ID password simple PASSWORD
no smart-link flush receive
```

VLAN-ID	VLAN 号，范围是 1~4094
PASSWORD	更新报文的密码，长度为 1~15

## 命令模式

端口配置模式

## 默认

默认不接收

## 使用说明

收到的更新包应该与接收设备有相同的 VLAN ID 和密码。否则，数据包将被丢弃。

## 举例说明

设置 Smart-link 组的接收更新报文的密码为 test。

```
Switch(config)# interface eth-0-9
Switch(config-if)# smart-link flush receive control-vlan 4 password simple test
Switch(config-if)# end
Switch# show smart-link
Relay smart-link flush packet is enabled
Smart-link received flush packet number:0
Smart-link processed flush packet number:0
Smart link Group Number is 1.
  Group-ID   State      MASTER      SLAVE
  1          disabled  N/A         N/A
```

## 相关命令

flush send

show smart-link

### 15.6.11 smart-link tcn enable

此命令用来使能 Smart-link 的 tcn 功能。

## 命令语法

smart-link tcn enable

no smart-link tcn enable

## 命令模式

全局配置模式

## 默认

未使能

## 使用说明

无

## 举例说明

使能 smart link 的 tcn 功能

```
Switch(config)# smart-link tcn enable
```

## 相关命令

```
show smart-link
```

## 15.6.12 smart-link tcn query-count

此命令用来设置 Smart-link 的 tcn 发送的 query 报文的次数。

## 命令语法

```
smart-link tcn query-count QUERY-COUNT
```

```
no smart-link tcn query-count
```

QUERY-COUNT	Tcn 发送的 query 报文次数。范围是 1-10
-------------	-----------------------------

## 命令模式

全局配置模式

## 默认

2

## 使用说明

无

## 举例说明

设置 smart link 的 tcn 功能发送的 query 报文的次数为 5。

```
Switch(config)# smart-link tcn query-count 5
```

## 相关命令

```
show smart-link
```



## 15.6.13 smart-link tcn query-interval

此命令用来设置 Smart-link 的 tcn 发送的 query 报文的间隔时间。

### 命令语法

```
smart-link tcn query-count QUERY-INTERVAL
```

```
no smart-link tcn query-interval
```

QUERY-INTERVAL	Tcn 发送的 query 报文间隔时间。范围是 1-255 秒
----------------	----------------------------------

### 命令模式

全局配置模式

### 默认

10

### 使用说明

无

### 举例说明

设置 smart link 的 tcn 功能发送的 query 报文的间隔时间为 50。

```
Switch(config)# smart-link tcn query-interval 50
```

### 相关命令

```
show smart-link
```

## 15.6.14 show smart-link

使用此命令显示 Smart-link 的信息。

### 命令语法

```
show smart-link
```

### 命令模式

特权模式

## 默认

无

## 使用说明

该命令用于显示 Smart-link 组的概要信息。

## 举例说明

```
Switch# show smart-link
Relay smart-link flush packet is enabled
Smart-link received flush packet number:7
Smart-link processed flush packet number:0
Smart link Group Number is 1.
Group-ID      State      MASTER      SLAVE
1             enabled    eth-0-1     eth-0-2
```

## 相关命令

无

## 15.6.15 show smart-link group

使用此命令显示 Smart-link 组的信息。

## 命令语法

```
show smart-link group (GROUP-ID)
```

GROUP-ID	组 ID, 范围 1~16
----------	---------------

## 命令模式

特权模式

## 默认

无

## 使用说明

该命令用于显示指定 Smart-link 组或者全部 Smart-link 组的详细信息。

## 举例说明

```
Switch# show smart-link group 1
```

**相关命令**

无

**15.6.16 clear smart-link statistic**

使用此命令清除 Smart-link 的统计。

**命令语法**

clear smart-link statistic

**命令模式**

特权模式

**默认**

无

**使用说明**

用作清除 Smart-link 的统计

**举例说明**

Switch# clear smart-link statistic

**相关命令**

无

**15.6.17 debug smart-link**

使用此命令打开 smart link 的 debug 信息。

**命令语法**

debug smart-link (all | flush | instance | interface | restore)

all	打开所有 smart link 的日志
flush	打开所有 smart link 的 FDB 更新信息日志
instance	打开所有 smart link 的实例信息日志
interface	打开所有 smart link 的端口信息日志
restore	打开所有 smart link 的链路恢复信息日志
mib	打开所有 smart-link 的 snmp mib 信息日志

trap	打开所有 smart-link 的 snmp trap 信息日志
------	----------------------------------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch# debug smart-link all
```

## 相关命令

无

# 15.7 Multi-Link 命令

## 15.7.1 multi-link group

此命令用来创建一个 Multi-link 组。

## 命令语法

```
multi-link group GROUP-ID
no multi-link group (GROUP-ID | all)
```

GROUP-ID	组 ID, 范围 1~16
all	所有的组

## 命令模式

全局配置模式

## 默认

无

## 使用说明

最多 16 个组可以使用

## 举例说明

创建一个 Multi-link 组。

```
Switch(config)# multi-link group 1
```

## 相关命令

```
show multi-link group
```

## 15.7.2 multi-link relay enable

使用此命令允许设备转发 Multi-link 更新报文。

## 命令语法

```
multi-link relay enable
```

```
no multi-link relay enable
```

## 命令模式

全局配置模式

## 默认

开启

## 使用说明

默认情况下设备会在对应 vlan 中广播该报文。使用 no 命令关闭该转发功能。

## 举例说明

```
Switch(config)# no multi-link relay enable
```

## 相关命令

无

## 15.7.3 interface

使用此命令为 multi link 组设置主端口或副端口。no 命令删除主端口或副端口。

## 命令语法

```
interface (IFPHYSICAL|IFAGG) priority <1-4>
```

```
no interface (priority <1-4> | all)
```

IFPHYSICAL	物理接口,例如 eth-0-1
IFAGG	汇聚链路接口
<1-4>	接口优先级（越小优先级越高）
all	所有接口

## 命令模式

组模式

## 默认

默认不指定任何端口

## 使用说明

每个 Multi-link 组都至少有两个端口。端口类型可以是物理接口或 agg 接口。

注意：端口必须关闭 STP 后才可以加入 multi link 组。

## 举例说明

创建一个 Multi-link 组

```
Switch(config)# interface eth-0-9
Switch(config-if)# spanning-tree port disable
Switch(config-if)# exit
Switch(config)# interface eth-0-13
Switch(config-if)# spanning-tree port disable
Switch(config-if)# exit
Switch(config)# multi-link group 1
Switch(config-multilink-group)# interface eth-0-9 priority 1
Switch(config-multilink-group)# interface eth-0-10 priority 2
Switch(config-multilink-group)# interface eth-0-12 priority 4
Switch(config-multilink-group)# end
Switch# show multi-link group 1
Multi-link group 1 information:
The multi-link group was enabled.
=====
Auto-restore:
state      time      count     Last-time
disabled   60        0         N/A
=====
```

```

Protected instance: 0
Load balance instance:
=====
INTERFACE:
Role    Member    DownCount  Last-Down-Time    FlushCount  Last-Flush-Time
PRI1    eth-0-9    0          N/A                0           N/A
PRI2    eth-0-10   0          N/A                0           N/A
PRI3    N/A        0          N/A                0           N/A
PRI4    eth-0-12   0          N/A                0           N/A
=====
Instance states in the member interfaces:
  A - ACTIVE ,   B -BLOCK , D-The interface is link-down
Map-instance-ID P1 (eth-0-9 )  P2 (eth-0-10) P3 (N/A )     P4 (eth-0-12)
0                A          B          D          B

```

## 相关命令

show multi-link group

### 15.7.4 protected mstp instance

此命令设置 Multi-link 组保护的 MSTP 实例。

## 命令语法

protected mstp instance *INSTANCE-ID*

no protected mstp instance (all | *INSTANCE-ID*)

INSTANCE-ID	MSTP 实例 ID。范围是 0~4094
all	所用的 MSTP 实例

## 命令模式

组配置模式

## 默认

默认不保护任何组

## 使用说明

Multi-link 只保护指定的 MSTP instance。如果 vlan 没有加入任何 MSTP instance 则会默认加入 instance 0。

注意：加入 MSTP 实例的 vlan 被删除了,那么在 Multi-link 组内被自动删除。

## 举例说明

### 创建 Multi-link 组内的 MSTP 实例

```
Switch(config)# multi-link group 1
Switch(config-multilink-group)# protected mstp instance 0
Switch(config-multilink-group)# protected mstp instance 10
Switch(config-multilink-group)# protected mstp instance 100
Switch(config-multilink-group)# end
Switch# show multi-link group 1
Multi-link group 1 information:
The multi-link group was enabled.
=====
Auto-restore:
state          time          count         Last-time
disabled       60            0             N/A
=====
Protected instance: 0 10 100
Load balance instance:
=====
INTERFACE:
Role  Member    DownCount  Last-Down-Time    FlushCount  Last-Flush-Time
PRI1  eth-0-9    0          N/A               0           N/A
PRI2  eth-0-10  0          N/A               0           N/A
PRI3  N/A       0          N/A               0           N/A
PRI4  eth-0-12  0          N/A               0           N/A
=====
Instance states in the member interfaces:
A - ACTIVE , B -BLOCK , D-The interface is link-down
Map-instance-ID  P1(eth-0-9 )  P2(eth-0-10)  P3(N/A )  P4(eth-0-12)
0                A             B             D         B
10               A             B             D         B
100              A             B             D         B
```

## 相关命令

show multi-link group

## 15.7.5 load-balance instance

此命令被 Multi-link 组用来实现负载均衡。

## 命令语法

load-balance instance *INSTANCE-ID* priority <2-4>

no load-balance instance (all | *INSTANCE-ID*)

INSTANCE-ID	MSTP 实例 ID。范围是 0~4094
<2-4>	负载均衡对应的端口优先级
all	所用的 MSTP 实例



## 命令模式

组模式

## 默认

未启用

## 使用说明

负载均衡的实例的流量将走 Multi-link 组的对应优先级的端口。

## 举例说明

设置实例 10 为负载均衡。

```
Switch(config)# multi-link group 1
```

```
Switch(config-multilink-group)# load-balance instance 10 priority 2
```

## 相关命令

```
show multi-link group
```

## 15.7.6 restore time

此命令设置 Multi-link 组的自动切换时间。

## 命令语法

```
restore time RESTORE-TIME
```

```
no restore time
```

RESTORE-TIME	链路自动切换时间（秒），范围是 30~1200
--------------	-------------------------

## 命令模式

组模式

## 默认

默认恢复时间 60 秒

## 使用说明

当主接口恢复，链接不会立即切换，需要等待一段时间。这段时间就是切换时间。

## 举例说明

设置 Multi-link 组的切换时间为 30 秒

```
Switch(config)# multi-link group 1
```

```
Switch(config-multilink-group)# restore time 30
```

## 相关命令

```
show multi-link group
```

### 15.7.7 restore enable

此命令被用来启用切换时间

## 命令语法

```
restore enable
```

```
no restore enable
```

## 命令模式

组模式

## 默认

该功能默认不启用

## 使用说明

当高优先级接口出现故障时，链接将切换到次高优先级端口。如果高优先级接口恢复，链接不会被切换以保持流量稳定。如果启用恢复功能，链接将被切换。

注：如果配置了负载均衡实例，此功能强烈建议打开。

## 举例说明

在 Multi-link 组内启用恢复时间功能

```
Switch(config)# multi-link group 1
```

```
Switch(config-multilink-group)# restore enable
```

## 相关命令

```
show multi-link group
```

### 15.7.8 flush send

此命令配置是否发送 multi-link 更新报文。

## 命令语法

```
flush send control-vlan VLAN-ID password simple PASSWORD  
no flush send
```

VLAN-ID	VLAN 号，范围是 1~4094
PASSWORD	更新报文的密码，长度为 1~15

## 命令模式

组模式

## 默认

默认不发送

## 使用说明

当主（转发）链路出现故障，流量切换到副端口时发送 flush fdb 报文通知上游更新 FDB。

## 举例说明

设置 Multi-link 的发送更新报文的密码。

```
Switch(config)# multi-link group 1
```

```
Switch(config-multilk-group)# flush send control-vlan 4 password simple test
```

## 相关命令

```
show multi-link group  
multi-link flush receive
```

### 15.7.9 group enable

使用此命令关闭或开启组。

## 命令语法

```
group enable  
no group enable
```

## 命令模式

组模式

**默认**

无

**使用说明**

无

**举例说明**

启用 Multi-link 组

```
Switch(config)# multi-link group 1
Switch(config-multilink-group)# group enable
```

**相关命令**

```
show multi-link group
```

**15.7.10 multi-link flush receive**

此命令被用作是否接收更新报文。

**命令语法**

```
multi-link flush receive control-vlan VLAN-ID password simple PASSWORD
no multi-link flush receive
```

VLAN-ID	VLAN 号，范围是 1~4094
PASSWORD	更新报文的密码，长度为 1~15

**命令模式**

端口配置模式

**默认**

默认不接收

**使用说明**

收到的更新包应该与接收设备有相同的 VLAN ID 和密码。否则，数据包将被丢弃。

**举例说明**

设置 Multi-link 组的接收更新报文的密码为 test。

```
Switch(config)# interface eth-0-9
Switch(config-if)# multi-link flush receive control-vlan 4 password simple test
Switch(config-if)# end
Switch# show multi-link

Relay multi-link flush packet is enabled

Multi-link received flush packet number:0

Multi-link processed flush packet number:0

Multi-link tcn is enabled

Multi-link tcn query count      :2

Multi-link tcn query interval  :3

Multi-link Group Number is 1.

  Group-ID   State      Pri-1      Pri-2      Pri-3      Pri-4
-----
    1        enabled    eth-0-9    eth-0-10   N/A        eth-0-12
```

## 相关命令

```
flush send
show multi-link
```

### 15.7.11 multi-link tcn enable

此命令用来使能 Multi-link 的 tcn 功能。

## 命令语法

```
multi-link tcn enable
no multi-link tcn enable
```

## 命令模式

全局配置模式

## 默认

未使能

## 使用说明

无

## 举例说明

使能 multi-link 的 tcn 功能

```
Switch(config)# multi-link tcn enable
```

## 相关命令

```
show multi-link
```

### 15.7.12 multi-link tcn query-count

此命令用来设置 Multi-link 的 tcn 发送的 query 报文的次数。

## 命令语法

```
multi-link tcn query-count QUERY-COUNT
```

```
no multi-link tcn query-count
```

QUERY-COUNT	Tcn 发送的 query 报文次数。范围是 1-10
-------------	-----------------------------

## 命令模式

全局配置模式

## 默认

2

## 使用说明

无

## 举例说明

设置 multi-link 的 tcn 功能发送的 query 报文的次数为 5。

```
Switch(config)# multi-link tcn query-count 5
```

## 相关命令

```
show multi-link
```

### 15.7.13 multi-link tcn query-interval

此命令用来设置 Multi-link 的 tcn 发送的 query 报文的间隔时间。

## 命令语法

```
multi-link tcn query-count QUERY-INTERVAL
```

```
no multi-link tcn query-interval
```

QUERY-INTERVAL	Tcn 发送的 query 报文间隔时间。范围是 1-255 秒
----------------	----------------------------------

## 命令模式

全局配置模式

## 默认

10

## 使用说明

无

## 举例说明

设置 multi-link 的 tcn 功能发送的 query 报文的间隔时间为 50。

```
Switch(config)# multi-link tcn query-interval 50
```

## 相关命令

```
show multi-link
```

### 15.7.14 show multi-link

使用此命令显示 Multi-link 的信息。

## 命令语法

```
show multi-link
```

## 命令模式

特权模式

## 默认

无

## 使用说明

该命令用于显示 Multi-link 组的概要信息。

## 举例说明

```
Switch# show multi-link

Relay multi-link flush packet is enabled

Multi-link received flush packet number:0

Multi-link processed flush packet number:0

Multi-link tcn is enabled

Multi-link tcn query count      :2

Multi-link tcn query interval  :3

Multi-link Group Number is 1.

  Group-ID   State      Pri-1      Pri-2      Pri-3      Pri-4
-----
    1        enabled   eth-0-9    eth-0-10   N/A        eth-0-12
```

## 相关命令

无

### 15.7.15 show multi-link group

使用此命令显示 Multi-link 组的信息。

## 命令语法

```
show multi-link group (GROUP-ID|)
```

GROUP-ID	组 ID, 范围 1~16
----------	---------------

## 命令模式

特权模式

## 默认

无

## 使用说明

该命令用于显示指定 Multi-link 组或者全部 Multi-link 组的详细信息。

## 举例说明

```
Switch# show multi-link group 1
```



## 相关命令

无

### 15.7.16 clear multi-link statistic

使用此命令清除 Multi-link 的统计。

## 命令语法

```
clear multi-link statistic
```

## 命令模式

特权模式

## 默认

无

## 使用说明

用作清除 Multi-link 的统计

## 举例说明

```
Switch# clear multi-link statistic
```

## 相关命令

无

### 15.7.17 debug multi-link

使用此命令打开 multi-link 的 debug 信息。

## 命令语法

```
debug multi-link (all | flush | instance | interface | restore)
```

all	打开所有 multi-link 的日志
flush	打开所有 multi-link 的 FDB 更新信息日志
instance	打开所有 multi-link 的实例信息日志
interface	打开所有 multi-link 的端口信息日志
restore	打开所有 multi-link 的链路恢复信息日志

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

```
Switch# debug multi-link all
```

## 相关命令

无

## 15.7.18 multilink-enhance interface

使用此命令配置发送 `enhance` 增强报文的接口。

## 命令语法

```
multilink-enhance interface (IFPHYSICAL|IFAGG)  
no multilink-enhance interface
```

## 命令模式

组模式

## 默认

无

## 使用说明

配置的发送增强报文的接口一般为 `multilink` 组外接口，在配置 `multilink` 增强的发送接口时，需要配置 `flush send` 的 `control vlan` 和 `password`。

## 举例说明

启用 Multi-link 增强功能，启用接口为 `eth-0-1`

```
Switch(config)# multi-link group 1
```

```
Switch(config-multilk-group)# multilink-enhance interface eth-0-1
```

## 相关命令

show multi-link group

### 15.7.19 multilink-enhance receive

使用此命令配置接受 multilink 增强报文的接口。

## 命令语法

```
multilink-enhance receive control-vlan VLAN-ID password simple PASSWORD interface  
(IFPHYSICAL|IFAGG)
```

```
no multilink-enhance receive interface (IFPHYSICAL|IFAGG)
```

## 命令模式

组模式

## 默认

无

## 使用说明

配置 multilink group 中接受增强报文的接口，该接口必须为 multilink group 优先级最低成员且已配。该接口不允许配置负载均衡。当配置增强接受接口，就允许往 multilink 组里面添加优先级更低的成员。

## 举例说明

启用 Multi-link 接受增强报文的接口

```
Switch(config)# multi-link group 1
```

```
Switch(config-multilink-group)# multilink-enhance receive control-vlan 10 password b  
interface eth-0-2
```

## 相关命令

show multi-link group

### 15.7.20 multilink-enhance send-interval

使用此命令配置发送增强报文的间隔时间。

## 命令语法

```
multilink-enhance send-interval <1-255>
```

```
no multilink-enhance send-interval
```

## 命令模式

组模式

## 默认

10s

## 使用说明

无。

## 举例说明

配置 multilk 增强报文的发送时间间隔为 20s

```
Switch(config)# multi-link group 1
```

```
Switch(config-multilk-group)# multilink-enhance send-interval 20
```

## 相关命令

```
show multi-link group
```

## 15.7.21 multilink-enhance timeout

使用此命令配置检测是否持续收到增强报文的时间间隔。

## 命令语法

```
multilink-enhance timeout <1-255>
```

```
no multilink-enhance timeout
```

## 命令模式

组模式

## 默认

10s

## 使用说明

配置增强报文接受的超时时间，若在规定的时间内没有收到，则对应的 multilink 接口恢复到原样。

## 举例说明

配置 multilk 增强报文的接受超时时间间隔为 20s

```
Switch(config)# multi-link group 1
```

```
Switch(config-multilink-group)# multilink-enhance timeout 20
```

## 相关命令

```
show multi-link group
```

# 15.8 Monitor Link 命令

## 15.8.1 monitor-link group

该命令用于创建 monitor link 组。

## 命令语法

```
monitor link group GROUP-ID  
no monitor link group GROUP-ID
```

GROUP-ID	Monitor link 组编号。范围是 1-16
----------	---------------------------

## 命令模式

全局配置模式

## 默认

默认没有任何组创建

## 使用说明

该命令用于创建 monitor link 组。组编号范围是 1~16。

## 举例说明

如何创建一个组

```
Switch# configure terminal  
Switch(config)# monitor-link group 1
```

## 相关命令

```
no monitor-link group
```

## 15.8.2 monitor-link uplink interface

该命令为 monitor link 组创建上联端口。

## 命令语法

monitor-link uplink interface (*IFPHYSICAL*|*IFAGG*)

no monitor-link uplink interface (*IFPHYSICAL*|*IFAGG*)

IFPHYSICAL	物理端口名称
IFAGG	AGG 端口名称

## 命令模式

组配置模式

## 默认

默认不指定端口

## 使用说明

各类端口中只有物理端口和 AGG 端口才可以作为 monitor link 的上联端口

## 举例说明

为 monitor link 组添加上联端口 eth-0-1

```
Switch(config)# monitor-link group 1
Switch(config-mtlk-group)# monitor-link uplink interface eth-0-1
```

## 相关命令

show monitor-link group

### 15.8.3 monitor-link uplink smart-link group

该命令将一个 smart link 组加入到 monitor link 组并作为上联端口。

## 命令语法

monitor-link uplink smart-link group *GROUP-ID*

no monitor-link uplink smart-link group *GROUP-ID*

GROUP-ID	Smart link 组编号。范围是 1-16
----------	-------------------------

## 命令模式

组配置模式

## 默认

不指定任何 smart link 组

## 使用说明

只有正式启用(enable)的 smart link 组才可以作为 monitor link 组的上联端口

## 举例说明

将 smart link 组 1 做为 monitor link 组的上联端口

```
Switch(config)# monitor-link group 1
Switch(config-mtlk-group)# monitor-link uplink smart-link group 1
```

## 相关命令

show monitor-link group

## 15.8.4 no monitor-link uplink

该命令删除 monitor-link 组的所有上联端口。

## 命令语法

no monitor-link uplink

## 命令模式

组配置模式

## 默认

无

## 使用说明

该命令用于删除 monitor-link 组的所有上联端口，包括端口或 smart link 组

## 举例说明

删除本 monitor-link 组的所有上联端口

```
Switch(config-mtlk-group)# no monitor-link uplink
```

## 相关命令

show monitor-link group

### 15.8.5 monitor-link downlink interface

该命令为 monitor link 组创建下联端口。

## 命令语法

monitor-link downlink interface (*IFPHYSICAL*|*IFAGG*)

no monitor-link downlink interface (*IFPHYSICAL*|*IFAGG*)

IFPHYSICAL	物理端口名称
IFAGG	AGG 端口名称

## 命令模式

组配置模式

## 默认

默认不指定端口

## 使用说明

各类端口中只有物理端口和 AGG 端口才可以作为 monitor link 的下联端口

## 举例说明

为 monitor link 组添加下联端口 eth-0-1

```
Switch(config)# monitor-link group 1
Switch(config-mtlk-group)# monitor-link downlink interface eth-0-1
```

## 相关命令

show monitor-link group

### 15.8.6 monitor-link recover-time

该命令用于指定下联端口恢复时间。

## 命令语法

monitor-link recover-time *RECOVER\_TIME*



no monitor-link recover-time

RECOVER_TIME	Monitor link 组下量端口恢复时间范围（秒）。范围是 0-60
--------------	--------------------------------------

## 命令模式

全局配置模式

## 默认

默认是 3 秒

## 使用说明

该命令用于指定下联端口恢复时间。如果上联端口状态恢复为 up，所有的下联端口状态也将在指定的恢复时间后改为 up。以防止上联端口不停 up/down 导致下联端口频繁改变状态。

## 举例说明

全局将恢复时间改为 1 秒

```
Switch# configure terminal
Switch(config)# monitor-link recover-time 1
```

## 相关命令

show monitor-link group

### 15.8.7 show monitor-link group

该命令用于显示指定 monitor-link 组的信息。

## 命令语法

show monitor-link group (*GROUP-ID*)

GROUP-ID	Monitor link 组编号。范围是 1-16
----------	---------------------------

## 命令模式

特权模式

## 默认

无

## 使用说明

该命令用于显示指定 **monitor link** 组的状态和信息。

## 举例说明

```
Switch# show monitor-link group
Group Id: 1
Monitor link status: UP
Role      Member      Last-up-time      Last-down-time      upcount
downcount
UpLk 1   eth-0-2      2011/07/15,01:34:17  2011/07/15,01:34:14  1          1
```

## 相关命令

无

## 15.8.8 debug monitor-link

该命令用于 debug monitor-link 信息。

## 命令语法

```
debug monitor-link
```

## 命令模式

特权模式

## 默认

无

## 使用说明

该命令用于 debug monitor-link 组触发事件的信息

## 举例说明

打开 **monitor-link** 组的 debug 信息

```
Switch# debug monitor-link
```

## 相关命令

无

## 15.9 VRRP 命令

### 15.9.1 advertisement-interval

使用该命令配置 master 虚拟路由器发送的一系列的宣告报文的时间间隔。可以用相应的 no 来配置成默认值。

#### 命令语法

```
advertisement-interval INTERVAL
```

```
no advertisement-interval
```

<b>INTERVAL</b>	虚拟路由器发送的一系列的宣告报文的时间间隔。单位是秒，默认值是 1 秒，有效范围是 1~255 秒
-----------------	---

#### 命令模式

路由模式

#### 默认

无

#### 使用说明

master 虚拟路由器发送的宣告用于向 backup 路由器通告它当前的优先权以及状态。

如果运行 VRRP 协议的路由器的通告时间没有设置的话，它可以从 master 路由器那边学到。Master 路由器上面的通告时间总是可以覆盖同一个 VRRP 组中所有其他路由器设备的通告时间，只要你配置了命令 learnmaster-mode 为 TRUE。同一个 VRRP 组中的通告时间必须保持一致。如果路由器之间设定的通告时间不一致，那么这些路由器之间将不能互相通信，在经过一定的时间间隔后，各自都会成为 master。

#### 举例说明

设置 Master 路由器发送宣告报文的时间间隔为 4 秒：

```
Switch(config)#router vrrp 1  
Switch(config-router)#advertisement-interval 4
```

#### 相关命令

```
advertisement-interval msec
```

## 15.9.2 advertisement-interval msec

使用该命令来配置 **master** 虚拟路由器发送的一系列的宣告报文的时间间隔（以毫秒为单位）。可以用相应的 **no** 来配置成默认值。

### 命令语法

**advertisement-interval msec** *INTERVAL*

**no advertisement-interval msec**

<b>INTERVAL</b>	路由器发送宣告报文的间隔，以毫秒为单位,范围 100-900
-----------------	--------------------------------

### 命令模式

路由模式

### 默认

无

### 使用说明

以毫秒为单位的通告报文时间间隔必须是 100 的倍数。使用毫秒模式可以使系统更快的检测到网络状态变化，加快网络收敛速度。

### 举例说明

设置 Master 路由器发送宣告报文的时间间隔为 100 毫秒：

```
Switch(config)#router vrrp 1
Switch(config-router)#advertisement-interval msec 100
```

### 相关命令

**advertisement-interval**

## 15.9.3 interface (VRRP)

此命令用于在某个指定端口上启用 VRRP。使用关键字 **no** 在这个端口上删除 VRRP。

### 命令语法

**interface** INTERFACE-ID

**no interface**

<b>INTERFACE-ID</b>	接口 ID
---------------------	-------

## 命令模式

路由模式

## 默认

无

## 使用说明

在同一个接口上，启用 VRRP 的数量不要超过 3。

## 举例说明

设置在端口 eth-0-1 上启动 VRRP：

```
Switch(config)# router vrrp 1
Switch(config-router)# interface eth-0-1
```

## 相关命令

router vrrp

## 15.9.4 learnmaster-mode

该命令开启备份路由器学习主路由器的发送通告报文时间间隔的功能。使用 `learnmaster-mode false` 命令关闭学习功能。

## 命令语法

learnmaster-mode (true|false)

true	开启备份路由器学习主路由器发送的时间间隔
false	关闭备份路由器学习主路由器发送的时间间隔

## 命令模式

路由模式

## 默认

无

## 使用说明

由于所有在同一个 VRRP 组内通信的路由器的通告报文时间间隔必须设成一致，因此，为了确保主路由器和从路由器配置的时间间隔是一致的，您可以开启学习功能。

## 举例说明

设置备份路由学习主路由器发送的时间间隔：

```
Switch(config)# router vrrp 1
Switch(config-router)# learnmaster-mode true
```

## 相关命令

router vrrp

### 15.9.5 preempt-mode

此命令设置交换机是否工作于抢占模式。

## 命令语法

preempt-mode (true | false)

## 命令模式

路由模式

## 默认

无

## 使用说明

交换机缺省工作于抢占模式；

处于 backup 状态的路由器如果收到一个报文，并且自己的抢占模式设为 FALSE 或者收到的报文里的优先级比自己本地的优先级高，则路由器继续保持 backup 状态，否则将在 master down 时间间隔后转为 master。

注意：如果是交换机自己拥有该虚拟 IP 地址(即 IP address owner)，则抢占模式一定是 TRUE 的。

如果交换机工作于抢占模式，则当 Master 路由器的 priority 发生变化或者 track 端口 Down 掉时，此交换机会参与 Master 路由器的竞选。

如果交换机工作于非抢占模式，当 Master 路由器的 priority 发生变化或者 track 端口 Down 掉时，此交换机不会参与 Master 路由器的竞选；

如果 Master 路由器 Down 掉，则不论交换机的 preempt-mode 设置为 true 或者 false，此交换机都会参与 Master 路由器的竞选。

## 举例说明

设置交换机工作于抢占模式且设置优先级为 200。

```
Switch(config)#router vrrp 1
Switch(config-router)#preempt-mode true
Switch(config-router)#priority 200
```

## 相关命令

preempt delay

### 15.9.6 preempt delay

配置 Master 路由器 Down 时候 backup 路由器的抢占延迟时间。

## 命令语法

preempt delay *TIME*

TIME	抢断延迟时间 0-3600 秒
------	-----------------

## 命令模式

路由模式

## 默认

无

## 使用说明

master 路由器 down 时间的默认算法  $= (3 * \text{adv\_interval}) + \text{skew\_time}$ 。当配置了 delay time 后, 算法为  $= (3 * \text{adv\_interval}) + \text{skew\_time} + \text{preempt\_delay}$ 。默认 delay time 为 0。backup 在经过 master down 时间还没有主路由器发布的通告报文, 就认为主路由器出现故障, 并将自己转变成 master 状态。

## 举例说明

设置 VRRP 为抢占模式, 优先级 200 且抢占时间延迟为 30 秒。

```
Switch(config)#router vrrp 1
Switch(config-router)#preempt-mode true
Switch(config-router)#priority 200
Switch(config-router)#preempt delay 30
```

## 相关命令

preempt-mode

### 15.9.7 priority(VRRP)

此命令设置本交换机在虚拟路由器组内的优先权。

使用关键字 **no** 恢复本交换机在虚拟路由器组内的优先权为默认值。

## 命令语法

priority *LEVEL*

no priority

LEVEL	本交换机在虚拟路由器组内的优先权，范围 1-254。
-------	----------------------------

## 命令模式

路由模式

## 默认

无

## 使用说明

虚拟路由器组使用竞选方式产生 **Master** 路由器，其他所有路由器作为 **Backup**；其中，优先级高的将作为 **Master** 路由器；如果优先级相同，则会比较网络接口的主 IP 地址，其中，IP 地址高的将作为 **Master** 路由器。缺省优先级为 100。

## 举例说明

设置本交换机在虚拟路由器组内的优先权为 254：

```
Switch(config)#router vrrp 1
Switch(config-router)#priority 254
```

## 相关命令

router vrrp

### 15.9.8 router vrrp

此命令设置交换机加入指定的虚拟路由器组并进入 VRRP 配置模式。

使用关键字 **no** 退出指定的虚拟路由器组。



## 命令语法

```
router vrrp GROUP
no router vrrp GROUP
```

GROUP	VRRP 组标志符,范围 1-255
-------	--------------------

## 命令模式

全局配置模式

## 默认

无

## 使用说明

在同一个虚拟路由器组内的路由器，必须配置相同的虚拟路由器组标志符。在使用 **no** 退出指定的虚拟路由器之前，必须先 **disable VRRP**，使其处于 **init** 状态。

## 举例说明

设置交换机加入虚拟路由器组 1 并进入其配置模式：

```
Switch(config)# router vrrp 1
```

## 相关命令

无

### 15.9.9 track (VRRP)

此命令设置在本交换机上运行的虚拟路由器组监视端口。

使用关键字 **no** 删除监视端口。

## 命令语法

```
track OBJ_ID (decrement VALUE)
no track
```

OBJ_ID	跟踪对象 ID 1~500
decrement	优先级递减
VALUE	递减值<1-255>

## 命令模式

路由模式

## 默认

无

## 使用说明

使用 track 来监视一个处于 up 状态的端口，一般这个端口是报文的上行链路。当这个端口 down 掉的时候，master 路由器的优先级将会减少，相应的设置了抢占模式为 TRUE 的 backup 路由器就可以成为 master 路由器。因此，递减值的设置一定要大于 master 和 backup 路由器的优先级之差。

一个特定的 VRRP 组中只能有一个 track 对象，后一个配置的 track 对象总是会将前一个给覆盖掉。

## 举例说明

配置在本交换机上运行的虚拟路由器组监视端口为 eth-0-1:

```
Switch(config)#track 10 interface eth-0-1 linkstate
Switch(config)# router vrrp 1
Switch(config-router)#track 10
```

## 相关命令

router vrrp

### 15.9.10 enable / disable

此命令启用或关闭 VRRP 路由协议。

## 命令语法

enable / disable

## 命令模式

路由模式

## 默认

无

## 使用说明

无

## 举例说明

设置交换机开启 VRRP 功能

```
Switch(config-router)#enable
```

设置交换机关闭 VRRP 功能

```
Switch(config-router)#disable
```

## 相关命令

无

## 15.9.11 virtual-ip

此命令设置虚拟 VRRP 路由器的虚拟 IP 地址，使用关键字 **no** 删除该虚拟 IP。

## 命令语法

```
virtual-ip IP-ADDRESS
```

```
no virtual-ip
```

IP-ADDRESS	虚拟路由器的 IP 地址
------------	--------------

## 命令模式

路由模式

## 默认

无

## 使用说明

VRRP 组中的所有路由器都必须与这个虚拟路由器使用相同的主网络地址。否则的话，VRRP 组中的成员就无法相互通信，并且错误配置的将会导致同一个 VRRP 组中的所有路由器都变成 **master** 路由器。虚拟 IP 地址和 VRRP 接口必须在同一个子网内，如果虚拟 IP 地址跟接口的 IP 地址一致，它被称为 IP 地址拥有者。

## 举例说明

设置本设备的虚拟 IP 地址为 10.0.1.20。

```
Switch(config)#interface eth-0-1
Switch(config-if)#no switchport
Switch(config-if)#ip address 10.0.1.1/24
Switch(config)#router vrrp 1
Switch(config-router)#interface eth-0-1
```

```
Switch(config-router)#virtual-ip 10.0.1.20
Switch(config-router)#enable
```

## 相关命令

```
router vrrp
```

## 15.9.12 show vrrp

使用此命令查看 VRRP 协议的配置信息。

## 命令语法

```
show vrrp (GROUP |)
```

GROUP	VRRP 组编号；如果未指定，则查看所有 VRRP 组配置信息
-------	---------------------------------

## 命令模式

特权模式

## 默认

无

## 使用说明

假如没有指定 VRRP 组，那么显示所有的 VRRP 组

## 举例说明

显示交换机配置的所有 VRRP 信息：

```
Switch# show vrrp
VRID <1>
  State                : Master
  Virtual IP           : 10.0.20.254 (Not IP owner)
  Interface            : eth-0-10
  VMAC                 : 0000.5e00.0101
  Advt timer           : 1
  Preempt mode         : TRUE
  Conf pri             : 200           Run pri   : 200
  Master router ip    : 10.0.20.1
  Master priority     : 200
  Master advt timer   : 1
  Master down timer   : 3
  Preempt delay       : 100 second(s)
  Learn master mode   : FALSE
```

## 相关命令

```
router vrrp
```

# 15.10 Track 命令

## 15.10.1 delay up

在 track 模式下，使用 `delay up` 命令，来指定一个 track 对象的通信状态迁移的延迟时间(s)。返回默认值，使用相应的 `no` 命令。

## 命令语法

```
delay up seconds
```

```
no delay up
```

seconds	范围：1 ~ 180
---------	------------

## 命令模式

Track 模式

## 默认

无

## 使用说明

无

## 举例说明

下面是一个例子，用于表示，检测 eth-0-1 端口的端口状态迁移(从 down->up)，设定延迟时间为 30s:

```
Switch(config)# track 1 interface eth-0-1 linkstate
Switch(config-track)# delay up 30
```

## 相关命令

```
delay down
```

## 15.10.2 delay down

在 track 模式下，使用 `delay up` 命令，来指定一个 track 对象的通信状态迁移的延迟时间 (s)。返回默认值，使用相应的 `no` 命令。

### 命令语法

`delay down seconds`

`no delay down`

seconds	time range is from 1 to 180
---------	-----------------------------

### 命令模式

Track 模式

### 默认

无

### 使用说明

无

### 举例说明

下面是一个例子，用于表示，检测 eth-0-1 端口的端口状态迁移(从 up->down)，设定延迟时间为 30s:

```
Switch(config)# track 1 interface eth-0-1 linkstate
Switch(config-track)# delay down 30
```

### 相关命令

`delay up`

## 15.10.3 frequency

设定 IP SLA 操作的频率。使用相应的 `no` 命令来返回默认值。

### 命令语法

`frequency seconds`

`no frequency`

seconds	范围 1 - 4800. ( frequency > interval * ( packets-per-test - 1 ) + timeout)
---------	---

## 命令模式

IP SLA 模式

## 默认

默认值是 60s

## 使用说明

无

## 举例说明

下面的例子讲 IP SLA 操作的频率设置成了 10s。

```
Switch(config)# ip sla monitor 1
Switch(config-ipsla)# frequency 10
```

## 相关命令

show ip sla monitor

### 15.10.4 ip sla monitor

在 CONFIG 模式使用 IP SLA monitor 来创建一个 IP SLA 并进入 IP SLA 配置模式。删除这个 IP SLA 的话用它相应的 no 命令。

## 命令语法

```
ip sla monitor entrynumber
no ip sla monitor entrynumber
```

entrynumber	ip sla 的标识, 范围 1~255
-------------	----------------------

## 命令模式

配置模式

## 默认

无

## 使用说明

无

## 举例说明

在下面的例子中，`ip sla monitor` 命令创建了一个 IP SLA，并进入了 IP SLA 配置模式：

```
Switch(config)# ip sla monitor 1
Switch(config-ipsla)#
```

## 相关命令

`show ip sla monitor`

## 15.10.5 description string

配置 IP SLA 的描述信息。删除这个 IP SLA 的话用它相应的 `no` 命令。

## 命令语法

`description string`

`no description`

string	描述信息，长度不超过 255 个字符
--------	--------------------

## 命令模式

IPSLA 模式

## 默认

无

## 使用说明

无

## 举例说明

在下面的例子中，设置 IP SLA 的描述信息：

```
Switch(config)# ip sla monitor 1
Switch(config-ipsla)#description thisisanexampler
```



## 相关命令

## 15.10.6 show ip sla monitor ip sla monitor schedule

在 CONFIG 模式使用 `ip sla monitor schedule` 来启用一个 IP SLA 的条目。删除这个 IP SLA 条目的话用它相应的 `no` 命令。

## 命令语法

`ip sla monitor schedule (entrynumber)`

entrynumber	用于标识这个 IP SLA，它的范围是 1~255
-------------	---------------------------

## 命令模式

配置模式

## 默认

无

## 使用说明

无

## 举例说明

下面是一个如何启用一个 IP SLA 监测的例子：

```
Switch(config)# ip sla monitor 1
Switch(config-ipsla)# exit
Switch(config)# ip sla monitor schedule 1
```

## 相关命令

`show ip sla monitor`

## 15.10.7 timeout

设定 IP SLA 操作等待其请求响应的超时时间，使用相应的 `no` 命令来让它返回默认值。

## 命令语法

`timeout seconds`

`no timeout`

seconds	时间范围 1 - 4800. ( frequency > interval * ( packets-per-test - 1 ) + timeout)
---------	---

## 命令模式

IP SLA 模式

## 默认

无

## 使用说明

默认值是 5 秒

## 举例说明

下面的例子描述了如何设定 IP SLA 的超时时间:

```
Switch(config)# ip sla monitor 1
Switch(config-ipsla)# timeout 10
```

## 相关命令

show ip sla monitor

## 15.10.8 threshold

设定 IP SLA 操作进行网络监测统计时的上限阈值，使用相应的 no 命令来让它返回默认值。

## 命令语法

threshold *milliseconds*

no threshold

milliseconds	时间范围 1 - 4800000.( 超时时间 ≥ 阈值)
--------------	-------------------------------

## 命令模式

IP SLA 模式

## 默认

无

## 使用说明

默认值是 5000 毫秒

## 举例说明

下面的例子描述了如何设定 IP SLA 的阈值时间：

```
Switch(config)# ip sla monitor 1
Switch(config-ipsla)# threshold 10000
```

## 相关命令

show ip sla monitor

## 15.10.9 interval

设定 IP SLA 操作一次检测中两次 icmp 请求的时间间隔，使用相应的 no 命令来让它返回默认值。

## 命令语法

**interval** *seconds*

no interval

seconds	时间范围 1 - 4800.( frequency > interval * ( packets-per-test - 1 ) + timeout)
---------	--

## 命令模式

IP SLA 模式

## 默认

6

## 使用说明

无

## 举例说明

下面的例子描述了如何设定 IP SLA 的超时时间：

```
Switch(config)# ip sla monitor 1
Switch(config-ipsla)# interval 10
```

## 相关命令

show ip sla monitor

## 15.10.10 ttl

设定 IP SLA 操作进行网络监测统计时的 icmp 请求报文的 ttl，使用相应的 no 命令来让它返回默认值。

### 命令语法

ttl *value*

no ttl

value	范围 1 - 255
-------	------------

### 命令模式

IP SLA 模式

### 默认

64

### 使用说明

无

### 举例说明

下面的例子描述了如何设定 IP SLA 的 ttl:

```
Switch(config)# ip sla monitor 1
Switch(config-ipsla)# ttl 100
```

### 相关命令

show ip sla monitor

## 15.10.11 tos

设定 IP SLA 操作进行网络监测统计时的 icmp 请求报文的 tos，使用相应的 no 命令来让它返回默认值。

### 命令语法

tos *value*

no tos

value	范围 1 - 255
-------	------------

### 命令模式

IP SLA 模式

### 默认

0

### 使用说明

无

### 举例说明

下面的例子描述了如何设定 IP SLA 的 tos:

```
Switch(config)# ip sla monitor 1
Switch(config-ipsla)# tos 100
```

### 相关命令

show ip sla monitor

## 15.10.12 data-size

设定 IP SLA 操作进行网络监测统计时的 icmp 请求报文数据大小, 使用相应的 no 命令来让它返回默认值。

### 命令语法

data-size *size*

no data-size

size	范围 1 - 8100
------	-------------

### 命令模式

IP SLA 模式

### 默认

28

### 使用说明

无

## 举例说明

下面的例子描述了如何设定 IP SLA 的 icmp 报文数据大小：

```
Switch(config)# ip sla monitor 1
Switch(config-ipsla)# data-size 100
```

## 相关命令

```
show ip sla monitor
```

### 15.10.13 data-pattern

设定 IP SLA 操作进行网络监测统计时的 icmp 请求报文携带字段内容，使用相应的 no 命令来让它返回默认值。

## 命令语法

```
data-pattern string
```

```
no data-pattern
```

string	十进制字符串，范围 0 -FFFFFFFF
--------	-----------------------

## 命令模式

IP SLA 模式

## 默认

ABCDABCD

## 使用说明

无

## 举例说明

下面的例子描述了如何设定 IP SLA 的 icmp 报文携带数据：

```
Switch(config)# ip sla monitor 1
Switch(config-ipsla)# data-pattern abababab
```

## 相关命令

```
show ip sla monitor
```

## 15.10.14 fail-percent

设定 IP SLA 操作进行网络监测统计时的 fail 百分比，使用相应的 no 命令来让它返回默认值。

### 命令语法

fail-percent *percent*

no fail-percent

percent	范围 1 - 100
---------	------------

### 命令模式

IP SLA 模式

### 默认

100

### 使用说明

无

### 举例说明

下面的例子描述了如何设定 IP SLA 的 fail 百分比：

```
Switch(config)# ip sla monitor 1
Switch(config-ipsla)# fail-percent 90
```

### 相关命令

show ip sla monitor

## 15.10.15 packets-per-test

设定 IP SLA 操作进行网络监测统计时的单次检测发送 icmp 请求的次数，使用相应的 no 命令来让它返回默认值。

### 命令语法

packets-per-test *number*

no probe-count

number	范围 1 - 10( frequency > interval * ( packets-per-test - 1 ) + timeout)
--------	---

## 命令模式

IP SLA 模式

## 默认

3

## 使用说明

无

## 举例说明

下面的例子描述了如何设定 IP SLA 一次检测发送 5 次 icmp 请求:

```
Switch(config)# ip sla monitor 1
Switch(config-ipsla)# packets-per-test 5
```

## 相关命令

show ip sla monitor

### 15.10.16 statistics (packet | test)

设定 IP SLA 统计信息总的个数以及显示最近几次 test 记录, 使用相应的 no 命令来让它返回默认值。

## 命令语法

```
statistics (packet <0-1000>|test <1-10>)
```

```
no statistics packet
```

```
no statistics test
```

## 命令模式

IP SLA 模式

## 默认

packet: 50; test: 5

## 使用说明

无

## 举例说明

下面的例子描述了如何设定 IP SLA 总记录数为 60, 记录最近 6 次检测结果:

```
Switch(config)# ip sla monitor 1
```



```
Switch(config-ipsla)# statistics packet 60
Switch(config-ipsla)# statistics test 6
```

## 相关命令

show ip sla monitor

### 15.10.17 clear ip sla statistics

清空某个 ipsla entry 的所有统计信息。

## 命令语法

```
clear ip sla statistics entry_id
```

entry_id	范围 1 - 255
----------	------------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面的例子描述了如何清空 ipsla monitor 1 的统计信息：

```
Switch # clear ip sla statistics 1
```

## 相关命令

### 15.10.18 show ip sla monitor track

在配置模式下，使用 track 命令来指定一个 track 对象。

## 命令语法

```
track object_id
```

object_id	track 对象的标识，范围 1-500
-----------	----------------------

## 命令模式

配置模式

## 默认

无

## 使用说明

无

## 举例说明

下面的例子描述了如何在端口 `eth-0-1` 上创建一个 `track` 对象：

```
Switch(config)# track 1 interface eth-0-1 linkstate
Switch(config-track)#
```

## 相关命令

`show track`

## 15.10.19 track interface linkstate

在全局配置模式下，使用 `track interface linkstate` 命令来创建一个 `track` 接口状态的 `track` 对象。使用相应的 `no` 命令来删除这个 `track` 对象。

## 命令语法

```
track object_id interface IFNAME linkstate
```

```
no track object_id
```

<code>object_id</code>	track 对象的标识，范围 1-500
<code>IFNAME</code>	接口名

## 命令模式

配置模式

## 默认

无

## 使用说明

无

## 举例说明

下面的例子描述了如何在端口 eth-0-1 上创建一个 track 对象:

```
Switch(config)# track 1 interface eth-0-1 linkstate
Switch(config-track)#
```

## 相关命令

show track

### 15.10.20 track rtr reachability

在全局配置模式下, 使用 track rtr reachability 命令, 来创建一个用于 track IP SLA 条目的 track 对象。使用相应的 no 命令来删除这个 track 对象。

当 IP SLA 条目的状态为 OK 或者超出阈值时, track 对象处于 up 状态; 否则的话 track 对象就处于 down 状态。

## 命令语法

track *object\_id* rtr entrynum reachability

**no** track *object\_id*

object_id	track 对象的标识, 范围 1-500
entrynumber	IP SLA 监视条目的标识符, 范围 1-255

## 命令模式

配置模式

## 默认

无

## 使用说明

无

## 举例说明

下面的例子描述了如何创建一个用于 track IP SLA 监视条目的 track 对象:

```
Switch(config)# ip sla monitor 1
Switch(config-ipsla)# exit
Switch(config)# track 1 rtr 1 reachability
Switch(config-track)#
```

## 相关命令

show track

### 15.10.21 track rtr state

在全局配置模式下，使用 `track rtr state` 命令，来创建一个用于 track IP SLA 条目的 track 对象。使用相应的 `no` 命令来删除这个 track 对象。

当 IP SLA 条目的状态为 OK 时，track 对象处于 up 状态；否则的话 track 对象就处于 down 状态。

## 命令语法

**track** *object\_id* **rtr** *entrynum* **state**

**no track** *object\_id*

object_id	track 对象的标识，范围 1~500
entrynumber	IP SLA 监视条目的标识符，范围 1~255

## 命令模式

配置模式

## 默认

无

## 使用说明

无

## 举例说明

下面的例子描述了如何创建一个用于 track IP SLA 监视条目的 track 对象：

```
Switch(config)# ip sla monitor 1
Switch(config-ipsla)# exit
Switch(config)# track 1 rtr 1 state
Switch(config-track)#
```

## 相关命令

show track

### 15.10.22 track bfd

在全局配置模式下，使用 `track bfd` 命令，来创建一个用于 bfd 会话的 track 对象。使用相应的 `no` 命令来删除这个 track 对象。

当 bfd 会话的状态为 up 时，track 对象处于 up 状态；否则的话 track 对象就处于 down 状态。

## 命令语法

**track** *object\_id* bfd source interface IFNAME destination A.B.C.D

**no track** *object\_id*

object_id	track 对象的标识，范围 1~500
interface IFNAME	接口名
Destination A.B.C.D	BFD 会话的目的地址

## 命令模式

配置模式

## 默认

无

## 使用说明

源端口必须是一个三层接口，且配置好 ip 地址。

目的 ip 必须和源端口的 ip 地址在同一网段内。

## 举例说明

下面的例子描述了如何创建一个用于 track bfd 监视条目的 track 对象：

```
Switch (config)# interface eth-0-9
Switch (config-if)# no switchport
Switch (config-if)# no shutdown
Switch (config-if)# ip address 9.9.9.1/24
Switch (config-if)# quit
Switch (config)# track 1 bfd source interface eth-0-9 destination 9.9.9.2
Switch (config-track)#
```

## 相关命令

**show track**

### 15.10.23 type icmp-echo

定义一个 ICMP 报文的 echo 操作，并且输入其目的 IP 地址。

使用相应的 no 命令来删除这个 echo 操作。

## 命令语法

**type icmp-echo** *A.B.C.D* (**source-interface** *IFNAME*) (**source-ip** *A.B.C.D*)

**no type icmp-echo**

A.B.C.D	指定 ICMP 报文的地址
source-interface IFNAME	指定 ICMP 报文的出接口
source-ip A.B.C.D	指定 ICMP 报文的源 IP 地址

## 命令模式

IP SLA 模式

## 默认

无

## 使用说明

**source-interface** 指定的源接口需要是报文实际能路由转发出去的接口之一，否则报文可能无法发出。

## 举例说明

下面的例子描述了如何在 IP SLA 中定义一个 ICMP 报文的 echo 操作：

```
Switch(config)#ip sla monitor 1
Switch(config-ipsla)# type icmp-echo 192.168.0.1
```

## 相关命令

**show ip sla monitor**

## 15.10.24 show ip sla monitor

在特权模式下，使用 `show ip sla monitor` 命令，来显示 IP SLA 条目以及该 entry 的所有统计信息，以及最近几次的检测结果。

### 命令语法

```
show ip sla monitor (entrynumber) (statistics (packet | test)|)
```

entrynumber	IP SLA 监视条目的标识符，范围 1-255
-------------	--------------------------

### 命令模式

特权模式

### 默认

无

### 使用说明

无

### 举例说明

下面的例子描述了应该如何显示 IP SLA 监视条目：

```
Switch# show ip sla monitor
Entry 1
  Type                : Echo
  Admin state         : Enable
  Destination address : 192.168.0.1
  Frequency            : 3 seconds
  Timeout             : 2 seconds
  Threshold           : 1 seconds
  Running Frequency   : 3 seconds
  Vrf                 : vpn1
  Return code         : OK
```

### 相关命令

`ip sla monitor`

## 15.10.25 show track

在特权模式使用 `show track` 命令来显示 track 对象：

## 命令语法

```
show track object_id
```

<i>object_id</i>	track 对象的标识, 范围 1-500
------------------	-----------------------

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面的例子描述了应该如何显示 track 对象:

```
Switch#show track
Track 2
  Type           : Response Time Reporter(RTR) Reachability
  Interface      : eth-0-2
  State          : down
  Delay up       : 30 seconds
  Delay down     : 30 seconds
```

## 相关命令

track

### 15.10.26 vrf

在 IP SLA 模式下, 使用 vrf 命令, 来在 VPN 下使用 IP SLA 操作, 使用相应的 no 命令来返回默认。

## 命令语法

```
vrf vrfname
```

```
no vrf
```

<i>vrfname</i>	VRF 名
----------------	-------



## 命令模式

IP SLA 模式

## 默认

无

## 使用说明

无

## 举例说明

下面的例子模式了如何在 VPN 下使用 IP SLA 操作：

```
Switch(config)# ip sla monitor 1
Switch(config-ipsla)# vrf vpn1
```

## 相关命令

show ip sla monitor

# 15.11 VARP 命令

## 15.11.1 ip virtual-router mac

使用该命令配置配置交换机虚拟 MAC。可以用相应的 no 来配置成默认值。

## 命令语法

**ip virtual-router mac** *mac-addr*

**no ip virtual-router mac**

mac-addr	虚拟 MAC 地址
----------	-----------

## 命令模式

全局配置模式

## 默认

无

## 使用说明

虚拟 MAC 地址为相应的虚拟 IP 地址提供对应的二层地址。这个地址只有在接收报文的时候使用，对于交换机发出或转发的普通报文不会使用该地址。对于 ARP 报文，只有在回复虚拟 IP 地址的请求时会使用虚拟 MAC 地址。

## 举例说明

设置交换机的虚拟 MAC 地址为 1.1.1:

```
Switch(config)# ip virtual-router mac 1.1.1
```

## 相关命令

```
ip virtual-router address
```

### 15.11.2 ip virtual-router address

使用该命令来配置虚拟 IP 地址。可以用相应的 no 来配置成默认值。

## 命令语法

```
ip virtual-router address IP-address
```

```
no ip virtual-router address
```

IP-address	虚拟 IP 地址
------------	----------

## 命令模式

端口配置模式

## 默认

无

## 使用说明

本命令配置端口上的虚拟 IP 地址。该虚拟地址需要和端口上的地址在一个网段。如果虚拟 MAC 没有配置，系统不会回复虚拟 IP 地址的 ARP 请求。

## 举例说明

设置端口上的虚拟地址为 1.1.1.1:

```
Switch(config-if)# ip virtual-router address 1.1.1.1
```

## 相关命令

ip virtual-router mac

## 15.12 IP 双向转发检测配置

### 15.12.1 bfd interval

使用该命令配置期望的 BFD 收发包速率及检测倍数。

使用该命令的“no”格式恢复默认值。

## 命令语法

bfd interval {mintx <3-1000> | minrx <3-1000> | multiplier <2-15>}

no bfd interval

参数	描述
mintx <3-1000>	配置 BFD 发包速率
minrx <3-1000>	配置 BFD 收包速率
multiplier <2-15>	配置 BFD 检测间隔倍数

## 命令模式

端口配置模式

## 默认配置

默认发送速率和接收速率为 20 毫秒。

默认检测间隔倍数为 3。

## 使用说明

使用该命令配置期望的 BFD 收发包速率及检测倍数。

这个配置将影响接口上所有的 BFD 会话。实际的收发包速率需要和会话的对端协商决定。

## 举例说明

这个例子将接口期望的收包速率和发包速率都设置为 3 毫秒，将检测间隔倍数设置为 3:

```
Switch (config-if)# bfd interval mintx 3 minrx 3 multiplier 3
```

## 相关命令

无

### 15.12.2 bfd NAME peer-ip interface

使用该命令配置一条单跳 BFD 会话。

使用该命令的“no”格式删除这条会话。

## 命令语法

**bfd** NAME peer-ip A.B.C.D (vrf NAME|) interface (IFPHYSICAL|IFVLAN|IFAGG) (source-ip A.B.C.D |) (auto|local *discr-id* remote *discr-id*)

**no bfd** NAME

参数	描述
NAME	bfd session 的名称，长度为 1-16
peer-ip A.B.C.D	指定 bfd session 的目的 ip 地址
vrf NAME	bfd session 的 vrf 域
interface	单跳 bfd session 绑定的接口
Source-ip A.B.C.D	指定 bfd 的源 ip 地址
auto	自动分配 bfd session 的本地标识符
local <i>discr-id</i>	指定 bfd 本地标识符 <1-8191>
remote <i>discr-id</i>	指定 bfd 源端标识符

## 命令模式

全局配置模式

## 默认配置

默认情况下系统不会创建 bfd session。

## 使用说明

使用此命令创建静态单跳 bfd，如果创建的 bfd 配置参数满足条件，即可以创建 bfd session。当不满足条件时，配置保存，但是不会创建 bfd session。用户需要自己检测创建 bfd 不满足条件。配置时不做合法性检查，用户可以通过 show bfd static configurations 查看配置的 bfd 信息。

满足条件：1.目的 ip 地址与绑定接口的 ip 地址在同网段内。

2.若配置 vrf 信息，则 vrf 要与绑定的接口在同一个 vrf 内。若没有配置，则获取接口上的 vrf 信息

3.若指定源 ip 地址，则该指定的源 ip 地址要为绑定接口上的 ip 地址。若没有指定，则获取与目的 ip 地址同网段的 ip 地址

若指定本地和源端标识符，则使用指定的。若没有指定，则系统自动分配本地标识符

## 举例说明

这个例子表明创建一个名为 test 的 bfd session。

```
Switch (config)# bfd test peer-ip 9.9.9.2 interface eth-0-9 local 10 remote 20
```

## 相关命令

ip route

### 15.12.3 bfd NAME peer-ip

使用该命令配置一条多跳 BFD 会话。

使用该命令的“no”格式删除这条会话。

## 命令语法

```
bfd NAME peer-ip A.B.C.D source-ip A.B.C.D (auto|local discr-id remote discr-id)
```

**no bfd NAME**

参数	描述
NAME	bfd session 的名称，长度为 1-16
peer-ip A.B.C.D	指定 bfd session 的目的 ip 地址
Source-ip A.B.C.D	指定 bfd 的源 ip 地址
auto	自动分配 bfd session 的本地标识符
local <i>discr-id</i>	指定 bfd 本地标识符 <1-8191>
remote <i>discr-id</i>	指定 bfd 源端标识符

## 命令模式

全局配置模式

## 默认配置

默认情况下系统不会创建 bfd session。

## 使用说明

使用此命令创建静态多跳 bfd，如果创建的 bfd 配置参数满足条件，即可以创建 bfd session。当不满足条件时，配置保存，但是不会创建 bfd session。用户需要自己检测创建 bfd 不满足条件。配置时不做合法性检查，用户可以通过 show bfd static configurations 查看配置的 bfd 信息。

满足条件：1. 指定源 ip 地址，则该指定的源 ip 地址要为绑定接口上的 ip 地址。

若指定本地和源端标识符，则使用指定的。若没有指定，则系统自动分配本地标识符

## 举例说明

这个例子表明创建一个名为 test 的 bfd session。

```
Switch (config)# bfd test peer-ip 9.9.9.2 source 10.10.10.1 local 10 remote 20
```

## 相关命令

ip route

### 15.12.4 bfd set interval

使用该命令配置 bfd session 的收发包间隔时间。

使用该命令的“no”格式删除这条配置。

## 命令语法

```
bfd set interval mintx <1-1000> minrx <1-1000> multiplier <2-15>
```

**no bfd set interval**

参数	描述
mintx <1-1000>	bfd session 支持最小的发包时间
minrx <1-1000>	bfd session 支持最小的收包时间
multiple <2-15>	检测倍数

## 命令模式

BFD 配置模式

## 默认配置

默认情况下 BFD 收发包时间来源于接口上的收发配置时间，接口默认收发包时间为 20ms。

## 使用说明

使用此命令为该 bfd session 配置最小支持的收包和发包时间以及检测倍数，peer session 控制。

## 举例说明

这个例子表明为 bfd test 配置收发包时间。

```
Switch (config)# bfd test
Switch(config-ip-bfd)# bfd set interval mintx 30 minrx 30 multiplier 5
```

## 相关命令

```
show bfd session detail
```

### 15.12.5 bfd global dscp

使用该命令全局配置多跳的 DSCP 值。

使用该命令的“no”格式删除这条配置。

## 命令语法

```
bfd global dscp <0-63>
```

```
no bfd global dscp
```

参数	描述
<0-63>	多跳报文 IP 头携带的 DSCP 字段值，报文优先级

## 命令模式

全局配置模式

## 默认配置

默认情况下多跳 BFD DSCP 值为 56

## 使用说明

使用此命令为多跳 bfd session 全局配置 DSCP 值

## 举例说明

这个例子表明全局模式下配置多跳的 DSCP 值为 63。

```
Switch (config)# bfd global dscp 63
```

## 相关命令

show bfd session detail

### 15.12.6 bfd set dscp

使用该命令配置 bfd session 的 dscp 值，peer session 配置。

使用该命令的“no”格式删除这条配置。

## 命令语法

bfd set dscp <0-63>

**no bfd set dscp**

参数	描述
dscp <0-63>	多跳报文 IP 头携带的 DSCP 字段值，报文优先级

## 命令模式

BFD 配置模式

## 默认配置

默认情况下多跳 BFD 的 IP 头 DSCP 值为 56，如果配置全局模式且又为每个 session 配置了 DSCP，则以 BFD session 上配置的 DSCP 值为标准。

## 使用说明

在全局配置 DSCP 和 bfd session 上都配置了 DSCP 时，bfd session 上配置的 DSCP 生效，如果删除 bfd session 配置，则恢复到全局配置的 DSCP 值。

## 举例说明

这个例子表明为 bfd test 配置 DSCP 值为 63。

```
Switch (config)# bfd test
Switch(config-ip-bfd)# bfd set dscp 63
```

## 相关命令

show bfd session detail

### 15.12.7 ip route

使用该命令配置将一条 BFD 会话与静态路由绑定。

使用该命令的“no”格式删除这个配置。



## 命令语法

**ip route prefix nexthop bind bfd NAME**

**no ip route prefix nexthop bind bfd**

参数	描述
prefix	IP 目的地址网段（例如 10.0.0.0/8）
nexthop	IP 网关地址
NAME	bfd session 的名称

## 命令模式

全局配置模式

## 默认配置

默认情况下系统不会为静态路由绑定 bfd session。

## 使用说明

使用该命令将一条 BFD 会话与静态路由绑定。

如果静态路由被删除，那么该静态路由与 bfd 也解除绑定，但是 bfd session 依然存在，不受影响。

## 举例说明

这个例子配置将一条网段为 1.1.1.0/24 下一跳地址为 9.9.9.2 的静态路由绑定到名为 test 的 bfd session 上：

```
Switch (config)# ip route 1.1.1.0/24 9.9.9.2 bind bfd test
```

## 相关命令

ip route

## 15.12.8 ip ospf bfd

使用该命令在接口上使能 BFD 和 OSPF 联动。

使用该命令的“no”格式在接口上去使能 BFD 和 OSPF 联动。

## 命令语法

**ip ospf bfd**

**no ip ospf bfd**

## 命令模式

端口配置模式

## 默认配置

默认情况下 BFD 和 OSPF 联动不使能。

## 使用说明

使用该命令在接口上使能 BFD 和 OSPF 联动。

当 OSPF 邻居建立，并且状态达到 two-way 以后（不包含 two-way），系统建立 BFD 会话。

当 OSPF 邻居删除或者状态回到 two-way 及以前（包含 two-way），BFD 会话拆除。

## 举例说明

这个例子在接口上使能了 BFD 和 OSPF 联动：

```
Switch (config-if)# ip ospf bfd
```

## 相关命令

无

### 15.12.9 bfd

使用这个命令配置 VRRP 和 BFD 联动。

使用这个命令的 no 格式去使能。

## 命令语法

```
bfd ip_nexthop_address { increase priority }
```

```
no bfd
```

## 命令模式

VRRP 配置模式

## 默认配置

默认情况下 BFD 和 VRRP 联动不使能。

## 使用说明

这个命令可以在单个 VRRP 实例中使能 BFD

BFD 会话在两端 VRRP 接口都配置好、虚 IP 创建以后开始建立。

如果链路断开或者 VRRP 配置被删掉，BFD 会话也会被删掉。

## 举例说明

下面这个例子在 VRRP 实例中绑定了 BFD：

```
Switch (config-router) # bfd 9.9.9.2
```

下面这个例子在 VRRP 实例中绑定了 BFD，并修改了链路断开时 VRRP 的优先级：

```
Switch (config-router) # bfd 9.9.9.2 increase 30
```

## 相关命令

无

### 15.12.10 show bfd

使用该命令显示 BFD 模块运行状态。

## 命令语法

```
show bfd
```

## 命令模式

特权模式

## 默认配置

无。

## 使用说明

使用该命令显示 BFD 模块运行状态。

## 举例说明

这个例子是该命令的显示结果：

```
Switch # show bfd
BFD ID: 00      Start Time:Thu May  2 03:09:41 2013
Number of Sessions:  2
Slow Timer: 1000      Image type: DISTRIBUTED
Echo Mode: Disabled   BFD Notifications disabled
Next Session Discriminator:  10
BFD Clients:
STATIC -> Client ID: 1
OSPF-> Client ID: 4
```

## 相关命令

无

## 15.12.11 show bfd static configurations

使用该命令显示 BFD 的静态配置。

### 命令语法

```
show bfd static configurations (word|)
```

### 命令模式

特权模式

### 默认配置

无。

### 使用说明

使用该命令显示 BFD 的静态配置信息。

后面跟参数为 `bfd session` 的名称，指定名称，只显示这个 `bfd` 的静态配置

### 举例说明

这个例子是该命令的显示结果：

```
Switch # show bfd static configurations
```

```
-----  
-----  
Name           Type           VRF           LocalDiscr   RemoteDiscr   Src Ip  
Dst Ip         interface      Status  
test1          single-hop default   -             -             10.10.10.1  
10.10.10.2     vlan10         active  
test2          single-hop centec    -             -             9.9.9.1  
9.9.9.2        vlan4094       active  
test3          single-hop default   8191          4294967295   10.10.10.1  
10.10.10.3     vlan10         active
```

### 相关命令

无

## 15.12.12 show bfd session

使用该命令显示 BFD 的会话。

### 命令语法

```
show bfd session ( detail | )
```

```
show bfd session SRC DST interface IFNAME ( detail | )
```

```
show bfd session SRC DST ( detail | )
```

show bfd session *DISCRIMINATOR index* (detail)

参数	描述
detail	显示会话详细信息
SRC	源端 IP 地址
DST	对端 IP 地址
IFNAME	BFD 接口
DISCRIMINATOR index	BFD 会话 ID

## 命令模式

特权模式

## 默认配置

无。

## 使用说明

使用该命令显示 BFD 的会话。

使用关键字“detail”显示详细信息。

可以通过指定源端、目的端 IP 地址和会话所在的接口过滤显示结果。

## 举例说明

这个例子是该命令的显示结果：

```
DUT1# show bfd session
Abbreviation:
LD: Local Discriminator.  RD: Remote Discriminator
S: Single hop session.   M: Multi hop session.
SD: Static Discriminator. DD: Dynamic Discriminator
A: Admin down.         D:Down.      I:Init.      U:Up.
=====
LD          RD          TYPE ST  UP-Time  Remote-Addr  VRF
8191       4294967295  S-SD D   00:00:00  10.10.10.3   default
8192        0             S-DD D   00:00:00  11.11.11.2   yoush
8193        0             S-DD D   00:00:00  10.10.10.2   default
8194        0             S-DD D   00:00:00  9.9.9.2      centec
Number of Sessions:    4
DUT1# show bfd session detail
=====
Session Interface : vlan10          Session Name : test3
Lower Layer : IPv4                 Version : 1
Session Type : Single Hop          Session State : Down
Discriminator Type : Static        DSCP : 0
```

```

Local Discriminator : 8191                Local Address : 10.10.10.1
Remote Discriminator: 4294967295         Remote Address: 10.10.10.3
Local Port : 49155                       Remote Port : 3784
vrf : default
Diagnostics : None
Timers in Milliseconds :
Min Tx: 20                               Min Rx: 20           Multiplier: 3
Neg Tx: 4                                Neg Rx: 20           Neg detect mult: 3
Sess up time : 00:00:00
Sess down time : 00:00:00
Bind Application : -
-----
Session Interface : vlan11                Session Name : -
Lower Layer : IPv4                       Version : 1
Session Type : Single Hop                 Session State : Down
Discriminator Type : Dynamic              DSCP : 0
Local Discriminator : 8192                Local Address : 11.11.11.1
Remote Discriminator: 0                   Remote Address: 11.11.11.2
Local Port : 49152                       Remote Port : 3784
vrf : yoush
Diagnostics : None
Timers in Milliseconds :
Min Tx: 20                               Min Rx: 20           Multiplier: 3
Neg Tx: 4                                Neg Rx: 20           Neg detect mult: 3
Sess up time : 00:00:00
Sess down time : 00:00:00
Bind Application : VRRP

```

## 相关命令

无

### 15.12.13 show bfd interface

使用该命令显示 BFD 在接口上的配置状态。

## 命令语法

**show bfd interface** (*IFNAME* | **all** |)

参数	描述
IFNAME	BFD 接口
all	显示所有接口

## 命令模式

特权模式

## 默认配置

无。

## 使用说明

使用该命令显示 BFD 在接口上的配置状态。

可显示指定接口，或显示全部接口。

## 举例说明

这个例子是该命令的显示结果：

```
Switch # show bfd interface eth-0-9
Interface:   eth-0-9  ifindex: 9 state:   UP
Interface level configuration: NO ECHO, NO SLOW TMR
Timers in Milliseconds
Min Tx: 1   Min Rx: 1   Multiplier: 3
-----
Number of Sessions: 2
BFD discriminator: 8193   BFD state: DOWN
BFD discriminator: 8191   BFD state: DOWN
```

## 相关命令

无

# 16 EVPN 相关命令行参考

## 16.1 Overlay 命令

### 16.1.1 vlan overlay enable

使用此命令使能或去使能 vlan 的 overlay 功能。

#### 命令语法

**vlan** *vlan\_id* **overlay** (enable |disable)

vlan	Vlan id, 范围 2~4094
enable	使能 vlan 的 overlay 功能
disable	去使能 vlan 的 overlay 功能，默认 vlan 的 overlay 功能是去使能的

#### 命令模式

vlan 配置模式

#### 默认

去使能

#### 使用说明

在配置 overlay 的 vlan 和 vni 的映射关系之前需要先使能 vlan 的 overlay 功能

#### 举例说明

下面的例子显示了使能 vlan 2 的 overlay 功能：

```
Switch(config-vlan)# vlan 2 overlay enable
```



## 相关命令

无

### 16.1.2 overlay

使用此命令进入 `overlay` 配置模式。使用关键词 `exit` 退出 `overlay` 配置模式。

## 命令语法

`overlay`

## 命令模式

全局配置模式

## 默认

无

## 使用说明

无

## 举例说明

下面的例子显示了如何进去 `overlay` 配置模式：

```
Switch(config)# overlay
Switch(config-overlay)#
```

## 相关命令

无

### 16.1.3 overlay 负载分担模式

使用此命令配置 `overlay` 的负载分担模式。

## 命令语法

`overlay ecmp-mode (normal |advanced)`

## 命令模式

`overlay` 配置模式

## 默认

普通模式

## 使用说明

普通的负载分担模式可以支持所有类型的上联口，但是仅能支持 1K 个远端 vtep。推荐在小型的传统数据中心中使用。而增强型的负载分担模式则无法支持 `vlan interface` 作为上联口，但是能支持超过 4K 的远端 vtep，推荐在大型的新型 spine-leaf 架构的数据中心中使用。

## 举例说明

下面的例子显示了如何配置 overlay 的负载分担模式：

```
Switch(config-overlay)# overlay ecmp-mode advanced
```

## 相关命令

无

### 16.1.4 overlay 映射

使用此命令配置 vlan 和 vni 的映射关系。

## 命令语法

**vlan** *vlan\_id* **vni** *vni*

**no vlan** *vlan\_id* **vni**

vlan_id	Range <2-4094>.
vni	Range <1-16777215>.

## 命令模式

overlay 配置模式

## 默认

无

## 使用说明

该命令用于绑定 vlan 和 overlay 的 vni 的关系，这就意味着一旦一个 vlan 和 vni 绑定了，vlan 下所有的端口也就属于 vni 的广播域了，并且可以在 vni 的广播域内进行单播，组播和广播了。

## 举例说明

- 下面的例子显示了设置 vlan 和 vni 的映射：

```
Switch(config-overlay)# vlan 20 vni 20000
```

- 下面的例子显示了如何删除 vlan 和 vni 的映射：

```
Switch(config-overlay)# no vlan 20 vni
```

## 相关命令

无

### 16.1.5 overlay 源 vtep

使用该命令为 overlay 设置源 vtep 的 ip 地址。

使用关键词 no 删除 overlay 的源 vtep 的 ip 地址。

## 命令语法

```
source A.B.C.D
```

```
no source
```

A.B.C.D	Overlay 的 vtep 的源地址，必须是是一个有效的 ip 地址
---------	-------------------------------------

## 命令模式

overlay 配置模式

## 默认

无

## 使用说明

Overlay vtep 的源地址用于对 overlay 的原始报文进行加封装和解封装。建议源地址采用某个 3 层口地址（比如环回口）并保证该地址的路由是可达的。

## 举例说明

- 下面的例子显示了如何配置 overlay 的源地址：

```
Switch(config-overlay)# source 1.1.1.1
```

- 下面的例子显示了如何删除 overlay 的源地址：

```
Switch(config-overlay)# no source
```

## 相关命令

无

### 16.1.6 overlay 动态隧道功能

## 命令语法

```
vtep reachability protocol bgp
```

```
no vtep reachability protocol bgp
```

## 命令模式

overlay 配置模式

## 使用说明

此命令用于开启或者关闭 overlay 的动态创建 VxLAN 隧道功能

## 举例说明

下面的例子创建了一个远端的 vxlan 的 vtep:

```
Switch(config-overlay)# vtep reachability protocol bgp
```

## 相关命令

无

## 16.1.7 overlay 上联口

使用该命令设置 overlay 的上联口。

## 命令语法

```
overlay uplink (enable | disable)
```

enable	使能 overlay 的上联口
disable	去使能 overlay 的上联口

## 命令模式

端口配置模式

## 默认

去使能

## 使用说明

此命令只能在以太类型的端口上使用，如果该端口是 3 层路由端口或者 3 层链路聚合的路由端口，则其能同时在普通和增强型的 overlay 的负载分担模式下工作，如果该端口属于 vlan interface，则只能在普通的 overlay 负载分担模式下工作。

## 举例说明

- 下面的例子使能端口上的 overlay 上联口功能：  
Switch(config)# interface eth-0-1  
Switch(config-if)# overlay uplink enable
- 下面的例子去使能端口上的 overlay 上联口功能：  
Switch(config-if)# overlay uplink disable

## 相关命令

无

### 16.1.8 show overlay

使用该命令显示 overlay 相关信息。

## 命令语法

show overlay (vlan <2-4094>)

<2-4094>	Vlan id
----------	---------

## 命令模式

EXEC 模式

## 默认

无

## 使用说明

无

## 举例说明

下面的例子显示了所有的 overlay 相关信息：

```
Switch# show overlay
-----
ECMP Mode      : Normal
Source VTEP    : 1.1.11.1

Vlan Vni      Type   IP-Address   Src-Address   Split-Horizon   State
-----
1000 11000    VxLAN  100.67.1.1   1.1.11.1      Enable          UP
1002 11002    VxLAN  100.67.1.1   1.1.11.1      Enable          UP
```

下面的例子显示了 `vlan 1002` 的 `overlay` 相关信息：

```
Switch# show overlay vlan 1002
-----
ECMP Mode      : Normal
Source VTEP    : 1.1.11.1
-----
VLAN ID        : 1002
VNI            : 11002
Remote VTEP NUM: 1
                Index: 1, Ip address: 100.67.1.1, Source ip: 1.1.11.1, Type: VxLAN
DVR Gateway NUM: 0
-----
```

下面的例子显示了 `overlay remote-vtep` 的相关信息：

```
Switch # show overlay remote-vtep
Index Type   Router-Mac   IP-Address      Source-IP        Split-Horizon   keep-
vtag dscp-strategy
-----
1      VxLAN      -            100.67.1.1     1.1.11.1        Enable
Disable Dscp-copy
```

## 相关命令

无

## 16.2 VXLAN 命令

### 16.2.1 vxlan

使用该命令配置 `vxlan` 数据结构中的 `vxlan` 特性。

使用 `no` 命令删除一个 `vxlan`。

## 命令语法

**vxlan** *vxlan-id*

**no vxlan** *vxlan-id*

vxlan-id	vxlan ID, 取值范围为 1~8192
----------	------------------------

## 命令模式

全局配置模式

## 默认

无

## 使用说明

配置该命令会进入 vxlan 配置模式。

## 举例说明

创建一个 vxlan 实例：

```
Switch(config)# vxlan 1000
```

## 16.2.2 vxlan vni

使用该命令配置 vxlan 和 vni 的映射关系。

使用 **no** 命令删除该映射关系。

## 命令语法

**vxlan vni** *vni-id*

**no vxlan vni**

vni-id	vni ID, 取值范围为 1~16777216
--------	--------------------------

## 命令模式

vxlan 配置模式

## 默认

无

## 使用说明

一个 vxlan 只能映射一个 vni。

## 举例说明

配置 vxlan 和 vni 的映射关系：

```
Switch(config-vxlan)# vxlan vni 10000
```

## 16.2.3 vtep reachability protocol bgp

此命令用于开启或者关闭 overlay 的动态创建 VxLAN 隧道功能。

## 命令语法

**vtep reachability protocol bgp**  
**no vtep reachability protocol bgp**

## 命令模式

overlay 配置模式

## 默认

关闭

## 使用说明

无

## 举例说明

开启 overlay 的动态创建 VxLAN 隧道功能：

```
Switch(config-overlay)# vtep reachability protocol bgp
```

## 16.2.4 remote-vtep virtual-mac

使用此命令配置 overlay 的 vtep 的虚拟 MAC 地址。

使用 **no** 命令删除配置。

## 命令语法

**remote-vtep virtual-mac mac-address**

**no remote-vtep virtual-mac**

mac-address	Overlay vtep 的虚拟 MAC 地址
-------------	-------------------------

## 命令模式

overlay 配置模式

## 默认

无

## 使用说明

此命令用于配置 overlay 的所有的 remote-vtep 的虚拟 MAC 地址，当 DVR 的路由没有指定 inner 的 mac 目的地址时，采用该 overlay 下配置的虚拟 MAC 地址作为 inner 的 mac 目的地址。



EVPN 路由中如果配置了 overlay 的 vtep 的虚拟 MAC 地址，EVPN 的路由中会携带该 MAC。

## 举例说明

配置 vtep 的虚拟 MAC 地址：

```
Switch(config-overlay)# remote-vtep virtual-mac a.a.a
```

## 16.2.5 vxlan remote-vtep

使用此命令配置 overlay vxlan 的远端 vtep。

使用关键词 **no** 删除 overlay vxlan 的远端 vtep。

## 命令语法

```
vxlan vxlan-id remote-vtep index [ tunnel-aware inner ]
```

```
no vxlan vxlan-id remote-vtep index
```

vxlan-id	取值范围 1~8192
index	Overlay 远端 vtep 的索引，取值范围是 1~65535
inner	使用内层头部信息作为 ACL、Flow tracing 等

## 命令模式

overlay 配置模式

## 默认

无

## 使用说明

此命令用于指定 overlay vxlan 的远端 vtep，必须保证该索引对应的远端 vtep 已经被创建。

## 举例说明

配置 overlay vxlan 的远端 vtep 3：

```
Switch(config-vxlan)# vxlan 20 vni 20000
Switch(config-overlay)# vxlan 20 remote-vtep 3
```

## 16.2.6 mac-address-table forward remote-vtep vxlan

使用该命令设置 overlay 的静态 fdb。

使用 **no** 命令删除配置的静态 fdb。

## 命令语法

**mac-address-table** *mac-addr* **forward remote-vtep** *index vxlan vxlan-id*

**no mac-address-table** *mac-addr* **forward remote-vtep** *index vxlan vxlan-id*

mac-addr	目的单播 MAC 地址,特定 VXLAN 中带有目的 MAC 地址的报文将通过特定的接口转发出去
index	Overlay 远端 vtep 的索引, 取值范围为 1~65535
vxlan-id	特定的 VXLAN。带有特定 MAC 地址的报文所属的 VXLAN, 取值范围为 1~8192

## 命令模式

全局配置模式

## 默认

无

## 使用说明

无

## 举例说明

配置一条 overlay 的静态 fdb:

```
Switch(config)# mac-address-table 1.1.1 forward remote-vtep 2 vxlan 2
```

删除一条 overlay 的静态 fdb:

```
Switch(config-if)# no mac-address-table 1.1.1 forward remote-vtep 2 vxlan 2
```

## 16.2.7 encapsulation mode

使用此命令配置本地接口的 vxlan 匹配的封装模式。

使用 **no** 命令删除此配置。

## 命令语法

**encapsulation mode** { **default** | **untagged** | **tagged** *vid* }

**no encapsulation mode** { **default** | **untagged** | **tagged** *vid* }

default	允许接口接收所有报文, 不区分报文中是否带 VLAN Tag
untagged	该类型接口只接收不带 VLAN Tag 的报文
tagged	该类型接口只接收带有指定 VLAN Tag 的报文

vid	指定 VLAN Tag ID
-----	----------------

## 命令模式

接口配置模式

## 默认

无

## 使用说明

此命令用于配置与本地接口的 vxlan 报文匹配的封装模式，该命令必须在二层物理口下配置。

## 举例说明

配置端口的 vxlan 匹配模式：

```
Switch(config-if)# encapsulation mode tagged
```

## 16.2.8 encapsulation vxlan

使用此命令配置本地接口的 vxlan 匹配规则。

使用 **no** 命令删除此配置。

## 命令语法

```
encapsulation { default | untagged | tagged vid } vxlan vxlan-id
```

```
no encapsulation { default | untagged | tagged vid } vxlan vxlan-id
```

default	允许接口接收所有报文，不区分报文中是否带 VLAN Tag
untagged	该类型接口只接收不带 VLAN Tag 的报文
tagged	该类型接口只接收带有指定 VLAN Tag 的报文
vid	指定 VLAN Tag ID
vxlan-id	vxlan ID，取值范围为 1~8192

## 命令模式

接口配置模式

## 默认

无

## 使用说明

此命令用于配置本地接口的 vxlan 匹配规则，该命令必须在二层物理口下配置。

## 举例说明

配置端口的 vxlan 匹配规则：

```
Switch(config-if)# encapsulation tagged 20 vxlan 2000
```

## 16.2.9 show overlay

使用该命令显示 overlay 相关信息。

## 命令语法

```
show overlay [ vxlan vxlan-id ]
```

vxlan-id	vxlan ID，取值范围为 1~8192
----------	-----------------------

## 命令模式

全局配置模式

## 默认

无

## 使用说明

无

## 举例说明

显示所有的 overlay 相关信息：

```
Switch(config)# show overlay
-----
ECMP Mode      : Normal
Source VTEP    : 1.1.1.1
Remote VTEP Index: 1, Ip address: 2.2.2.2, Type: VxLAN
Remote VTEP Index: 2, Ip address: 3.3.3.3, Type: VxLAN
-----
VXLAN ID      : 2
VNI           : 20000
Remote VTEP NUM: 2
      Index: 1, Ip address: 2.2.2.2, Type: VxLAN
      Index: 2, Ip address: 3.3.3.3, Type: VxLAN
DVR Gateway NUM: 0
-----
VXLAN ID      : 3
VNI           : 3000
```

```
Remote VTEP NUM: 1
  Index: 2, Ip address: 3.3.3.3, Type: VxLAN
DVR Gateway NUM: 0
-----
```

显示 vxlan 2 的 overlay 相关信息:

```
Switch(config)# show overlay vxlan 2
-----
```

```
ECMP Mode      : Normal
Source VTEP    : 1.1.1.1
Remote VTEP Index: 1, Ip address: 2.2.2.2, Type: VxLAN
Remote VTEP Index: 2, Ip address: 3.3.3.3, Type: VxLAN
-----
```

```
VXLAN ID      : 2
VNI           : 20000
Remote VTEP NUM: 2
  Index: 1, Ip address: 2.2.2.2, Type: VxLAN
  Index: 2, Ip address: 3.3.3.3, Type: VxLAN
DVR Gateway NUM: 0
-----
```

## 16.2.10 interface vxlan

使用该命令创建一个三层 vxlan 接口。

使用 **no** 命令删除 vxlan 接口。

### 命令语法

```
interface vxlan vxlan-id
```

```
no interface vxlan vxlan-id
```

vxlan-id	vxlan id, 取值范围为 1~8192
----------	------------------------

### 命令模式

全局配置模式

### 默认

无

### 使用说明

使用该命令前确保 vxlan 实例已创建。

### 举例说明

```
创建一个 vxlan 接口:
Switch(config)# interface vxlan 1000
```

## 16.3 EVPN 命令

### 16.3.1 address-family l2vpn evpn

使用此命令使能并进入 EVPN 地址族配置模式。

使用相应的 `no` 命令关闭 EVPN 地址族配置。

#### 命令语法

```
address-family l2vpn evpn
```

```
no address-family l2vpn evpn
```

#### 命令模式

路由配置模式

#### 默认

未使能 EVPN 地址族配置

#### 使用说明

使用 `address-family l2vpn evpn` 命令，来进入 EVPN 地址族配置模式。

退出该模式使用相应的 `exit`，或者 `exit-address-family` 命令。

进入 EVPN 地址族配置模式之前，需要在全局配置模式下，使能 EVPN 功能

#### 举例说明

下面的例子显示了如何进入 EVPN 地址族配置模式：

```
Switch(config-router)# address-family l2vpn evpn
Switch(config-router-af)#
```

#### 相关命令

`exit-address-family`

### 16.3.2 neighbor activate

使用这个命令来使能和启用一个邻居路由器的指定 AF 路由信息交换功能。

使用相应的 `no` 命令来删除这个配置。

#### 命令语法

```
(no) neighbor NEIGHBORID activate
```

NEIGHBORID	A.B.C.D TAG
A.B.C.D	以 IP 地址格式来指定 BGP 邻居的地址。
TAG	已经存在的对等组名。请参考 <code>neighbor peer-group</code> ， <code>neighbor remote-as</code> 命令来创建对等组。当这个参数被命令使用的时候，这个命令会被应用到指定组的所有对等体上。

## 命令模式

地址族模式和路由模式

## 默认

N/A

## 使用说明

在 TCP 连接被邻居打开以后，这个命令被用于使能或者取消和邻居路由器之间指定 AF 信息交换。

使能组播和 VPNv4 地址前缀类型的交换，邻居要在地址族模式下使用 `neighbor activate` 命令来激活。

## 举例说明

```
Switch# configure terminal
Switch(config)# router bgp 10
switch(config-router)# address-family l2vpn evpn
Switch(config-router-af)# neighbor 1.2.3.4 activate
```

## 相关命令

`neighbor remote-as`

### 16.3.3 neighbor send-community

使用此命令配置向 BGP 邻居发送团体属性。

使用相应的 `no` 命令取消该配置。

## 命令语法

**neighbor** (A.B.C.D|WORD) (both|extended|standard)

**no neighbor** (A.B.C.D|WORD) (|extended|standard)

A.B.C.D	指定邻居地址
---------	--------

WORD	指定对等体组
both	发送标准和扩展团体属性
extended	发送扩展团体属性
standard	发送标准团体属性

## 命令模式

EVPN 地址族模式

## 默认

无

## 使用说明

无

## 举例说明

下面的例子显示了如何设置发送团体属性：

```
Switch (config-router-af)# neighbor 1.1.1.1 send-community extended
```

## 相关命令

**address-family l2vpn evpn**

### 16.3.4 evpn

使用此命令使能 EVPN 功能并进入 EVPN 配置模式。

使用相应的 **no** 命令取消 EVPN 配置。

## 命令语法

evpn

no evpn

## 命令模式

全局配置模式

## 默认

未使能 EVPN 功能



## 使用说明

使用该命令可以使能 EVPN 功能。在进入 EVPN 配置模式后，可以创建 EVPN 实例。当 EVPN 功能关闭后，所有的 EVPN 实例将被删除。

## 举例说明

下面的例子显示了如何使能 EVPN 功能：

```
Switch(config)# evpn
Switch(config-evpn)#
```

## 相关命令

```
address-family l2vpn evpn
```

### 16.3.5 vni

使用此命令创建 EVPN 实例。

使用相应的 `no` 命令删除该实例。

## 命令语法

```
vni VAL
no vni VAL
```

<i>VAL</i>	指定 vni，有效范围为[1,16777215]
------------	--------------------------

## 命令模式

EVPN 配置模式

## 默认

无

## 使用说明

EVPN 实例的 RD 和 route-target 都需要配置，路由才会发布和学习。

## 举例说明

下面的例子显示了如何创建 EVPN 实例：

```
Switch(config-evpn)# vni 2001
Switch(config-evi)#
```

## 相关命令

Evpn

### 16.3.6 rd

使用此命令配置 EVPN 实例的 RD。

使用的 no 命令取消该配置。

## 命令语法

rd (auto| *RD-VALUE*)

no rd

auto	自动生成 RD, 格式为 “N:VXLAN ID”
RD-VALUE	指定 EVPN 实例的 RD, 格式为 “ASN:nn or IP:nn”

## 命令模式

EVPN 实例配置模式

## 默认

无

## 使用说明

无

## 举例说明

下面的例子显示了如何设置 EVPN 实例的 RD:

```
Switch (config-evi)# rd auto
```

## 相关命令

vni

### 16.3.7 route-target

使用此命令配置当前 EVPN 实例的 route-target。

使用的 no 命令取消该配置。

## 命令语法

**route-target (import|export|both) (auto | RT-VALUE)**

**no route-target (import|export|both) (auto| RT-VALUE)**

import	指定入方向 route-target
export	指定出方向 route-target
both	同时指定出方向和入方向
auto	指定自动生成 route-target
RT-VALUE	配置 route-target, 格式为 “ASN:nn or IP:nn”

## 命令模式

EVPN 实例配置模式

## 默认

无

## 使用说明

建立 EBGp 连接时, 需要手动配置 route-target, 否则可能会导致 EVPN 路由无法发布到本地实例。

## 举例说明

下面的例子显示了如何设置 EVPN 实例入方向 route-target:

```
Switch (config-evi)# route-target import auto
```

## 相关命令

vni

### 16.3.8 export map

使用此命令配置当前 EVPN 实例与出方向 route-map 关联。

使用相应的 no 命令取消该关联。

## 命令语法

**export map WORD**

**no export map**

WORD	指定 route-map 名称
------	-----------------

## 命令模式

EVPN 实例配置模式

## 默认

无

## 使用说明

无

## 举例说明

下面的例子显示了如何设置 EVPN 实例与出方向 route-map 关联:

```
Switch(config-evi)# export map rmap1
```

## 相关命令

vni

### 16.3.9 import map

使用此命令配置当前 EVPN 实例与入方向 route-map 关联。使用相应的 no 取消该关联。

## 命令语法

```
import map WORD
```

```
no import map
```

WORD	指定 route-map 名称
------	-----------------

## 命令模式

EVPN 实例配置模式

## 默认

无

## 使用说明

无

## 举例说明

下面的例子显示了如何设置 EVPN 实例与入方向 route-map 关联:

```
Switch(config-evi)# import map rmap1
```

## 相关命令

vni

### 16.3.10 overlay host-collect

使用此命令使能 EVPN 搜集主机信息。

使用相应的 no 命令关闭该功能。

## 命令语法

**overlay host-collect (enable|disable)**

## 命令模式

接口配置模式

## 默认

未使能

## 使用说明

在使能 EVPN 搜集主机信息后，还需要配置 EVPN 实例的 RD 和 Route-target，然后从 ARP 中获得的主机信息，才会通过 BGP 形成 EVPN 的 MAC/IP Advertisement 路由并发布出去。

## 举例说明

下面的例子显示了如何使能 EVPN 搜集主机信息:

```
Switch(config-if)# overlay host-collect enable
```

## 相关命令

evpn

### 16.3.11 suppress-arp

使用此命令使能抑制 ARP 功能。

使用相应的 `no` 命令删除抑制 ARP 功能。

## 命令语法

**suppress-arp**

**no suppress-arp**

## 命令模式

evi 配置模式

## 默认

无

## 使用说明

无

## 举例说明

下面的例子显示了如何使能 ARP 抑制功能：

```
Switch(config-evpn)# vni 20000
Switch(config-evi)# suppress-arp
```

## 相关命令

Evpn

### 16.3.12 show bgp evpn

使用此命令显示 EVPN 路由信息。

## 命令语法

**show bgp evpn (all|rd *VAL*|vni *VAL*) (route-type (mac-ip|))**

all	显示所有 EVPN 路由
rd <i>VAL</i>	指定 RD
vni <i>VAL</i>	指定 vni
route-type	指定 EVPN 路由类型
mac-ip	指定 MAC/IP Advertisement 路由

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面的例子显示了如何显示 EVPN 路由信息：

```
Switch# show bgp evpn all
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop          Metric LocPrf Weight Path
Route Distinguisher: 1:2001 (VNI 2001)
*> [2]:[0]:[48]:[8264.c465.9400]:[32]:[12.12.12.2]/136
      1.1.1.1                      32768 i
*> [2]:[0]:[48]:[8264.c465.9400]:[32]:[12.12.12.3]/136
      1.1.1.1                      32768 i
```

## 相关命令

evpn

### 16.3.13 show bgp evpn neighbors

使用此命令显示 EVPN BGP 邻居信息。

## 命令语法

**show bgp evpn neighbors** (*A.B.C.D*|summary)

A.B.C.D	指定邻居地址
summary	显示邻居摘要信息

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面的例子显示了如何显示邻居摘要信息：

```
Switch# show bgp evpn neighbors summary
BGP router identifier 12.12.12.1, local AS number 1
BGP table version is 10
1 BGP AS-PATH entries
0 BGP community entries
Neighbor          V          AS MsgRcvd MsgSent  TblVer  InQ  OutQ  Up/Down
State/PfxRcd
1.1.1.2           4           1    946    954     10    0    0 13:35:36
Total number of neighbors 1
```

## 相关命令

evpn

### 16.3.14 show overlay host-information

使用此命令显示通过 EVPN 学习到的主机信息。

## 命令语法

**show overlay host-information (vni *VAL* |summary)**

vni <i>VAL</i>	指定 vni
summary	显示摘要信息

## 命令模式

特权模式

## 默认

无

## 使用说明

无



## 举例说明

下面的例子显示了如何显示 EVPN 同步的主机信息：

```
Switch# show overlay host-information vni 2001
Mac          IP address      VTEP address    Tunnel Route
-----
8264.c465.9400 12.12.12.3      1.1.1.1         N      N
```

## 相关命令

evpn

### 16.3.15 show overlay suppress-arp

使用此命令显示通过 EVPN 学习到的 ARP 抑制表。

## 命令语法

**show overlay suppress-arp (vni <1-16777215> |summary)**

vni <1-16777215>	指定 vni
summary	显示摘要信息

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

下面的例子显示了如何显示 ARP 抑制表的信息：

```
Switch# show overlay suppress-arp vni 50000
Mac          IP address      vni
-----
ec84.b4ed.4f03 20.20.20.3      50000
```

## 相关命令

evpn

### 16.3.16 debug overlay evpn

使用此命令使能 Overlay 模块中 EVPN 调试功能。

使用相应的 no 命令关闭该调试。

#### 命令语法

```
debug overlay evpn  
no debug overlay evpn
```

#### 命令模式

特权模式

#### 默认

未使能

#### 使用说明

无

#### 举例说明

下面的例子显示了如何使能 Overlay 模块 EVPN 调试功能：

```
Switch# debug overlay evpn
```

#### 相关命令

overlay host-collect

# 17 堆叠配置命令

## 17.1 SCF 命令

### 17.1.1 scf domain

使用该命令配置 SCF 堆叠域 ID，并进入域名模式。

使用 **no** 命令删除配置的堆叠域 ID。

#### 命令语法

**scf domain** *domain-id*

**no scf domain**

domain-id	堆叠域 ID，取值范围为 1~255，默认值为 1
-----------	---------------------------

#### 命令模式

全局配置模式

#### 默认

1

#### 使用说明

在一个网络中可以配置多个 SCF，使用堆叠域 ID 区别不同的 SCF。所有 SCF 成员的域 ID 必须一致。配置重启后生效。

#### 举例说明

配置堆叠域 ID 为 100，并进入域名模式：

```
Switch#config terminal
```

```
Switch(config)# scf domain 100
```

```
Switch(config-scf-domain)#
```

## 17.1.2 scf member

使用该命令配置 SCF 堆叠成员编号。

使用 **no** 命令删除配置的堆叠成员编号。

### 命令语法

**scf member** *member-id*

**no scf member**

member-id	堆叠成员编号，取值范围为 1~9，默认值为 1
-----------	-------------------------

### 命令模式

域名模式

### 默认

1

### 使用说明

每个成员设备的 ID 必须不同，配置重启后生效。

### 举例说明

配置 SCF 堆叠成员编号为 5：

```
Switch#config terminal
```

```
Switch(config)# scf domain 100
```

```
Switch(config-scf-domain)# scf member 5
```

## 17.1.3 scf priority

使用该命令配置 SCF 堆叠成员的优先级。

使用 **no** 命令删除配置的堆叠成员优先级。

### 命令语法

**scf priority** *PRIORITY*

**no scf priority**

PRIORITY	堆叠成员优先级，取值范围为 1~255，默认值为 100
----------	------------------------------

### 命令模式

域名模式

## 默认

100

## 使用说明

该命令 **scf priority** 用于配置成员设备的优先级。优先级的值越小，被选举成为主设备的概率越大。配置重启后生效。

## 举例说明

配置堆叠成员的优先级为 20:

```
Switch#config terminal
Switch(config)# scf domain 100
Switch(config-scf-domain)# scf member 1
Switch(config-scf-domain)# scf priority 20
```

## 17.1.4 interface scf

使用该命令创建 SCF 堆叠口，并进入堆叠口配置模式。

使用 **no** 命令删除配置的 SCF 堆叠口。

## 命令语法

```
interface scf port-number
no interface scf port-number
```

port-number	堆叠端口号，取值范围为 1~2
-------------	-----------------

## 命令模式

全局配置模式

## 默认

无

## 使用说明

只能选择一条或者两条 VSL 链路，且链路带宽、类型要一致，VSL 编号本地有效。在堆叠口配置模式下，可以绑定对应的物理口成员。

## 举例说明

创建 SCF 堆叠口，并进入堆叠口配置模式:

```
Switch(config)# interface scf 1
```

Switch(config-scf-if)#

## 17.1.5 port-member interface

使用该命令可以在堆叠口模式下绑定对应的物理口成员。

使用 **no** 命令删除配置的物理口成员。

### 命令语法

**port-member interface** *eth-number*

**no port-member interface** *eth-number*

eth-number	物理端口号，取值范围为 1~8
------------	-----------------

### 命令模式

堆叠口配置模式

### 默认

无

### 使用说明

无

### 举例说明

在堆叠口模式下，绑定对应的物理口成员：

```
Switch(config)# interface scf 1
```

```
Switch(config-scf-if)# port-member interface eth-1-0-1
```

```
Switch(config-scf-if)# port-member interface eth-1-0-2
```

```
Switch(config-scf-if)# end
```

## 17.1.6 switch convert mode scf

使用该命令可以将工作模式切换到 SCF 模式。

使用 **no** 命令清除堆叠工作模式，切换到独立工作模式。

### 命令语法

**switch convert mode scf**

**no switch convert mode scf**

## 命令模式

特权模式

## 默认

无

## 使用说明

配置在重启后生效。

## 举例说明

切换工作模式到 SCF 模式：

```
Switch# switch convert mode scf
```

## 17.1.7 scf sync image to

使用该命令可以对所有或指定成员设备进行升级。

## 命令语法

```
scf sync image to { all | member-id }
```

member-id	指定的成员设备编号，取值范围为 1~9
-----------	---------------------

## 命令模式

特权模式

## 默认

无

## 使用说明

以主控设备版本为最新版本，针对某一成员或全部成员进行版本升级同步。

## 举例说明

升级所有成员设备：

```
Switch# scf sync image to all
```

```
start sending image data...
```

```
The image was successfully sent to member 3
```

## 17.1.8 show scf upgrade progress

使用该命令可以查看版本同步升级进度。

### 命令语法

**show scf upgdate progress**

### 命令模式

特权模式

### 默认

无

### 使用说明

各字段信息如下：

Member_id	SCF 中的成员编号，同一个 SCF 中的多个成员编号需要不一致
SCF_Upgrade_State	版本升级状态，ready 表示开始传输版本，wait reboot 表示传输完成等待重启

### 举例说明

查看版本同步升级进度：

```
Switch# show scf upgrade progress
```

```
-----
Member_id      SCF_Upgrade_State
1              -
3              ready
```

## 17.1.9 reboot

使用该命令可以重启所有的堆叠设备或者重启某个成员设备。

### 命令语法

**reboot { all | member-id }**

member-id	指定的成员设备编号，取值范围为 1~9
-----------	---------------------



## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

重启所有的堆叠设备：

```
Switch#reboot all
```

```
Building configuration...
```

```
The SCF System configuration has been modified. Save? [yes/no]: y
```

```
Reboot system? [yes/no]y
```

## 17.1.10 scf redundancy switch

使用该命令可以将堆叠系统中 standby 成员转化为 active，原本的 active 成员设备会重启。

## 命令语法

```
scf redundancy switch
```

## 命令模式

特权模式

## 默认

无

## 使用说明

无

## 举例说明

配置堆叠主备倒换：

```
Switch# scf redundancy switch
```

## 17.1.11 show scf

使用该命令可以显示 SCF 中所有堆叠成员的相关信息。

### 命令语法

**show scf**

### 命令模式

特权模式

### 默认

无

### 使用说明

堆叠成员相关信息包括成员 ID、域 ID，优先级、状态、角色等信息，在选举完成后才能正常显示。选举未完成时，提示% The election is not completed, please try again later。

各字段信息如下：

Member	成员编号，同一个 SCF 中的多个成员编号需要不一致
Domain	堆叠域编号，同一个 SCF 中多个成员的域 ID 保持一致
Priority	堆叠成员的优先级
MAC	堆叠成员的 MAC 地址
Member-status	堆叠成员站点运行状态：INIT, COLLECTING, ACTIVE, STANDBY, MEMBER 和 CONFLICT INIT：设备的缺省值状态 COLLECTING：拓扑收集状态 ACTIVE：被选举成为 ACTIVE STANDBY：被选举成为 STANDBY MEMBER：被选举成为 MEMBER CONFLICT：设备与堆叠系统存在冲突
Version	堆叠成员的版本

## 举例说明

显示 SCF 中所有堆叠成员的相关信息：

```
Switch# show scf
```

```
Member Domain Priority MAC Status Version
-----
8 10 100 0009.0625.af49 STANDBY 11.001.001.T4
9 10 100 0009.0425.9f49 ACTIVE 11.001.001.T4
```

### 17.1.12 show scf topology

使用该命令可以查看堆叠拓扑信息，包括堆叠口连接情况，以及各堆叠成员简要信息。

## 命令语法

```
show scf topology
```

## 命令模式

特权模式

## 默认

无

## 使用说明

各字段信息如下：

Introduction	解释说明，[num]代表 member id，(num)代表堆叠口编号
Topology	显示堆叠成员连接方式 第一个设备拓扑与最后一个设备拓扑一致时表示环形拓扑 拓扑不稳定时提示 The link is unstable, please try again later
Member	成员设备编号
Status	成员设备状态，取值可能为：ACTIVE、STANDBY、MEMBER
MAC	成员设备的 MAC 地址

## 举例说明

查看堆叠拓扑信息：

```
Switch# show scf topology
```

Introduction:

'[num]' means member num, '(num)' means scf aggregate port num.

Topology:

```
[1](2)-----(1)[3]
```

Member	Status	MAC
-----		
1	STANDBY	0009.0625.8f48
3	ACTIVE	0009.0625.8f01

### 17.1.13 show running-config scf

使用该命令可以显示本设备堆叠相关配置。

#### 命令语法

```
show running-config scf
```

#### 命令模式

特权模式

#### 默认

无

#### 使用说明

无

#### 举例说明

查看本设备堆叠相关配置:

```
Switch# show running-config scf
```

```
Building configuration...
```

```
!
```

```
scf domain 10
```

```
scf member 1
```

```
scf priority 120
```

```
!
```

```
switch convert mode scf
!
interface scf2
  port-member interface eth-1-0-24
!
```

### 17.1.14 show scf config

使用该命令可以显示堆叠系统各成员设备的堆叠相关配置。

#### 命令语法

```
show scf config
```

#### 命令模式

特权模式

#### 默认

无

#### 使用说明

无

#### 举例说明

查看显示堆叠系统各成员设备的堆叠相关配置：

```
Switch ## show scf config
Building configuration...
```

```
=====
Member: 7
!
scf domain 10
scf member 7
scf priority 100
!
switch convert mode scf
!
interface scf1
  port-member interface eth-7-0-23
```

```
port-member interface eth-7-0-24
!  
interface scf2  
!
```

---

### 17.1.15 scf clear config

使用该命令可以删除非堆叠配置文件或所有配置文件。

#### 命令语法

```
scf clear config [ all ]
```

#### 命令模式

特权模式

#### 默认

无

#### 使用说明

当命令不包含 all 参数时，仅删除非堆叠配置文件（scf-member-conf 目录文件）。当命令包含 all 参数时，删除所有配置文件（scf-member-conf 目录文件 + startup-config.conf + scf-config.conf），仅限 active 角色操作。

#### 举例说明

删除所有配置文件：

```
Switch# scf clear config all
```

```
Are you sure to delete all configuration file ? [yes/no]: y
```