



全千兆二层网管交换机

TL-SG3210/TL-SG3216/TL-SG3424/TL-SG3424P

命令行手册

声明

Copyright © 2015 普联技术有限公司

版权所有，保留所有权利

未经普联技术有限公司明确书面许可，任何单位或个人不得擅自仿制、复制、誊抄或转译本手册部分或全部内容，且不得以营利为目的进行任何方式（电子、影印、录制等）的传播。

TP-LINK®为普联技术有限公司注册商标。本手册提及的所有商标，由各自所有人拥有。本手册所提到的产品规格和资讯仅供参考，如有内容更新，恕不另行通知。除非有特殊约定，本手册仅作为使用指导，所作陈述均不构成任何形式的担保。

目 录

手册概述	1
第 1 章 命令行使用指导	4
1.1 使用命令行	4
1.2 命令行模式	16
1.3 命令行安全等级	18
1.4 命令行格式约定	18
第 2 章 用户界面	20
2.1 enable	20
2.2 service password-encryption	20
2.3 enable password	20
2.4 enable secret	21
2.5 disable	22
2.6 configure	22
2.7 exit	23
2.8 end	23
2.9 show history	23
2.10 clear history	24
第 3 章 IEEE 802.1Q VLAN 配置命令	25
3.1 vlan	25
3.2 interface vlan	25
3.3 name	26
3.4 switchport mode	26
3.5 switchport access vlan	27
3.6 switchport trunk allowed vlan	27
3.7 switchport general allowed vlan	28
3.8 switchport pvid	28
3.9 show vlan summary	29
3.10 show vlan brief	29
3.11 show vlan	29
3.12 show interface switchport	30
第 4 章 MAC VLAN 配置命令	31
4.1 mac-vlan mac-address	31
4.2 show mac-vlan	31
第 5 章 协议 VLAN 配置命令	33
5.1 protocol-vlan template	33
5.2 protocol-vlan vlan	33
5.3 protocol-vlan group	34
5.4 show protocol-vlan template	34
5.5 show protocol-vlan vlan	35
第 6 章 语音 VLAN 配置命令	36
6.1 voice vlan	36

6.2	voice vlan aging time	36
6.3	voice vlan priority	37
6.4	voice vlan mac-address	37
6.5	switchport voice vlan mode	37
6.6	switchport voice vlan security	38
6.7	show voice vlan	38
6.8	show voice vlan oui	39
6.9	show voice vlan switchport	39
第 7 章	GVRP 配置命令	40
7.1	gvrp(global)	40
7.2	gvrp (interface)	40
7.3	gvrp registration	41
7.4	gvrp timer	41
7.5	show gvrp global	42
7.6	show gvrp interface	42
第 8 章	EtherChannel 配置命令	43
8.1	channel-group	43
8.2	port-channel load-balance	43
8.3	lacp system-priority	44
8.4	lacp port-priority	44
8.5	show etherchannel	45
8.6	show etherchannel load-balance	45
8.7	show lacp	45
8.8	show lacp sys-id	46
第 9 章	用户管理配置命令	47
9.1	user name (password)	47
9.2	user name (secret)	48
9.3	user access-control ip-based	49
9.4	user access-control mac-based	49
9.5	user access-control port-based	50
9.6	line	50
9.7	password	51
9.8	login	52
9.9	login local	52
9.10	telnet	53
9.11	show telnet-status	53
9.12	show user account-list	53
9.13	show user configuration	54
第 10 章	HTTP 和 HTTPS 配置命令	55
10.1	ip http server	55
10.2	ip http max-users	55
10.3	ip http session timeout	56
10.4	ip http secure-server	56
10.5	ip http secure-protocol	57
10.6	ip http secure-ciphersuite	57
10.7	ip http secure-max-users	57
10.8	ip http secure-session timeout	58
10.9	ip http secure-server download certificate	58

10.10	ip http secure-server download key	59
10.11	show ip http configuration	60
10.12	show ip http secure-server.....	60
第 11 章	绑定列表配置命令	61
11.1	ip source binding.....	61
11.2	ip source binding index	62
11.3	ip dhcp snooping.....	62
11.4	ip dhcp snooping global	63
11.5	ip dhcp snooping information option	63
11.6	ip dhcp snooping information strategy	64
11.7	ip dhcp snooping information remote-id.....	64
11.8	ip dhcp snooping information circuit-id.....	65
11.9	ip dhcp snooping trust.....	65
11.10	ip dhcp snooping mac-verify	65
11.11	ip dhcp snooping limit rate	66
11.12	ip dhcp snooping decline	66
11.13	show ip source binding	67
11.14	show ip dhcp snooping	67
11.15	show ip dhcp snooping information.....	67
11.16	show ip dhcp snooping interface.....	68
第 12 章	ARP 防护配置命令	69
12.1	ip arp inspection(global).....	69
12.2	ip arp inspection trust.....	69
12.3	ip arp inspection (interface)	69
12.4	ip arp inspection limit-rate	70
12.5	ip arp inspection recover	70
12.6	show ip arp inspection	71
12.7	show ip arp inspection interface.....	71
12.8	show ip arp inspection statistics.....	71
12.9	clear ip arp inspection statistics	72
第 13 章	DoS 防护命令	73
13.1	ip dos-prevent.....	73
13.2	ip dos-prevent type	73
13.3	show ip dos-prevent.....	74
第 14 章	IEEE 802.1X 配置命令	75
14.1	dot1x system-auth-control	75
14.2	dot1x auth-method.....	75
14.3	dot1x guest-vlan(global)	76
14.4	dot1x quiet-period	76
14.5	dot1x timeout	76
14.6	dot1x max-reauth-req	77
14.7	dot1x.....	77
14.8	dot1x guest-vlan(interface)	78
14.9	dot1x port-control.....	78
14.10	dot1x port-method.....	79
14.11	radius.....	79
14.12	radius server-account	80
14.13	show dot1x global	81

14.14	show dot1x interface	81
14.15	show radius accounting	81
14.16	show radius authentication	82
第 15 章	系统日志配置命令	83
15.1	logging buffer	83
15.2	logging file flash	83
15.3	logging file flash frequency	84
15.4	logging file flash level	84
15.5	clear logging	85
15.6	logging host index	85
15.7	show logging local-config	86
15.8	show logging loghost	86
15.9	show logging buffer	86
15.10	show logging flash	87
第 16 章	SSH 配置命令	88
16.1	ip ssh server	88
16.2	ip ssh version	88
16.3	ip ssh algorithm	88
16.4	ip ssh timeout	89
16.5	ip ssh max-client	89
16.6	ip ssh download	90
16.7	show ip ssh	90
第 17 章	地址配置命令	92
17.1	mac address-table static	92
17.2	mac address-table aging-time	92
17.3	mac address-table filtering	93
17.4	mac address-table max-mac-count	93
17.5	show mac address-table	94
17.6	show mac address-table aging-time	94
17.7	show mac address-table max-mac-count interface gigabitEthernet	95
17.8	show mac address-table interface gigabitEthernet	95
17.9	show mac address-table count	96
17.10	show mac address-table address	96
17.11	show mac address-table vlan	96
17.12	clear mac address-table	97
第 18 章	系统配置命令	98
18.1	system-time manual	98
18.2	system-time ntp	98
18.3	system-time dst predefined	99
18.4	system-time dst date	99
18.5	system-time dst recurring	100
18.6	hostname	101
18.7	location	101
18.8	contact-info	101
18.9	ip management-vlan	102
18.10	ip address	102
18.11	ip address-alloc dhcp	103
18.12	ip address-alloc bootp	103

18.13	reset.....	104
18.14	reboot	104
18.15	copy running-config startup-config.....	104
18.16	copy startup-config tftp.....	105
18.17	copy tftp startup-config.....	105
18.18	firmware upgrade.....	106
18.19	ping.....	106
18.20	tracert	107
18.21	show system-time	108
18.22	show system-time dst	108
18.23	show system-time ntp	108
18.24	show system-info.....	109
18.25	show running-config.....	109
18.26	show cable-diagnostics interface.....	109
第 19 章 IPv6 地址配置命令		111
19.1	ipv6 enable	111
19.2	ipv6 address autoconfig.....	111
19.3	ipv6 address link-local	112
19.4	ipv6 address dhcp.....	112
19.5	ipv6 address ra	113
19.6	ipv6 address eui-64	113
19.7	ipv6 address	114
19.8	show ipv6 interface vlan	114
第 20 章 以太网配置命令.....		115
20.1	interface gigabitEthernet.....	115
20.2	interface range gigabitEthernet.....	115
20.3	description	116
20.4	shutdown	116
20.5	flow-control	117
20.6	media-type.....	117
20.7	duplex	117
20.8	speed.....	118
20.9	storm-control broadcast.....	118
20.10	storm-control multicast.....	119
20.11	storm-control unicast	119
20.12	bandwidth	120
20.13	clear counters	120
20.14	show interface status	121
20.15	show interface counters.....	121
20.16	show interface description	122
20.17	show interface flowcontrol	122
20.18	show interface configuration	123
20.19	show storm-control	123
20.20	show bandwidth	123
第 21 章 QoS 配置命令		125
21.1	qos.....	125
21.2	qos dscp	125
21.3	qos queue cos-map	126
21.4	qos queue dscp-map	127

21.5	qos queue mode	127
21.6	show qos interface	128
21.7	show qos cos-map	128
21.8	show qos dscp-map	129
21.9	show qos queue mode	129
21.10	show qos status	129
第 22 章	端口监控配置命令	131
22.1	monitor session destination interface	131
22.2	monitor session source interface	131
22.3	show monitor session	132
第 23 章	端口隔离配置命令	133
23.1	port isolation	133
23.2	show port isolation	133
第 24 章	环路监测配置命令	135
24.1	loopback-detection(global)	135
24.2	loopback-detection interval	135
24.3	loopback-detection recovery-time	135
24.4	loopback-detection(interface)	136
24.5	loopback-detection config	136
24.6	loopback-detection recover	137
24.7	show loopback-detection global	137
24.8	show loopback-detection interface	137
第 25 章	PoE 配置命令	139
25.1	power inline consumption (global)	139
25.2	power inline supply	139
25.3	power inline priority	140
25.4	power inline consumption (interface)	140
25.5	power time-range	140
25.6	holiday	141
25.7	absolute	141
25.8	periodic	142
25.9	power holiday	142
25.10	power inline time-range	143
25.11	power profile	143
25.12	power inline profile	144
25.13	show power inline	145
25.14	show power inline configuration interface	145
25.15	show power inline information interface	145
25.16	show power time-range	146
25.17	show power holiday	146
25.18	show power profile	146
第 26 章	ACL 配置命令	148
26.1	time-range	148
26.2	absolute	148
26.3	periodic	149
26.4	holiday	149
26.5	holiday(global)	150

26.6	access-list create	150
26.7	mac access-list	151
26.8	access-list standard	151
26.9	access-list extended	152
26.10	rule.....	153
26.11	access-list policy name	154
26.12	access-list policy action	154
26.13	redirect interface	155
26.14	s-condition	155
26.15	s-mirror	156
26.16	qos-remark	156
26.17	access-list bind(interface)	157
26.18	access-list bind(vlan)	157
26.19	show time-range	158
26.20	show holiday	158
26.21	show access-list.....	158
26.22	show access-list policy	159
26.23	show access-list bind.....	159
第 27 章 MSTP 配置命令		160
27.1	spanning-tree(global).....	160
27.2	spanning-tree(interface).....	160
27.3	spanning-tree common-config	161
27.4	spanning-tree mode.....	161
27.5	spanning-tree mst configuration.....	162
27.6	instance	162
27.7	name.....	163
27.8	revision	163
27.9	spanning-tree mst instance.....	164
27.10	spanning-tree mst	164
27.11	spanning-tree priority	165
27.12	spanning-tree tc-defend.....	165
27.13	spanning-tree timer	166
27.14	spanning-tree hold-count	166
27.15	spanning-tree max-hops	167
27.16	spanning-tree bpdupfilter	167
27.17	spanning-tree bpduguard.....	168
27.18	spanning-tree guard loop.....	168
27.19	spanning-tree guard root	169
27.20	spanning-tree guard tc.....	169
27.21	spanning-tree mcheck	169
27.22	show spanning-tree active	170
27.23	show spanning-tree bridge.....	170
27.24	show spanning-tree interface.....	170
27.25	show spanning-tree interface-security	171
27.26	show spanning-tree mst.....	171
第 28 章 IGMP 配置命令		173
28.1	ip igmp snooping(global).....	173
28.2	ip igmp snooping(interface)	173
28.3	ip igmp snooping immediate-leave	173
28.4	ip igmp snooping drop-unknown	174

28.5	ip igmp snooping vlan-config	174
28.6	ip igmp snooping multi-vlan-config.....	175
28.7	ip igmp snooping filter(global).....	176
28.8	ip igmp snooping filter(interface).....	177
28.9	ip igmp snooping filter add-id	177
28.10	ip igmp snooping filter mode	177
28.11	ip igmp snooping filter maxgroup	178
28.12	clear ip igmp snooping statistics	178
28.13	show ip igmp snooping	179
28.14	show ip igmp snooping interface.....	179
28.15	show ip igmp snooping vlan.....	180
28.16	show ip igmp snooping multi-vlan	180
28.17	show ip igmp snooping groups	180
28.18	show ip igmp snooping filter	181
第 29 章 MLD 配置命令		182
29.1	ipv6 mld snooping	182
29.2	ipv6 mld snooping router-aging-time	182
29.3	ipv6 mld snooping member-aging-time	183
29.4	ipv6 mld snooping report-suppression	183
29.5	ipv6 mld snooping unknown-filter.....	183
29.6	ipv6 mld snooping last-listener query-inteval	184
29.7	ipv6 mld snooping last-listener query-count.....	184
29.8	ipv6 mld snooping multicast-vlan	185
29.9	ipv6 mld snooping multicast-vlan vlan-id	185
29.10	ipv6 mld snooping vlan	185
29.11	ipv6 mld snooping vlan router-aging-time	186
29.12	ipv6 mld snooping vlan member-aging-time	186
29.13	ipv6 mld snooping vlan immediate-leave	187
29.14	ipv6 mld snooping vlan mrouter	187
29.15	ipv6 mld snooping vlan static.....	188
29.16	ipv6 mld snooping querier vlan	188
29.17	ipv6 mld snooping querier vlan max-response-time.....	189
29.18	ipv6 mld snooping querier vlan query-interval	189
29.19	ipv6 mld snooping querier vlan query-source	189
29.20	ipv6 mld snooping filter(global)	190
29.21	ipv6 mld snooping filter(interface)	190
29.22	ipv6 mld snooping filter-mode	191
29.23	ipv6 mld snooping filter-id	191
29.24	ipv6 mld snooping max-group.....	192
29.25	clear ipv6 mld snooping statistics	192
29.26	show ipv6 mld snooping	192
29.27	show ipv6 mld snooping vlan	193
29.28	show ipv6 mld snooping static-mcast	193
29.29	show ipv6 mld snooping group	193
29.30	show ipv6 mld snooping filter.....	194
29.31	show ipv6 mld snooping interface.....	194
29.32	show ipv6 mld snooping interface filter	195
29.33	show ipv6 mld snooping querier	195
29.34	show ipv6 mld snooping statistics.....	195

第 30 章 SNMP 配置命令	197
30.1 snmp-server.....	197
30.2 snmp-server view.....	197
30.3 snmp-server group.....	198
30.4 snmp-server user.....	199
30.5 snmp-server community	200
30.6 snmp-server host.....	200
30.7 snmp-server engineID	201
30.8 snmp-server traps snmp	202
30.9 snmp-server traps link-status.....	203
30.10 snmp-server traps	203
30.11 snmp-server traps mac	204
30.12 snmp-server traps vlan	205
30.13 rmon history	205
30.14 rmon event.....	206
30.15 rmon alarm	207
30.16 show snmp-server	208
30.17 show snmp-server view	208
30.18 show snmp-server group	208
30.19 show snmp-server user	209
30.20 show snmp-server community	209
30.21 show snmp-server host.....	209
30.22 show snmp-server engineID	210
30.23 show rmon history.....	210
30.24 show rmon event	210
30.25 show rmon alarm	211
第 31 章 LLDP 配置命令	212
31.1 lldp	212
31.2 lldp hold-multiplier	212
31.3 lldp timer	213
31.4 lldp med-fast-count	214
31.5 lldp receive.....	214
31.6 lldp transmit	214
31.7 lldp snmp-trap	215
31.8 lldp tlv-select.....	215
31.9 lldp med-status	217
31.10 lldp med-tlv-select.....	217
31.11 lldp med-location.....	218
31.12 show lldp.....	218
31.13 show lldp interface	219
31.14 show lldp local-information interface	219
31.15 show lldp neighbor-information interface	219
31.16 show lldp traffic interface	220
第 32 章 集群配置命令	221
32.1 cluster ndp	221
32.2 cluster ntdp	222
32.3 cluster explore	222
32.4 cluster	223
32.5 cluster candidate.....	223
32.6 cluster individual	224

32.7	show cluster ndp.....	224
32.8	show cluster ntdp.....	224
32.9	show cluster neighbour.....	225
32.10	show cluster manage role.....	225

手册概述

本手册提供 CLI（Command Line Interface, 命令行界面）参考信息，适用于 TP-LINK TL-SG3210/TL-SG3216/TL-SG3424/TL-SG3424P 全千兆二层网管交换机。由于这三个机型的配置方法相似，本手册将以 TL-SG3210 为例进行介绍。

各章节内容安排如下：

第 1 章：命令行使用指导

主要介绍 CLI 的使用方法、命令行模式、使用命令行、命令行分级及命令行格式约定。

第 2 章：用户界面

主要介绍用户登录和退出操作模式的相关配置命令。

第 3 章：IEEE 802.1Q VLAN 配置命令

主要介绍 IEEE 802.1Q VLAN 的相关配置命令。

第 4 章：MAC VLAN 配置命令

主要介绍 MAC-Based VLAN 的相关配置命令。

第 5 章：协议 VLAN 配置命令

主要介绍协议 VLAN 的相关配置命令。

第 6 章：语音 VLAN 的配置命令

主要介绍语音 VLAN 的相关配置命令。

第 7 章：GVRP 配置命令

主要介绍 GVRP 的相关配置命令。

第 8 章：Etherchannel 配置命令

主要介绍端口汇聚和 LACP 的相关配置命令。

第 9 章：用户管理配置命令

主要介绍用户管理信息的相关配置命令。

第 10 章：HTTP 和 HTTPS 配置命令

主要介绍交换机 HTTP 和 HTTPS 管理服务的相关配置命令。

第 11 章：绑定列表配置命令

主要介绍 IP-MAC-VID-PORT 四元绑定表的相关配置命令。

第 12 章：ARP 防护配置命令

主要介绍防 ARP 欺骗、防 ARP 攻击、报文统计的相关配置命令。

第 13 章：DoS 防护命令

主要介绍 DoS 防护和攻击检测的相关配置命令。

第 14 章：IEEE 802.1X 配置命令

主要介绍 IEEE 802.1X 认证的相关配置命令。

第 15 章：系统日志配置命令

主要介绍系统日志的查看、输出，日志服务器的相关配置命令。

第 16 章：SSH 配置命令

主要介绍 SSH 配置管理的相关命令。

第 17 章：地址配置命令

主要介绍端口安全设置和地址表管理的相关配置命令。

第 18 章：系统配置命令

主要介绍系统信息、网络参数配置，系统软件复位，系统文件升级，交换机重启及连通性测试等系统相关配置命令。

第 19 章：IPv6 地址配置命令

主要介绍 IPv6 地址相关配置命令。

第 20 章：以太网配置命令

主要介绍以太网端口的流量控制、协商模式、风暴抑制、带宽限制的相关配置命令。

第 21 章：QoS 配置命令

主要介绍 QoS（服务质量）的相关配置命令。

第 22 章：端口监控配置命令

主要介绍端口监控的相关配置命令。

第 23 章：端口隔离配置命令

主要介绍端口隔离的相关配置命令。

第 24 章：环路监测配置命令

主要介绍环路监测的相关配置命令。

第 25 章：PoE 配置命令

主要介绍 PoE（以太网供电）的相关配置命令。

第 26 章：ACL 配置命令

主要介绍访问控制的相关配置命令。

第 27 章：MSTP 配置命令

主要介绍生成树配置的相关配置命令。

第 28 章：IGMP 配置命令

主要介绍 IGMP 侦听、组播地址表管理、组播过滤等组播管理相关配置命令。

第 29 章：MLD 配置命令

主要介绍 MLD 侦听的相关配置命令。

第 30 章：SNMP 配置命令

主要介绍 SNMP（简单网络管理协议）配置、通知管理、RMON（远程网络监视）等 SNMP 相关配置命令。

第 31 章：LLDP 配置命令

主要介绍 LLDP（链路层发现协议）以及 LLDP-MED 的相关配置命令。

第 32 章：集群配置命令

主要介绍拓扑发现、拓扑收集、集群管理的相关配置命令。

第1章 命令行使用指导

1.1 使用命令行

用户可以通过两种方式登录交换机来使用命令行：

1. 通过Console口进行本地登录；
2. 通过以太网端口利用Telnet进行本地或远程登录；
3. 通过以太网端口利用SSH进行本地或远程登录。

1.1.1. 通过 Console 口进行本地登录

1. 首先，将计算机（或终端）的串口通过配置电缆与以太网交换机的 Console 口连接。
2. 选择开始→所有程序→附件→通讯→超级终端，打开超级终端。

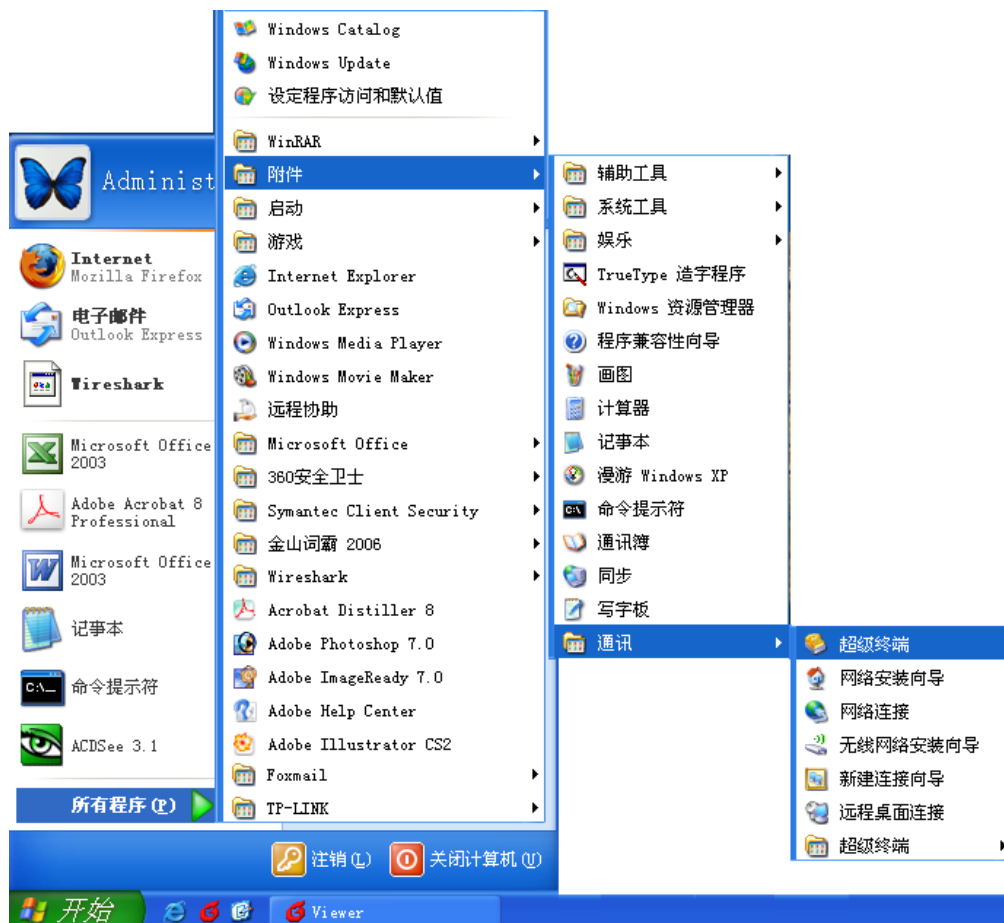


图 1-1 打开超级终端

3. 弹出如图 1-2 所示的连接描述窗口，在名称处键入一个名称，点击**确定**。



图 1-2 连接描述

4. 在图 1-3 中选择连接串口，点击**确定**。



图 1-3 连接端口选择

5. 在图 1-4 中对端口进行参数设置：每秒位数“38400”，数据位“8”，奇偶校验“无”，停止位“1”，数据流控制“无”，然后点击**确定**。



图 1-4 端口属性设置

6. 在超级终端主窗口中输入回车键，可以看到“TL-SG3210>”的提示符，说明已成功登录交换机。如图 1-5 所示。

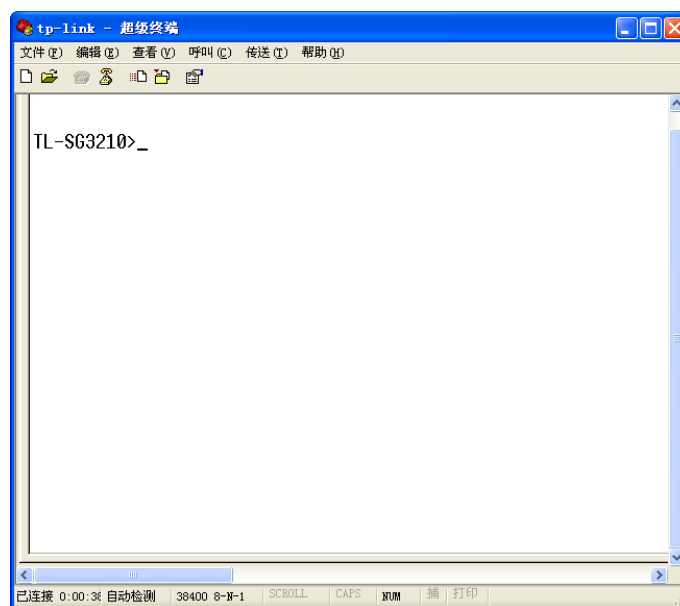


图 1-5 登录交换机

1.1.2. 配置特权模式密码

在首次使用 Telnet 或 SSH 进行远程登录之前，需要先用串口线连接主机及交换机的 Console 口，在超级终端上配置进入特权模式的密码。

按照 [1.1.1 通过 Console 口进行本地登录](#) 所述步骤登录交换机，再按照下图所示设置进入交换机特权模式的密码。

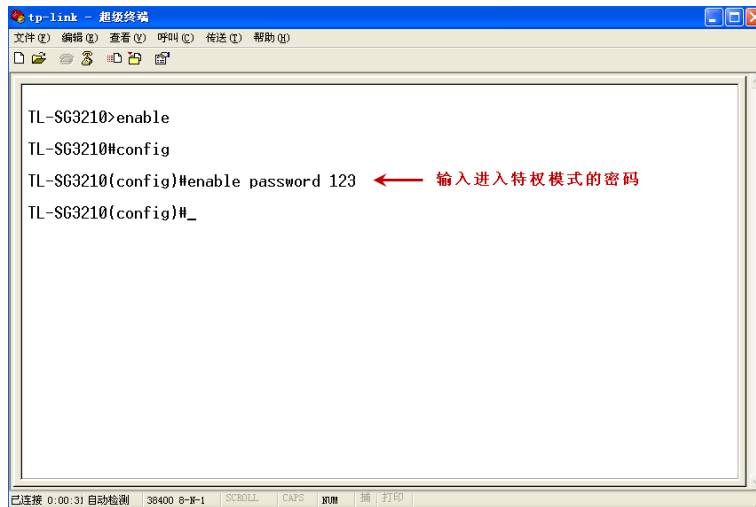


图 1-6 设置特权模式密码

1.1.3. 通过 Telnet 进行登录

在首次使用 Telnet 进行登录之前，设置好进入特权模式的密码后，您还需要在超级终端上配置 Telnet 登录模式和登录认证信息。

Telnet 登录模式有两种：Login local 模式和 Login 模式。请根据需要自行选择其中一种模式进行登录。

Login local 模式：需要登录输入用户名和密码，默认值均为 admin。

Login 模式：无需登录用户名和密码，但是需要输入一个连接密码才能建立 Telnet 连接进行访问。

➤ Login Local 模式

如图 1-7 所示，首先在超级终端中配置 Telnet 登录模式为“login local”。

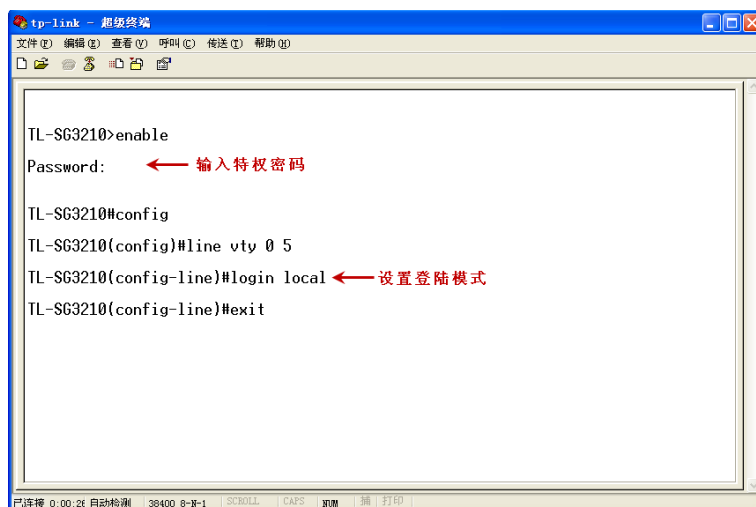


图 1-7 设置 login local 模式

然后便可在 login local 模式下进行 Telnet 登录了：

1. 请先确保本交换机与计算机在同一局域网内。选择**开始**→**运行**，打开运行窗口。



图 1-8 打开运行窗口

2. 弹出如图 1-9 所示的运行窗口，输入 telnet 192.168.0.1，点击**确定**按钮进入 DOS 界面。

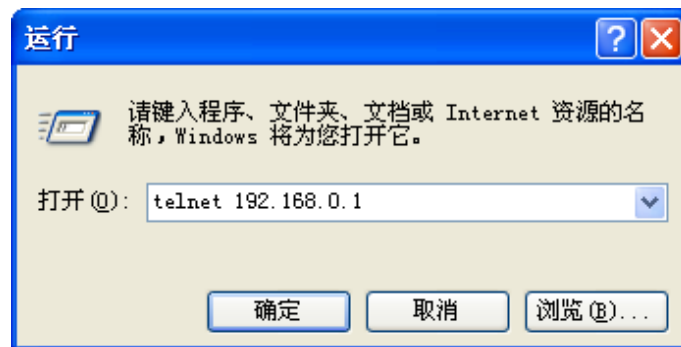


图 1-9 运行窗口

3. 输入登录的用户名和密码（默认值均为“admin”），回车即可进入用户模式，如图 1-10。

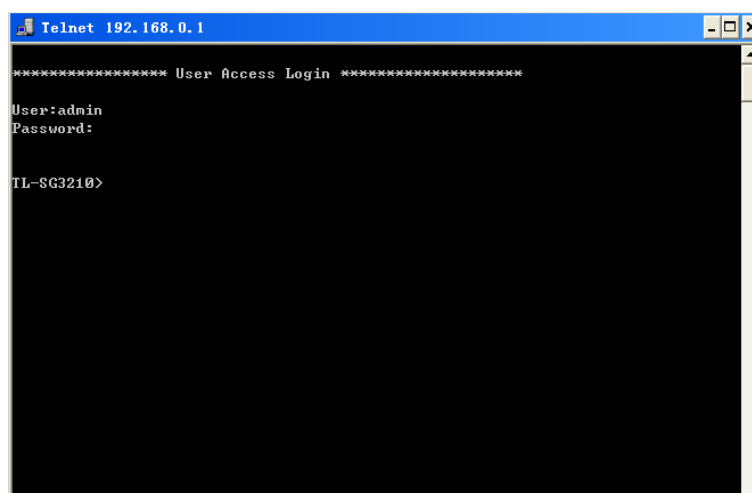


图 1-10 进入用户模式

此时便可在 Telnet 连接中使用 CLI 命令管理交换机了。

4. 可以输入 **enable** 命令进入特权模式。系统会提示输入密码，这里输入我们在超级终端中设置的密码 123。

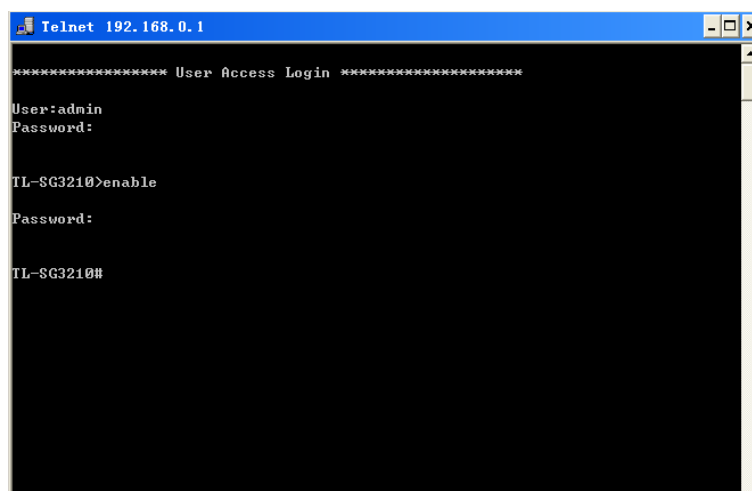


图 1-11 进入用户模式

➤ Login 模式

如图 1-12 所示，首先在超级终端上将 Telnet 登录模式配置为“login”，并将连接密码设置为“456”。

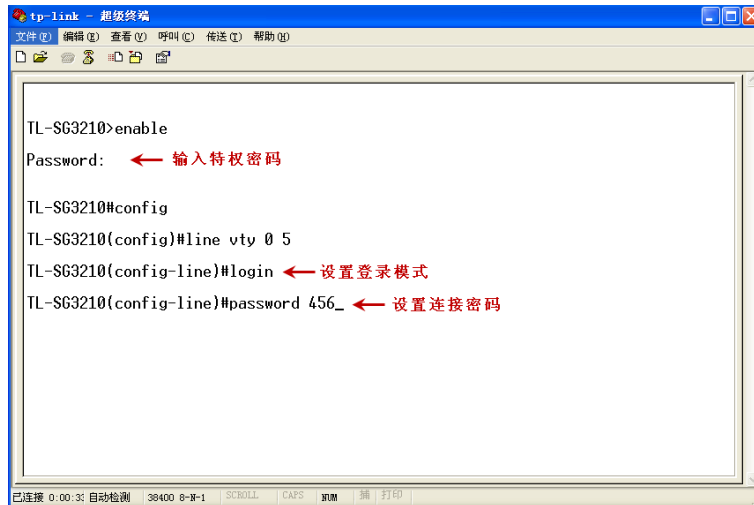


图 1-12 配置 login 模式

此时便可在 login 模式下进行 Telnet 登录了：

1. 在运行窗口中输入 **telnet 192.168.0.1**，按下回车键。

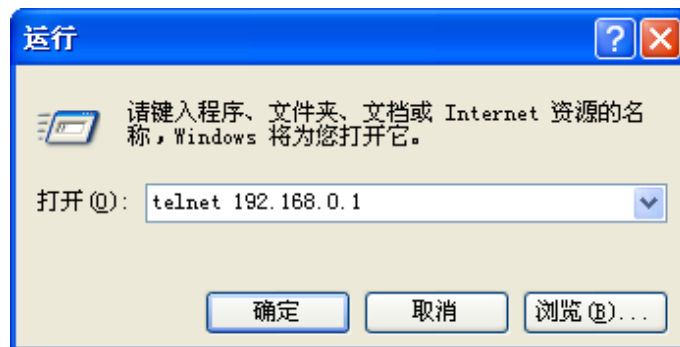


图 1-13 连接交换机

2. 输入在超级终端中设置的连接密码 **456** 进入用户模式。

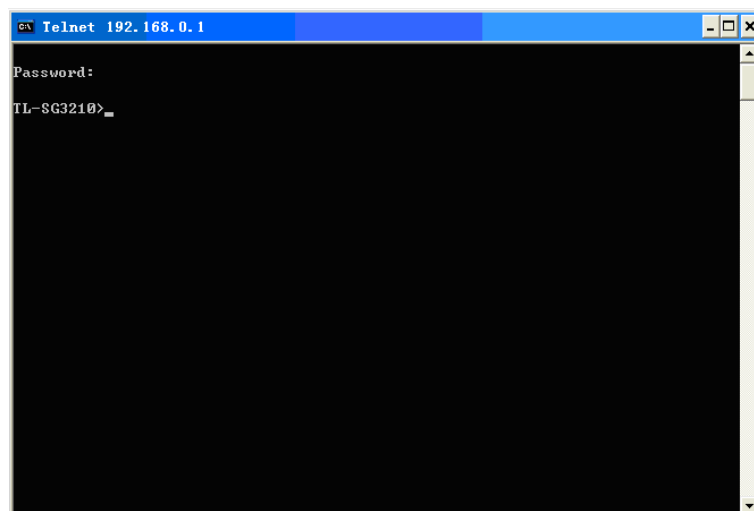


图 1-14 进入用户模式

3. 可以输入 **enable** 命令进入特权模式，系统会提示输入密码，这里输入我们在超级终端中设置的密码 123。

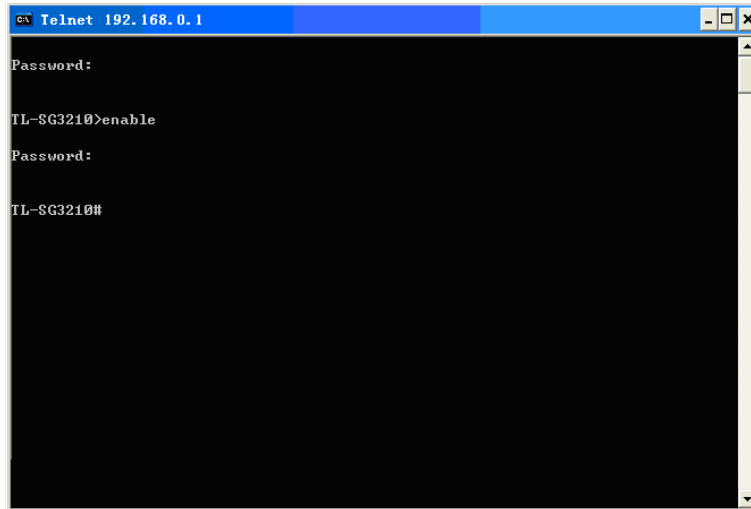


图 1-15 进入特权模式

1.1.4. 通过 SSH 进行登录

推荐使用第三方客户端软件 PuTTY 来建立 SSH 连接。在首次使用 SSH 进行登录之前请先设置好进入特权模式的密码。SSH 登录有两种认证模式：

密码认证模式：需要登录输入用户名和密码，默认值均为 **admin**。

密钥认证模式：无需登录用户名和密码，但是需要先通过 Putty 密钥生成器生成一对公钥和私钥，将公钥导入交换机，私钥导入客户端软件进行认证。

进行 SSH 登录之前，请按照下图所示步骤在超级终端中开启交换机的 SSH 功能。

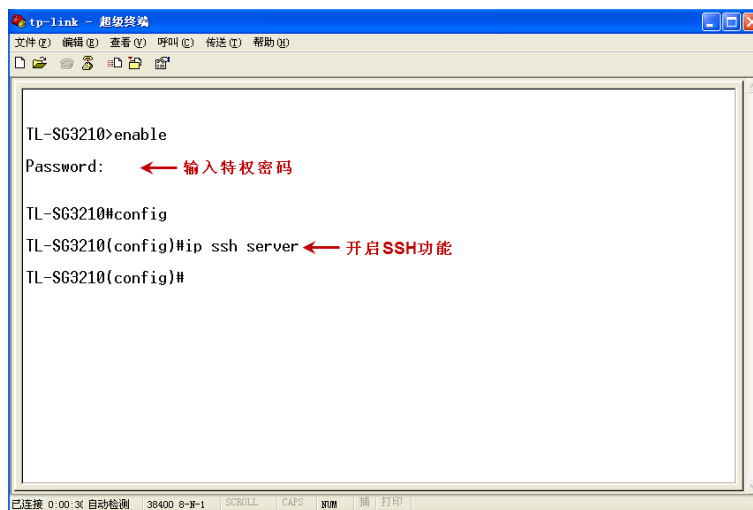


图 1-16 开启SSH功能

➤ 密码认证模式

1. 打开软件，登录 PuTTY 的主界面。在“Host Name”处填写交换机的 IP 地址；“Port”保持默认的 22；“Connection type”处选择 **SSH** 的接入方式。如下图所示。

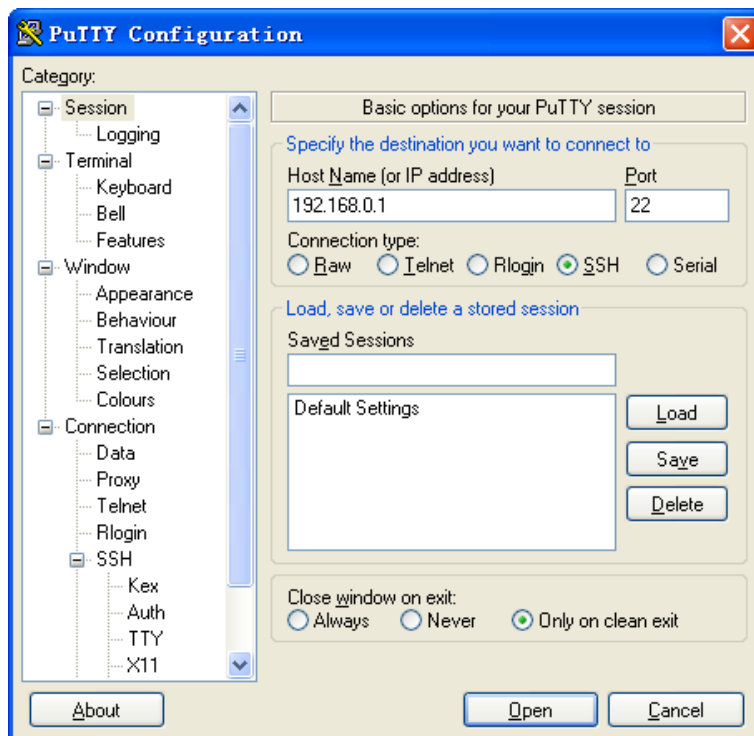


图 1-17 登录PuTTY主界面

2. 点击<Open>按钮，即可登录到交换机。操作方法与 telnet 相同，输入登录用户名和登录密码，即可继续进行配置操作。如下图所示。

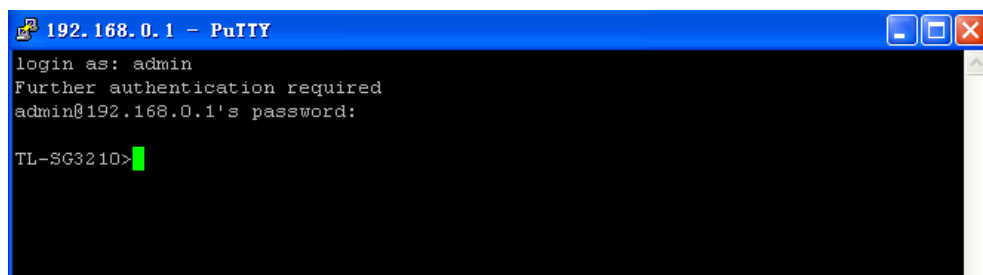


图 1-18 登录交换机

➤ 密钥认证模式

1. 选择密钥类型和密钥长度，并生成 SSH 密钥。如下图所示。

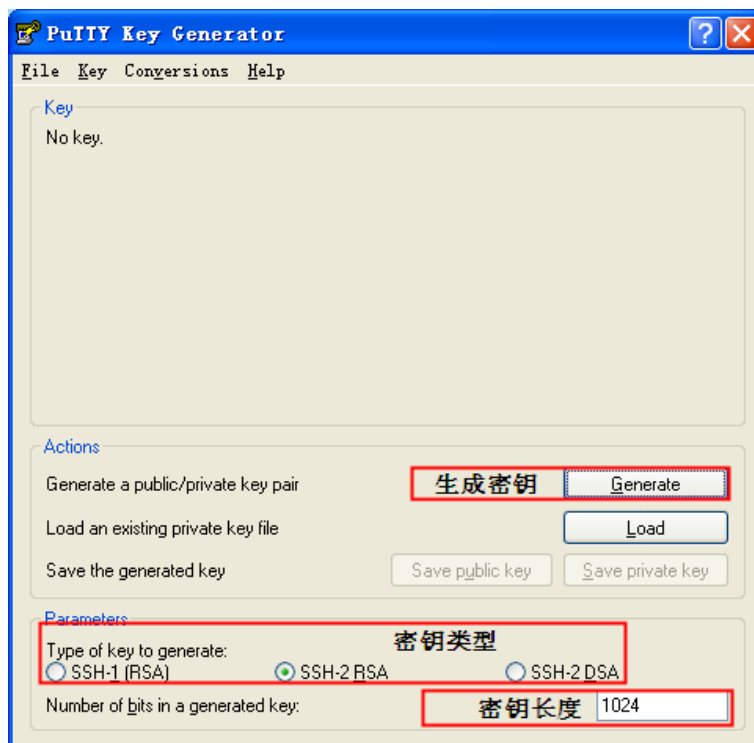


图 1-19 选择密钥类型和密钥长度



注意:

- 密钥长度的范围为 256 至 3072 比特。
- 生成密钥的过程中，在软件的空白处快速的随意晃动鼠标，产生随机数据，可以加快密钥生成的速度。

2. 密钥生成后，将公钥和私钥文件保存在一个 TFTP 服务器中。如下图所示。

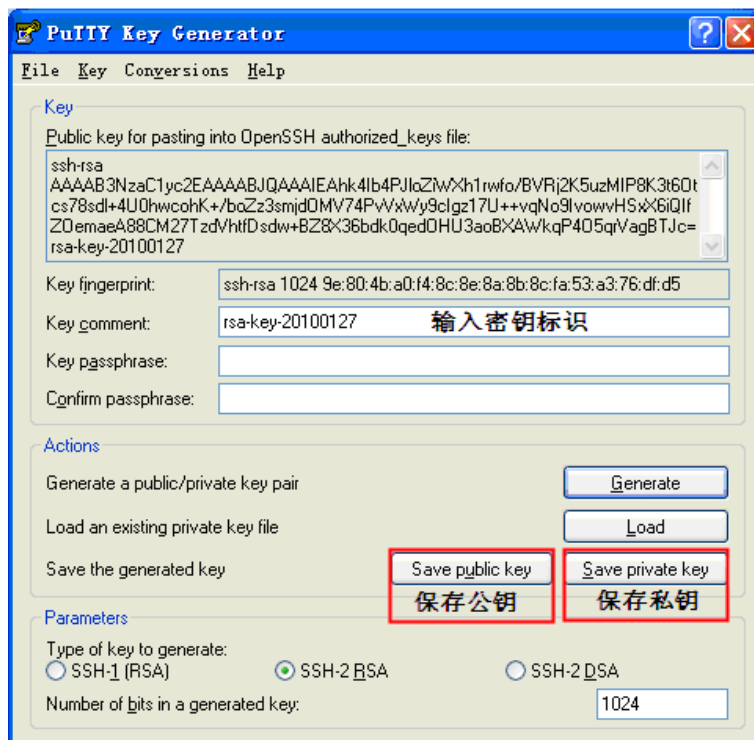


图 1-20 保存公钥和私钥

3. 在超级终端上，将保存至 TFTP 服务器上的公钥文件导入交换机中。

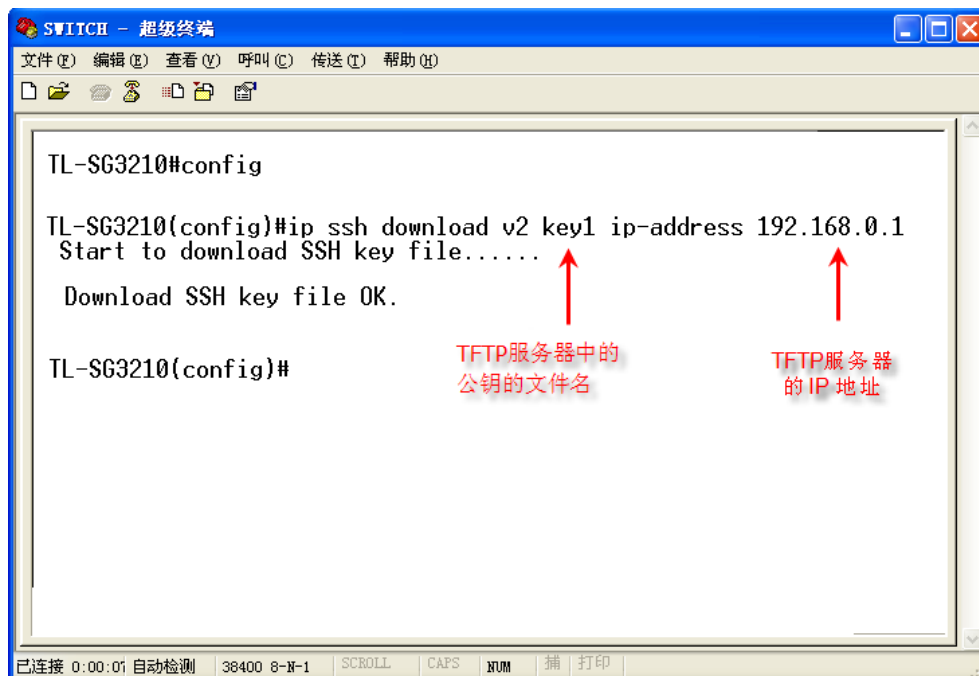


图 1-21 导入公钥文件至交换机



注意：

- 密钥类型要与密钥文件的类型保持一致。
- 载入 SSH 密钥的过程不能被中断。

4. 导入公钥文件后，打开 PuTTY 的主界面，输入 IP 地址。

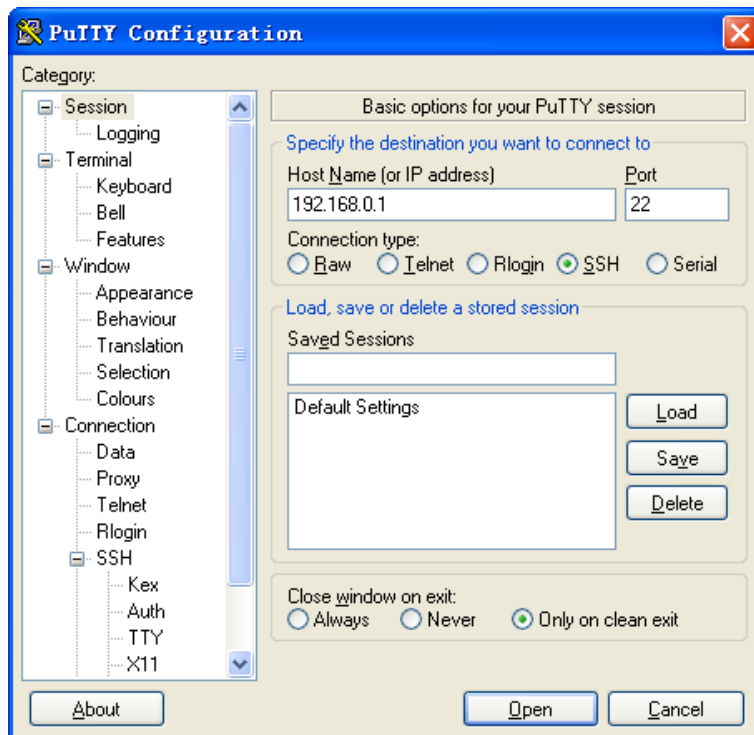


图 1-22 打开 PuTTY 的主界面

5. 将私钥文件导入至 SSH 客户端软件中。如下图所示。

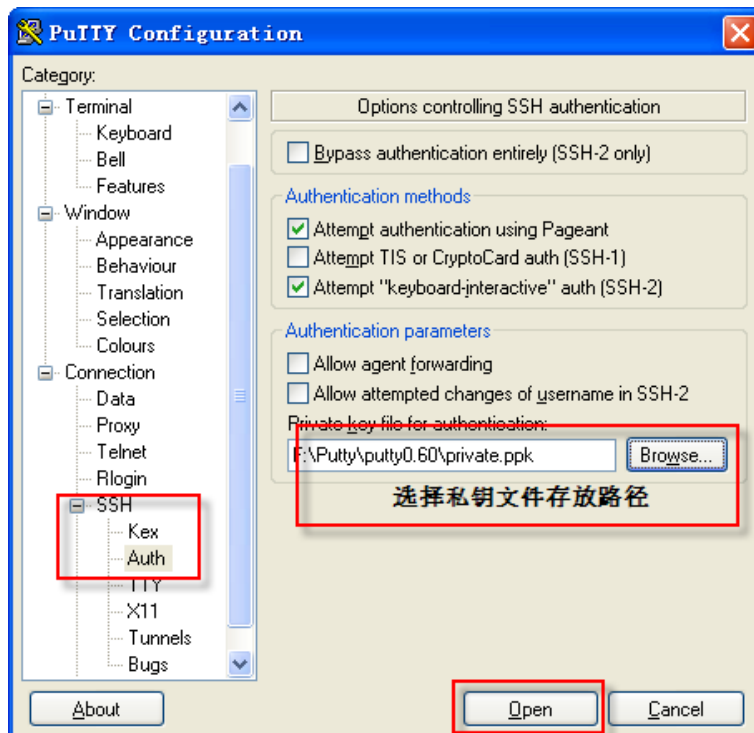


图 1-23 导入私钥文件至SSH客户端

6. 协商成功后，输入用户名进行登录，如果你不需要输入密码即可登陆成功，表明密钥认证已经成功。如下图所示。

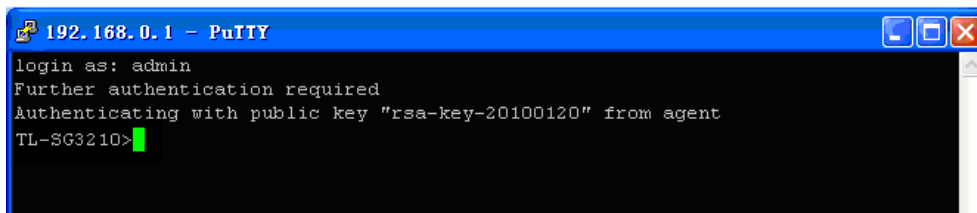
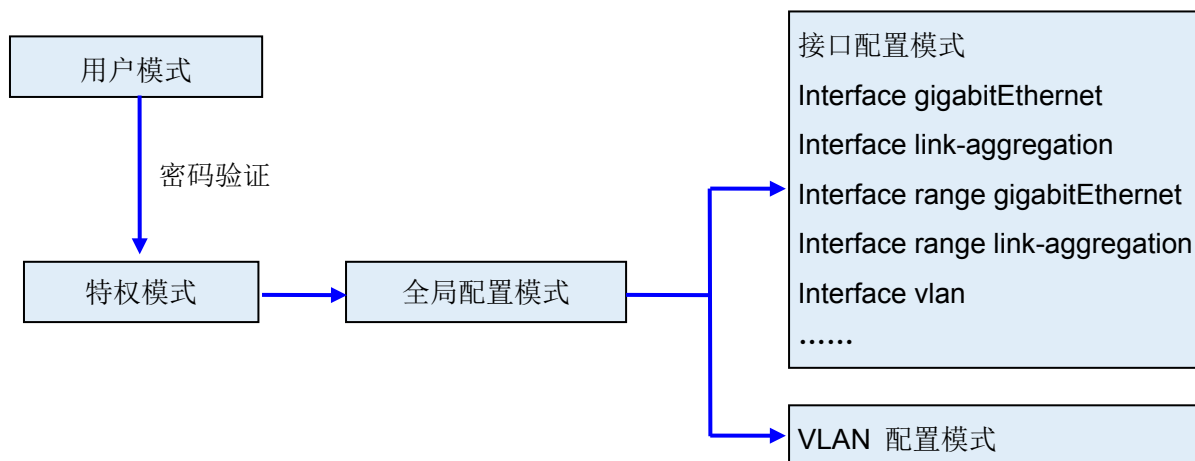


图 1-24 登录交换机

1.2 命令行模式

CLI 按功能划分为五种模式，即：用户模式、特权模式、全局配置模式、接口配置模式和 VLAN 配置模式，其中接口配置模式又分为以太网端口配置模式和汇聚端口配置模式等，如下图：



下表列出了各模式的访问方法、提示符以及如何离开各模式：

模式	访问方法	提示符	离开或访问下一模式
用户模式	与交换机建立连接即进入该模式	TL-SG3210>	输入 exit 命令断开与交换机连接（Console 口接入时无法断开）；输入 enable 命令，进入特权模式。
特权模式	在用户模式下，使用 enable 命令进入该模式	TL-SG3210#	输入 disable 命令或 exit 命令，返回用户模式；输入 configure 命令，进入全局配置模式。

模式	访问方法	提示符	离开或访问下一模式
全局配置模式	在特权模式下，使用 configure 命令进入该模式	TL-SG3210(config)#	输入 exit 命令或 end 命令，或者键入Ctrl+Z组合键，返回特权模式； 输入 interface type number 命令，进入接口配置模式； 输入 vlan 命令，进入VLAN配置模式。
接口配置模式	在全局配置模式下键入 interface gigabitEthernet port 或 interface range gigabitEthernet por-list 进入该模式	TL-SG3210(config-if)# 或 TL-SG3210(config-if-range)#	输入 end 命令，或键入Ctrl+Z组合键，返回特权模式； 输入 exit 命令，返回全局配置模式； 在 interface 命令中必须指明要进入哪一个接口配置子模式。
VLAN配置模式	在全局配置模式下，使用 vlan vlan-list 命令进入该模式	TL-SG3210(config-vlan)#	输入 end 命令，或键入Ctrl+Z组合键返回特权模式； 输入 exit 命令，返回全局配置模式。

说明：

- 通过Console口或Telnet方式与交换机建立连接后即进入用户模式。
- 各个模式都有各自的命令，要进行相应的命令配置必须要先进入对应的模式：
 - 全局配置模式：**提供全局配置的命令，如：生成树，队列调度模式等；
 - 接口配置模式：**分为多个接口，每个接口都有各自相应的命令：
 - interface gigabitEthernet：**配置一个以太网端口的参数，如双工模式，流控状态等。
 - interface range gigabitEthernet：**包含的命令跟**interface gigabitEthernet**基本一样，配置多个以太网端口的参数。
 - interface link-aggregation：**配置汇聚端口的参数，广播风暴等。
 - interface range link-aggregation：**配置多个汇聚端口的参数。
 - interface vlan：**配置VLAN接口参数。
 - VLAN配置模式：**创建VLAN，增加端口到指定VLAN。
- 有一些命令是全局的，在所有命令模式下都可执行：
 - show：**显示交换机各种信息，如：统计信息、端口信息、VLAN信息等。
 - history：**显示历史命令。

1.3 命令行安全等级

交换机主要分两个安全等级：用户级和管理级。

用户级只能在用户模式下进行简单的查询操作；管理级能在特权模式、全局配置模式、接口配置模式、VLAN 配置模式下对交换机进行监控、配置、管理等操作。

通过 Telnet 或 SSH 远程登录时，输入正确的用户名和密码后将进入用户模式，即获得用户级权限。不过当用户类型为受限用户时，则不允许登录访问命令行。在用户模式下，可通过输入命令 **enable** 并输入特权模式密码进入特权模式。特权模式密码需要先通过 Console 口进行本地连接，在超级终端上进行设置。

通过 Console 口进行本地连接时，无需输入用户名和密码即可进入用户模式，使用 **enable** 命令进入特权模式时缺省情况下无密码，可以在全局配置模式下通过 **enable password** 命令设置管理级密码。无密码情况下键入 **enable** 命令直接进入特权模式，有密码情况下输入管理级密码才能进入特权模式。进入特权模式即获得管理级权限。

1.4 命令行格式约定

1.4.1. 基本格式约定

本文档中对 CLI 命令的叙述遵循以下约定：

- 在中括号 [] 中的任何参数都是可选的。
- 在大括号 {} 中的任何参数都是必需的。
- 如果有多个选项，则使用竖线 “|” 分隔每个选项。

例如：**speed { 10 | 100 | 1000 }**

- 关键词（命令中保持不变，必须照输的部分）以粗体形式出现。

例如：**show logging**

- 常量（枚举量，只能选择其一）以普通字体形式出现。

例如：**switchport type { access | trunk | general }**

- 变量（命令中必须以实际值进行替代的部分）以斜体形式出现。

例如：**bridge aging-time *aging-time***

1.4.2. 特殊字符

若变量为字符串形式，输入时请注意：

- ” < > , \ & 这六个字符是不允许输入的。

- 若字符串中包含空格，则字符串首尾需添加单引号“'”或双引号“”，如'hello world'、“hello world”。此时单/双引号中的两个（或多个）单词会作为一个字符串参数输入；如果不加单/双引号，它们会被解析成两个（或多个）字符串。

1.4.3. 参数格式

变量中有些参数是有特定的输入格式的：

- MAC 地址必须以 XX:XX:XX:XX:XX:XX 的格式输入。
- 端口编号格式为：设备编号/插槽位/端口序号。对于 TL-SG3210/TL-SG3216/TL-SG3424/TL-SG3424P 交换机，设备编号为 1，插槽位取值为 0，而端口序号为设备上该端口的编号，具体请查看设备前面板。
例如：端口编号 1/0/3 表示设备上编号为 3 的端口。
- 输入一组端口号(port-list)或一组 VLAN ID(vlan-list)时，可以输入一个或多个值，每个值之间用逗号隔开，连续的一组值可以用连接符-表示。
例如：1/0/1,1/0/3-5,1/0/7 表示端口 1/0/1，1/0/3，1/0/4，1/0/5，1/0/7。

第2章 用户界面

2.1 enable

该命令用于从用户模式进入特权模式。

命令

enable

模式

用户模式

示例

设置了从用户模式进入特权模式的密码时：

```
TL-SG3210>enable
```

```
Enter password
```

```
TL-SG3210#
```

2.2 service password-encryption

该命令用于设置密码或写入配置文件时，使用对称加密算法加密密码。加密密码可以防止配置文件中的密码被读取。它的 no 命令用于禁用全局密码加密功能。

命令

service password-encryption

no service password-encryption

模式

全局配置模式

示例

开启全局密码加密功能：

```
TL-SG3210(config)# service password-encryption
```

2.3 enable password

该命令用于设置从用户模式切换到特权模式的管理级密码，它的 no 命令用于清空密码。通过此命令可以使用对称加密算法加密密码。

命令

enable password { [0] password | 7 encrypted-password }

no enable password

参数

0 —— 一种加密类型，表示接下来需要输入没有进行加密的密码，0 为默认加密类型。

password —— 管理级密码，由 1~31 个字符组成，密码区分大小写，允许输入数字、英文字母、下划线和十六种特殊字符（!\$%&'()*,-./\[]{}）。默认为空。

7 —— 一种加密类型，表示接下来需要输入进行过对称加密的密码，此类型密码长度固定。

encrypted-password —— 固定长度的进行过对称加密的密码，可以从其他交换机的配置文件中复制得到。配置了加密密码之后，当要再次进入此模式时，需要输入相应的未加密密码。

模式

全局配置模式

说明

如果在此配置的密码为未加密的密码，但通过 [service password-encryption](#) 命令启用了全局密码加密功能，那么交换机配置文件中的密码将会显示为对称加密格式。

示例

将用户模式切换到特权模式时的管理级密码设置为不加密密码 admin:

```
TL-SG3210(config)# enable password 0 admin
```

2.4 enable secret

该命令用于设置从用户模式切换到特权模式的管理级密码，且此密码使用 MD5 加密算法加密，它的 no 命令用于恢复默认配置。

命令

```
enable secret { [ 0 ] password | 5 encrypted-password }
```

```
no enable secret
```

参数

0 —— 一种加密类型，表示接下来需要输入没有进行加密的密码，0 为默认加密类型。

password —— 管理级密码，由 1~31 个字符组成，密码区分大小写，允许输入数字、英文字母、下划线和十六种特殊字符（!\$%&'()*,-./\[]{}）。默认为空。此密码将在交换机配置文件中显示为 MD5 加密格式。

5 —— 一种加密类型，表示接下来需要输入进行过 MD5 加密的密码，此类型密码长度固定。

encrypted-password —— 固定长度的进行过 MD5 加密的密码，可以从其他交换机的配置文件中复制得到。配置了加密密码之后，当要再次进入此模式时，需要输入相应的未加密密码。

模式

全局配置模式

说明

当同时配置了 `enable password` 和 `enable secret` 命令时，`enable secret` 配置的密码生效。

示例

将用户模式切换到特权模式时的管理级密码设置为不加密密码 `admin`，且此密码将在交换机配置文件中以 MD5 加密格式显示：

```
TL-SG3210(config)# enable secret 0 admin
```

2.5 disable

该命令用于从特权模式返回到用户模式。

命令

disable

模式

特权模式

示例

从特权模式返回到用户模式：

```
TL-SG3210# disable
```

```
TL-SG3210>
```

2.6 configure

该命令用于从特权模式进入全局配置模式。

命令

configure

模式

特权模式

示例

从特权模式进入全局配置模式：

```
TL-SG3210# configure
```

```
TL-SG3210(config)#
```

2.7 exit

该命令用于退出当前配置模式返回上一层配置模式。

命令

exit

模式

所有配置模式

示例

从接口配置模式返回到全局模式，再返回到特权模式：

```
TL-SG3210 (config-if)# exit
```

```
TL-SG3210 (config)#exit
```

```
TL-SG3210#
```

2.8 end

该命令用于返回特权模式。

命令

end

模式

所有配置模式

示例

从接口配置模式直接返回到特权模式：

```
TL-SG3210(config-if)#end
```

```
TL-SG3210#
```

2.9 show history

该命令用于显示系统启动后用户在当前模式下最近输入的 20 条命令。

命令

show history

模式

特权模式以及所有配置模式

示例

显示用户之前在当前模式下输入的命令：

```
TL-SG3210(config)#show history
```

```
1 show history
```

2.10 clear history

该命令用于清空系统启动后在当前模式下输入过的命令，下一次使用 **history** 命令时将不会显示这些被清空的命令。

命令

```
clear history
```

模式

特权模式以及所有配置模式

示例

清空系统启动后在当前模式下输入过的命令：

```
TL-SG3210(config)#clear history
```

第3章 IEEE 802.1Q VLAN 配置命令

VLAN（Virtual Local Area Network，虚拟局域网）是一种在一个物理网络上划分多个逻辑网络的技术，具有控制广播域范围，增强网络安全性，可以灵活创建虚拟工作组等优点。

3.1 vlan

该命令用于进入 VLAN 配置模式并创建 IEEE 802.1Q VLAN，它的 no 命令用于删除 IEEE 802.1Q VLAN。

命令

vlan *vlan-list*

no vlan *vlan-list*

参数

vlan-list —— VLAN ID List，取值范围 2~4094。可是是其中的任意一个值或者一个数值段。

模式

全局配置模式

示例

创建 VLAN 2-10 以及 VLAN 100:

```
TL-SG3210(config)# vlan 2-10,100
```

删除 VLAN 2:

```
TL-SG3210(config)# no vlan 2
```

3.2 interface vlan

该命令用于创建 VLAN 接口并进入 VLAN 接口模式。它的 no 命令用于删除 VLAN 接口。

命令

interface vlan *vlan-id*

no interface vlan *vlan-id*

参数

vlan-id —— VLAN ID，取值范围 1-4094。

模式

全局配置模式

示例

创建 VLAN 接口 2:

```
TL-SG3210(config)# interface vlan 2
```

3.3 name

该命令用于配置 IEEE 802.1Q VLAN 描述字符，它的 no 命令用于清空描述字符。

命令

name *descript*

no name

参数

descript —— VLAN 描述字符，长度为 1-16 个字符。

模式

VLAN 配置模式 (vlan)

示例

将 vid=2 的 VLAN 描述成 “VLAN002”:

```
TL-SG3210(config)# vlan 2
```

```
TL-SG3210(config-if)# name VLAN002
```

3.4 switchport mode

该命令用于配置以太网端口的链路类型。

命令

switchport mode { access | trunk | general }

参数

access | trunk | general —— 以太网端口链路类型，共支持三种类型。

模式

接口配置模式 (interface gigabitEthernet / interface range gigabitEthernet)

示例

配置以太网端口 3 的链路类型为 general:

```
TL-SG3210(config)# interface gigabitEthernet 1/0/3
```

```
TL-SG3210(config-if)#switchport mode general
```

3.5 switchport access vlan

该命令用于把 access 类型的端口添加到 IEEE 802.1Q VLAN，它的 no 命令用于把端口从 IEEE 802.1Q VLAN 中移除。

命令

switchport access vlan *vlan-id*

no switchport access vlan

参数

vlan-id —— VLAN ID，取值范围 2-4094。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

配置以太网端口 3 链路类型为 access 并将其添加到 VLAN2 中：

```
TL-SG3210(config)# interface gigabitEthernet 1/0/3
```

```
TL-SG3210(config-if)# switchport mode access
```

```
TL-SG3210(config-if)# switchport access vlan 2
```

3.6 switchport trunk allowed vlan

该命令用于把 trunk 类型的端口添加到 IEEE 802.1Q VLAN，它的 no 命令用于端口从 IEEE 802.1Q VLAN 中移除。

命令

switchport trunk allowed vlan *vlan-list*

no switchport trunk allowed vlan *vlan-list*

参数

vlan-list —— 指定 IEEE 802.1Q VLAN ID，取值范围 2-4094，可多选，格式为：2-3, 5。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

配置以太网端口 2 链路类型为 trunk 并将其添加到 VLAN2 中：

```
TL-SG3210(config)# interface gigabitEthernet 1/0/2
```

```
TL-SG3210(config-if)# switchport mode trunk
```

```
TL-SG3210(config-if)# switchport trunk allowed vlan 2
```

3.7 switchport general allowed vlan

该命令用于把 general 类型的端口添加到 IEEE 802.1Q VLAN，并配置端口的出口规则。它的 no 命令用于把端口从 IEEE 802.1Q VLAN 中移除。

命令

```
switchport general allowed vlan vlan-list { tagged | untagged }  
no switchport general allowed vlan vlan-list
```

参数

vlan-list —— 指定 IEEE 802.1Q VLAN ID，取值范围 2-4094，可多选，格式为：2-3, 5。
tagged | untagged —— 出口规则，tagged 或者 untagged。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

配置以太网端口 4 链路类型为 general，将其添加到 VLAN2 中，并指定出口规则为 tagged：

```
TL-SG3210(config)# interface gigabitEthernet 1/0/4  
TL-SG3210(config-if)# switchport mode general  
TL-SG3210(config-if)# switchport general allowed vlan 2 tagged
```

3.8 switchport pvid

该命令用于设置交换机端口的 PVID。

命令

```
switchport pvid vlan-id
```

参数

vlan-id —— VLAN ID，取值范围 1-4094。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

设置端口 3 的 PVID 为 1：

```
TL-SG3210(config)# interface gigabitEthernet 1/0/3  
TL-SG3210(config-if)# switchport pvid 1
```


3.9 show vlan summary

该命令用于显示 IEEE 802.1Q VLAN 的统计信息。

命令

show vlan summary

模式

特权模式以及所有配置模式

示例

显示 IEEE 802.1Q VLAN 的统计信息：

```
TL-SG3210(config)# show vlan summary
```

3.10 show vlan brief

该命令用于显示 IEEE 802.1Q VLAN 的概要信息。

命令

show vlan brief

模式

特权模式以及所有配置模式

示例

显示 IEEE 802.1Q VLAN 的概要信息：

```
TL-SG3210(config)# show vlan brief
```

3.11 show vlan

该命令用于显示指定的 IEEE 802.1Q VLAN 的详细信息。

命令

show vlan [id *vlan-list*]

参数

vlan-list —— VLAN ID，取值范围为 1-4094，可多选，格式为：2-3, 5。该参数缺省时，显示所有 IEEE 802.1Q VLAN 的信息。

模式

特权模式以及所有配置模式

示例

显示所有 VLAN 的详细信息：

```
TL-SG3210(config)# show vlan
```

显示 vid=2 的 VLAN 的详细信息:

```
TL-SG3210(config)# show vlan id 2
```

显示 vid=3-10 的 VLAN 的详细信息

```
TL-SG3210(config)# show vlan id 3-10
```

3.12 show interface switchport

该命令用于显示以太网口的信息。

命令

```
show interface switchport [ fastEthernet port | gigabitEthernet port ]
```

参数

port —— 以太网端口号

模式

特权模式以及所有配置模式

示例

显示以太网口 1/0/3 的详细信息:

```
TL-SG3210(config)# show interface switchport gigabitEthernet 1/0/3
```

第4章 MAC VLAN 配置命令

MAC VLAN 功能是按照 MAC 地址来划分 VLAN 的一种方法。每个 MAC 地址对应一个 VLAN ID，交换机给端口收到的无 tag 帧和优先级 tag 帧分配此 VLAN ID。

4.1 mac-vlan mac-address

该命令用于创建 MAC VLAN 条目。它的 no 命令用于删除 MAC VLAN 条目。

命令

mac-vlan mac-address *mac-addr* vlan *vlan-id* [*description* *descript*]

no mac-vlan mac-address *mac-addr*

参数

mac-addr —— 源 MAC 地址，格式为 XX:XX:XX:XX:XX:XX。

vlan-id —— 指定 IEEE 802.1 Q VLAN ID，取值范围 1-4094。

descript —— 对该 MAC VLAN 条目的描述，长度为 0-8 个字符。该参数缺省时，描述字符为空。

模式

全局配置模式

示例

创建 vid=2，MAC 地址为 00:11:11:01:01:12 的 MAC-Based VLAN 条目，命名为 RD：

```
TL-SG3210(config)# mac-vlan mac-address 00:11:11:01:01:12 vlan 2 description  
RD
```

4.2 show mac-vlan

该命令用于显示 MAC VLAN 条目信息。可以显示根据 MAC 地址或 VLAN ID 过滤的信息。

命令

show mac-vlan { all | mac-address *mac-addr* | vlan *vlan-id* }

参数

mac-addr —— 源 MAC 地址，格式为 XX:XX:XX:XX:XX:XX。

vlan-id —— 指定 IEEE 802.1 Q VLAN ID，取值范围 1-4094。

模式

特权模式和所有配置模式

示例

显示所有 MAC VLAN 条目信息：

```
TL-SG3210(config)# show mac-vlan all
```

显示 MAC 地址为 00:11:11:01:01:12 的 MAC VLAN 条目信息：

```
TL-SG3210(config)# show mac-vlan mac-address 00:11:11:01:01:12
```

显示 VLAN ID 为 4 的 MAC VLAN 条目信息：

```
TL-SG3210(config)# show mac-vlan vlan 4
```

第5章 协议 VLAN 配置命令

协议 VLAN 是按照协议来划分 VLAN 的一种方法。每个协议对应一个 VLAN ID，交换机给端口收到的无 tag 帧和优先级 tag 帧分配此 VLAN ID。

5.1 protocol-vlan template

该命令用于创建 Protocol VLAN 协议模板。它的 no 命令用于删除 Protocol VLAN 协议模板。

命令

```
protocol-vlan template name protocol-name ether-type type frame { 802_3 | ether_2  
| snap | llc }
```

```
no protocol-vlan template template-idx
```

参数

protocol-name —— 协议名称，由 1-8 个字符组成。

type —— 以太网协议类型，由 4 位十六进制数组成。

802_3 | ether_2 | snap | llc —— 数据帧类型，802_3, ether_2, snap 和 llc。

template-idx —— 协议模板序号。可用 [show protocol-vlan template](#) 命令获取各序号对应的模板。

模式

全局配置模式

示例

创建一个协议类型为 0x2024，数据帧类型为 Ethernet II 的 Protocol VLAN 协议模板，并命名为“TP”。

```
TL-SG3210(config)# protocol-vlan template name TP ether-type 2024 frame  
ether_2
```

5.2 protocol-vlan vlan

该命令用于创建 Protocol VLAN 条目，它的 no 命令则用于删除 Protocol VLAN 条目。

命令

```
protocol-vlan vlan vlan-id { template template-idx }
```

```
no protocol-vlan vlan entry-id
```

参数

vlan-id —— VLAN ID，取值范围 1-4094。

template-idx —— 协议模板序号。可用 [show protocol-vlan template](#) 命令获取各序号对应的模板。

entry-id —— 协议 VLAN 序号。可用 [show protocol-vlan vlan](#) 命令获取各序号对应的协议 VLAN 条目。

模式

全局配置模式

示例

创建 vid=2，协议模板序号为 3 的 Protocol VLAN 条目：

```
TL-SG3210(config)# protocol-vlan vlan 2 template 3
```

5.3 protocol-vlan group

该命令用于绑定指定的端口与协议 VLAN，以组成一个协议 VLAN 组。它的 no 命令用于删除协议 VLAN 组。

命令

protocol-vlan group *group-id*

no protocol-vlan group *group-id*

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

参数

group-id —— 协议 VLAN 序号。可用 [show protocol-vlan vlan](#) 命令获取各序号对应的协议 VLAN 条目。

示例

将端口 3 与序号为 2 的协议 VLAN 绑定：

```
TL-SG3210(config)# interface gigabitEthernet 1/0/3
```

```
TL-SG3210(config-if)# protocol-vlan group 2
```

5.4 show protocol-vlan template

该命令用于显示 Protocol VLAN 协议模块配置信息。

命令

show protocol-vlan template

模式

特权模式和所有配置模式

示例

显示 Protocol VLAN 协议模板配置信息：

```
TL-SG3210(config)# show protocol-vlan template
```

5.5 show protocol-vlan vlan

该命令用于显示 Protocol VLAN 条目信息。

命令

```
show protocol-vlan vlan
```

模式

特权模式和所有配置模式

示例

显示 Protocol VLAN 条目信息：

```
TL-SG3210(config)# show protocol-vlan vlan
```

第6章 语音 VLAN 配置命令

语音 VLAN 是为语音数据流而专门划分的 VLAN。通过划分 Voice VLAN 并将连接语音设备的端口加入 Voice VLAN，可以为语音数据流配置 QoS 参数，提高语音数据流的传输优先级、保证通话质量。

6.1 voice vlan

该命令用于开启 Voice VLAN 功能，它的 no 命令用于禁用 Voice VLAN 功能。

命令

voice vlan *vlan-id*

no voice vlan

参数

vlan-id —— VLAN ID，取值范围 2-4094。

模式

全局配置模式

示例

开启 vid=10 的 Voice VLAN 功能：

```
TL-SG3210(config)# voice vlan 10
```

6.2 voice vlan aging time

该命令用于配置 Voice VLAN 老化时间，它的 no 命令用于恢复默认老化时间，默认值为 1440。

命令

voice vlan aging time *time*

no voice vlan aging time

参数

time —— 老化时间，取值范围 1-43200 (分钟)。

模式

全局配置模式

示例

配置 Voice VLAN 老化时间为 2880 分钟：

```
TL-SG3210(config)# voice vlan aging time 2880
```


6.3 voice vlan priority

该命令用于配置 Voice VLAN 优先级，它的 no 命令用于恢复默认优先级，默认值为 6。

命令

voice vlan priority *pri*

no voice vlan priority

参数

pri —— 优先级，取值范围 0-7。

模式

全局配置模式

示例

将 Voice VLAN 优先级配置为 3：

```
TL-SG3210(config)# voice vlan priority 3
```

6.4 voice vlan mac-address

该命令用于创建或删除 Voice VLAN OUI。它的 no 命令用于删除指定的 Voice VLAN OUI。

命令

voice vlan mac-address *mac-addr* **mask** *mask* [**description** *descript*]

no voice vlan mac-address *mac-addr*

参数

mac-addr —— OUI 设备 MAC 地址。格式为 XX:XX:XX:XX:XX:XX。

mask —— MAC 地址掩码。格式为 XX:XX:XX:XX:XX:XX。

descript —— OUI 描述，1-16 个字符。缺省情况下为空。

模式

全局配置模式

示例

创建 MAC 地址为 00:11:11:11:11:11，掩码为 FF:FF:FF:00:00:00 的 Voice VLAN OUI，将其描述为 TP- Phone：

```
TL-SG3210(config)# voice vlan mac-address 00:11:11:11:11:11 mask  
FF:FF:FF:00:00:00 description TP- Phone
```

6.5 switchport voice vlan mode

该命令用于配置以太网端口的 Voice VLAN 成员模式。

命令

switchport voice vlan mode { manual | auto }

参数

manual | auto —— 端口的成员模式。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

配置以太网端口 3 的 voice vlan 成员模式为 manual:

```
TL-SG3210(config)# interface gigabitEthernet 1/0/3
```

```
TL-SG3210(config-if)# switchport voice vlan mode manual
```

6.6 switchport voice vlan security

该命令用于配置以太网端口的 Voice VLAN 安全模式。

命令

switchport voice vlan security

no switchport voice vlan security

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

启用以太网端口 3 的 Voice VLAN 安全模式:

```
TL-SG3210(config)# interface gigabitEthernet 1/0/3
```

```
TL-SG3210(config-if)# switchport voice vlan security
```

6.7 show voice vlan

该命令用于显示 Voice VLAN 全局配置。

命令

show voice vlan

模式

特权模式和所有配置模式

示例

显示 Voice VLAN 全局配置信息:

```
TL-SG3210(config)# show voice vlan
```

6.8 show voice vlan oui

该命令用于显示 Voice VLAN OUI 配置信息。

命令

show voice vlan oui

模式

特权模式和所有配置模式

示例

显示 Voice VLAN OUI 配置信息：

```
TL-SG3210(config)# show voice vlan oui
```

6.9 show voice vlan switchport

该命令用于显示以太网端口的 Voice VLAN 配置信息。

命令

show voice vlan switchport [gigabitEthernet *port*]

参数

port —— 以太网端口。该参数缺省时，显示所有端口的配置信息。

模式

特权模式和所有配置模式

示例

显示所有端口的配置信息：

```
TL-SG3210(config)# show voice vlan switchport
```

显示端口 2 的配置信息：

```
TL-SG3210(config)# show voice vlan switchport gigabitEthernet 1/0/2
```

第7章 GVRP 配置命令

GARP（Generic Attribute Registration Protocol,通用属性注册协议），GVRP 功能是该协议的一种应用，通过在端口动态注册和注销 VLAN 信息来达到创建或删除 VLAN 的目的，并传播该信息到其它交换机中，减少配置 VLAN 时烦琐的手动操作。

7.1 gvrp(global)

该命令用于全局启用 GVRP 功能，它的 no 命令用于禁用 GVRP 功能。

命令

gvrp

no gvrp

模式

全局配置模式

示例

全局启用 GVRP 功能：

```
TL-SG3210(config)# gvrp
```

7.2 gvrp (interface)

该命令用于在指定端口上启用 GVRP 功能，它的 no 命令用于禁用该端口的 GVRP 功能。

命令

gvrp

no gvrp

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

说明

类型为 trunk 的端口才能启用 GVRP 功能。

示例

启用端口 2-6 的 GVRP 功能：

```
TL-SG3210(config)# interface range gigabitEthernet 1/0/2-6
```

```
TL-SG3210(config-if-range)# gvrp
```

7.3 gvrp registration

该命令用于配置指定端口的 GVRP 注册模式，它的 no 命令用于恢复默认的注册模式。

命令

gvrp registration { normal | fixed | forbidden }

no gvrp registration

参数

normal | fixed | forbidden —— 注册模式，默认的为 normal。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

配置端口 2-6 的 GVRP 注册模式为 fixed：

```
TL-SG3210(config)# interface range gigabitEthernet 1/0/2-6
```

```
TL-SG3210(config-if-range)# gvrp registration fixed
```

7.4 gvrp timer

该命令用于配置 GVRP 定时器，它的 no 命令用于恢复默认配置。

命令

gvrp timer { leaveall | join | leave } value

no gvrp timer {leaveall | join | leave}

参数

leaveall | join | leave —— 分别表示 leave All、join 和 leave 三个定时器。每个端口启动 GARP 后，同时启动 LeaveAll 定时器，端口将对外循环发送 LeaveAll 消息，以使其它端口重新注册其所有的属性信息。GARP 端口可以将每个 Join 数据包向外发送两次来保证消息的可靠传输，两次发送之间的时间间隔用 Join 定时器来控制。接收到 Leave 数据包的 GARP 端口启动 Leave 定时器，如果在该定时器超时之前没有收到 Join 数据包，则注销相应属性信息。

value —— 定时器值，leave All 的取值范围 1000-30000(厘秒)，默认值为 1000；join 的取值范围 20-1000(厘秒)，默认值为 20；leave 的取值范围 60-3000(厘秒)，默认值为 60。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

将端口 6 的 leaveall 定时器设为 2000，并将 join 定时器恢复默认配置：

```
TL-SG3210(config)# interface gigabitEthernet 1/0/6
```

```
TL-SG3210(config-if)# gvrp timer leaveall 2000
```

```
TL-SG3210(config-if)# no gvrp timer join
```

7.5 show gvrp global

该命令用于显示 GVRP 全局状态。

命令

```
show gvrp global
```

模式

特权模式和所有配置模式

示例

显示 GVRP 全局状态：

```
TL-SG3210(config)# show gvrp global
```

7.6 show gvrp interface

该命令用于显示以太网端口的 GVRP 配置信息。

命令

```
show gvrp interface [ gigabitEthernet port ]
```

参数

port —— 以太网端口号，缺省时显示所有端口的 GVRP 配置信息。

模式

特权模式和所有配置模式

示例

显示所有端口的 GVRP 配置信息：

```
TL-SG3210(config)# show gvrp interface
```

显示端口 2 的 GVRP 配置信息：

```
TL-SG3210(config)# show gvrp interface gigabitEthernet 1/0/2
```

第8章 EtherChannel 配置命令

EtherChannel 配置命令用于配置 LAG 和 LACP 功能。

LAG(Link Aggregation Group,端口汇聚组)是将交换机的多个物理端口汇聚成一个逻辑端口的功能,可以增加带宽,提高连接的可靠性。

LACP (Link Aggregation Control Protocol,链路汇聚控制协议)是基于 IEEE 802.3ad 标准用来实现链路动态汇聚与解汇聚的协议。聚合的双方通过协议交互聚合信息,将匹配的链路聚合在一起收发数据,具有很高的灵活性并提供了负载均衡的能力。

8.1 channel-group

该命令用于把端口添加到汇聚组,并设置其模式。它的 no 命令用于将端口从汇聚组移除。

命令

channel-group num mode { on | active | passive }

no channel-group

参数

num —— 汇聚组组号,取值范围 1-8,最多可配置 8 个汇聚组。

on —— 开启静态 LAG。

active —— 开启主动模式 LACP。

passive —— 开启被动模式 LACP。

模式

接口配置模式 (interface gigabitEthernet / interface range gigabitEthernet)

示例

添加端口 2-4 到汇聚组 1,并开启静态 LAG 模式:

```
TL-SG3210(config)# interface range gigabitEthernet 1/0/2-4
```

```
TL-SG3210(config-if-range)# channel-group 1 mode on
```

8.2 port-channel load-balance

该命令用于选择汇聚组的负载均衡算法。它的 no 命令用于恢复默认值,即 src-dst-mac。

命令

port-channel load-balance { src-dst-mac | src-dst-ip }

no port-channel load-balance

参数

src-dst-mac —— 源目的 MAC 地址。算法将基于源目的 MAC 地址实现负载均衡。

src-dst-ip —— 源目的 IP 地址。算法将基于源目的 IP 地址实现负载均衡。

模式

全局配置模式

示例

将 LAG 的负载均衡算法设置为 src-dst-mac:

```
TL-SG3210(config)# port-channel load-balance src-dst-mac
```

8.3 lacp system-priority

该命令用于配置全局的系统优先级，它的 no 命令用于恢复默认值。

命令

lacp system-priority *pri*

no lacp system-priority

参数

pri —— 系统优先级，取值范围 0-65535。默认值为 32768。

模式

全局配置模式

示例

配置 LACP 的系统优先级为 1024:

```
TL-SG3210(config)# lacp system-priority 1024
```

8.4 lacp port-priority

该命令用于配置 LACP 端口优先级，它的 no 命令用于恢复默认值。

命令

lacp port-priority *pri*

no lacp port-priority

参数

pri —— 端口优先级，取值范围 0-65535。默认值为 32768。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

将端口 1-3 的端口优先级设置为 1024:


```
TL-SG3210(config)# interface range gigabitEthernet 1/0/1-3
```

```
TL-SG3210(config-if-range)# lacp port-priority 1024
```

将端口 4 的端口优先级设置为 2048:

```
TL-SG3210(config)# interface range gigabitEthernet 1/0/4
```

```
TL-SG3210(config-if)# lacp port-priority 2048
```

8.5 show etherchannel

该命令用于显示汇聚组信息。

命令

```
show etherchannel [ channel-group-num ] { detail | summary }
```

参数

channel-group-num —— 汇聚组组号，取值范围 1-8。该参数缺省时，显示所有组的信息。

detail —— 详述信息。

summary —— 概述信息。

模式

特权模式和所有配置模式

示例

显示汇聚组 1 的详述信息:

```
TL-SG3210 (config)# show etherchannel 1 detail
```

8.6 show etherchannel load-balance

该命令用于显示负载均衡算法。

命令

```
show etherchannel load-balance
```

模式

特权模式和所有配置模式

示例

显示负载均衡算法:

```
TL-SG3210 (config)# show etherchannel load-balance
```

8.7 show lacp

该命令用于显示特定汇聚组的 LACP 信息。

命令

show lacp [*channel-group-num*] { internal | neighbor }

参数

channel-group-num —— 组号，取值范围 1-8。该参数缺省时，显示所有 LACP 类型组的信息。

internal —— 本端 LACP 信息。

neighbor —— 对端 LACP 信息。

模式

特权模式和所有配置模式

示例

显示汇聚组 1 的本端 LACP 信息：

```
TL-SG3210 (config)# show lacp 1 internal
```

8.8 show lacp sys-id

该命令用于显示 LACP 系统优先级。

命令

show lacp sys-id

模式

特权模式和所有配置模式

示例

显示 LACP 系统优先级：

```
TL-SG3210 (config)# show lacp sys-id
```

第9章 用户管理配置命令

用户配置用来管理通过 Web、CLI 或 SSH 方式登录交换机的用户信息，以达到保护交换机配置的目的。

9.1 user name (password)

该命令用于添加一个新用户账户或修改已存在的用户账户的信息，它的 **no** 命令用于删除已存在的账户。通过此命令可以使用对称加密算法加密用户登录密码。

命令

```
user name name [ privilege admin | guest ] password { [ 0 ] password | 7 encrypted-password }
```

```
no user name name
```

参数

name —— 用户名，1-16 个字符，只能由数字、英文字母和下划线组成。

admin | guest —— 用户类型，**admin**：管理员，可以编辑、修改和查看所有不同功能的配置；**guest**：受限用户，仅能查看功能配置，无权编辑和修改。添加用户时，默认用户类型为 **admin**。

0 —— 一种加密类型，表示接下来需要输入没有进行加密的密码，**0** 为默认加密类型。

password —— 用户登录密码，由 1~31 个字符组成，密码区分大小写，允许输入数字、英文字母、下划线和十六种特殊字符（!\$%&'()*+,-./[]{}）。

7 —— 一种加密类型，表示接下来需要输入进行过对称加密的密码，此类型密码长度固定。

encrypted-password —— 固定长度的进行过对称加密的密码，可以从其他交换机的配置文件中复制得到。配置了加密密码之后，当要再次进入此模式时，需要输入相应的未加密密码。

模式

全局配置模式

说明

1. 如果在此配置的密码为未加密的密码，但通过 [service password-encryption](#) 命令启用了全局密码加密功能，那么交换机配置文件中的密码将会显示为对称加密格式。
2. 如果改变通过 Telnet 或 Console 口连接登录上交换机的当前用户的密码，那么交换机将断开当前连接，并且，用户再次登录交换机时，需要输入新设置的密码。

示例

添加并启用一个用户名为 **tplink**，密码为不加密类型 **password** 的管理员账户：

```
TL-SG3210(config)#user name tplink privilege admin password 0 admin
```

9.2 user name (secret)

该命令用于添加一个新用户账户或修改已存在的用户账户的信息，它的 **no** 命令用于删除已存在的账户。通过此命令可以使用 MD5 加密算法加密用户登录密码。

命令

```
user name name [ privilege admin | guest ] secret { [ 0 ] password | 5 encrypted-password }
```

```
no user name name
```

参数

name —— 用户名，1-16 个字符，只能由数字、英文字母和下划线组成。

admin | guest —— 用户类型，**admin**：管理员，可以编辑、修改和查看所有不同功能的配置；**guest**：受限用户，仅能查看功能配置，无权编辑和修改。添加用户时，默认用户类型为 **admin**。

0 —— 一种加密类型，表示接下来需要输入没有进行加密的密码，**0** 为默认加密类型。

password —— 用户登录密码，由 1~31 个字符组成，密码区分大小写，允许输入数字、英文字母、下划线和十六种特殊字符（!\$%&'()*~.-/[]{}）。此密码将在交换机配置文件中显示为 MD5 加密格式。

5 —— 一种加密类型，表示接下来需要输入进行过 MD5 加密的密码，此类型密码长度固定。

encrypted-password —— 固定长度的进行过 MD5 加密的密码，可以从其他交换机的配置文件中复制得到。配置了加密密码之后，当要再次进入此模式时，需要输入相应的未加密密码。

模式

全局配置模式

说明

1. 当同时配置了 **user name (password)**和 **user name (secret)**命令时，只有最后配置的密码生效。
2. 如果改变通过 **Telnet** 或 **Console** 口连接登录上交换机的当前用户的密码，那么交换机将断开当前连接，并且，用户再次登录交换机时，需要输入新设置的密码。

示例

添加并启用一个用户名为 **tplink**，密码为不加密类型 **password** 的管理员账户，且此密码将在交换机配置文件中以 MD5 加密格式显示：

```
TL-SG3210(config)#user name tplink privilege admin secret 0 admin
```

9.3 user access-control ip-based

该命令用于启用基于 IP 地址的身份限制，只有处于所设 IP 网段的设备才可以访问本交换机。它的 **no** 命令用于取消用户身份限制。

命令

```
user access-control ip-based { ip-addr ip-mask } [ snmp ] [ telnet ] [ ssh ] [ http ]  
[ https ] [ ping ] [ all ]
```

```
no user access-control
```

参数

ip-addr / ip-mask —— 源 IP 地址和 IP 掩码。只有处于所设 IP 网段的设备才可以访问本交换机。

[snmp] [telnet] [ssh] [http] [https] [ping] [all] ——指定访问接口。默认情况下启用这些接口。

模式

全局配置模式

示例

启用 IP 地址为 192.168.0.148 的身份限制：

```
TL-SG3210(config)# user access-control ip-based 192.168.0.148 255.255.255.255
```

9.4 user access-control mac-based

该命令用于启用基于 MAC 地址的身份限制，只允许所设的 MAC 地址通过 Web 访问交换机。

命令

```
user access-control mac-based { mac-addr } [ snmp ] [ telnet ] [ ssh ] [ http ] [ https ]  
[ ping ] [ all ]
```

```
no user access-control
```

参数

mac-addr —— 源 MAC 地址。只有拥有该 MAC 地址的设备才可以访问本交换机。

[snmp] [telnet] [ssh] [http] [https] [ping] [all] ——指定访问接口。默认情况下启用这些接口。

模式

全局配置模式

示例

启用 MAC 地址为 00:00:13:0A:00:01 的身份限制：

```
TL-SG3210(config)# user access-control mac-based 00:00:13:0A:00:01
```

9.5 user access-control port-based

该命令用于启用基于端口的身份限制，只允许连接在所设的端口上的主机通过 WEB 访问交换机。

命令

```
user access-control port-based interface { gigabitEthernet port | range  
gigabitEthernet port-list } [ snmp ] [ telnet ] [ ssh ] [ http ] [ https ] [ ping ] [ all ]
```

```
no user access-control
```

参数

port —— 以太网端口号。

port-list —— 以太网端口列表，最多可指定 5 个端口。

[snmp] [telnet] [ssh] [http] [https] [ping] [all] ——指定访问接口。默认情况下启用这些接口。

模式

全局配置模式

示例

启用 2-6 五个端口的身份限制：

```
TL-SG3210(config)# user access-control port-based interface range  
gigabitEthernet 1/0/2-6
```

9.6 line

该命令用于进入 line 配置模式，以配置用户的登录模式及连接密码等参数。

命令

```
line [ console linenum | vty startlinenum endlinenum ]
```

参数

linenum —— 指定需要配置的 Console 口的端口号，本交换机只有一个 Console 口，故该值为 0。

startlinenum —— 指定需要配置的虚拟终端连接的起始序号，取值范围为 0-15。0 表示从第一个通过 Telnet 或 SSH 登录的用户开始，配置生效；1 表示从第二个登录的用户开始，并依次类推。

endlinenum ——指定需要配置的虚拟终端连接的结束序号，取值范围为 0-15，并且不能小于 **startlinenum**。0 表示配置只对第一个通过 Telnet 或 SSH 登录的用户有效；1 表示到第二个登录的用户为止，配置有效，并依次类推。

模式

全局配置模式

示例

进入 Console 端口配置模式以配置 Console 口的连接密码等参数：

```
TL-SG3210(config)# line console 0
```

进入虚拟终端配置模式，配置前 6 个通过 Telnet 或 SSH 连接的用户的登录模式及连接密码等参数：

```
TL-SG3210(config)# line vty 0 5
```

9.7 password

该命令用于配置连接密码，它的 no 命令用于清除密码。

命令

password {[0] password | 7 encrypted-password }

no password

参数

0 —— 一种加密类型，表示接下来需要输入没有进行加密的密码，0 为默认加密类型。

password —— 配置连接密码，由 1~31 个字符组成，密码区分大小写，允许输入数字、英文字母、下划线和十六种特殊字符（!\$%&'()*,-./[]{}）。默认为空。

7 —— 一种加密类型，表示接下来需要输入进行过对称加密的密码，此类型密码长度固定。

encrypted-password —— 固定长度的进行过对称加密的密码，可以从其他交换机的配置文件中复制得到。配置了加密密码之后，当要再次进入此模式时，需要输入相应的未加密密码。

模式

line 配置模式

说明

如果在此配置的密码为未加密的密码，但通过 [service password-encryption](#) 命令启用了全局密码加密功能，那么交换机配置文件中的密码将会显示为对称加密格式。

示例

配置 Console 端口 0 的连接密码为不加密密码 `tplink`:

```
TL-SG3210(config)# line console 0
TL-SG3210(config-line)# password 0 tplink
```

配置虚拟终端连接 0-5 的连接密码为不加密密码 `tplink`:

```
TL-SG3210(config)# line vty 0 5
TL-SG3210(config-line)# password 0 tplink
```

9.8 login

该命令用于设置交换机登录模式为 `login` 模式，即无需输入登录用户名和密码，但是需要输入一个连接密码才能建立 Telnet 连接进行访问。

命令

login

模式

Line 配置模式

示例

配置 Console 端口 0 的连接模式为 `login`:

```
TL-SG3210(config)# line console 0
TL-SG3210(config-line)# login
```

配置建立 Telnet 连接的模式为 `login`:

```
TL-SG3210(config)# line vty 0 5
TL-SG3210(config-line)# login
```

9.9 login local

该命令用于设置交换机登录模式为 `login local` 模式，即输入用户名和密码登录，默认用户名/密码为 `admin/admin`。

命令

login local

模式

Line 配置模式

示例

配置 Console 端口 0 的连接模式为 `login local`:


```
TL-SG3210(config)# line console 0
```

```
TL-SG3210(config-line)# login local
```

配置建立 Telnet 连接的模式为 login local:

```
TL-SG3210(config)# line vty 0 5
```

```
TL-SG3210(config-line)# login local
```

9.10 telnet

该命令用于 Telnet 登录功能的开启和关闭，telnet enable 表示开启功能，telnet disable 表示关闭功能。默认状态为 enable。

命令

```
telnet enable
```

```
telnet disable
```

模式

全局配置模式

示例

关闭 Telnet 功能:

```
TL-SG3210(config)# telnet disable
```

9.11 show telnet-status

该命令用于显示 Telnet 功能配置信息。

命令

```
show telnet-status
```

模式

特权模式和所有配置模式

示例

显示 Telnet 功能是否启用:

```
TL-SG3210(config)# show telnet-status
```

9.12 show user account-list

该命令用于显示当前用户账户列表。

命令

```
show user account-list
```

模式

特权模式和所有配置模式

示例

显示当前用户账户列表：

```
TL-SG3210(config)# show user account-list
```

9.13 show user configuration

该命令用于显示用户安全配置，包括身份限制，登录数限制，超时配置等。

命令

show user configuration

模式

特权模式和所有配置模式

示例

显示用户安全配置：

```
TL-SG3210(config)# show user configuration
```

第10章 HTTP 和 HTTPS 配置命令

在 HTTP(HyperText Transfer Protocol,超文本传输协议)或者 HTTPS(Hyper Text Transfer Protocol over Secure Socket Layer, 基于安全套接层的超文本传输协议)帮助下,可以通过一个标准的浏览器管理交换机。HTTP 是用于交换和发送超文本内容的协议。

SSL(Secure Sockets Layer,安全套接层)是一个安全协议,它为基于 TCP 的应用层协议(如 HTTP)提供安全连接。SSL 采用非对称加密技术,用密钥对进行信息的加密/解密,密钥对由一个公钥(包含在证书中)和一个私钥构成。初始时交换机里已有默认的证书(自签名证书)和对应私钥,用户也可以通过证书/密钥导入功能替换默认的密钥对。

10.1 ip http server

该命令用于全局开启 HTTP 服务器功能,它的 no 命令用于禁用该功能。默认情况下启用此功能。HTTP 和 HTTPS 服务器不能同时禁用。

命令

ip http server

no ip http server

模式

全局配置模式

示例

关闭 HTTP 功能:

```
TL-SG3210(config)# no ip http server
```

10.2 ip http max-users

该命令用于配置允许连接到HTTP服务器的最大用户数,它的no命令用于取消限制。

命令

ip http max-users *admin-num* *guest-num*

no ip http max-users

参数

admin-num ——以管理员身份登录到 HTTP 服务器的最大数量,范围从 1 到 16。管理员和访客的总数应该少于 16。

guest-num ——在访客身份登录到 HTTP 服务器的最大数量,范围从 0 到 15。管理员和访客的总数应小于 16。

模式

全局配置模式

示例

配置管理员和访客登录到 HTTP 服务器的最大数量为 5 和 3:

```
TL-SG3210(config)# ip http max-users 5 3
```

10.3 ip http session timeout

该命令用于配置 HTTP 服务器的连接超时时间。它的 **no** 命令可以恢复出厂默认的超时时间，默认的超时时间为 10 分钟。

命令

```
ip http session timeout minutes
```

```
no ip http session timeout
```

参数

minutes ——超时时间，范围从 5 到 30 分钟。默认情况下，该值为 10。

模式

全局配置模式

示例

配置 HTTP 连接超时时间为 15 分钟:

```
TL-SG3210(config)# ip http session timeout 15
```

10.4 ip http secure-server

该命令用于全局开启 SSL 功能，它的 **no** 命令用于禁用该功能。默认情况下启用此功能。HTTP 和 HTTPS 服务器不能同时禁用。

命令

```
ip http secure-server
```

```
no ip http secure-server
```

模式

全局配置模式

示例

全局关闭 SSL 功能:

```
TL-SG3210(config)# no ip http secure-server
```

10.5 ip http secure-protocol

该命令用于配置 SSL 协议版本，它的 no 命令用于恢复默认 SSL 版本。默认情况下，交换机支持 SSLv3 和 TLSv1。

命令

```
ip http secure-protocol { [ ssl3 ] [ tls1 ] }  
no ip http session
```

参数

ssl3 ——SSL 3.0 协议。

tls1 ——TLS 1.0 协议。

模式

全局配置模式

示例

配置 SSL 连接使用的协议为 SSL 3.0:

```
TL-SG3210(config)# ip http secure-protocol ssl3
```

10.6 ip http secure-ciphersuite

该命令用于配置交换机支持的 SSL 连接的密码套件，它的 no 命令用于恢复默认密码套件。

命令

```
ip http secure-ciphersuite { [ 3des-ede-cbc-sha ] [ rc4-128-md5 ] [ rc4-128-sha ]  
[ des-cbc-sha ] }  
no ip http secure-ciphersuite
```

参数

[3des-ede-cbc-sha] [rc4-128-md5] [rc4-128-sha] [des-cbc-sha] ——指定 SSL 连接使用的加密算法和摘要算法。

默认情况下，交换机支持所有这些密码套件。

模式

全局配置模式

示例

配置 SSL 连接使用的密码套件为 3des-ede-cbc-sha:

```
TL-SG3210(config)# ip http secure-ciphersuite 3des-ede-cbc-sha
```

10.7 ip http secure-max-users

该命令用于配置允许登录 HTTPS 服务器的最大用户数，它的 no 命令用于取消限制。

命令

ip http secure-max-users *admin-num guest-num*
no ip secure-max-users

参数

admin-num ——以管理员身份登录到 HTTPS 服务器的最大数量，范围从 1 到 16。管理员和访客的总数应该少于 16。

guest-num ——在访客身份登录到 HTTPS 服务器的最大数量，范围从 0 到 15。管理员和访客的总数应小于 16。

模式

全局配置模式

示例

配置管理员和访客登录到 HTTPS 服务器的最大数量为 5 和 3:

```
TL-SG3210(config)# ip secure-max-users 5 3
```

10.8 ip http secure-session timeout

该命令用于配置 HTTPS 服务器的连接超时时间。它的 no 命令可以恢复出厂默认的超时时间，默认的超时时间为 10 分钟。

命令

ip http secure-session timeout *minutes*
no ip http secure-session timeout

参数

minutes ——超时时间，范围从 5 到 30 分钟。默认情况下，该值为 10。

模式

全局配置模式

示例

配置 HTTPS 连接超时时间为 15 分钟:

```
TL-SG3210(config)# ip http secure-session timeout 15
```

10.9 ip http secure-server download certificate

该命令用于通过 TFTP 方式导入 SSL 证书。

命令

ip http secure-server download certificate *ssl-cert ip-address ip-addr*

参数

ssl-cert —— 选择要导入的 SSL 证书名称，可输入 1~25 个字符。证书必须为 BASE64 编码格式。

ip-addr —— TFTP 服务器的 IP 地址。支持 IPv4 和 IPv6 地址。例如 IPv4 地址 192.168.0.10，IPv6 地址 fe80::1234。

模式

全局配置模式

示例

通过 IP 地址为 192.168.0.148 的 TFTP 服务器导入名为 ssl.cert 的 SSL 证书：

```
TL-SG3210(config)# ip http secure-server download certificate ssl.cert ip-address  
192.168.0.148
```

通过 IP 地址为 fe80::1234 的 TFTP 服务器导入名为 ssl.cert 的 SSL 证书：

```
TL-SG3210(config)# ip http secure-server download certificate ssl.cert ip-address  
fe80::1234
```

10.10 ip http secure-server download key

该命令用于通过 TFTP 方式导入 SSL 密钥。

命令

ip http secure-server download key *ssl-key* *ip-address* *ip-addr*

参数

ssl-key —— 选择要导入的 SSL 密钥文件名称，可输入 1~25 个字符。密钥必须为 BASE64 编码格式。

ip-addr —— TFTP 服务器的 IP 地址。支持 IPv4 和 IPv6 地址。例如 IPv4 地址 192.168.0.10，IPv6 地址 fe80::1234。

模式

全局配置模式

示例

通过 IP 地址为 192.168.0.148 的 TFTP 服务器导入名为 ssl.key 的 SSL 密钥：

```
TL-SG3210(config)# ip http secure-server download key ssl.key ip-address  
192.168.0.148
```

通过 IP 地址为 fe80::1234 的 TFTP 服务器导入名为 ssl.key 的 SSL 密钥：

```
TL-SG3210(config)# ip http secure-server download key ssl.key ip-address  
fe80::1234
```

10.11 show ip http configuration

该命令是用来显示的 HTTP 服务器的配置信息，包括状态、会话超时时间、访问控制、最大用户数和空闲超时时间等。

命令

```
show ip http configuration
```

模式

特权模式和所有配置模式

示例

显示 HTTP 服务器的配置信息：

```
TL-SG3210(config)# show ip http configuration
```

10.12 show ip http secure-server

该命令用于显示 SSL 的全局配置信息。

命令

```
show ip http secure-server
```

模式

特权模式和所有配置模式

示例

显示 SSL 全局配置信息：

```
TL-SG3210(config)# show ip http secure-server
```


第11章 绑定列表配置命令

四元绑定功能可以将局域网中计算机的 IP 地址、MAC 地址、VLAN 和端口进行绑定，ARP 防护功能将使用四元绑定条目对数据包进行过滤。

11.1 ip source binding

该命令用于手动添加 IP-MAC-VID-PORT 四元绑定条目。如果已经掌握了局域网中计算机用户的相关信息，包括 IP 地址、MAC 地址、VLAN 以及连接端口等，可以手动四元绑定。

命令

```
ip source binding hostname ip-addr mac-addr vlan vid interface gigabitEthernet  
port { none | arp-detection } [ forced-source { arp-scanning | dhcp-snooping } ]  
no ip source binding index idx
```

参数

hostname —— 需要绑定的主机名，1-20 个字符。

ip-addr —— 源 IP 地址。

mac-addr —— 源 MAC 地址。

vid —— 需要绑定的 VLAN，取值范围 1-4094。

port —— 需要绑定的交换机端口号。

none | arp-detection —— 该条目执行的 ACL 动作，arp-detection 表示 ARP 防护；none 表示不应用 ARP 防护。

arp-scanning | dhcp-snooping —— 可选参数 forced-source 用于强制将新添加条目的来源从 manual 修改为 arp-scanning 或者 dhcp-snooping，以模拟 arp-scan 或 dhcp-snooping 添加绑定条目，使非手动绑定条目可以保存配置。

idx —— 指定要删除的条目序号。可使用命令 [show ip source binding](#) 获取各条目对应的序号。注意，这里的序号是指该条目在绑定表中的序号，故显示时不一定是按习惯上的从小到大递增的顺序，而是显示该条目在绑定表中的实际序号。

模式

全局配置模式

示例

手动添加一条四元绑定条目，主机名为 host1，IP 地址为 192.168.0.1，MAC 地址为 00:00:00:00:00:01，VID 为 2，端口号为 5，并将该条目同时应用于 ARP 防护：

```
TL-SG3210(config)# ip source binding host1 192.168.0.1 00:00:00:00:00:01 vlan 2  
interface gigabitEthernet 1/0/5 arp-detection
```

删除绑定表中序号为 5 的 IP-MAC-VID-PORT 条目：

```
TL-SG3210(config)# no ip source binding index 5
```

11.2 ip source binding index

该命令用于修改已有 IP-MAC-VID-PORT 四元绑定条目。

命令

```
ip source binding index idx {hostname hostname | mac mac-addr | vlan vlan-id |  
interface gigabitEthernet port | none | arp-detection }
```

参数

idx —— 指定要修改的条目序号。可使用命令 [show ip source binding](#) 获取各条目对应的序号。注意，这里的序号是指该条目在绑定表中的序号，故显示时不一定是按习惯上的从小到大递增的顺序，而是显示该条目在绑定表中的实际序号。

hostname —— 需要修改的主机名，1-20 个字符。

mac-addr —— 源 MAC 地址。

vlan-id —— 需要修改的 VLAN，取值范围 1-4094。

port —— 需要修改的交换机端口号。

none | arp-detection —— 该条目执行的 ACL 动作，arp-detection 表示 ARP 防护；none 表示不应用 ARP 防护。

模式

全局配置模式

示例

修改条目序号为 1，主机名为 tp-link 的四元绑定条目：

```
TL-SG3210(config)#ip source binding index 1 hostname tp-link
```

11.3 ip dhcp snooping

该命令用于全局开启 DHCP 侦听功能，它的 no 命令用于禁用 DHCP Snooping。通过 DHCP 侦听功能，交换机可以侦听用户动态申请 IP 地址的过程，并记录局域网中计算机的 IP 地址、MAC 地址、VLAN 以及连接端口等信息，自动进行四元绑定。

命令

```
ip dhcp snooping
```

```
no ip dhcp snooping
```

模式

全局配置模式

示例

全局开启 DHCP Snooping:

```
TL-SG3210(config)# ip dhcp snooping
```

11.4 ip dhcp snooping global

该命令用于 DHCP Snooping 全局配置，它的 no 命令用于恢复默认配置。

命令

```
ip dhcp snooping global { [global-rate global-rate] [dec-threshold dec-threshold]
[dec-rate dec-rate] }
```

```
no ip dhcp snooping global
```

参数

global-rate —— 全局流量控制，配置交换机每秒允许转发的 DHCP 消息的数目，超出的部分将被丢弃，可选项为 0、10、20、30、40、50，单位 pps（packet/second）。默认值为 0，表示禁用。

dec-threshold —— Decline 保护阈值，配置触发特定端口 Decline 保护所需的 Decline 报文最小流量，可选项为 0、5、10、15、20、25、30，单位 pps（packet/ second）。默认值为 0，表示禁用。

dec-rate —— Decline 保护流量限制，如果端口 Decline 消息流量超出阈值，则将相应端口的端口流量限制设置为该值，可选项为 5、10、15、20、25、30，单位 pps（packet/second）。默认值为 5。

模式

全局配置模式

示例

配置 DHCP Snooping 全局流量控制为 30 pps，Decline 保护阈值为 20 pps，Decline 保护流量阈值为 20 pps:

```
TL-SG3210(config)# ip dhcp snooping global global-rate 30 dec-threshold 20
dec-rate 20
```

11.5 ip dhcp snooping information option

该命令用于开启 DHCP Snooping 的 Option 82 功能，它的 no 命令用于关闭 Option 82 功能。

命令

```
ip dhcp snooping information option
```

```
no ip dhcp snooping information option
```

模式

全局配置模式

示例

开启 DHCP Snooping 的 Option 82 功能：

```
TL-SG3210(config)# ip dhcp snooping information option
```

11.6 ip dhcp snooping information strategy

该命令用于选择对接收到的包含 Option 82 选项请求报文的配置处理策略，它的 no 命令用于恢复默认选项。

命令

ip dhcp snooping information strategy { keep | replace | drop }

no ip dhcp snooping information strategy

参数

keep —— 保持该报文中的 Option 82 选项不变并进行转发。默认选项。

replace ——按照配置的填充内容填充 Option 82 选项，并替换报文中原有的 Option 82 选项进行转发。

drop —— 丢弃该报文。

模式

全局配置模式

示例

将接收到的请求报文的 Option 82 选项替换为用户自定义的选项内容，并进行转发：

```
TL-SG3210(config)# ip dhcp snooping information strategy replace
```

11.7 ip dhcp snooping information remote-id

该命令用于配置 Option 82 的 Remote ID 子选项内容。no 命令用于恢复默认值。

命令

ip dhcp snooping information remote-id *string*

no ip dhcp snooping information remote-id

参数

string —— 用户自定义配置的 Remote ID 子选项内容。长度为 1-32 个字符。

模式

全局配置模式

示例

配置 Option 82 的 Remote ID 子选项为 tpink:

```
TL-SG3210(config)# ip dhcp snooping information remote-id tpink
```

11.8 ip dhcp snooping information circuit-id

该命令用于配置 Option 82 的 Circuit ID 子选项内容。no 命令用于恢复默认值。

命令

ip dhcp snooping information circuit-id *string*

no ip dhcp snooping information circuit-id

参数

string —— 用户自定义配置的 Circuit ID 子选项内容。长度为 1-32 个字符。

模式

全局配置模式

示例

配置 Option 82 的 Circuit ID 子选项为 tpink:

```
TL-SG3210(config)# ip dhcp snooping information circuit-id tpink
```

11.9 ip dhcp snooping trust

该命令用于配置端口为授信端口，只有授信端口才能接收来自 DHCP 服务器端的消息，它的 no 命令用于取消授信端口配置。

命令

ip dhcp snooping trust

no ip dhcp snooping trust

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

启用交换机端口 2 为授信端口：

```
TL-SG3210(config)# interface gigabitEthernet 1/0/2
```

```
TL-SG3210(config-if)# ip dhcp snooping trust
```

11.10 ip dhcp snooping mac-verify

该命令用于启用端口的 MAC 验证功能，它的 no 命令用于禁用 MAC 验证。DHCP 消息中有两个字段存储着客户端的 MAC 地址，MAC 验证功能会对这两个字段进行比较，如果不同，则将消息丢弃。

命令

ip dhcp snooping mac-verify
no ip dhcp snooping mac-verify

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

启用端口 2 的 MAC 验证功能：

```
TL-SG3210(config)# interface gigabitEthernet 1/0/2
TL-SG3210(config-if)# ip dhcp snooping mac-verify
```

11.11 ip dhcp snooping limit rate

该命令用于配置端口的流量控制，超出流量部分的 DHCP 数据包将被丢弃，它的 no 命令用于恢复默认配置。

命令

ip dhcp snooping limit rate value
no ip dhcp snooping limit rate

参数

value —— 端口流量控制，可选项为 0、5、10、15、20、25、30，单位 pps（packet per second）。默认值为 0，表示禁用。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

将端口 2 的流量控制设为 20pps：

```
TL-SG3210(config)# interface gigabitEthernet 1/0/2
TL-SG3210(config-if)# ip dhcp snooping limit rate 20
```

11.12 ip dhcp snooping decline

该命令用于启用端口的 decline 侦听功能，它的 no 命令用于禁用 decline 侦听。

命令

ip dhcp snooping decline
no ip dhcp snooping decline

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

启用端口 2 的 decline 侦听功能：

```
TL-SG3210(config)# interface gigabitEthernet 1/0/2
TL-SG3210(config-if)# ip dhcp snooping decline
```

11.13 show ip source binding

该命令用于显示 IP-MAC-VID-PORT 四元绑定表。

命令

show ip source binding

模式

特权模式和所有配置模式

示例

显示 IP-MAC-VID-PORT 四元绑定表：

```
TL-SG3210(config)# show ip source binding
```

11.14 show ip dhcp snooping

该命令用于显示 DHCP Snooping 当前状态信息。

命令

show ip dhcp snooping

模式

特权模式和所有配置模式

示例

显示 DHCP Snooping 当前状态信息：

```
TL-SG3210(config)# show ip dhcp snooping
```

11.15 show ip dhcp snooping information

该命令用于显示 DHCP Snooping 的 Option 82 选项配置。

命令

show ip dhcp snooping information

模式

特权模式和所有配置模式

示例

显示 DHCP Snooping 的 Option 82 选项配置：

```
TL-SG3210# show ip dhcp snooping information
```

11.16 show ip dhcp snooping interface

该命令用于显示 DHCP Snooping 端口配置信息。

命令

```
show ip dhcp snooping interface [ gigabitEthernet port ]
```

参数

port —— 交换机端口号，缺省时显示所有端口的配置信息。

模式

特权模式和所有配置模式

示例

显示所有端口的 DHCP Snooping 配置信息：

```
TL-SG3210# show ip dhcp snooping interface
```


第12章 ARP 防护配置命令

防 ARP 欺骗功能可以针对局域网中常见的网关欺骗和中间人攻击等 ARP 欺骗进行防护，有效抑制局域网中的 ARP 欺骗。

12.1 ip arp inspection(global)

该命令用于全局开启 ARP 防护，它的 no 命令用于禁用 ARP 防护功能。

命令

```
ip arp inspection
no ip arp inspection
```

模式

全局配置模式

示例

全局开启 ARP 防护：

```
TL-SG3210(config)# ip arp inspection
```

12.2 ip arp inspection trust

该命令用于配置 ARP 防护的信任端口，它的 no 命令用于清空信任端口列表。上联端口、路由端口以及 LAG 端口等特殊端口均应配置为信任端口。在启用防 ARP 欺骗功能之前，应先配置 ARP 信任端口，以免影响正常通信。

命令

```
ip arp inspection trust
no ip arp inspection trust
```

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

配置端口 2 为 ARP 防护的信任端口：

```
TL-SG3210(config)# interface gigabitEthernet 1/0/2
TL-SG3210(config-if)# ip arp inspection trust
```

12.3 ip arp inspection (interface)

该命令用于开启端口的 ARP 防护功能，它的 no 命令用于禁用 ARP 防护功能。

命令

ip arp inspection
no ip arp inspection

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

开启端口 2-6 的 ARP 防护功能：

```
TL-SG3210(config)# interface range gigabitEthernet 1/0/2-6
TL-SG3210(config-if-range)# ip arp inspection
```

12.4 ip arp inspection limit-rate

该命令用于配置端口的 ARP 超速速率，它的 no 命令用于恢复默认超速速率。

命令

ip arp inspection limit-rate *value*
no ip arp inspection limit-rate

参数

value —— 超速速率值，取值范围 10-100，单位 pps（packet/second）。默认值为 15。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

将端口 5 的 ARP 超速速率设置为 50pps：

```
TL-SG3210(config)# interface gigabitEthernet 1/0/5
TL-SG3210(config-if)# ip arp inspection limit-rate 50
```

12.5 ip arp inspection recover

该命令用于将处于 ARP 过滤状态的端口恢复为 ARP 转发状态。

命令

ip arp inspection recover

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

将端口 5 恢复为 ARP 转发状态：

```
TL-SG3210(config)# interface gigabitEthernet 1/0/5
TL-SG3210(config-if)# ip arp inspection recover
```

12.6 show ip arp inspection

该命令用于显示 ARP 防护全局配置，包括启用状态和信任端口列表。

命令

```
show ip arp inspection
```

模式

特权模式和所有配置模式

示例

显示 ARP 防护全局配置：

```
TL-SG3210(config)# show ip arp inspection
```

12.7 show ip arp inspection interface

该命令用于显示 ARP 防护端口配置信息。

命令

```
show ip arp inspection interface [ gigabitEthernet port ]
```

参数

port—— 交换机端口号，缺省时显示所有端口的配置信息。

模式

特权模式和所有配置模式

示例

显示所有端口的 ARP 防护配置信息：

```
TL-SG3210(config)# show ip arp inspection interface
```

显示端口 2 的配置：

```
TL-SG3210(config)# show ip arp inspection interface gigabitEthernet 1/0/2
```

12.8 show ip arp inspection statistics

该命令用于显示 ARP 非法报文统计。

命令

```
show ip arp inspection statistics
```

模式

特权模式和所有配置模式

示例

显示 ARP 非法报文统计：

```
TL-SG3210(config)# show ip arp inspection statistics
```

12.9 clear ip arp inspection statistics

该命令用于对 ARP 非法报文统计进行清零。

命令

clear ip arp inspection statistics

模式

特权模式和所有配置模式

示例

对 ARP 非法报文统计进行清零：

```
TL-SG3210(config)# clear ip arp inspection statistics
```

第13章 DoS 防护命令

DoS 攻击是指网络中攻击者或者恶意程序向目标主机发送大量的服务请求，恶意消耗网络资源。启用 DoS 防护功能后，交换机对收到的特殊数据包的特定字段进行解析，并针对这些信息定义防护措施，从而保护局域网的正常运行。

13.1 ip dos-prevent

该命令用于全局启用 DoS 防护功能，它的 no 命令用于禁用 DoS 防护功能。

命令

ip dos-prevent

no ip dos-prevent

模式

全局配置模式

示例

全局启用 DoS 防护功能：

```
TL-SG3210(config)# ip dos-prevent
```

13.2 ip dos-prevent type

该命令用于选择启用 DoS 攻击防护类型，它的 no 命令用于禁用相应的防护类型。

命令

ip dos-prevent type { land | scan-synfin | xma-scan | null-scan | port-less-1024 | blat | ping-flood | syn-flood }

no ip dos-prevent type { land | scan-synfin | xma-scan | null-scan | port-less-1024 | blat | ping-flood | syn-flood }

参数

land —— Land 攻击。

scan-synfin —— Scan SYNFIN 攻击。

xma-scan —— Xma Scan 攻击。

null-scan —— NULL Scan 攻击。

port-less-1024 —— 源端口小于 1024 的 SYN 报文。

blat —— Blat 攻击。

ping-flood —— Ping flooding 攻击。

syn-flood —— SYN/SYN-ACK flooding 攻击。

模式

全局配置模式

示例

启用 Land 攻击防护功能：

```
TL-SG3210(config)# ip dos-prevent type land
```

13.3 show ip dos-prevent

该命令用于显示 DoS 攻击防护全局配置信息，包括启用状态、攻击防护类型、攻击次数统计等。

命令

show ip dos-prevent

模式

特权模式和所有配置模式

示例

显示 DoS 攻击防护全局配置信息：

```
TL-SG3210(config)# show ip dos-prevent
```

第14章 IEEE 802.1X 配置命令

IEEE 802.1X 能为局域网计算机提供认证功能，并根据认证结果对受控端口的授权状态进行控制，主要用于解决以太网内认证和安全方面的问题。

14.1 dot1x system-auth-control

该命令用于全局开启 IEEE 802.1X 功能，它的 no 命令用于禁用 IEEE 802.1X 功能。

命令

```
dot1x system-auth-control
no dot1x system-auth-control
```

模式

全局配置模式

示例

开启 IEEE 802.1X 功能：

```
TL-SG3210(config)# dot1x system-auth-control
```

14.2 dot1x auth-method

该命令用于配置 IEEE 802.1X 的认证方法，它的 no 命令用于恢复默认配置。

命令

```
dot1x auth-method { pap | eap-md5 }
no dot1x auth-method
```

参数

pap | eap-md5 —— 认证方法。选择 pap 时，用户端与交换机之间运行 EAP 协议，交换机将 EAP 消息转换为其它认证协议（如 RADIUS），传递用户认证信息给认证服务器系统。选择 eap-md5 时，交换机与认证服务器之间运行 EAP 协议，EAP 帧中继封装认证数据，将该协议承载在其它高层次协议中（如 RADIUS），以便穿越复杂的网络到达认证服务器。默认选项为 eap-md5。

模式

全局配置模式

示例

设置 IEEE 802.1X 认证方法为 pap：

```
TL-SG3210(config)# dot1x auth-method pap
```

14.3 dot1x guest-vlan(global)

该命令用于全局开启 Guest VLAN 功能，它的 no 命令用于全局禁用 Guest VLAN 功能。

命令

dot1x guest-vlan *vid*

no dot1x guest-vlan

参数

vid —— 启用 Guest VLAN 的 VLAN ID，取值范围 1~4094。Guest VLAN 中的用户可以访问指定的网络资源。

模式

全局配置模式

示例

启用 VLAN 5 为 Guest VLAN：

```
TL-SG3210(config)# dot1x guest-vlan 5
```

14.4 dot1x quiet-period

该命令用于开启 IEEE 802.1X 特性的静默功能，它的 no 命令用于关闭该功能。

命令

dot1x quiet-period

no dot1x quiet-period

模式

全局配置模式

示例

开启 IEEE 802.1X 静默功能：

```
TL-SG3210(config)# dot1x quiet-period
```

14.5 dot1x timeout

该命令用于配置静默时长、客户端响应超时时长，它的 no 命令用于恢复默认配置。

命令

dot1x timeout { quiet-period *time* | reauth-period *time* }

no dot1x timeout { quiet-period | reauth-period }

参数

quiet-period time —— 静默时长。用户认证失败后，在静默时间内不再处理同一用户的 IEEE 802.1X 认证请求。取值范围 1~999（秒），默认值为 10。

reauth-period time —— 客户端响应超时时长，即交换机等待客户端响应的最大等待时间。若交换机在设定时间内没有收到客户端的回复，则重发报文。取值范围 1~9（秒），默认值为 3。

模式

全局配置模式

示例

设置静默时长为 12 秒：

```
TL-SG3210(config)# dot1x timeout quiet-period 12
```

14.6 dot1x max-reauth-req

该命令用于配置客户端请求报文重复发送次数，它的 no 命令用于恢复默认设置。

命令

dot1x max-reauth-req times

no dot1x max-reauth-req

参数

times —— 认证报文的最大重复发送次数，取值范围 1~9（次），默认值为 3。

模式

全局配置模式

示例

设置最大重复发送次数为 5：

```
TL-SG3210(config)# dot1x max-reauth-req 5
```

14.7 dot1x

该命令用于开启端口的 IEEE 802.1X 特性，它的 no 命令用于禁用端口的 IEEE 802.1X 特性。

命令

dot1x

no dot1x

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

开启端口 1 的 IEEE 802.1X 特性：

```
TL-SG3210(config)# interface gigabitEthernet 1/0/1
TL-SG3210(config-if)# dot1x
```

14.8 dot1x guest-vlan(interface)

该命令用于开启端口的 Guest VLAN 功能，它的 no 命令用于禁用端口的 Guest VLAN 功能。在开启端口的 Guest VLAN 功能前，请确保相应端口的接入控制类型为 port-based，详见 [dot1x port-method](#)。

命令

```
dot1x guest-vlan
no dot1x guest-vlan
```

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

开启端口 2 的 Guest VLAN 功能：

```
TL-SG3210(config)# interface gigabitEthernet 1/0/2
TL-SG3210(config-if)# dot1x guest-vlan
```

14.9 dot1x port-control

该命令用于配置 IEEE 802.1X 在指定端口的接入控制模式，它的 no 命令用于恢复默认配置。

命令

```
dot1x port-control { auto | authorized-force | unauthorized-force }
no dot1x port-control
```

参数

auto | authorized-force | unauthorized-force —— 控制模式，有 auto（自动）、authorized-force（强制已认证）、unauthorized-force（强制不认证）三个选项。选择 auto 时，端口需要进行认证；选择 authorized-force 时，端口不需认证即可访问网络；选择 unauthorized-force 时，端口永远无法通过认证。默认选项为 auto。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

设置端口 1 的接入控制模式为强制已认证：

```
TL-SG3210(config)# interface gigabitEthernet 1/0/1
TL-SG3210(config-if)# dot1x port-control authorized-force
```

14.10 dot1x port-method

该命令用于配置 IEEE 802.1X 在指定端口的接入控制类型，它的 no 命令用于恢复默认配置。

命令

```
dot1x port-method { mac-based | port-based }
```

```
no dot1x port-method
```

参数

mac-based | port-based —— 控制类型，有 mac-based（基于 MAC）和 port-based（基于 Port）两个选项。选择 mac-based 时，该端口连接的所有计算机都需认证；选择 port-based 时，该端口连接的某个用户通过认证后，其他用户均无须认证即可访问网络。默认选项为 mac-based。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

设置端口 5 的接入控制类型为基于 Port 认证：

```
TL-SG3210(config)# interface gigabitEthernet 1/0/5
```

```
TL-SG3210(config-if)# dot1x port-method port-based
```

14.11 radius

该命令用于配置主认证服务器的相关参数。认证服务器是为交换机提供认证服务的实体。认证服务器可以存储有关用户的信息，包括用户名、密码以及其它参数，用于实现对用户的认证、授权和计费，通常为 RADIUS（Remote Authentication Dial-In User Service，远程认证拨号用户服务）服务器。

命令

```
radius { [auth-pri ip] [auth-sec ip] [auth-port port] [acct-pri ip] [acct-sec ip]  
[acct-port port] [auth-key { [ 0 ] password | 7 encrypted-password } ] [acct-key { [ 0 ]  
password | 7 encrypted-password } ] }
```

```
no radius { auth-port | auth-key | auth-pri | auth-sec | acct-port | acct-key | acct-pri |  
acct-sec }
```

参数

auth-pri ip —— 主认证服务器的 IP 地址。

auth-sec ip —— 备份认证服务器的 IP 地址。

auth-port port —— 认证服务器提供认证服务的协议端口。取值范围 1~65535，默认值为 1812。

acct-pri ip —— 主计费服务器的 IP 地址。

acct-sec ip —— 备份计费服务器的 IP 地址。

acct-port port —— 计费服务器提供计费服务的协议端口。取值范围 1~65535，默认值为 1813。

auth-key { [0] password | 7 encrypted-password } —— 授权共享密钥，即交换机与服务器共享的密钥。

0: 一种加密类型，表示接下来需要输入没有进行加密的密码，0 为默认加密类型。

password: 授权共享密钥，由 1~31 个字符组成，不允许输入问号和空格。

7: 一种加密类型，表示接下来需要输入进行过对称加密的密码，此类型密码长度固定。

encrypted-password: 固定长度的进行过对称加密的密码，可以从其他交换机的配置文件中复制得到。

在此设置的 **password** 或 **encrypted-password** 将以对称加密格式显示。

acct-key { [0] password | 7 encrypted-password } —— 授权共享密钥，即交换机与服务器共享的密钥。

0: 一种加密类型，表示接下来需要输入没有进行加密的密码，0 为默认加密类型。

password: 授权共享密钥，由 1~31 个字符组成，不允许输入问号和空格。

7: 一种加密类型，表示接下来需要输入进行过对称加密的密码，此类型密码长度固定。

encrypted-password: 固定长度的进行过对称加密的密码，可以从其他交换机的配置文件中复制得到。

在此设置的 **password** 或 **encrypted-password** 将以对称加密格式显示。

模式

全局配置模式

示例

设置主认证服务器的 IP 地址为 10.20.1.100，密码为不加密密码 **tplink**：

```
TL-SG3210(config)# radius auth-pri 10.20.1.100 auth-key 0 tplink
```

14.12 radius server-account

该命令用于启用计费服务器的计费功能，它的 **no** 命令用于禁用计费功能。

命令

radius server-account

no radius server-account

模式

全局配置模式

示例

启用计费功能：

```
TL-SG3210(config)# radius server-account
```

14.13 show dot1x global

该命令用于显示 801.X 全局配置信息。

命令

```
show dot1x global
```

模式

特权模式和所有配置模式

示例

显示 801.X 全局配置信息：

```
TL-SG3210(config)# show dot1x global
```

14.14 show dot1x interface

该命令用于显示 801.X 端口配置信息。

命令

```
show dot1x interface [ gigabitEthernet port ]
```

参数

port —— 以太网端口号。缺省时显示所有端口的配置信息。

模式

特权模式和所有配置模式

示例

显示 801.X 端口配置信息：

```
TL-SG3210(config)# show dot1x interface
```

显示端口 1 的 802.1X 配置信息：

```
TL-SG3210(config)# show dot1x interface gigabitEthernet 1/0/1
```

14.15 show radius accounting

该命令用于显示 RADIUS 计费服务器的配置信息。

命令

```
show radius accounting
```

模式

特权模式和所有配置模式

示例

显示 RADIUS 计费服务器配置信息：

```
TL-SG3210(config)# show radius accounting
```

14.16 show radius authentication

该命令用于显示 RADIUS 认证服务器的配置信息。

命令

show radius authentication

模式

特权模式和所有配置模式

示例

显示 RADIUS 认证服务器配置信息：

```
TL-SG3210(config)# show radius authentication
```

第15章 系统日志配置命令

系统日志信息对交换机的配置和运行进行分类记载，为监控设备的运行状态和诊断设备故障提供支持。

15.1 logging buffer

该命令用于配置系统日志缓冲区的信息输入等级和状态，它的 **no** 命令用于关闭系统日志缓冲区功能。保存在本设备上的系统日志信息为本地日志，本地日志有两个输出方向（即可以保存到两个不同的地方）：日志缓冲区和日志文件。日志缓冲区是用于保存系统日志的一块内存区域，缓冲区中的信息可通过 [show logging buffer](#) 命令查看，在断电重启后这些信息将会丢失。本命令用来配置日志缓冲区的相关参数。

命令

logging buffer level

no logging buffer

参数

level —— 严重级别，共分为 0~7 八个等级，级别值越小，紧急程度越高。只允许级别小于或等于该值的日志信息保存到日志缓冲区。默认值为 6，表示 0~6 七个等级的日志信息会保存到日志缓冲区。

模式

全局配置模式

示例

启用日志缓冲区并设置严重级别为 5：

```
TL-SG3210(config)# logging buffer 5
```

15.2 logging file flash

该命令用于配置系统日志文件的状态，它的 **no** 命令用于关闭系统日志文件功能。日志文件是 Flash 里的一块存储区域。日志文件的信息可通过 [show logging flash](#) 命令查看，在断电重启后这些信息不会丢失。

命令

logging file flash

no logging file flash

模式

全局配置模式

示例

启用系统日志文件功能：

```
TL-SG3210(config)# logging file flash
```

15.3 logging file flash frequency

该命令用于设置在日志缓冲区中的系统日志文件同步到 flash 的频率，它的 no 命令用于恢复默认值。

命令

logging file flash frequency { periodic *periodic* | immediate }

no logging file flash frequency

参数

periodic —— 同步周期，取值范围 1~48（时），默认值为 24。

immediate —— 在缓冲区中的系统日志文件会立刻被同步到 flash 中。此选项会降低 flash 的使用寿命，因此不推荐使用。

模式

全局配置模式

示例

设置同步周期为 10 小时：

```
TL-SG3210(config)# logging file flash frequency periodic 10
```

15.4 logging file flash level

该命令用于配置系统日志文件的信息输入等级，它的 no 命令用于恢复默认值。

命令

logging file flash level *level*

no logging file flash level

参数

level —— 严重级别，共分为 0~7 八个等级，级别值越小，紧急程度越高。只允许级别小于或等于该值的日志信息保存到日志文件中。默认值为 2，表示允许级别为 0~2 的日志信息保存到日志文件中。

模式

全局配置模式

示例

设置日志文件严重级别为 7：

```
TL-SG3210(config)# logging file flash level 7
```


15.5 clear logging

该命令用于清空当前日志缓冲区或日志文件中的信息。

命令

clear logging [*buffer* | *flash*]

参数

buffer | *flash* —— 要清空的输出方向，有 **buffer**（日志缓冲区）和 **flash**（日志文件）两个选项，缺省时表示两者的信息都被清空。

模式

全局配置模式

示例

清空当前日志缓冲区中的系统日志信息：

```
TL-SG3210(config)# clear logging buffer
```

15.6 logging host index

该命令用于配置日志服务器，它的 **no** 命令用于清空指定日志服务器的配置信息。日志服务器用于接收本交换机发送的系统日志消息，通过查看日志服务器可以对本交换机的配置情况和运行状态进行远程监控。

命令

logging host index *idx* *host-ip* *level*

no logging host index *idx*

参数

idx —— 日志服务器的序号，取值范围 1~4。

host-ip —— 日志服务器的 IP 地址。

level —— 严重级别，共分为 0~7 八个等级，级别值越小，紧急程度越高。只允许级别小于或等于该值的日志信息发送到该服务器。默认值为 6，表示允许级别为 0~6 的日志信息发送到该服务器。

模式

全局配置模式

示例

启用日志服务器 2，并设置该服务器的 IP 地址为 192.168.0.148，严重级别为 5：

```
TL-SG3210(config)# logging host index 2 192.168.0.148 5
```

15.7 show logging local-config

该命令用于显示本地日志（包括日志缓冲区和日志文件）的配置信息。

命令

show logging local-config

模式

特权模式和所有配置模式

示例

显示本地日志配置信息：

```
TL-SG3210(config)# show logging local-config
```

15.8 show logging loghost

该命令用于显示日志服务器的配置信息。

命令

show logging loghost [*index*]

参数

index —— 要显示配置信息的日志服务器序号，缺省时显示所有日志服务器的配置信息。

模式

特权模式和所有配置模式

示例

显示日志服务器 2 的配置信息：

```
TL-SG3210(config)# show logging loghost 2
```

15.9 show logging buffer

该命令用于显示日志缓冲区中的日志信息，可根据严重级别进行过滤显示。

命令

show logging buffer [*level level*]

参数

level —— 严重级别（0~7），只显示级别小于或等于该值的日志信息，缺省时显示日志缓冲区中的所有日志信息。

模式

特权模式和所有配置模式

示例

显示日志缓冲区中级别为 0-5 的日志信息：

```
TL-SG3210(config)# show logging buffer level 5
```

15.10 show logging flash

该命令用于显示日志文件中的日志信息，可根据严重级别进行过滤显示。

命令

```
show logging flash [level level]
```

参数

level —— 严重级别（0~7），只显示级别小于或等于该值的日志信息，缺省时显示日志文件中的所有日志信息。

模式

特权模式和所有配置模式

示例

显示日志文件中级别为 0~3 的日志信息：

```
TL-SG3210(config)# show logging flash level 3
```

第16章 SSH 配置命令

SSH（Security Shell）采用加密和认证功能，可以为远程登录管理提供安全保障，以保证管理信息的安全。

16.1 ip ssh server

该命令用于启用 SSH 服务器功能，它的 no 命令用于禁用 SSH 服务器功能。

命令

ip ssh server

no ip ssh server

模式

全局配置模式

示例

启用 SSH 服务器功能：

```
TL-SG3210(config)# ip ssh server
```

16.2 ip ssh version

该命令用于启用 SSH 的协议版本，它的 no 命令用于禁用 SSH 协议版本。

命令

ip ssh version { v1 | v2 }

no ip ssh version { v1 | v2 }

参数

v1 | v2 —— 要启用的 SSH 协议版本，分别对应 SSH v1 和 SSH v2。

模式

全局配置模式

示例

启用 SSH v2：

```
TL-SG3210(config)# ip ssh version v2
```

16.3 ip ssh algorithm

该命令用于配置 SSH 功能的算法。它的 no 命令用于禁用指定的算法。

命令

ip ssh algorithm { AES128-CBC | AES192-CBC | AES256-CBC | Blowfish-CBC | Cast128-CBC | 3DES-CBC | HMAC-SHA1 | HMAC-MD5 }

no ip ssh algorithm

参数

{ AES128-CBC | AES192-CBC | AES256-CBC | Blowfish-CBC | Cast128-CBC | 3DES-CBC | HMAC-SHA1 | HMAC-MD5 } ——指定的 SSH 算法。

模式

全局配置模式

示例

指定 SSH 的算法为 AES128-CBC:

```
TL-SG3210(config)# ip ssh algorithm AES128-CBC
```

16.4 ip ssh timeout

该命令用于设置 SSH 的静默时长，它的 no 命令用于恢复默认配置。

命令

ip ssh timeout *value*

no ip ssh timeout

参数

value —— 静默时长，当此时间内客户端未有动作时，连接会自动断开。单位为秒，取值范围 1~120，默认值为 120。

模式

全局配置模式

示例

配置 SSH 静默时长为 100 秒:

```
TL-SG3210(config)# ip ssh timeout 100
```

16.5 ip ssh max-client

该命令用于配置 SSH 的最大连接数，它的 no 命令用于恢复默认配置。

命令

ip ssh max-client *number*

no ip ssh max-client

参数

number —— SSH 最大连接数，取值范围 1~5，默认值为 5。

模式

全局配置模式

示例

配置 SSH 最大连接数为 3:

```
TL-SG3210(config)# ip ssh max-client 3
```

16.6 ip ssh download

该命令用于通过 TFTP 方式导入 SSH 密钥文件。

命令

```
ip ssh download { v1 | v2 } key-file ip-address ip-addr
```

参数

v1 | v2 —— 选择要导入的密钥类型，v1 表示 SSH-1，v2 表示 SSH-2。

key-file —— 选择要导入的密钥文件名称，可输入 1~25 个字符。导入的文件必须是密钥长度为 256~3072 比特的 SSH 公钥。

ip-addr —— TFTP 服务器的 IP 地址。支持 IPv4 和 IPv6 地址。例如 IPv4 地址 192.168.0.10，IPv6 地址 fe80::1234。

模式

全局配置模式

示例

通过 IP 地址为 192.168.0.148 的 TFTP 服务器导入名为 ssh-key 的 SSH-1 密钥文件:

```
TL-SG3210(config)# ip ssh download v1 ssh-key ip-address 192.168.0.148
```

通过 IP 地址为 fe80::1234 的 TFTP 服务器导入名为 ssh-key 的 SSH-1 密钥文件:

```
TL-SG3210(config)# ip ssh download v1 ssh-key ip-address fe80::1234
```

16.7 show ip ssh

该命令用于显示 SSH 的全局配置信息。

命令

```
show ip ssh
```

模式

特权模式和所有配置模式

示例

显示 SSH 全局配置信息:

```
TL-SG3210(config)# show ip ssh
```

第17章 地址配置命令

地址配置通过端口安全设置和地址表管理来提高网络安全，管理地址信息。

17.1 mac address-table static

该命令用于添加静态地址条目，它的 **no** 命令用于删除对应条目。静态地址由用户手工添加和删除，不受老化时间的限制。对于网络拓扑相对固定的使用环境来说，使用静态地址绑定可以提高交换机的转发效率，减少网络中的广播流量。

命令

```
mac address-table static mac-addr vid vid interface gigabitEthernet port  
no mac address-table static { mac-addr | vid vid | mac mac-addr vid vid | interface  
gigabitEthernet port }
```

参数

mac-addr —— 要添加的地址条目的 MAC 地址。

vid —— 地址条目所属的 VLAN ID，取值范围 1~4094。

port —— 地址条目对应的端口。

模式

全局配置模式

示例

添加静态地址条目，该条目将 MAC 地址 00:02:58:4f:6c:23、VLAN1 和端口 1 绑定：

```
TL-SG3210(config)# mac address-table static 00:02:58:4f:6c:23 vid 1 interface  
gigabitEthernet 1/0/1
```

17.2 mac address-table aging-time

该命令用于配置动态地址老化时间，它的 **no** 命令用于恢复默认配置。

命令

```
mac address-table aging-time aging-time  
no mac address-table aging-time
```

参数

aging-time —— 要设置的地址老化时间，取值范围为 0 或 10~630（秒），为 0 时表示不启用自动老化功能。默认值为 300。

模式

全局配置模式

示例

设置地址老化时间为 500 秒：

```
TL-SG3210(config)# mac address-table aging-time 500
```

17.3 mac address-table filtering

该命令用于添加过滤地址条目，它的 **no** 命令用于删除对应条目。通过配置过滤地址，允许交换机对不期望转发的数据帧进行过滤。过滤地址不会被老化，只能手动进行配置和删除。

命令

```
mac address-table filtering mac-addr vid vid
```

```
no mac address-table filtering {[ mac-addr ] [ vid vid ]}
```

参数

mac-addr —— 要添加的地址条目的 MAC 地址。

vid —— 地址条目所属的 VLAN ID，取值范围 1~4094。

模式

全局配置模式

示例

添加过滤地址条目，过滤 VLAN1 的 MAC 地址 00:1e:4b:04:01:5d：

```
TL-SG3210(config)# mac address-table filtering 00:1e:4b:04:01:5d vid 1
```

17.4 mac address-table max-mac-count

该命令用于设置端口安全参数，它的 **no** 命令用于恢复默认配置。端口安全通过限制端口的最大学习 MAC 数目，来防范 MAC 地址攻击和控制端口的网络流量。如果端口启用端口安全功能，将自动学习接入设备的 MAC 地址，当学习地址数达到最大值时停止学习。此后，MAC 地址未被学习的网络设备将不能再通过该端口接入网络，保证安全性。

命令

```
mac address-table max-mac-count { [max-number num] [mode { dynamic | static | permanent } ] [ status { disable | enable } ] }
```

```
no mac address-table max-mac-count
```

参数

num —— 端口最多可以学习的 MAC 地址数目，取值范围 0~64，缺省时为 64。

mode —— 端口地址学习模式，有 **dynamic**（动态）、**static**（静态）和 **permanent**（永久）三个选项。选择 **dynamic** 时，MAC 地址学习受老化时间的限制，老化时间过后，

所学的 MAC 地址将被删除；选择 **static** 时，MAC 地址学习不受老化时间的限制，只能手动进行删除，但交换机重启后学习到的条目将清空；选择 **permanent** 时，MAC 地址学习不受老化时间的限制，只能手动进行删除，交换机重启后学习到的条目保持不变。缺省时为 **dynamic**。

status —— 是否启用端口安全功能，默认为禁用（**disable**）。

模式

接口配置模式（**interface gigabitEthernet / interface range gigabitEthernet**）

示例

启用端口 1 的安全功能，并设置学习模式为静态，最大可学习 MAC 地址数为 30：

```
TL-SG3210(config)# interface gigabitEthernet 1/0/1
TL-SG3210(config-if)# mac address-table max-mac-count max-number 30 mode
static status enable
```

17.5 show mac address-table

该命令用于显示地址条目信息。

命令

show mac address-table { dynamic | static | drop | all }

参数

dynamic | static | drop | all —— 要显示的地址类型。

模式

特权模式和所有配置模式

示例

显示所有地址条目信息：

```
TL-SG3210(config)# show mac address-table all
```

17.6 show mac address-table aging-time

该命令用于显示地址老化时间。

命令

show mac address-table aging-time

模式

特权模式和所有配置模式

示例

显示地址老化时间：

```
TL-SG3210(config)# show mac address-table aging-time
```

17.7 show mac address-table max-mac-count interface gigabitEthernet

该命令用于显示端口的安全配置，即端口最大可学习 MAC 地址数和学习模式。

命令

```
show mac address-table max-mac-count interface gigabitEthernet [port]
```

参数

port —— 要显示安全配置信息的端口号，缺省时显示所有端口的安全配置信息。

模式

特权模式和所有配置模式

示例

显示所有端口的安全配置信息：

```
TL-SG3210(config)# show mac address-table max-mac-count interface  
gigabitEthernet
```

显示端口 1 的安全配置信息：

```
TL-SG3210(config)# show mac address-table max-mac-count interface  
gigabitEthernet 1/0/1
```

17.8 show mac address-table interface gigabitEthernet

该命令用于显示端口的地址配置信息。

命令

```
show mac address-table interface gigabitEthernet port
```

参数

port —— 要显示地址配置信息的端口号，缺省时显示所有端口的地址配置信息。

模式

特权模式和所有配置模式

示例

显示端口 1 的地址配置信息：

```
TL-SG3210(config)# show mac address-table interface gigabitEthernet 1/0/1
```

17.9 show mac address-table count

该命令用于显示地址表总数。

命令

show mac address-table count

模式

特权模式和所有配置模式

示例

显示地址表总数：

```
TL-SG3210(config)# show mac address-table count
```

17.10 show mac address-table address

该命令用于显示指定 MAC 地址的信息。

命令

show mac address-table address *mac-addr*

参数

mac-addr —— 指定 MAC 地址。

模式

特权模式和所有配置模式

示例

显示地址为 00:00:00:00:23:00 的信息：

```
TL-SG3210(config)# show mac address-table address 00:00:00:00:23:00
```

17.11 show mac address-table vlan

该命令用于显示指定 VLAN 的 MAC 地址配置。

命令

show mac address-table vlan *vid*

参数

vid —— 指定 VLAN ID。

模式

特权模式和所有配置模式

示例

显示 VLAN1 的地址配置信息：

```
TL-SG3210(config)# show mac address-table vlan 1
```

17.12 clear mac address-table

该命令用于清除指定类型的所有 MAC 地址。

命令

```
clear mac address-table { dynamic | filtering | static }
```

参数

dynamic | filtering | static ——指定的类型

模式

特权模式和所有配置模式

示例

清除所有的动态地址条目信息：

```
TL-SG3210(config)# clear mac address-table dynamic
```

第18章 系统配置命令

系统配置用来配置系统信息、IP 地址等参数，并且可以对交换机进行重启、复位、升级系统文件等操作。

18.1 system-time manual

该命令用于手动设置交换机的系统时间。

命令

system-time manual *time*

参数

time —— 手动设置交换机的系统时间，格式为 MM/DD/YYYY-HH:MM:SS。

模式

全局配置模式

示例

设置交换机系统时间为 03/20/2013 17:30:35:

```
TL-SG3210(config)# system-time manual 03/20/2013-17:30:35
```

18.2 system-time ntp

该命令用于设置交换机从网络中 NTP 服务器上获取 UTC 时间。

命令

system-time ntp { *time-zone* } { *ntp-server* } { *backup-ntp-server* } { *fetching-rate* }

参数

time-zone —— 选择交换机所在的时区。以正二时区为例，UTC时间的格式为：UTC+02:00。取值范围是UTC-12:00到UTC+13:00。

ntp-server —— 设置首选 NTP 服务器的 IP 地址。

backup-ntp-server —— 设置备选 NTP 服务器的 IP 地址。

fetching-rate —— 设置从 NTP 服务器获取时间的频率。

模式

全局配置模式

示例

设置交换机系统时间获取方式为 NTP，时区为 UTC-12:00，首选 NTP 服务器 IP 地址为 133.100.9.2，备选 NTP 服务器的 IP 地址为 139.78.100.163，获取频率为 11 小时：

```
TL-SG3210(config)# system-time ntp UTC-12:00 133.100.9.2 139.79.100.163 11
```

18.3 system-time dst predefined

该命令用于从预定义的夏令时样式中选择夏令时配置，配置可循环使用。

命令

```
system-time dst predefined [ USA | Australia | Europe | New-Zealand ]
```

参数

USA | Australia | Europe | New-Zealand —— 夏令时样式。有四个可选值，分别为USA, Australia, Europe, New-Zealand，默认为Europe。

四个值代表夏令时起止区间如下：

USA：三月第二个周日的2: 00am ~ 十一月第一个周日的2: 00am

Australia：十月第一个周日2: 00am ~ 四月第一个周日3: 00am

Europe：三月最后一个周日1: 00am ~ 十月最后一个周日1: 00am

New-Zealand：九月最后一个周日2: 00am ~ 四月第一个周日3: 00am

模式

全局配置模式

示例

设置交换机的夏令时起止时间为 Europe 标准：

```
TL-SG3210(config)# system-time dst predefined Europe
```

18.4 system-time dst date

该命令用于设置一次性的夏令时，开始日期的年份默认为当前年份。夏令时起止区间必须小于一年，可跨年设置。

命令

```
system-time dst date {smonth} {sday} {stime} {emonth} {eday} {etime} [offset]
```

参数

smonth —— 开始月，取值如下：Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec。

sday —— 开始日，取值范围 1~31，各月天数不尽相同，请根据实际情况填写。

stime —— 开始时刻，格式为：hh:mm。

emonth —— 结束月，取值如下：Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec。

eday —— 结束日，取值范围 1~31，各月天数不尽相同，请根据实际情况填写。

etime —— 结束时刻，格式为：hh:mm。

offset —— 可选参数，夏令时时间调整大小，取值范围为 1-1440。默认为 60 分钟。

模式

全局配置模式

示例

设置交换机夏令时的起止时间日期为 4 月 1 日 0 点到 10 月 1 日 0 点，夏令时时间调整大小为 30 分钟：

```
TL-SG3210(config)# system-time dst date Apr 1 00:00 Oct 1 00:00 30
```

18.5 system-time dst recurring

该命令用于设置可循环的夏令时配置。可以跨年设置。

命令

```
system-time dst recurring {sweek} {sday} {smonth} {stime} {eweeek} {eday} {emonth}  
{etime} [offset]
```

参数

sweek —— 开始周，取值如下：first, second, third, fourth, last

sday —— 开始日，取值如下：Sun, Mon, Tue, Wed, Thu, Fri, Sat

smonth —— 开始月，取值如下：Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec

stime —— 开始时刻，格式为：hh:mm

eweeek —— 结束周，取值如下：first, second, third, fourth, last

eday —— 结束日，取值如下：Sun, Mon, Tue, Wed, Thu, Fri, Sat

emonth —— 结束月，取值如下：Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec

etime —— 结束时刻，格式为：hh:mm

offset —— 可选参数，夏令时时间调整大小，取值范围为 1-1440。默认为 60 分钟。

模式

全局配置模式

示例

设置交换机夏令时的起止时间日期为 5 月的第一个星期天 2:00am 到 10 月最后一个星期天 2:00am，夏令时时间调整大小为 45 分钟：


```
TL-SG3210(config)# system-time dst recurring first Sun May 02:00 last Sun Oct
02:00 45
```

18.6 hostname

该命令用于设置设备名称，它的 no 命令用于清空设备名称信息。

命令

hostname *hostname*

no hostname

参数

hostname —— 设备名称，1~32 个字符，默认为 TL-SG3210。

模式

全局配置模式

示例

设置设备名称为 TP-LINK:

```
TL-SG3210(config)# hostname TP-LINK
```

18.7 location

该命令用于设置设备位置，它的 no 命令用于清空设备位置信息。

命令

location *location*

no location

参数

location —— 设备位置，1~32 个字符，默认为 SHENZHEN。

模式

全局配置模式

示例

设置设备位置为 GUANGZHOU:

```
TL-SG3210(config)# location GUANGZHOU
```

18.8 contact-info

该命令用于设置联系方法，它的 no 命令用于清空相应信息。

命令

contact-info *contact_info*

no contact-info

参数

contact_info —— 联系方法，1~32 个字符，默认为 www.tp-link.com.cn。

模式

全局配置模式

示例

设置联系方法为 www.tp-link.com:

```
TL-SG3210(config)# contact-info www.tp-link.com
```

18.9 ip management-vlan

该命令用于配置交换机的管理 VLAN，只有连接到管理 VLAN 成员端口的计算机才可以通过 Web、telnet、SSL 或 SSH 等方式来管理交换机。默认的管理 VLAN 为 VLAN1。

命令

ip management-vlan {*vlan-id*}

参数

vlan-id —— 配置交换机的管理 VLAN，取值范围 1~4094。

模式

全局配置模式

示例

将 VLAN4 设置为交换机的管理 VLAN:

```
TL-SG3210(config)# ip management-vlan 4
```

18.10 ip address

该命令用于设置系统的 IP 地址，子网掩码和默认网关，它的 no 命令用于恢复默认设置。默认情况下系统 IP 地址为 192.168.0.1，子网掩码为 255.255.255.0，网关为空。设置管理 IP 必须在管理 VLAN 的接口模式下进行。

命令

ip address {*ip-addr*} {*ip-mask*} [*gateway*]

no ip address

参数

ip-addr —— 系统 IP 地址。

ip-mask —— 子网掩码。

gateway —— 系统网关。

模式

接口配置模式（interface vlan）

示例

将系统的 IP 地址设置为 192.168.0.69，子网掩码设置为 255.255.255.0（交换机的管理 VLAN 为 VLAN1）：

```
TL-SG3210(config)# interface vlan 1
```

```
TL-SG3210(config-if)# ip address 192.168.0.69 255.255.255.0
```

18.11 ip address-alloc dhcp

该命令用于启用 DHCP Client 功能，通过 DHCP Client 方式获取 IP 地址。启用 DHCP Client 功能必须在管理 VLAN 的接口模式下进行。

命令

```
ip address-alloc dhcp
```

模式

接口配置模式（interface vlan）

示例

开启系统的 DHCP Client 功能（交换机的管理 VLAN 为 VLAN1）：

```
TL-SG3210(config)# interface vlan 1
```

```
TL-SG3210(config-if)# ip address-alloc dhcp
```

18.12 ip address-alloc bootp

该命令用于启用 BOOTP 协议，通过 BOOTP 协议获取 IP 地址。启用 BOOTP 协议必须在管理 VLAN 的接口模式下进行。

命令

```
ip address-alloc bootp
```

模式

接口配置模式（interface vlan）

示例

启用 BOOTP 协议（交换机的管理 VLAN 为 VLAN1）：

```
TL-SG3210(config)# interface vlan 1
```

```
TL-SG3210(config-if)# ip address-alloc bootp
```

18.13 reset

该命令用于把交换机软件复位，软件复位后，交换机配置将恢复成出厂默认状态，用户配置数据将丢失。

命令

reset

模式

特权模式

示例

对交换机进行软件复位：

```
TL-SG3210# reset
```

18.14 reboot

该命令用于重启交换机。在重启期间，请注意不要关闭设备电源，以免损坏设备。

命令

reboot

模式

特权模式

示例

重新启动交换机：

```
TL-SG3210# reboot
```

18.15 copy running-config startup-config

该命令用于保存当前用户配置。

命令

copy running-config startup-config

模式

特权模式

示例

保存当前用户的配置:

```
TL-SG3210# copy running-config startup-config
```

18.16 copy startup-config tftp

该命令用于通过 TFTP 方式导出配置文件。

命令

```
copy startup-config tftp ip-address ip-addr filename name
```

参数

ip-addr —— TFTP 服务器的 IP 地址。支持 IPv4 和 IPv6 地址。例如 IPv4 地址 192.168.0.10，IPv6 地址 fe80::1234。

name —— 指定导出的配置文件名。

模式

特权模式

示例

通过 IP 地址为 192.168.0.148 的 TFTP 服务器导出配置文件，并将导出的配置文件命名为 config.cfg:

```
TL-SG3210# copy startup-config tftp ip-address 192.168.0.148 filename config
```

通过 IP 地址为 fe80::1234 的 TFTP 服务器导出配置文件，并将导出的配置文件命名为 config.cfg:

```
TL-SG3210# copy startup-config tftp ip-address fe80::1234 filename config
```

18.17 copy tftp startup-config

该命令用于通过 TFTP 方式导入配置文件。

命令

```
copy tftp startuup-config ip-address ip-addr filename name
```

参数

ip-addr —— TFTP 服务器的 IP 地址。支持 IPv4 和 IPv6 地址。例如 IPv4 地址 192.168.0.10，IPv6 地址 fe80::1234。

name —— 要导入的配置文件名。

模式

特权模式

示例

通过 IP 地址为 192.168.0.148 的 TFTP 服务器导入名为 config.cfg 的配置文件：

```
TL-SG3210# copy tftp startup-config ip-address 192.168.0.148 filename config
```

通过 IP 地址为 fe80::1234 的 TFTP 服务器导入名为 config.cfg 的配置文件：

```
TL-SG3210# copy tftp startup-config ip-address fe80::1234 filename config
```

18.18 firmware upgrade

该命令用于通过 TFTP 方式升级系统文件。

命令

firmware upgrade ip-address *ip-addr* filename *name*

参数

ip-addr —— TFTP 服务器的 IP 地址。支持 IPv4 和 IPv6 地址。例如 IPv4 地址 192.168.0.10，IPv6 地址 fe80::1234。

name —— 指定系统文件名。

模式

特权模式

示例

通过 IP 地址为 192.168.0.148 的 TFTP 服务器升级系统文件，系统文件名为 firmware.bin：

```
TL-SG3210# firmware upgrade ip-address 192.168.0.148 filename firmware.bin
```

通过 IP 地址为 fe80::1234 的 TFTP 服务器升级系统文件，系统文件名为 firmware.bin：

```
TL-SG3210# firmware upgrade ip-address fe80::1234 filename firmware.bin
```

18.19 ping

该命令用于检测从交换机到某一网络节点之间的链路是否连通。

命令

ping [ip | ipv6] { *ip_addr* } [-n *count*] [-l *count*] [-i *count*]

参数

ip —— 表示用于 ping 检测的 IP 地址类型必须为 IPv4。

ipv6 —— 表示用于 ping 检测的 IP 地址类型必须为 IPv6。

ip_addr —— 要检测的目标节点的 IP 地址。如果未选择 *ip* | *ipv6* 参数字段，则此处既可输入 IPv4 地址，也可输入 IPv6 地址。

count (-n) —— 发送报文的次数，取值范围 1~10，默认值为 4。

count (-l) —— 发送报文的长度，取值范围 1~1024（字节），默认值为 64。

count (-i) —— 发送报文的时间间隔，取值范围 100~1000（毫秒），默认值为 1000。

模式

用户模式和特权模式

示例

检测交换机与 IP 地址为 192.168.0.131 的网络设备是否连通，其中测试报文的长度为 512 字节，报文每隔 1000 毫秒发送一次，若发送 8 次后没有收到回复，则连接失败：

```
TL-SG3210# ping 192.168.0.131 -n 8 -l 512
```

检测交换机与 IP 地址为 fe80::1234 的网络设备是否连通，其中测试报文的长度为 512 字节，报文每隔 1000 毫秒发送一次，若发送 8 次后没有收到回复，则连接失败：

```
TL-SG3210# ping fe80::1234 -n 8 -l 512
```

18.20 tracert

该命令用于检测测试报文从交换机传送到目的设备所经过的网关的连通性。

命令

```
tracert [ ip | ipv6 ] ip_addr [ maxHops ]
```

参数

ip —— 表示用于 tracert 检测的 IP 地址类型必须为 IPv4。

ipv6 —— 表示用于 tracert 检测的 IP 地址类型必须为 IPv6。

ip_addr —— 要检测的目的设备的 IP 地址。如果未选择 *ip* | *ipv6* 参数字段，则此处既可输入 IPv4 地址，也可输入 IPv6 地址。

maxHops —— 最大路由跳数，取值范围 1~30，默认值为 4。

模式

用户模式和特权模式

示例

检测交换机与 IP 地址为 192.168.0.131 的网络设备是否连通，若经过 20 跳路由后仍未连通，则连接失败：

```
TL-SG3210# tracert 192.168.0.131 20
```

检测交换机与 IP 地址为 fe80::1234 的网络设备是否连通，若经过 20 跳路由后仍未连通，则连接失败：

```
TL-SG3210# tracert fe80::1234 20
```

18.21 show system-time

该命令用于显示交换机的系统时间信息。

命令

show system-time

模式

特权模式和所有配置模式

示例

显示交换机的系统时间信息：

```
TL-SG3210# show system-time
```

18.22 show system-time dst

该命令用于显示交换机的夏令时配置信息。

命令

show system-time dst

模式

特权模式和所有配置模式

示例

显示夏令时信息：

```
TL-SG3210# show system-time dst
```

18.23 show system-time ntp

该命令用于显示当前系统时间的 NTP 配置信息。

命令

show system-time ntp

模式

特权模式和所有配置模式

示例

显示 NTP 配置信息：

```
TL-SG3210# show system-time ntp
```


18.24 show system-info

该命令用于显示系统描述、系统名称、系统位置、联系方法、硬件版本、软件版本、系统时间和运行时间等信息。

命令

show system-info

模式

特权模式和所有配置模式

示例

显示系统信息：

```
TL-SG3210# show system-info
```

18.25 show running-config

该命令用于显示系统或一个指定端口的当前操作配置。

命令

show running-config [interface { fastEthernet *port* | gigabitEthernet *port* }]

参数

port —— 指定显示当前操作配置的端口号。

模式

特权模式和所有配置模式

示例

显示系统的当前操作配置：

```
TL-SG3210# show running-config
```

18.26 show cable-diagnostics interface

该命令用于显示对端口进行线缆检测后的结果。线缆检测功能能够检测与交换机相连的线缆是否有故障以及故障的位置，利用此功能可以辅助日常工程安装诊断。

命令

show cable-diagnostics interface gigabitEthernet *port*

参数

port —— 指定进行线缆检测的端口号。

模式

特权模式和所有配置模式

示例

显示对端口 3 进行线缆检测的结果：

```
TL-SG3210# show cable-diagnostics interface gigabitEthernet 1/0/3
```

第19章 IPv6 地址配置命令

IPv6 地址配置命令需在 VLAN 接口模式下设置，输入 **enable**→**configure**→**interface vlan {vlan-id}** 可进入管理 VLAN 的接口配置模式。默认情况下，交换机管理 VLAN 是 VLAN1。可以在全局配置模式下通过 **ip management-vlan {vlan-id}** 命令设置管理 VLAN。

19.1 ipv6 enable

该命令用于开启全局 IPv6 功能，它的 **no** 命令用于禁用全局 IPv6 功能。

在进行 IPv6 地址配置管理之前，必须先开启 IPv6 功能，交换机默认开启 IPv6 功能。

禁用 IPv6 功能会卸载掉主机的 IPv6 协议栈，使得先前配置的 IPv6 地址都不生效，任何基于 IPv6 地址的模块都将失效，例如：SSH，SSL，TFTPv6 等。启用 IPv6 功能则重新恢复原先配置的 IPv6 地址。

命令

```
ipv6 enable
no ipv6 enable
```

模式

接口配置模式（interface vlan）

示例

在交换机管理 VLAN 是 VLAN1 条件下，开启全局 IPv6 功能：

```
TL-SG3210 (config)# interface vlan 1
TL-SG3210 (config-if)# ipv6 enable
```

19.2 ipv6 address autoconfig

该命令用于开启 IPv6 链路本地地址的自动配置功能。

交换机只有一个链路本地地址，有自动配置和手动配置两种配置方式。为确保链路本地地址的唯一性，当自动配置的链路本地地址生效后，手动配置的链路本地地址将被删除。

命令

```
ipv6 address autoconfig
```

模式

接口配置模式（interface vlan）

示例

在交换机管理 VLAN 是 VLAN1 条件下，开启 IPv6 链路本地地址的自动配置功能：

```
TL-SG3210(config)# interface vlan 1
TL-SG3210(config-if)# ipv6 address autoconfig
```

19.3 ipv6 address link-local

该命令用于使用自动配置方式配置交换机的 IPv6 链路本地地址，它的 no 命令用于删除配置的链路本地地址。

命令

ipv6 address *ipv6-addr* link-local

no ipv6 address *ipv6-addr* link-local

参数

ipv6-addr —— 交换机的 IPv6 链路本地地址，该地址必须是以 fe80::/10 为前缀的标准 IPv6 地址，否则该命令无效。

模式

接口配置模式（interface vlan）

示例

在交换机管理 VLAN 是 VLAN1 条件下，配置交换机的 IPv6 链路本地地址为 fe80::1234:

```
TL-SG3210(config)# interface vlan 1
```

```
TL-SG3210(config-if)# ipv6 address fe80::1234 link-local
```

19.4 ipv6 address dhcp

该命令用于启用 DHCPv6 Client 功能。该功能开启后，交换机将通过 DHCPv6 服务器获取 IPv6 全球地址。它的 no 命令用于删除 DHCPv6 服务器分配的地址，或禁用 DHCPv6 Client 功能。

命令

ipv6 address dhcp

no ipv6 address dhcp

模式

接口配置模式（interface vlan）

示例

在交换机管理 VLAN 是 VLAN1 条件下，开启 DHCPv6 Client 功能：

```
TL-SG3210(config)# interface vlan 1
```

```
TL-SG3210(config-if)# ipv6 address dhcp
```

19.5 ipv6 address ra

该命令用于通过地址前缀和从接收到的 RA（Router Advertisement）消息中得到的其他配置参数配置交换机的 IPv6 全球地址，它的 no 命令用于禁用该功能。

命令

ipv6 address ra

no ipv6 address ra

模式

接口配置模式（interface vlan）

示例

在交换机管理 VLAN 是 VLAN1 条件下，开启“使用 RA 消息进行全球地址自动配置”功能：

```
TL-SG3210(config)# interface vlan 1
TL-SG3210(config-if)# ipv6 address ra
```

19.6 ipv6 address eui-64

该命令用于手动配置 EUI-64 格式的 IPv6 全球地址。仅需指定一个地址前缀，系统将自动生成一个全球地址。它的 no 命令用于删除配置的 EUI-64 格式的 IPv6 全球地址。

命令

ipv6 address *ipv6-addr* eui-64

no ipv6 address *ipv6-addr* eui-64

参数

ipv6-addr —— EUI-64 格式的 IPv6 全球地址的地址前缀，例如 3ffe::1/64。

模式

接口配置模式（interface vlan）

示例

在交换机管理 VLAN 是 VLAN1 条件下，配置一个 EUI-64 格式的 IPv6 全球地址，该地址的地址前缀为 3ffe::1/64：

```
TL-SG3210(config)# interface vlan 1
TL-SG3210(config-if)# ipv6 address 3ffe::1/64 eui-64
```

19.7 ipv6 address

该命令用于手动配置 IPv6 全球地址，它的 no 命令用于删除配置的 IPv6 全球地址。

命令

```
ipv6 address ipv6-addr  
no ipv6 address ipv6-addr
```

参数

ipv6-addr —— IPv6 全球地址，例如 3ffe::1/64。

模式

接口配置模式（interface vlan）

示例

在交换机管理 VLAN 是 VLAN1 条件下，配置一个 IPv6 全球地址 3001::1/64：

```
TL-SG3210(config)# interface vlan 1  
TL-SG3210(config-if)# ipv6 address 3001::1/64
```

19.8 show ipv6 interface vlan

该命令用于显示交换机管理VLAN接口已配置的IPv6功能信息，包括IPv6功能开启状态、链路本地地址、全球地址和IPv6组播组等。

命令

```
show ipv6 interface vlan vlan-id
```

参数

vlan-id —— 交换机管理 VLAN 的 VLAN ID。

模式

特权模式和所有配置模式

示例

显示交换机管理 VLAN 接口已配置的 IPv6 功能信息：

```
TL-SG3210(config)# show ipv6 interface vlan 1
```

第20章 以太网配置命令

以太网配置用来配置以太网端口的流量控制、协商模式、风暴抑制、带宽限制等。

20.1 interface gigabitEthernet

该命令用于进入接口配置命令模式，对单个千兆以太网端口进行配置。

命令

interface gigabitEthernet *port*

参数

port —— 要配置的千兆以太网端口。

模式

全局配置模式

示例

进入接口配置模式，对以太网端口 2 进行配置：

```
TL-SG3210(config)# interface gigabitEthernet 1/0/2
```

20.2 interface range gigabitEthernet

该命令用于进入接口配置命令模式，对多个以太网端口进行同时配置。

命令

interface range gigabitEthernet *port-list*

参数

port-list —— 要配置的千兆以太网端口列表。端口之间需用逗号隔开（逗号前后不能有空格）；连续的一组端口可以用“-”符号表示，如 1/0/5-7 表示端口 5 到 7；组与组之间用逗号隔开。

模式

全局配置模式

说明

在 **interface range** 配置模式下，同一命令会作用到列表中的所有端口上。但各个端口是相互独立的，如果命令在一个端口上执行失败，不会影响其他端口上的执行。

示例

进入接口配置模式，并将以太网端口 5,6,8 加入到一个端口组里，对它们同时进行配置：

```
TL-SG3210(config)# interface range gigabitEthernet 1/0/5-6,1/0/8
```

20.3 description

该命令用于设置端口描述，它的 no 命令用于清空相应端口的描述。

命令

description *string*

no description

参数

string —— 端口描述的内容，可输入 1~16 个字符。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

为端口 5 添加端口描述 Port#5：

```
TL-SG3210(config)# interface gigabitEthernet 1/0/5
```

```
TL-SG3210(config-if)# description Port#5
```

20.4 shutdown

该命令用于禁用以太网端口，它的 no 命令用于重新启用相应端口。

命令

shutdown

no shutdown

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

关闭以太网端口 3：

```
TL-SG3210(config)# interface gigabitEthernet 1/0/3
```

```
TL-SG3210(config-if)# shutdown
```


20.5 flow-control

该命令用于启用端口的流量控制，它的 **no** 命令用于禁用相应端口的流控。启用流控能够同步接收端和发送端的速率，防止因速率不一致而导致的网络丢包。

命令

flow-control

no flow-control

模式

接口配置模式（**interface gigabitEthernet / interface range gigabitEthernet**）

示例

开启以太网端口 3 的流量控制：

```
TL-SG3210(config)# interface gigabitEthernet 1/0/3
```

```
TL-SG3210(config-if)# flow-control
```

20.6 media-type

该命令用于设置 Combo 口的介质类型。设置交换机 Combo 口的速率和双工模式之前必须先用此命令设置 Combo 的介质类型。此命令适用于含有 Combo 口的 TL-SG3216/ TL-SG3424/ TL-SG3424P，TL-SG3210 的 SFP 端口为独立的 SFP 口，故此命令不适用于该机型。

命令

media-type { rj45 | sfp }

参数

rj45 | sfp —— Combo 口的介质类型。

模式

接口配置模式（**interface gigabitEthernet / interface range gigabitEthernet**）

示例

配置交换机 TL-SG3216 的 Combo 口 16T 介质类型为 SFP：

```
TL-SG3216(config)# interface gigabitEthernet 1/0/16
```

```
TL-SG3216(config-if)# media-type sfp
```

20.7 duplex

该命令用于设置端口的双工模式，它的 **no** 命令用于恢复默认设置。

命令

duplex { full | half }

no duplex

参数

full | half —— 端口双工模式，分别为全双工模式和半双工模式。缺省时为全双工。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

设置以太网端口 3 为全双工模式：

```
TL-SG3210(config)# interface gigabitEthernet 1/0/3
```

```
TL-SG3210(config-if)# duplex full
```

20.8 speed

该命令用于设置端口的速率模式，它的 no 命令用于恢复默认设置。

命令

speed { 10 | 100 | 1000 | auto }

no speed

参数

10 | 100 | 1000 | auto —— 端口速率模式，分别为 10M、100M、1000M、自协商模式。缺省时为 auto。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

设置以太网端口 3 的速率模式为 100M：

```
TL-SG3210(config)# interface gigabitEthernet 1/0/3
```

```
TL-SG3210(config-if)# speed 100
```

20.9 storm-control broadcast

该命令用于开启交换机的风暴抑制对网络上出现的广播包进行过滤，以及设置广播包的最大接收速度，它的 no 命令用于禁止对网络上出现的广播包进行过滤。当交换机发现广播包超出您设定的最大速率时，会自动丢弃，以防止网络广播风暴的发生。

命令

storm-control broadcast [rate rate]

no storm-control broadcast

参数

rate —— 广播包的最大接收速度，超出流量部分的数据包将被丢弃。单位为 bps，取值范围 128Kbps | 256Kbps | 512Kbps | 1m | 2m | 4m | 5m | 10m | 20m | 40m | 50m。缺省时为 128 Kbps。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

启用端口 5 的广播包抑制，并设置广播包最大接收速率为 256Kbps：

```
TL-SG3210(config)# interface gigabitEthernet 1/0/5
```

```
TL-SG3210(config-if)# storm-control broadcast rate 256k
```

20.10 storm-control multicast

该命令用于开启交换机的风暴抑制对网络上出现的组播包进行过滤，它的 **no** 命令用于禁止对网络上出现的组播包进行过滤。当交换机发现组播包超出您设定的最大速率时，会自动丢弃，以防止网络广播风暴的发生。

命令

storm-control multicast [rate rate]

no storm-control multicast

参数

rate —— 组播包的最大接收速度，超出流量部分的数据包将被丢弃。单位为 bps，取值范围 128Kbps | 256Kbps | 512Kbps | 1m | 2m | 4m | 5m | 10m | 20m | 40m | 50m。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

启用端口 5 的组播包抑制，设置组播包最大接收速率为 512Kbps：

```
TL-SG3210(config)# interface gigabitEthernet 1/0/5
```

```
TL-SG3210(config-if)# storm-control multicast 512k
```

20.11 storm-control unicast

该命令用于开启交换机的风暴抑制对网络上出现的 UL 包进行过滤，它的 **no** 命令用于禁止对网络上出现的 UL 包进行过滤。当交换机发现 UL 包超出您设定的最大速率时，会自动丢弃，以防止网络广播风暴的发生。

命令

storm-control unicast [rate rate]
no storm-control unicast

参数

rate —— UL 包抑制，即 UL 包的最大接收速度，超出流量部分的数据包将被丢弃。单位为 bps，取值范围 128Kbps | 256Kbps | 512Kbps | 1m | 2m | 4m | 5m | 10m | 20m | 40m | 50m。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

启用端口 5 的 UL 包抑制，设置 UL 包最大接收速率为 2Mbps：

```
TL-SG3210(config)# interface gigabitEthernet 1/0/5
TL-SG3210(config-if)# storm-control unicast 2m
```

20.12 bandwidth

该命令用于配置以太网端口的带宽限制，它的 no 命令用于禁用端口带宽限制。

命令

bandwidth { [ingress ingress-rate] [egress egress-rate] }
no bandwidth { all | ingress | egress }

参数

ingress-rate —— 配置入口带宽限制，单位为 Kbps。取值范围为 1-1000000。系统会自动选择与所填写的数值最相近的 64Kbps 的整数倍值做为入口带宽。

egress-rate —— 配置出口带宽限制，单位为 Kbps。取值范围为 1-1000000。系统会自动选择与所填写的数值最相近的 64Kbps 的整数倍值做为出口带宽。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

配置端口 5 的入口带宽为 1Mbps，出口带宽为 10Mbps：

```
TL-SG3210(config)# interface gigabitEthernet 1/0/5
TL-SG3210(config-if)# bandwidth ingress 1024 egress 10240
```

20.13 clear counters

该命令用于清除所有以太网端口的统计信息。

命令**clear counters****模式**

全局配置模式

示例

清除所有以太网端口的统计信息：

TL-SG3210(config)# clear counters

20.14 show interface status

该命令用于显示以太网端口的连接状态。

命令**show interface [gigabitEthernet *port*] status****参数***port* —— 要显示连接状态的以太网端口，缺省时显示所有端口的状态。**模式**

特权模式和所有配置模式

示例

显示所有以太网端口的连接状态：

TL-SG3210(config)# show interface status

显示端口 1 连接状态：

TL-SG3210(config)# show interface gigabitEthernet 1/0/1 status

20.15 show interface counters

该命令用于显示以太网端口的统计信息。

命令**show interface [gigabitEthernet *port*] counters****参数***port* —— 要显示统计信息的以太网端口，缺省时显示所有端口的信息。**模式**

特权模式和所有配置模式

示例

显示所有端口的统计信息：

```
TL-SG3210(config)# show interface counters
```

显示以太网端口 3 的统计信息：

```
TL-SG3210(config)# show interface gigabitEthernet 1/0/3 counters
```

20.16 show interface description

该命令用于显示以太网端口的描述信息。

命令

```
show interface [ gigabitEthernet port ] description
```

参数

port —— 要显示配置信息的以太网端口，缺省时显示所有端口的信息。

模式

特权模式和所有配置模式

示例

显示所有以太网端口的描述信息：

```
TL-SG3210# show interface description
```

显示端口 2 的描述信息：

```
TL-SG3210# show interface gigabitEthernet 1/0/2 description
```

20.17 show interface flowcontrol

该命令用于显示以太网端口的流控信息。

命令

```
show interface [ gigabitEthernet port ] flowcontrol
```

参数

port —— 要显示流控信息的以太网端口，缺省时显示所有端口的信息。

模式

特权模式和所有配置模式

示例

显示所有以太网端口的流控信息：

```
TL-SG3210# show interface flowcontrol
```

显示所有端口 2 的流控信息：

```
TL-SG3210# show interface gigabitEthernet 1/0/2 flowcontrol
```

20.18 show interface configuration

该命令用于显示以太网端口的配置信息，包括端口状态、流量控制、协商模式和端口描述等。

命令

show interface [gigabitEthernet *port*] configuration

参数

port —— 要显示配置信息的以太网端口，缺省时显示所有端口的信息。

模式

特权模式和所有配置模式

示例

显示以太网端口 5 的配置信息：

```
TL-SG3210# show interface gigabitEthernet 1/0/5 configuration
```

20.19 show storm-control

该命令用于显示端口的风暴抑制信息。

命令

show storm-control [interface { gigabitEthernet *port* | range gigabitEthernet *port-list* }]

参数

port /port-list —— 要显示风暴抑制信息的端口号/端口列表，缺省时显示所有端口的风暴抑制信息。

模式

特权模式和所有配置模式

示例

显示端口 4，5，6，7 的风暴抑制信息：

```
TL-SG3210(config)# show storm-control interface gigabitEthernet 1/0/4-7
```

20.20 show bandwidth

该命令用于显示端口的带宽限制信息。

命令

show bandwidth [interface { gigabitEthernet *port* | range gigabitEthernet *port-list* }]

参数

port /port-list —— 要显示风暴抑制信息的端口号/端口列表，缺省时显示所有端口的带宽限制信息。

模式

特权模式和所有配置模式

示例

显示所有端口 5 的带宽限制信息：

```
TL-SG3210(config)# show bandwidth interface gigabitEthernet 1/0/5
```


第21章 QoS 配置命令

QoS（Quality of Service，服务质量）功能用以提高网络传输的可靠性，提供更高质量的网络服务。

21.1 qos

该命令用于设置基于端口的 CoS，它的 no 命令用于恢复某端口的默认 CoS。

命令

qos cos-id

no qos

参数

cos-id —— 端口对应的 CoS 优先级等级，可选范围为 0~7，表示 CoS0~CoS7。默认值为 0。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

说明

端口优先级只是端口的一个属性值，在设置了端口优先级后，数据流会根据端口的 CoS 值以及 IEEE 802.1P 中 CoS 到 TC 之间的映射关系来确定数据流的出口队列。

示例

设置端口 5 的优先级等级为 3：

```
TL-SG3210(config)# interface gigabitEthernet 1/0/5
```

```
TL-SG3210(config-if)# qos 3
```

21.2 qos dscp

该命令用于启用 DSCP 优先级的 DSCP 值与 CoS 优先级的映射关系，它的 no 命令用于禁用该映射关系。

命令

qos dscp

no qos dscp

模式

全局配置模式

说明

DSCP(DiffServ Code Point, 区分服务编码点)是 IEEE 对 IP ToS 字段的重定义, 利用该字段可以将 IP 报文划分为 64 个优先级。开启 DSCP 优先级后, IP 数据流会根据数据包的 DSCP 值到 CoS 优先级, CoS 优先级到 TC 队列之间的映射关系来确定数据包的出口队列。

示例

启用 DSCP 优先级的 DSCP 值和 CoS 优先级的映射关系:

```
TL-SG3210(config)# qos dscp
```

21.3 qos queue cos-map

该命令用于设置 IEEE 802.1P 的优先级 tag 和出口队列的映射关系, 它的 no 命令用于恢复默认设置。IEEE 802.1P 对 IEEE 802.1Q tag 中的 Pri 字段给予了推荐性的定义, 利用该字段可以将数据包划分为 8 个优先级。启用 IEEE 802.1P 优先级后, 交换机根据数据包是否带有 IEEE 802.1Q tag 来确定所使用的优先级模式。对于带有 tag 的数据包, 应用 IEEE 802.1P 优先级, 否则应用基于端口的优先级。

命令

```
qos queue cos-map tag/cos-id tc-id
```

```
no qos queue cos-map
```

参数

tag/cos-id —— IEEE 802.1P 协议里规定的 8 个优先级, 取值范围是 0~7。

tc-id —— tag 对应的出口队列优先级, 可选范围为 0~3, 分别对应 4 个不同等级的出口队列 TC0~TC3。

模式

全局配置模式

说明

1. 默认情况下, tag 和出口队列的对应关系是:
0-TC1, 1-TC0, 2-TC0, 3-TC1, 4-TC2, 5-TC2, 6-TC3, 7-TC3。
2. 优先级等级 TC0、TC1...TC3 中, 数字越大, 表示优先级越高。

示例

设置 tag 优先级 0 的对应出口队列优先级为 TC3:

```
TL-SG3210(config)# qos queue cos-map 0 3
```

21.4 qos queue dscp-map

该命令用于设置 DSCP 优先级的 DSCP 值和 CoS 优先级的映射关系, 它的 **no** 命令用于恢复默认设置。DSCP (DiffServ Code Point, 区分服务编码点) 是 IEEE 对 IP ToS 字段的重定义, 利用该字段可以将 IP 报文划分为 64 个优先级。启用 DSCP 优先级后, 如果转发的数据包是 IP 报文, 则交换机应用 DSCP 优先级; 如果是非 IP 报文, 交换机则根据是否启用了 IEEE 802.1P 优先级以及数据帧是否带有 tag 来决定采用哪种优先级模式。

命令

qos queue dscp-map *dscp-list cos-id*

no qos queue dscp-map

参数

dscp-list —— DSCP 值列表, 可选择一个或多个 DSCP 值, 连续的一组 DSCP 值可以用“-”符号表示, 不连续的值之间、不同组之间需用逗号隔开, 如 1,4-7,11 表示选择 1,4,5,6,7,11。DSCP 值的可选范围为 0~63。

cos-id —— DSCP 值对应的 CoS 优先级, 可选范围为 0~7, 分别对应 8 个不同等级的 CoS 优先级 CoS 0~CoS 7。

模式

全局配置模式

说明

1. 默认情况下, DSCP 值与 CoS 值的对应关系如下: (0-7) - CoS 0, (8-15) - CoS 1, (16-23) - CoS 2, (24-31) - CoS 3, (32-39) - CoS 4, (40-47) - CoS 5, (48-55) - CoS 6, (56-63) - CoS 7。

示例

设置 DSCP 值 10,11,12 对应的 CoS 优先级为 CoS 2:

```
TL-SG3210(config)# qos queue dscp-map 10-12 2
```

21.5 qos queue mode

该命令用于设置出口队列调度模式, 它的 **no** 命令用于恢复默认配置。在网络拥塞时, 通常采用队列调度来解决多个数据流同时竞争使用资源的问题。交换机将根据设置的优先级队列和队列调度算法来控制报文的转发次序。本交换机以 TC0、TC1...TC3 表示不同的优先级队列。

命令

qos queue mode { sp | wrr | sp+wrr | equ }

no qos queue mode

参数

sp —— 严格优先级模式。在此模式下，高优先级队列会占用全部带宽，只有在高优先级队列为空后，低优先级队列才进行数据转发。

wrr —— 加权轮询优先级模式。在此模式下，所有优先级队列按照预先分配的权重比同时发送数据包。TC0 到 TC3 的权重比值是 1: 2: 4: 8。

sp+wrr —— sp 和 wrr 的混合模式。在此模式下，交换机提供了 sp 和 wrr 两个调度组，其中 sp 组和 wrr 组之间遵循的是严格优先级调度规则，而 wrr 组内部队列遵循的是 wrr 调度规则。在该调度模式下，TC3 属于 sp 组；TC0、TC1 和 TC2 属于 wrr 组，权重比是 1: 2: 4。这样在调度的时候首先是 TC3 按照 sp 的调度模式独自占用带宽，然后是 wrr 组的成员 TC0、TC1 和 TC2 按照权重比 1: 2: 4 的比例占用带宽。

equ —— 无优先级模式，默认选项。在此模式下所有的队列公平地占用带宽，所有队列的权重比是 1: 1: 1: 1。

模式

全局配置模式

示例

设置出口队列的调度模式为加权轮询优先级模式：

```
TL-SG3210(config)# qos queue mode wrr
```

21.6 show qos interface

该命令用于显示基于端口优先级的配置信息。

命令

```
show qos interface [ gigabitEthernet port | range gigabitEthernet port-list ]
```

参数

port /port-list —— 要显示基于端口优先级配置信息的以太网端口号/端口列表，缺省时显示所有端口的信息。

模式

特权模式和所有配置模式

示例

显示以太网端口 5 的 QoS 配置信息：

```
TL-SG3210# show qos interface gigabitEthernet 1/0/5
```

21.7 show qos cos-map

该命令用于显示 IEEE 802.1P 优先级的配置信息。

命令

show qos cos-map

模式

特权模式和所有配置模式

示例

显示 IEEE 802.1P 优先级的配置信息：

```
TL-SG3210# show qos cos-map
```

21.8 show qos dscp-map

该命令用于显示 DSCP 优先级的配置信息。

命令

show qos dscp-map

模式

特权模式和所有配置模式

示例

显示 DSCP 优先级的配置信息：

```
TL-SG3210# show qos dscp-map
```

21.9 show qos queue mode

该命令用于显示出口队列的调度规则。

命令

show qos queue mode

模式

特权模式和所有配置模式

示例

显示出口队列的调度规则：

```
TL-SG3210# show qos queue mode
```

21.10 show qos status

该命令用于显示 IEEE 802.1P 优先级和 DSCP 优先级的启用状态。

命令

show qos status

模式

特权模式和所有配置模式

示例

显示 IEEE 802.1P 优先级和 DSCP 优先级的启用状态：

```
TL-SG3210# show qos status
```

第22章 端口监控配置命令

端口监控是将被监控端口的报文复制到监控端口，在监控端口接入数据分析设备，利用该设备分析经过监控端口的报文，达到网络监控和故障排除的目的。

22.1 monitor session destination interface

该命令用于启用端口监控功能，并设置监控端口。它的 **no** 命令用于删除某个监控组。

命令

```
monitor session session_num destination interface gigabitEthernet port  
no monitor session session_num
```

参数

session_num —— 监控组组号。取值范围 1-4。

port —— 监控端口号。

模式

全局配置模式

示例

设置端口 1 为监控组 1 的监控端口：

```
TL-SG3210(config)# monitor session 1 destination interface gigabitEthernet 1/0/1
```

删除监控组 1：

```
TL-SG3210(config)# no monitor session 1
```

22.2 monitor session source interface

该命令用于设置被监控端口，它的 **no** 命令用于删除相应的被监控端口。

命令

```
monitor session session_num source interface gigabitEthernet port-list mode  
no monitor session session_num source interface gigabitEthernet port-list mode
```

参数

session_num —— 监控组组号。取值范围 1-4。

port-list —— 被监控端口列表，可选择一个或多个端口。

mode —— 监控模式。有三种选择：**rx**、**tx** 以及 **both**。**rx**（入口监控模式），将被监控端口收到的数据复制到监控端口，进行监控。**tx**（出口监控模式），将被监控端口发出的数据复制到监控端口，进行监控。**both**，同时进行入口监控和出口监控。

模式

全局配置模式

说明

1. 被监控端口个数不做限制，但它不可以同时为监控端口。
2. 监控端口和被监控端口可以处于同一 VLAN 中，也可以不处于同一 VLAN 中。
3. 监控端口和被监控端口不能为汇聚端口成员。

示例

设置端口 4,5,7 为监控组 1 的被监控端口，并开启入口监控：

```
TL-SG3210(config)# monitor session 1 source interface gigabitEthernet  
1/0/4-5,1/0/7 rx
```

删除监控组 1 的端口 4 及其配置：

```
TL-SG3210(config)# no monitor session 1 source interface gigabitEthernet 1/0/4  
rx
```

22.3 show monitor session

该命令用于显示监控组的监控信息。

命令

show monitor session [session_num]

参数

session_num —— 指定监控组组号，缺省情况下显示所有监控组的监控信息。取值范围 1-4。

模式

特权模式和所有配置模式

示例

显示监控组 1 的监控配置信息：

```
TL-SG3210# show monitor session 1
```

显示所有监控组的监控配置信息：

```
TL-SG3210# show monitor session
```


第23章 端口隔离配置命令

端口隔离功能可以严格限制一个端口到另外一组端口的数据转发，从而提高网络的安全性。

23.1 port isolation

该命令用于设置每个端口的端口隔离功能，限制每个端口仅可以向转发端口列表中的端口转发数据包。它的 **no** 命令用于删除相应设置。

命令

port isolation gi-forward-list *gi-forward-list*

no port isolation

参数

gi-forward-list —— 转发端口列表，可选择一个或多个端口。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

由端口 1 仅可以向端口 2,5,6,7 转发数据包：

```
TL-SG3210(config)# interface gigabitEthernet 1/0/1
```

```
TL-SG3210(config-if)# port isolation gi-forward-list 1/0/2,1/0/5-7
```

23.2 show port isolation

该命令用于查看每个端口的转发端口列表。

命令

show port isolation interface [*gigabitEthernet port*]

参数

port —— 选择希望查看转发端口列表信息的端口号。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

显示端口 6 的转发端口列表：

```
TL-SG3210# show port isolation interface gigabitEthernet 1/0/6
```

显示所有端口的转发端口列表：

```
TL-SG3210# show port isolation interface
```


第24章 环路监测配置命令

环路监测功能可以检测出交换机物理端口所连接的网络中是否存在环路，从而降低网络中产生广播风暴的风险。

24.1 loopback-detection(global)

该命令用于启用全局环路监测功能。它的 no 命令用于关闭全局环路监测功能。

命令

loopback-detection

no loopback-detection

模式

全局配置模式

示例

启用交换机环路监测功能：

```
TL-SG3210(config)# loopback-detection
```

24.2 loopback-detection interval

该命令用于配置环路监测的时间间隔，交换机在每个周期内发送一个监测报文来监测网络是否存在环路。

命令

loopback-detection interval [*interval-time*]

参数

interval-time —— 配置环路监测的间隔时间，默认为 30 秒。

模式

全局配置模式

示例

配置环路监测的间隔时间为 50 秒：

```
TL-SG3210(config)# loopback-detection interval 50
```

24.3 loopback-detection recovery-time

该命令用于配置端口阻塞后的恢复时间。

命令

loopback-detection recovery-time *recovery-time*

参数

recovery-time —— 当端口监测到网络出现环路时，将阻塞端口。在配置的恢复时间后，阻塞的端口将恢复正常属性，并重新监测环路。恢复时间请设置为监测间隔时间的整数倍，取值范围为 1-100 个监测时间间隔，默认为 3。

模式

全局配置模式

示例

配置环路监测的恢复时间为 5 个监测间隔时间：

```
TL-SG3210(config)# loopback-detection recovery-time 5
```

24.4 loopback-detection(interface)

该命令用于启用指定端口的环路监测功能。它的 no 命令用于关闭全局环路监测功能。

命令

loopback-detection

no loopback-detection

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

启用端口 2-5 的环路监测功能：

```
TL-SG3210(config)# interface range gigabitEthernet 1/0/2-5
```

```
TL-SG3210(config-if-range)# loopback-detection
```

24.5 loopback-detection config

该命令用于配置端口阻塞后的处理模式和恢复模式。

命令

loopback-detection config [**process-mode** { alert | port-based }] [**recovery-mode** { auto | manual }]

参数

process-mode —— 选择端口发现环路时的处理模式。有两个选项：

Alert: 端口上发现环路时只发出报警信息。

Port based: 端口上发现环路时发出报警信息，同时阻塞端口。

recovery-mode —— 选择端口被阻塞后的恢复模式。有两个选项：

Auto: 端口被阻塞后经过自动恢复时间后会自动解除阻塞。

Manual: 端口被阻塞后只能手动解除阻塞状态。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

配置端口 5 的环路监测处理模式为 port-based，恢复模式为 manual：

```
TL-SG3210(config)# interface gigabitEthernet 1/0/5
TL-SG3210(config-if)# loopback-detection config process-mode port-based
recovery-mode manual
```

24.6 loopback-detection recover

该命令用于将指定的阻塞端口恢复为正常状态。

命令

loopback-detection recover

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

将端口 5 由阻塞状态恢复为正常状态：

```
TL-SG3210(config)# interface gigabitEthernet 1/0/5
TL-SG3210(config-if)# loopback-detection recover
```

24.7 show loopback-detection global

该命令用于显示环路监测功能的全局配置参数。

命令

show loopback-detection global

模式

特权模式和所有配置模式

示例

查看环路监测功能的全局配置参数：

```
TL-SG3210# show loopback-detection global
```

24.8 show loopback-detection interface

该命令用于显示所有端口的环路监测功能配置参数及端口状态。

命令

show loopback-detection interface [gigabitEthernet *port*]

参数

port—— 指定端口号，缺省时显示所有端口的信息。

模式

特权模式和所有配置模式

示例

查看所有端口的环路监测功能配置参数及端口状态：

```
TL-SG3210# show loopback-detection interface
```

查看端口 5 的环路监测功能配置参数及端口状态：

```
TL-SG3210# show loopback-detection interface gigabitEthernet 1/0/5
```

第25章 PoE 配置命令



注意：

- 本书所列举的机型中只有 TL-SG3424P 支持 PoE 功能。

PoE(Power over Ethernet, 以太网供电, 又称远程供电)是指设备通过以太网线对外接 PD(Powered Device, 受电设备)设备(如 IP 电话、无线 AP、网络摄像机等)进行远程供电。

25.1 power inline consumption (global)

该命令用于配置 PoE 交换机所能提供的最大功率。

命令

power inline consumption {power limit}

参数

power limit——PoE 交换机所能提供的最大功率，取值范围为 1W-320W。

模式

全局配置模式

示例

配置 PoE 交换机所能提供的最大功率为 160W：

```
TL-SG3424P(config)# power inline consumption 160
```

25.2 power inline supply

该命令用于启用或禁用相应端口的 PoE 功能。

命令

power inline supply {enable|disable}

参数

enable|disable—— 启用或禁用相应端口的 PoE 功能。

模式

接口配置模式 (interface gigabitEthernet / interface range gigabitEthernet)

示例

启用端口 2 的 PoE 功能：

```
TL-SG3424P(config)# interface gigabitEthernet 1/0/2
```

```
TL-SG3424P(config-if)# power inline supply enable
```

25.3 power inline priority

该命令用于为相应的端口配置 PoE 优先级。

命令

power inline priority {low|middle|high}

参数

priority——当剩余功率不够时，与供电管理方式一起决定对新接入的 PD 的供电方式，优先级等级包括低（low）、中（middle）、高（high）三种。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

配置端口 2 的 PoE 优先级为低：

```
TL-SG3424P(config)# interface gigabitEthernet 1/0/2
TL-SG3424P(config-if)# power inline priority low
```

25.4 power inline consumption (interface)

该命令用于配置端口供电功率上限。

命令

power inline consumption {power limit}

参数

power limit——相应端口能提供的最大供电功率。取值范围为 1-300。功率上限为输入值乘以 0.1W。例如，要设置某端口最大供电功率为 5W，则此处应输入 50。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

配置端口 2 的最大供电功率为 5W：

```
TL-SG3424P(config)# interface gigabitEthernet 1/0/2
TL-SG3424P(config-if)# power inline consumption 50
```

25.5 power time-range

该命令用于添加时间段并进入 PoE 时间段设置模式。在 PoE 时间段设置模式下可进一步通过 holiday, absolute 或 periodic 命令具体配置该时间段。它的 no 命令用于删除相应的时间段。当用户需要某些端口在特定时间段供电时，可以先配置时间段，然后将其应用于这些端口即可。这些端口将只在指定的时间段内供电。

命令

```
power time-range {name}  
no power time-range {name}
```

参数

name——要添加的时间段名称。可输入 1-16 个字符。

模式

全局配置模式

示例

添加一个名为 tRange1 的时间段：

```
TL-SG3424P(config)# power time-range tRange1
```

25.6 holiday

该命令用于配置已创建的时间段是否包含 PoE 节假日。PoE 节假日可通过 power holiday 命令定义。

命令

```
holiday { exclude | include }
```

参数

exclude ——不包含 PoE 节假日，即 PoE 节假日期间交换机不为受电设备供电。

include —— 包含节假日，即 PoE 节假日期间交换机交换机仍为受电设备供电。默认选择该项。

模式

PoE 时间段设置模式（power time-range）

示例

将配置时间段 tRange3 为不包含节假日：

```
TL-SG3424P(config)# power time-range tRange3
```

```
TL-SG3424P(config-pwr-time-range)# holiday exclude
```

25.7 absolute

该命令用于配置已创建的时间段的绝对起始日期，设置后交换机将只在该起始日期期间为受电设备供电。它的 no 命令用于取消配置的绝对时间。

命令

```
absolute start start-date end end-date  
no absolute
```

参数

start-date ——起始日期，格式为 MM/DD/YYYY，如 01/01/2012。

end-date —— 结束日期，格式为 MM/DD/YYYY，如 12/31/2013。

模式

PoE 时间段设置模式（power time-range）

示例

配置时间段 tRange1 为从 2012 年 5 月 5 日至 2012 年 10 月 5 日：

```
TL-SG3424P(config)# power time-range tRange1
```

```
TL-SG3424P(config-pwr-time-range)# absolute start 05/05/2012 end 10/05/2012
```

25.8 periodic

该命令用于以周期模式配置已创建的时间段，即可让交换机在一周中的某几天为受电设备供电。它的 no 命令用于取消配置的周期时间。

命令

```
periodic { [ week-date week-day ] [ time-slice1 time-slice ] [ time-slice2 time-slice ]  
[ time-slice3 time-slice ] [ time-slice4 time-slice ] }
```

```
no periodic [ week-date | time-slice ]
```

参数

week-day ——周期模式，形式为 1-3, 6，也可输入 daily, off-day, working-day。其中 1-3, 6 表示周一、周二、周三和周六；daily 表示每天，即周一到周日；off-day 表示周末，即周六和周日；working-day 表示工作日，即周一到周五。缺省时禁止周期模式。

time-slice —— 创建时间片段，格式为 HH:MM-HH:MM，如 08:30-12:00。

week-date | time-slice——取消配置的周期时间中的周期模式或时间片段。

模式

PoE 时间段设置模式（power time-range）

示例

配置时间段 tRange2 为每周末的 08:30-12:00：

```
TL-SG3424P(config)# power time-range tRange2
```

```
TL-SG3424P(config-pwr-time-range)# periodic week-date off-day time-slice1  
08:30-12:00
```

25.9 power holiday

该命令用于创建 power time-range 假期模式的节假日，它的 no 命令用于删除相应节假日。

命令

power holiday *name* **start-date** *start-date* **end-date** *end-date*

no power holiday {*name*}

参数

name —— 节假日名称，可输入 1~16 个字符。

start-date —— 节假日的起始日期，格式为 MM/DD，如 05/01。

end-date —— 节假日的结束日期，格式为 MM/DD，如 05/03。

模式

全局配置模式

示例

定义节假日国庆节，并设置其起止时间为 10 月 1 日到 10 月 3 日：

```
TL-SG3424P(config)# power holiday NationalDay start-date 10/01 end-date 10/03
```

25.10 power inline time-range

该命令用于为端口配置供电的时间段。它的 no 命令用于取消已选的时间段。

命令

power inline time-range {*name*}

no power inline time-range

参数

name —— 已创建的时间段的名称。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

选择时间段 tRange2 作为端口 2 的供电时间段：

```
TL-SG3424P(config)# interface gigabitEthernet 1/0/2
```

```
TL-SG3424P(config-if)# power inline time-range tRange2
```

25.11 power profile

该命令用于创建一个新的 PoE profile 文件。它的 no 命令用于删除已配置的 PoE profile 文件。PoE profile 文件用于对具有相同属性的 PoE 接口进行批量配置，以简化用户的操作。在 PoE profile 文件中，配置了端口的三个 PoE 属性：状态、优先级、最大功率。创建一个 PoE profile 文件，然后将其应用于相应的端口，可简化配置过程。

命令

```
power profile name [supply {enable | disable} [priority {low | middle | high}
[consumption { power-limit | auto | class1 | class2 | class3 | class4 }]]]
no power profile name
```

参数

name——profile 文件的名称，可输入 1-16 个字符。如果文件的名称包含空格，请将该名称放在双引号中，如“File 2”。

supply——profile 文件中设置的端口 PoE 状态。

priority——profile 文件中设置的端口 PoE 优先级。

consumption——profile 文件中设置的端口 PoE 最大功率。有 *power-limit*, *auto*, *class1*, *class2*, *class3* 和 *class4* 五个可选项。*power-limit* 表示可手动输入具体数值，取值范围为 1-300，功率上限为输入值乘以 0.1W。例如，要设置某端口最大供电功率为 5W，则此处应输入 50。*auto* 表示由系统自动指定端口的 PoE 最大功率。*class1* 表示 4W。*class2* 表示 7W。*class3* 表示 15.4W。*class4* 表示 30W。

模式

全局配置模式

示例

创建一个 PoE profile 文件。profile 文件的名称是 IP Camera，PoE 状态为开启，PoE 优先级为低，最大功率为 5W。

```
TL-SG3424P(config)# power profile "IP Camera" supply enable priority low
consumption 50
```

25.12 power inline profile

该命令用于将 PoE profile 文件应用于所选的端口。它的 no 命令用于取消应用 PoE profile 文件。

命令

```
power inline profile name
no power inline profile
```

参数

name——已配置的 profile 文件的名称，可输入 1-16 个字符。如果文件的名称包含空格，请将该名称放在双引号中，如“File 2”。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

将名为 IP Camera 的 PoE profile 文件应用于端口 2：

```
TL-SG3424P(config)# interface gigabitEthernet 1/0/2
```

```
TL-SG3424P(config-if)# power inline profile "IP Camera"
```

25.13 show power inline

该命令用于显示系统 PoE 信息。

命令

```
show power inline
```

模式

特权模式和所有配置模式

示例

显示系统 PoE 信息：

```
TL-SG3424P# show power inline
```

25.14 show power inline configuration interface

该命令用于显示某端口的 PoE 配置信息。

命令

```
show power inline configuration interface [ gigabitEthernet port ]
```

参数

port —— 要显示 PoE 配置信息的端口号，缺省显示所有端口的 PoE 信息。

模式

特权模式和所有配置模式

示例

显示所有端口的 PoE 配置信息：

```
TL-SG3424P# show power inline configuration interface
```

25.15 show power inline information interface

该命令用于显示某端口的 PoE 信息。

命令

```
show power inline information interface [ gigabitEthernet port ]
```

参数

port —— 要显示 PoE 信息的端口号，缺省显示所有端口的 PoE 信息。

模式

特权模式和所有配置模式

示例

显示所有端口的 PoE 信息：

```
TL-SG3424P# show power inline information interface
```

25.16 show power time-range

该命令用于显示时间段配置信息。

命令

```
show power time-range
```

模式

特权模式和所有配置模式

示例

显示所有的时间段信息：

```
TL-SG3424P# show power time-range
```

25.17 show power holiday

该命令用于显示已定义的节假日。

命令

```
show power holiday
```

模式

特权模式和所有配置模式

示例

显示已定义的节假日：

```
TL-SG3424P# show power holiday
```

25.18 show power profile

该命令用于显示已定义的 PoE profile 文件。

命令

```
show power profile
```

模式

特权模式和所有配置模式

示例

显示已定义的 PoE profile 文件：

```
TL-SG3424P# show power profile
```

第26章 ACL 配置命令

ACL（Access Control List，访问控制列表），通过配置匹配规则、处理操作以及时间权限来实现对数据包的过滤，提供灵活的安全访问控制策略，为控制网络安全提供方便。

26.1 time-range

该命令用于添加时间段，它的 **no** 命令用于删除对应的时间段。当用户配置的 ACL 规则需要按时间段进行过滤时，可以先配置时间段，然后在相应的规则下通过时间段名称引用该时间段，这条规则只在该指定的时间段内生效，从而实现基于时间段的 ACL 过滤。

命令

time-range *name*

no time-range *name*

参数

name —— 要添加的时间段名称，可输入 1~16 个字符。

模式

全局配置模式

示例

添加一个名为 tSeg1 的时间段：

```
TL-SG3210(config)# time-range tSeg1
```

26.2 absolute

该命令用于配置时间段为绝对模式，它的 **no** 命令用于禁用绝对模式。

命令

absolute start *start-date* **end** *end-date*

no absolute

参数

start-date —— 绝对模式下的起始日期，形式为 MM/DD/YYYY，缺省时为 01/01/2000。

end-date —— 绝对模式下的结束日期，形式为 MM/DD/YYYY，缺省时为 01/01/2000。

若起始日期和结束日期同时缺省，则禁止绝对模式。

模式

时间段配置模式（time-range create）

示例

配置时间段 tSeg1 为绝对模式，时间范围为 2012 年 5 月 5 日至 2012 年 10 月 5 日：


```
TL-SG3210(config)# time-range tSeg1
```

```
TL-SG3210(config-time-range)# absolute start 05/05/2012 end 10/05/2012
```

26.3 periodic

该命令用于配置时间段为周期模式，它的 **no** 命令用于禁用周期模式。

命令

```
periodic [week-date week-day] [time-slice1 time-slice] [time-slice2 time-slice]
```

```
[time-slice3 time-slice] [time-slice4 time-slice]
```

```
no periodic
```

参数

week-day —— 周期模式，形式为 1-3, 6，也可输入 **daily**, **off-day**, **working-day**。其中 1-3, 6 表示周一、周二、周三和周六；**daily** 表示每天，即周一到周日；**off-day** 表示周末，即周六和周日；**working-day** 表示工作日，即周一到周五。缺省时禁止周期模式。

time-slice —— 添加时间片段，形式为 HH:MM-HH:MM。

模式

时间段配置模式（time-range create）

示例

编辑已添加的 tSeg1 时间段，时间范围为周末的 08:30-12:00：

```
TL-SG3210(config)# time-range tSeg1
```

```
TL-SG3210(config-time-range)# periodic week-date off-day time-slice1
```

```
08:30-12:00
```

26.4 holiday

该命令用于在时间段配置模式下将指定时间段配置为假日模式。它的 **no** 命令用于禁用假日模式。

命令

```
holiday
```

```
no holiday
```

模式

时间段配置模式（time-range create）

示例

编辑已添加的 tSeg1 时间段为假日模式：

```
TL-SG3210(config)# time-range tSeg1
```

```
TL-SG3210(config-time-range)# holiday
```

26.5 holiday(global)

该命令用于创建 [time-range](#) 假期模式的节假日，它的 no 命令用于删除相应节假日。

命令

```
holiday name start-date start-date end-date end-date
```

```
no holiday
```

参数

name —— 节假日名称，可输入 1~16 个字符。

start-date —— 节假日的起始日期，格式为 MM/DD，如 05/01。

end-date —— 节假日的结束日期，格式为 MM/DD，如 05/03。

模式

全局配置模式

示例

定义节假日国庆节，并设置其起止时间为 10 月 1 日到 10 月 3 日：

```
TL-SG3210(config)# holiday nationalday start-date 10/01 end-date 10/03
```

26.6 access-list create

该命令用于创建标准 IP ACL 和扩展 IP ACL。

命令

```
access-list create access-list-num
```

参数

access-list-num —— ACL ID 号，取值范围为 100-299，100-199 为标准 IP 访问控制列表，200-299 为扩展 IP 访问控制列表。

模式

全局配置模式

示例

创建一个 ID 号为 123 的标准 IP ACL：

```
TL-SG3210(config)# access-list create 123
```

26.7 mac access-list

该命令用于创建 MAC ACL，它的 no 命令用于删除对应的 MAC ACL。MAC ACL 根据数据包的源 MAC 地址、目的 MAC 地址、VLAN、二层协议类型等二层信息制定匹配规则，对数据包进行相应的分析处理。

命令

mac access-list access-list-num

no mac access-list access-list-num

参数

access-list-num —— 要添加规则的 ACL ID 号，取值范围为 0-99。

模式

全局配置模式

示例

创建一个 ID 号为 23 的 MAC ACL：

```
TL-SG3210(config)# mac access-list 23
```

26.8 access-list standard

该命令用于添加标准 IP ACL 规则，它的 no 命令用于删除对应规则。标准 IP ACL 可以根据数据包的 IP 地址信息制定匹配规则，对数据包进行相应的分析处理。

命令

access-list standard acl-id rule rule-id {deny | permit} [[sip source-ip] smask source-ip-mask] [[dip destination-ip] dmask destination-ip-mask] [tseg time-segment]

no access-list standard acl-id rule rule-id

参数

acl-id —— 要添加规则的 ACL ID 号。

rule-id —— 当前添加的规则 ID 号。

op —— 交换机对满足匹配规则的数据包的处理方式。其中 deny 表示丢弃数据包；permit 表示转发数据包。缺省时为 permit。

source-ip —— 规则包含的源 IP 地址。

source-ip-mask —— 源 IP 地址的掩码。若您输入了源 IP 地址，则必须输入相应的掩码。

destination-ip —— 规则包含的目的 IP 地址。

destination-ip-mask —— 目的 IP 地址的掩码。若您输入了目的 IP 地址，则必须输入相应的掩码。

time-segment —— 规则生效的时间段的名称，缺省时为无限制。

模式

全局配置模式

示例

创建一个 ID 号为 120 的标准 IP ACL, 为其添加规则 10, 其中源 IP 地址为 192.168.0.100, 掩码为 255.255.255.0, 规则生效的时间段为 tSeg1, 对满足此规则的数据包, 交换机予以转发:

```
TL-SG3210(config)# access-list create 120
```

```
TL-SG3210(config)# access-list standard 120 rule 10 permit sip 192.168.0.100 smask
255.255.255.0 tseg tSeg1
```

26.9 access-list extended

该命令用于添加扩展 IP ACL 规则, 它的 no 命令用于删除对应规则。

命令

```
access-list extended acl-id rule rule-id {deny | permit} [ [sip source-ip] smask
source-ip-mask] [ [dip destination-ip] dmask destination-ip-mask] [tseg time-segment]
[dscp dscp] [s-port s-port] [d-port d-port] [tcpflag tcpflag] [protocol protocol] [tos tos]
[pre pre]
```

```
no access-list extended acl-id rule rule-id
```

参数

acl-id —— 要添加规则的 ACL ID 号。

rule-id —— 当前添加的规则 ID 号。

op —— 交换机对满足匹配规则的数据包的处理方式。其中 deny 表示丢弃数据包; permit 表示转发数据包。缺省时为 permit。

source-ip —— 规则包含的源 IP 地址。

source-ip-mask —— 源 IP 地址的掩码。若您输入了源 IP 地址, 则必须输入相应的掩码。

destination-ip —— 规则包含的目的 IP 地址。

destination-ip-mask —— 目的 IP 地址的掩码。若您输入了目的 IP 地址, 则必须输入相应的掩码。

time-segment —— 规则生效的时间段的名称, 缺省时为无限制。

dscp —— 设置 dscp 的值, 范围 0-63。

s-port —— 当 IP 协议选择 TCP/UDP 时, 此处配置规则包含的 TCP/UDP 源端口号。

d-port —— 当 IP 协议选择 TCP/UDP 时, 此处配置规则包含的 TCP/UDP 目的端口号。

tcpflag —— 使用 TCP 协议时, 设置 flag 的值。

protocol —— 设置匹配的协议字段的值。

tos —— 规则包含的 IP ToS 字段信息。

Pre —— 规则包含的 IP Precedence 字段信息。

模式

全局配置模式

示例

创建一个 ID 号为 220 的扩展 IP ACL，为其添加规则 10，其中源 IP 地址为 192.168.0.100，掩码为 255.255.255.0，规则生效的时间段为 tSeg1，对满足此规则的数据包，交换机予以转发：

```
TL-SG3210(config)# access-list create 220
```

```
TL-SG3210(config)# access-list extended 220 rule 10 permit sip 192.168.0.100 smask
255.255.255.0 tseg tSeg1
```

26.10 rule

该命令用于编辑已创建的 MAC ACL 规则，它的 no 命令用于删除相应的规则。

命令

rule *rule-id* {deny | permit} [**smac** *source-mac* **smask** *source-mac-mask*] [**dmac** *destination-mac* **dmask** *destination-mac-mask*] [**vid** *vlan-id*] [**type** *ethernet-type*] [**pri** *user-pri*] [**tseg** *time-segment*]

no rule *rule-id*

参数

rule-id —— 当前添加的规则 ID 号。

op —— 交换机对满足匹配规则的数据包的处理方式。其中 deny 表示丢弃数据包；permit 表示转发数据包。缺省时为 permit。

source-mac —— 规则包含的源 MAC 地址。

source-mac-mask —— 源 MAC 地址的掩码。若您输入了源 MAC 地址，则必须输入相应的掩码。

destination-mac —— 规则包含的目的 MAC 地址。

destination-mac-mask —— 目的 MAC 地址的掩码。若您输入了目的 MAC 地址，则必须输入相应的掩码。

vlan-id —— 规则包含的 VLAN ID 号，取值范围为 1~4094。

ethernet-type —— 规则包含的以太网类型信息，输入格式为 4 位 16 进制数。

user-pri —— 用户优先级，取值范围为 0~7，缺省时为无限制。

time-segment —— 规则生效的时间段的名称，缺省时为无限制。

模式

Mac Access-list 配置模式

示例

编辑 MAC ACL 20 的规则 10，其中源 MAC 地址为 00:01:3F:48:16:23，掩码为 11:11:11:11:11:00，VLAN ID 为 2，用户优先级为 5，规则生效的时间段为 tSeg1，对满足此规则的数据包，交换机予以转发：

```
TL-SG3210(config)# mac access-list 20
```

```
TL-SG3210(config-mac-acl)# rule 10 permit smac 00:01:3F:48:16:23 smask  
11:11:11:11:11:00 vid 2 pri 5 tseg tSeg1
```

26.11 access-list policy name

该命令用于添加 Policy，它的 no 命令用于删除对应的 Policy 条目。Policy 功能将 ACL 和动作组合起来，组成一个访问控制策略，对符合相应 ACL 规则的数据包进行控制，添加的操作包括流镜像、流监控、QoS Remarking 和端口重定向。

命令

access-list policy name *name*

no access-list policy name *name*

参数

name —— 要添加的 Policy 名称，可输入 1~16 个字符。

模式

全局配置模式

示例

添加一个名为 policy1 的 Policy：

```
TL-SG3210(config)# access-list policy name policy1
```

26.12 access-list policy action

该命令用于为 Policy 添加 ACL 并进入 Action 配置模式以设置动作，它的 no 命令用于删除相应动作。

命令

access-list policy action *policy-name acl-id*

no access-list policy action *policy-name acl-id*

参数

policy-name —— 要设置的 Policy 的名称，可输入 1~16 个字符。

acl-id —— Policy 作用的 ACL 的 ID 号。

模式

全局配置模式

示例

为名为 policy1 的 Policy 添加 ACL 120:

```
TL-SG3210(config)# access-list policy action policy1 120
```

26.13 redirect interface

该命令用于为 Policy 添加重定向动作，设置将匹配了相应 ACL 的数据包转发到指定端口。

命令

redirect interface gigabitEthernet *port*

参数

port —— 端口重定向的出口端口，即将匹配了相应 ACL 的数据包转发到此处指定的端口。缺省时为所有端口。

模式

Action 配置模式

示例

为名为 policy1 的 Policy 添加动作，对符合 ACL 120 相应规则的数据包，转发到端口 2:

```
TL-SG3210(config)# access-list policy action policy1 120
```

```
TL-SG3210(config-action)# redirect interface gigabitEthernet 1/0/2
```

26.14 s-condition

该命令用于为 Policy 添加流监管动作。

命令

s-condition rate *rate* osd { none | discard }

参数

rate —— 流监管的额定速率，取值范围为 1~1000000（kbps）。

osd —— 流监管的超速处理，即对超过额定速率的数据包的处理方式，有不处理（none）和丢弃（discard）两个选项。缺省时为不处理。

模式

Action 配置模式

示例

为名为 policy1 的 Policy 添加动作，对符合 ACL 120 相应规则的数据包，若速率超过 1000kbps，交换机将予以丢弃：

```
TL-SG3210(config)# access-list policy action policy1 120
```

```
TL-SG3210(config-action)# s-condition rate 1000 osd discard
```

26.15 s-mirror

该命令用于为 Policy 添加流镜像动作。

命令

```
s-mirror interface gigabitEthernet port
```

参数

port —— 流镜像的镜像端口。

模式

Action 配置模式

示例

为名为 policy1 的 Policy 添加动作，将符合 ACL 120 相应规则的数据包复制到端口 2：

```
TL-SG3210(config)# access-list policy action policy1 120
```

```
TL-SG3210(config-action)# s-mirror interface gigabitEthernet 1/0/2
```

26.16 qos-remark

该命令用于为 Policy 添加 QoS 重标记动作，它的 no 命令用于删除相应动作。

命令

```
qos-remark dscp dscp priority pri
```

```
no qos-remark
```

参数

dscp —— QoS 重标记之 DSCP，为匹配了相应 ACL 的数据包指定 DSCP 域。取值范围为 0~63，缺省时为无限制。

pri —— QoS 重标记之本地优先级，为匹配了相应 ACL 的数据包指定优先级。取值范围为 0~3。

模式

Action 配置模式

示例

为名为 policy1 的 Policy 添加动作，对符合 ACL 120 相应规则的数据包，指定 DSCP 域为 30，优先级为 2：


```
TL-SG3210(config)# access-list policy action policy1 120
```

```
TL-SG3210(config-action)# qos-remark dscp 30 priority 2
```

26.17 access-list bind(interface)

该命令用于绑定 Policy 到指定端口，它的 no 命令用于取消绑定。

命令

```
access-list bind policy-name
```

```
no access-list bind policy-name
```

参数

policy-name —— 要绑定到端口的 Policy 名称。

模式

接口配置模式（interface gigabitEthernet）

示例

将 policy1 绑定到端口 2:

```
TL-SG3210(config)# interface gigabitEthernet 1/0/2
```

```
TL-SG3210(config-if)# access-list bind policy1
```

26.18 access-list bind(vlan)

该命令用于绑定 Policy 到指定 VLAN，它的 no 命令用于取消绑定。

命令

```
access-list bind policy-name
```

```
no access-list bind policy-name
```

参数

policy-name —— 要绑定到 VLAN 的 Policy 名称。

模式

接口配置模式（interface vlan）

示例

将 policy1 绑定到 VLAN 2:

```
TL-SG3210(config)# interface vlan 2
```

```
TL-SG3210(config-if)# access-list bind policy1
```

26.19 show time-range

该命令用于显示所有时间段的配置。

命令

show time-range

模式

特权模式和所有配置模式

示例

显示所有时间段配置：

```
TL-SG3210# show time-range
```

26.20 show holiday

该命令用于显示所有已定义的节假日。

命令

show holiday

模式

特权模式和所有配置模式

示例

显示节假日设置：

```
TL-SG3210# show holiday
```

26.21 show access-list

该命令用于显示 ACL 配置。

命令

show access-list [*acl-id*]

参数

acl-id —— 要显示配置的 ACL ID 号。

模式

特权模式和所有配置模式

示例

显示 ID 号为 20 的 MAC ACL 的配置：

```
TL-SG3210# show access-list 20
```

26.22 show access-list policy

该命令用于显示 Policy 配置。

命令

show access-list policy [*name*]

参数

name —— 要显示配置的 policy 的描述。

模式

特权模式和所有配置模式

示例

显示名为 policy1 的信息：

```
TL-SG3210# show access-list policy policy1
```

26.23 show access-list bind

该命令用于显示 Policy 绑定配置。

命令

show access-list bind

模式

特权模式和所有配置模式

示例

显示 Policy 绑定设置：

```
TL-SG3210# show access-list bind
```

第27章 MSTP 配置命令

MSTP（Multiple Spanning Tree Protocol，多生成树协议）是在 STP 和 RSTP 的基础上，根据 IEEE 协会制定的 IEEE 802.1S 标准建立的，用于在局域网中消除数据链路层物理环路的协议。生成树协议的基本思想是通过构造一棵或多棵自然树的方法达到裁剪冗余环路的目的，同时实现链路备份和路径最优化。

27.1 spanning-tree(global)

该命令用于全局开启生成树功能，它的 no 命令用于禁用生成树功能。

命令

spanning-tree

no spanning-tree

模式

全局配置模式

示例

开启交换机的生成树功能：

```
TL-SG3210(config) # spanning-tree
```

27.2 spanning-tree(interface)

该命令用于为指定端口开启生成树功能，它的 no 命令用于禁用生成树功能。

命令

spanning-tree

no spanning-tree

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

开启端口 2 的生成树功能：

```
TL-SG3210(config) # interface gigabitEthernet 1/0/2
```

```
TL-SG3210(config-if)# spanning-tree
```

27.3 spanning-tree common-config

该命令用于生成树协议端口配置，它的 **no** 命令用于恢复默认配置。CIST（Common and Internal Spanning Tree，公共和内部生成树）是连接一个交换网络内所有设备的单生成树。本命令用来配置端口基于 CIST 的参数以及所有实例的共用参数。

命令

spanning-tree common-config [**port-priority** *pri*] [**ext-cost** *ext-cost*] [**int-cost** *int-cost*] [**portfast** {enable | disable}] [**point-to-point** {auto | open | close}]

no spanning-tree common-config

参数

pri —— 端口优先级，它是确定端口是否会被对端设备选为根端口的重要依据，同等条件下优先级高的端口将被选为根端口。值越小，表示优先级越高。取值范围 0~240，间隔 16，缺省时为 128。

ext-cost —— 外部路径开销。它是在不同 MST 域之间的路径上，用于选择路径和计算路径开销的参考值，同时也是确定该端口是否会被选为根端口的依据。值越小，表示优先级越高，缺省时为自动。

int-cost —— 内部路径开销。它是在 MST 域内的路径上，用于选择路径和计算路径开销的参考值，同时也是确定该端口是否会被选为根端口的依据。值越小，表示优先级越高，缺省时为自动。

portfast —— 是否启用边缘端口，缺省时为禁用（disable）。边缘端口由阻塞状态向转发状态迁移时，可实现快速迁移，无需等待延迟时间。

point-to-point —— 点对点链路状态，有自动（auto）、强制开启（open）和强制关闭（close）三个选项，缺省时为自动。以点对点链路相连的两个端口，如果为根端口或者指定端口，则可以快速迁移到转发状态，从而减少不必要的转发延迟时间。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

启用端口 1 的 STP 功能，并设置其优先级为 64，内、外部路径开销均为 100，开启边缘端口：

```
TL-SG3210(config)# interface gigabitEthernet 1/0/1
```

```
TL-SG3210(config-if)# spanning-tree common-config port-priority 64 ext-cost  
100 int-cost 100 portfast enable point-to-point open
```

27.4 spanning-tree mode

该命令用于配置生成树的模式，它的 **no** 命令用于恢复默认配置。

命令

spanning-tree mode { stp | rstp | mstp }
no spanning-tree mode

参数

mode —— 生成树模式，有 **stp**、**rstp**、**mstp** 三个选项，默认为 **stp**。其中 **stp** 为生成树兼容模式；**rstp** 为快速生成树兼容模式；**mstp** 为多重生成树模式。

模式

全局配置模式

示例

设置生成树模式为 MSTP：

```
TL-SG3210(config)# spanning-tree mode mstp
```

27.5 spanning-tree mst configuration

该命令用于从全局配置模式下进入 MST 配置模式，它的 **no** 命令用于将相应的实例恢复为默认配置。

命令

spanning-tree mst configuration
no spanning-tree mst configuration

模式

全局配置模式

示例

进入 MST 配置模式：

```
TL-SG3210(config)# spanning-tree mst configuration  
TL-SG3210(config-mst)#
```

27.6 instance

该命令用于配置 VLAN-MSTP 实例映射，它的 **no** 命令用于移除映射关系或删除相应的实例。实例被删除后，与该实例有关的映射关系也会被移除。

命令

instance *instance-id* vlan *vlan-id*
no instance *instance-id* [vlan *vlan-id*]

参数

instance-id —— 实例 ID，范围为 1~8。
vlan-id —— 要加入该实例的 VLAN ID。

模式

MST 配置模式

示例

将 VLAN-100 映射到实例 1:

```
TL-SG3210(config)# spanning-tree mst configuration
```

```
TL-SG3210(config-mst)# instance 1 vlan 1-100
```

取消 VLAN1-50 对实例 1 的映射:

```
TL-SG3210(config)# spanning-tree mst configuration
```

```
TL-SG3210(config-mst)# no instance 1 vlan 1-50
```

27.7 name

该命令用于配置 MST 实例的域名。MSTP 可以将交换网络划分为多个域,有着相同域配置和 VLAN-实例映射关系的交换机被认为属于同一个 MST 域 (Multiple Spanning Tree Regions, 多生成树域)。域配置包括配置域名和修订级别。

命令

name *name*

参数

name —— 域名,用于标识 MST 域,可输入 1~32 个字符。

模式

MST 配置模式

示例

配置 MSTP 的域名为 region1:

```
TL-SG3210(config)# spanning-tree mst configuration
```

```
TL-SG3210(config-mst)# name region1
```

27.8 revision

该命令用于配置 MST 实例的修订级别。

命令

revision *revision*

参数

revision —— 修订级别,范围为 0~65535。

模式

MST 配置模式

示例

配置 MSTP 的修订级别为 100:

```
TL-SG3210(config)# spanning-tree mst configuration
```

```
TL-SG3210(config-mst)# revision 100
```

27.9 spanning-tree mst instance

该命令用于配置 MST 实例的优先级，它的 no 命令用于恢复对应实例的默认优先级。

命令

spanning-tree mst instance *instance-id* priority *pri*

no spanning-tree mst instance *instance-id* priority

参数

instance-id —— 实例 ID，范围为 1~8。

pri —— MSTI 优先级，它是在对应实例 ID 中，确定交换机是否会被选为根桥的重要依据。取值范围 0~61440，间隔 4096，缺省时为 32768。

模式

全局配置模式

示例

启用实例 1，并设置 MSTI 优先级为 4096:

```
TL-SG3210(config)# spanning-tree mst instance 1 priority 4096
```

27.10 spanning-tree mst

该命令用于 MSTP 实例端口配置，它的 no 命令用于恢复对应实例端口的默认配置。端口在不同的生成树实例中可以担任不同的角色，本命令用来配置不同实例 ID 中的端口的参数。

命令

spanning-tree mst instance *instance-id* { [port-priority *pri*] [cost *cost*] }

no spanning-tree mst instance *instance-id*

参数

instance-id —— 需要配置端口属性的实例 ID 号，取值范围 1~8。

pri —— 端口优先级，它是在对应实例 ID 中，确定端口是否会被对端设备选为根端口的重要依据。取值范围 0~240，间隔 16，缺省时为 128。

cost —— 路径开销。路径开销是在 MST 域内的对应实例中，用于选择路径和计算路径开销的参考值，同时也是确定该端口是否会被选为根端口的依据。值越小，表示优先级越高，缺省时为自动。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

设置实例 1 的端口 1 优先级为 64，路径开销为 2000：

```
TL-SG3210(config)# interface gigabitEthernet 1/0/1
```

```
TL-SG3210(config-if)# spanning-tree mst instance 1 port-priority 64 cost 2000
```

27.11 spanning-tree priority

该命令用于配置桥优先级，它的 no 命令用于恢复默认配置。

命令

spanning-tree priority *pri*

no spanning-tree priority

参数

pri —— 桥优先级。取值范围 0~61440，缺省时为 32768。

模式

全局配置模式

示例

设置桥优先级为 4096：

```
TL-SG3210(config)# spanning-tree priority 4096
```

27.12 spanning-tree tc-defend

该命令用于配置生成树的全局 TC 保护，它的 no 命令用于恢复默认配置。设备在接收到 TC 报文（网络拓扑发生变化的通知报文）后，会执行地址表项的删除操作。当设备受到恶意的 TC 报文攻击时，频繁地删除操作会给设备带来很大负担，给网络的稳定带来很大隐患。TC 保护可以限制一定周期内交换机接收 TC 报文的最大数目，从而控制地址表项的删除操作。

命令

spanning-tree tc-defend threshold *threshold* period *period*

no spanning-tree tc-defend

参数

threshold —— TC 保护阈值，取值范围 1~100（数据包），缺省时为 20。TC 保护阈值是在 TC 保护周期内，交换机收到 TC 报文的最大数目。超过该数目后，交换机在该周期内不再进行删除地址表的操作。

period —— TC 保护周期，取值范围 1~10（秒），缺省时为 5。

模式

全局配置模式

示例

设置 TC 保护阈值为 30 数据包，TC 保护周期为 10 秒：

```
TL-SG3210(config)# spanning-tree tc-defend threshold 30 period 10
```

27.13 spanning-tree timer

该命令用于配置生成树的联络时间、老化时间、传输延时，它的 **no** 命令用于恢复默认配置。

命令

```
spanning-tree timer { [forward-time forward-time] [hello-time hello-time] [max-age max-age] }
```

```
no spanning-tree timer
```

参数

forward-time —— 传输延时，即在网络拓扑改变后，交换机的端口状态迁移的延时时间，取值范围为 4~30（秒），默认值为 15，并且 $2 \times (\text{传输延时} - 1) \geq \text{老化时间}$ 。

hello-time —— 联络时间，即交换机发送协议报文的周期，用于检测链路是否存在故障，取值范围为 1~10（秒），默认值为 2，并且 $2 \times (\text{联络时间} + 1) \leq \text{老化时间}$ 。

max-age —— 老化时间，即协议报文在交换机中能够保存的最大生命期，取值范围为 6~40（秒），默认值为 20。

模式

全局配置模式

示例

设置生成树的传输延时为 16 秒，联络时间为 3 秒，老化时间为 22 秒：

```
TL-SG3210(config)# spanning-tree timer forward-time 16 hello-time 3 max-age 22
```

27.14 spanning-tree hold-count

该命令用于设置生成树流量限制，它的 **no** 命令用于恢复默认配置。

命令

```
spanning-tree hold-count value
```

no spanning-tree hold-count

参数

value —— 流量限制，即在每个联络时间内，端口最多能够发送的协议报文的速度。取值范围为 1~20（pps），默认值为 5。

模式

全局配置模式

示例

设置生成树流量限制为 8pps:

```
TL-SG3210(config)# spanning-tree hold-count 8
```

27.15 spanning-tree max-hops

该命令用于设置生成树协议报文被转发的最大跳数，它的 no 命令用于恢复默认配置。

命令

spanning-tree max-hops value

no spanning-tree max-hops

参数

value —— 最大跳数，即协议报文被转发的最大跳数，它限制了生成树的规模，取值范围为 1~40（跳），默认值为 20。

模式

全局配置模式

示例

设置最大跳数为 30:

```
TL-SG3210(config)# spanning-tree max-hops 30
```

27.16 spanning-tree bpdupfilter

该命令用于为指定端口开启 BPDU 过滤功能，启用了 BPDU 报文过滤功能的端口，将不再接收和转发任何 BPDU 报文，但是会向外发送自身的 BPDU 报文，从而防止交换机受到 BPDU 报文的攻击，保证 STP 计算的正确性。它的 no 命令用于禁用该功能。

命令

spanning-tree bpdupfilter

no spanning-tree bpdupfilter

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

为端口 2 开启 BPDU 过滤功能：

```
TL-SG3210 (config)# interface gigabitEthernet 1/0/2
TL-SG3210(config-if)# spanning-tree bpduguard
```

27.17 spanning-tree bpduguard

该命令用于为指定端口开启 BPDU 保护功能，启用了 BPDU 保护功能后，如果端口收到了 BPDU 报文，MSTP 就将这些端口关闭，同时通知网管这些端口被 MSTP 关闭，被关闭的端口只能由网络管理人员来恢复。它的 no 命令用于禁用该功能。

命令

spanning-tree bpduguard
no spanning-tree bpduguard

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

为端口 2 开启 BPDU 保护功能：

```
TL-SG3210(config)# interface gigabitEthernet 1/0/2
TL-SG3210(config-if)# spanning-tree bpduguard
```

27.18 spanning-tree guard loop

该命令用于启用环路保护功能，它的 no 命令用于禁用该功能。环路保护可以防止由于链路拥塞或者单项链路故障，导致下游设备重新计算生成树，从而产生的网络环路现象。

命令

spanning-tree guard loop
no spanning-tree guard loop

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

开启端口 2 的环路保护：

```
TL-SG3210(config)# interface gigabitEthernet 1/0/2
TL-SG3210(config-if)# spanning-tree guard loop
```

27.19 spanning-tree guard root

该命令用于启用根桥保护，它的 no 命令用于禁用该功能。根桥保护可以防止当前合法根桥失去根桥地位，从而引起的网络拓扑结构的错误变动。

命令

spanning-tree guard root

no spanning-tree guard root

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

开启端口 2 的根桥保护：

```
TL-SG3210(config)# interface gigabitEthernet 1/0/2
```

```
TL-SG3210(config-if)# spanning-tree guard root
```

27.20 spanning-tree guard tc

该命令用于启用 TC 保护，它的 no 命令用于禁用该功能。启用 TC 保护功能后，交换机在“TC 保护周期”内，收到 TC-BPDU 的最大数目为“TC 保护阈值”处所设的数目，超过该数目后，交换机在该周期内不再进行地址表删除操作。这样就可以避免频繁地删除转发地址表项。

命令

spanning-tree guard tc

no spanning-tree guard tc

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

开启端口 2 的 TC 保护：

```
TL-SG3210(config)# interface gigabitEthernet 1/0/2
```

```
TL-SG3210(config-if)# spanning-tree guard tc
```

27.21 spanning-tree mcheck

该命令用于启用协议迁移。

命令

spanning-tree mcheck

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

启用端口 2 的协议迁移：

```
TL-SG3210(config)# interface gigabitEthernet 1/0/2
```

```
TL-SG3210(config-if)# spanning-tree mcheck
```

27.22 show spanning-tree active

该命令用于显示生成树的当前运行状态信息。

命令

show spanning-tree active

模式

特权模式和所有配置模式

示例

显示生成树当前运行状态信息：

```
TL-SG3210# show spanning-tree active
```

27.23 show spanning-tree bridge

该命令用于显示生成树的参数配置信息。

命令

show spanning-tree bridge [forward-time | hello-time | hold-count | max-age |
max-hops | mode | priority | state]

模式

特权模式和所有配置模式

示例

显示生成树参数配置信息：

```
TL-SG3210# show spanning-tree bridge
```

27.24 show spanning-tree interface

该命令用于显示生成树的端口配置信息。

命令

show spanning-tree interface [gigabitEthernet port] [edge | ext-cost | int-cost |
mode | p2p | priority | role | state | status]

参数

port —— 要显示配置信息的端口号，缺省时显示所有端口的配置信息。

模式

特权模式和所有配置模式

示例

显示所有端口的生成树信息：

```
TL-SG3210# show spanning-tree interface
```

显示端口 2 的生成树信息：

```
TL-SG3210# show spanning-tree interface gigabitEthernet 1/0/2
```

显示端口 2 的生成树模式：

```
TL-SG3210# show spanning-tree interface gigabitEthernet 1/0/2 mode
```

27.25 show spanning-tree interface-security

该命令用于显示生成树的端口安全配置信息。

命令

```
show spanning-tree interface-security [ gigabitEthernet port ] [ bpdufilter |  
bpduguard | loop | root | tc | tc-defend ]
```

参数

port —— 要显示配置信息的端口号，缺省时显示所有端口的配置信息。

模式

特权模式和所有配置模式

示例

显示所有端口的安全配置信息：

```
TL-SG3210(config)# show spanning-tree interface-security
```

显示端口 1 的安全配置信息：

```
TL-SG3210(config)# show spanning-tree interface-security gigabitEthernet 1/0/1
```

显示所有端口的安全配置信息：

```
TL-SG3210(config)# show spanning-tree interface-security bpdufilter
```

27.26 show spanning-tree mst

该命令用于显示生成树的实例信息。

命令

```
show spanning-tree mst { configuration [digest] | instance instance-id | [ interface  
[ gigabitEthernet port ] ] }
```

参数

instance-id —— 要显示配置信息的实例 ID，取值范围 1~8。

port —— 要显示配置信息的端口号，缺省时显示所有端口的配置信息。

模式

特权模式和所有配置模式

示例

显示实例 1 的配置信息：

```
TL-SG3210(config)# show spanning-tree mst instance 1
```


第28章 IGMP 配置命令

IGMP Snooping（Internet Group Management Protocol Snooping，IGMP 侦听）是运行在交换机上的组播约束机制，用于管理和控制组播组。启用 IGMP 侦听功能可以有效地避免组播数据在网络中广播。

28.1 ip igmp snooping(global)

该命令用于 IGMP 全局配置，它的 no 命令用于禁用该功能。

命令

ip igmp snooping

no ip igmp snooping

模式

全局配置模式

示例

开启 IGMP 全局配置：

```
TL-SG3210(config)# ip igmp snooping
```

28.2 ip igmp snooping(interface)

该命令用于为指定端口配置 IGMP Snooping 功能，它的 no 命令用于禁用该功能。

命令

ip igmp snooping

no ip igmp snooping

模式

接口配置模式(interface gigabitEthernet / interface range gigabitEthernet)

示例

开启端口 3 的 IGMP Snooping 功能：

```
TL-SG3210(config)# interface gigabitEthernet 1/0/3
```

```
TL-SG3210(config-if)# ip igmp snooping
```

28.3 ip igmp snooping immediate-leave

该命令用于配置端口的快速离开功能，它的 no 命令用于禁用该功能。

命令

ip igmp snooping immediate-leave
no ip igmp snooping immediate-leave

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

开启端口 3 的快速离开功能：

```
TL-SG3210(config)# interface gigabitEthernet 1/0/3
TL-SG3210(config-if)# ip igmp snooping immediate-leave
```

28.4 ip igmp snooping drop-unknown

该命令用于开启未知组播报文丢弃功能，它的 no 命令用于禁用该功能。

命令

ip igmp snooping drop-unknown
no ip igmp snooping drop-unknown

模式

全局配置模式

示例

开启未知组播报文丢弃功能：

```
TL-SG3210(config)# ip igmp snooping drop-unknown
```

28.5 ip igmp snooping vlan-config

该命令用于启用指定 VLAN 的 IGMP SNOOPING 功能，并修改其 IGMP 参数以及创建静态组播地址条目。它的 no 命令用于禁用指定 VLAN 的 IGMP SNOOPING 功能。IGMP 侦听所建立的组播组是基于 VLAN 广播域的，不同的 VLAN 可以设置不同的 IGMP 参数，本命令用于配置每个 VLAN 的 IGMP 侦听参数。

命令

ip igmp snooping vlan-config *vlan-id-list* [*rtime router-time* | *mtime member-time* | *ltime leave-time* | *rport interface gigabitEthernet port*]
ip igmp snooping vlan-config *vlan-id* static *ip* interface gigabitEthernet *port*
no ip igmp snooping vlan-config *vlan-id-list*
no ip igmp snooping vlan-config *vlan-id* static *ip*

参数

vlan-id-list —— 需要修改 IGMP 参数的 VLAN ID 列表，取值范围 1~4094，格式为 1-3,5。

router-time —— 路由器端口时间。在所设时间内，如果交换机没有从路由器端口接收到查询报文，就认为该路由器端口失效。取值范围 60~600（秒），默认值为 300。

member-time —— 成员端口时间。在所设时间内，如果交换机没有接收到成员端口发送的报告报文，就认为该成员端口失效。取值范围 60~600（秒），默认值为 260。

leave-time —— 离开滞后时间，即主机发送离开报文到交换机把该主机端口从组播组中删除的间隔时间。取值范围 1~30（秒），默认值为 1。

port —— 交换机成员端口号。

vlan-id —— 组播 IP 的 VLAN ID，取值范围 1~4094。

ip —— 静态组播 IP 地址。

port-list —— 成员端口列表。

模式

全局配置模式

示例

启用 VLAN 1-3 的 IGMP 侦听功能，将它们的路由器端口时间设置为 300 秒、成员端口时间设置为 200 秒，并将 VLAN1-2 的离开滞后时间设置为 15 秒：

```
TL-SG3210(config)# ip igmp snooping vlan-config 1-3 rtime 300
```

```
TL-SG3210(config)# ip igmp snooping vlan-config 1-3 mtime 200
```

```
TL-SG3210(config)# ip igmp snooping vlan-config 1-2 ltime 15
```

在 VLAN 2 中添加静态组播地址条目，组播 IP 为 225.0.0.1，转发端口为端口 1-3：

```
TL-SG3210(config)# ip igmp snooping vlan-config 2 static 225.0.0.1 interface
gigabitEthernet 1/0/1-3
```

28.6 ip igmp snooping multi-vlan-config

该命令用于创建组播 VLAN，它的 no 命令用于删除相应的组播 VLAN。

命令

```
ip igmp snooping multi-vlan-config [ vlan-id ] [ rtime router-time | mtime
member-time | ltime leave-time | rport interface gigabitEthernet port ]
```

```
no ip igmp snooping multi-vlan-config
```

参数

vlan-id —— 需要修改配置的 VLAN ID，取值范围 2~4094。

router-time —— 路由器端口时间。在所设时间内，如果交换机没有从路由器端口接收到查询报文，就认为该路由器端口失效。取值范围 60~600（秒），默认值为 300。

member-time —— 成员端口时间。在所设时间内，如果交换机没有接收到成员端口发送的报告报文，就认为该成员端口失效。取值范围 60~600（秒），默认值为 260。

leave-time —— 离开滞后时间，即从主机发送离开报文到交换机把该主机端口从组播组中删除的间隔时间。取值范围 1~30（秒），默认值为 1。

port —— 交换机成员端口号。

模式

全局配置模式

示例

开启组播 VLAN 功能，并设置 VLAN 3 的路由器端口时间为 100 秒、成员端口时间为 100 秒、离开滞后时间为 3 秒，静态路由端口为端口 3：

```
TL-SG3210(config)# ip igmp snooping multi-vlan-config 3 rtime 100
TL-SG3210(config)# ip igmp snooping multi-vlan-config 3 mtime 100
TL-SG3210 (config)# ip igmp snooping multi-vlan-config 3 ltime 3
TL-SG3210 (config)# ip igmp snooping multi-vlan-config 3 rport interface
gigabitEthernet 1/0/3
```

28.7 ip igmp snooping filter(global)

该命令用于添加或修改组播过滤的过滤地址条目，它的 **no** 命令用于删除过滤地址条目。在启用了 IGMP 侦听功能后，可以通过配置组播过滤来限制端口能加入的组播地址范围，从而限制用户对组播节目的点播。组播地址范围为 224.0.0.0~239.255.255.255，可以加入的有效组播地址范围为 224.0.1.0~239.255.255.255。

命令

ip igmp snooping filter *id* *start-ip* *end-ip*

no ip igmp snooping filter *id*

参数

id —— 过滤地址 ID，范围为 1~30。

start-ip —— 过滤地址段的起始组播 IP 地址。

end-ip —— 过滤地址段的结束组播 IP 地址。

模式

全局配置模式

示例

添加 ID 号为 3 的组播过滤条目，过滤地址段为 225.1.1.1~226.3.2.1：

```
TL-SG3210(config)# ip igmp snooping filter 3 225.1.1.1 226.3.2.1
```

28.8 ip igmp snooping filter(interface)

该命令用于配置端口过滤，它的 no 命令用于恢复默认配置。当端口发送 IGMP 报告报文时，交换机会根据报文检查端口上配置的组播过滤地址 ID，如果组播地址未被过滤，则将这个端口加入到该组播组的转发端口列表中，否则交换机就会丢弃该 IGMP 报告报文，从而控制了用户所能加入的组播组。

命令

ip igmp snooping filter
no ip igmp snooping filter

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

开启端口 3 的组播过滤功能：

```
TL-SG3210(config)# interface gigabitEthernet 1/0/3
TL-SG3210(config-if)# ip igmp snooping filter
```

28.9 ip igmp snooping filter add-id

该命令用于为指定端口添加需要过滤的组播地址段，它的 no 命令用于删除对应的过滤地址。

命令

ip igmp snooping filter addr-id *addr-id list*
no ip igmp snooping filter addr-id *addr-id list*

参数

addr-id list —— 接口绑定过滤地址 ID，格式为 1-3, 5。

模式

接口配置模式(interface gigabitEthernet / interface range gigabitEthernet)

示例

绑定过滤地址 2-6 到快速端口 3：

```
TL-SG3210(config)# interface gigabitEthernet 1/0/3
TL-SG3210(config-if)# ip igmp snooping filter addr-id 2-6
```

28.10 ip igmp snooping filter mode

该命令用于配置指定端口的过滤模式。

命令

ip igmp snooping filter mode *mode*

参数

mode ——过滤动作模式，接受（accept）或拒绝（refuse）。选择 refuse 时，交换机将丢弃组播地址在在组播过滤地址段中的组播数据包；而选择 accept 时，交换机只处理组播地址在组播过滤地址段中的组播数据包。

模式

接口配置模式(interface gigabitEthernet / interface range gigabitEthernet)

示例

指定端口 3 的过滤模式为 accept:

```
TL-SG3210(config)# interface range gigabitEthernet 1/0/3
```

```
TL-SG3210(config-if-range)# ip igmp snooping filter mode accept
```

28.11 ip igmp snooping filter maxgroup

该命令用于指定端口最多能加入的组播组的数目。

命令

ip igmp snooping filter maxgroup *maxgroup*

参数

maxgroup —— 端口最多能加入的组播组数目。设定端口最多能加入的组播组数目是为了防止端口占用过大的带宽。

模式

接口配置模式(interface gigabitEthernet / interface range gigabitEthernet)

示例

指定端口 2-5 最多可加入 10 个组播组:

```
TL-SG3210(config)# interface range gigabitEthernet 1/0/2-5
```

```
TL-SG3210(config-if-range)# ip igmp snooping filter maxgroup 10
```

28.12 clear ip igmp snooping statistics

该命令是用于清除的 IGMP 报文统计信息。

命令

clear ip igmp snooping statistics

模式

特权模式和所有配置模式

示例

清除 IGMP 报文统计信息：

```
TL-SG3210(config)# clear ip igmp snooping statistics
```

28.13 show ip igmp snooping

该命令用于显示 IGMP 全局配置信息。

命令

```
show ip igmp snooping
```

模式

特权模式和所有配置模式

示例

显示 IGMP 全局配置信息：

```
TL-SG3210# show ip igmp snooping
```

28.14 show ip igmp snooping interface

该命令用于显示 IGMP 端口配置信息。

命令

```
show ip igmp snooping interface gigabitEthernet [ port | port-list ] { basic-config |  
filter | packet-stat }
```

参数

port —— 要显示配置信息的端口号。

port-list —— 要显示配置信息的端口列表。

basic-config | filter | packet-stat —— 选择要显示的相关配置信息。

模式

特权模式和所有配置模式

示例

显示所有端口的组播过滤配置信息：

```
TL-SG3210# show ip igmp snooping interface gigabitEthernet filter
```

显示端口 2 的 IGMP 基本配置信息：

```
TL-SG3210# show ip igmp snooping interface gigabitEthernet 1/0/2 basic-config
```

显示端口 1-4 的 IGMP 报文统计信息：

```
TL-SG3210# show ip igmp snooping interface gigabitEthernet 1/0/1-4 packet-stat
```

28.15 show ip igmp snooping vlan

该命令用于显示 IGMP VLAN 配置信息。

命令

```
show ip igmp snooping vlan [ vlan-id ]
```

参数

vlan-id —— 要显示 VLAN 号。

模式

特权模式和所有配置模式

示例

显示 VLAN 2 的 IGMP Snooping 配置信息：

```
TL-SG3210# show ip igmp snooping vlan 2
```

28.16 show ip igmp snooping multi-vlan

该命令用于显示组播 VLAN 配置信息。

命令

```
show ip igmp snooping multi-vlan
```

模式

特权模式和所有配置模式

示例

显示组播 VLAN 配置信息：

```
TL-SG3210# show ip igmp snooping multi-vlan
```

28.17 show ip igmp snooping groups

该命令用于显示所有组播组信息。可以在后面添加扩展参数以显示指定 VLAN 的动态组播和静态组播配置信息。

命令

```
show ip igmp snooping groups [ vlan vlan-id ] [ count | dynamic | dynamic count |  
static | static count ]
```

参数

vlan-id —— 需要显示组播信息的 VLAN 号。

count —— 显示所有组播组的数目。

dynamic —— 查看所有的动态组播组信息。

dynamic count —— 显示动态组播组的数目。

static—— 查看所有的静态组播组信息。

static count—— 显示静态组播组的数目。

模式

特权模式及所有配置模式

示例

显示组播组信息列表：

```
TL-SG3210#show ip igmp snooping groups
```

显示 VLAN 5 的所有组播组条目：

```
TL-SG3210(config)#show ip igmp snooping groups vlan 5
```

显示 VLAN 5 中的组播组条目个数：

```
TL-SG3210(config)#show ip igmp snooping groups vlan 5 count
```

显示 VLAN 5 中的动态组播组信息：

```
TL-SG3210(config)#show ip igmp snooping groups vlan 5 dynamic
```

显示 VLAN 5 中的静态组播组信息：

```
TL-SG3210(config)#show ip igmp snooping groups vlan 5 static
```

显示 VLAN 5 中的动态组播条目：

```
TL-SG3210(config)#show ip igmp snooping groups vlan 5 dynamic count
```

显示 VLAN 5 中的静态组播条目：

```
TL-SG3210(config)#show ip igmp snooping groups vlan 5 static count
```

28.18 show ip igmp snooping filter

该命令用于显示组播过滤地址表信息。

命令

```
show ip igmp snooping filter [ filter-addr-id-list ]
```

参数

filter-addr-id-list —— 要显示组播过滤地址信息的过滤地址 ID，可输入多条，格式为 1-3, 5，缺省时显示所有端口的配置信息。

模式

特权模式和所有配置模式

示例

显示所有组播过滤地址信息：

```
TL-SG3210(config)# show ip igmp snooping filter
```

第29章 MLD 配置命令

MLD Snooping（Multicast Listener Discovery Snooping，MLD 侦听）是运行在二层网络中的组播约束机制，负责管理 IPv6 组播数据在组播路由器和主机之间的传输。启用 MLD 侦听功能可以有效地避免组播数据在网络中广播。

29.1 ipv6 mld snooping

该命令用于开启全局 MLD 侦听功能，它的 no 命令用于禁用该功能。

命令

ipv6 mld snooping

no ipv6 mld snooping

模式

全局配置模式

示例

开启全局 MLD 侦听功能：

```
TL-SG3210(config)# ipv6 mld snooping
```

29.2 ipv6 mld snooping router-aging-time

该命令用于设置 MLD 侦听全局路由器端口时间，它的 no 命令用于恢复默认值。

命令

ipv6 mld snooping router-aging-time timer

no ipv6 mld snooping router-aging-time

参数

timer —— 全局路由器端口时间，如果在路由器端口老化时间内路由器端口没有收到任何查询报文，则该路由器端口将老化。取值范围 1~1000（秒），默认值为 260。

模式

全局配置模式

示例

设置 MLD 侦听全局路由器端口时间为 100 秒：

```
TL-SG3210(config)# ipv6 mld snooping router-aging-time 100
```

29.3 ipv6 mld snooping member-aging-time

该命令用于设置 MLD 侦听全局成员端口时间，它的 no 命令用于恢复默认值。

命令

ipv6 mld snooping member-aging-time *timer*

no ipv6 mld snooping member-aging-time

参数

timer —— 全局成员端口时间，如果在成员端口老化时间内成员端口没有收到任何报告报文，则该成员端口将老化。取值范围 200~1000（秒），默认值为 260。

模式

全局配置模式

示例

设置 MLD 侦听全局成员端口时间为 100 秒：

```
TL-SG3210(config)# ipv6 mld snooping member-aging-time 100
```

29.4 ipv6 mld snooping report-suppression

该命令用于开启 Report 报文抑制功能，它的 no 命令用于禁用该功能。该功能默认开启。

命令

ipv6 mld snooping report-suppression

no ipv6 mld snooping report-suppression

模式

全局配置模式

示例

禁用 Report 报文抑制功能：

```
TL-SG3210(config)# no ipv6 mld snooping report-suppression
```

29.5 ipv6 mld snooping unknown-filter

该命令用于开启未知组播报文过滤功能，它的 no 命令用于禁用该功能。该功能默认禁用。

命令

ipv6 mld snooping unknown-filter

no ipv6 mld snooping unknown-filter

模式

全局配置模式

示例

开启未知组播报文过滤功能：

```
TL-SG3210(config)# ipv6 mld snooping unknown-filter
```

29.6 ipv6 mld snooping last-listener query-interval

该命令用于设置特定组查询间隔，它的 no 命令用于恢复默认值。

命令

ipv6 mld snooping last-listener query-interval *interval*

no ipv6 mld snooping last-listener query-interval

参数

interval —— 特定组查询间隔，当某个组播组内没有成员端口时，将以特定组查询间隔为间隔时间发送特定组查询报文，以此判断是否还有成员要加入该组播组。取值范围 1~5（秒），默认值为 1。

模式

全局配置模式

示例

设置特定组查询间隔为 3 秒：

```
TL-SG3210(config)# ipv6 mld snooping last-listener query-interval 3
```

29.7 ipv6 mld snooping last-listener query-count

该命令用于设置特定组查询次数，它的 no 命令用于恢复默认值。

命令

ipv6 mld snooping last-listener query-count *num*

no ipv6 mld snooping last-listener query-count

参数

num —— 特定组查询次数，当某个组播组内没有成员端口时，将发送特定组查询次数的特定组查询报文，以此判断是否还有成员要加入该组播组。取值范围 1~7，默认值为 2。

模式

全局配置模式

示例

设置特定组查询次数为 3：

```
TL-SG3210(config)# ipv6 mld snooping last-listener query-count 3
```

29.8 ipv6 mld snooping multicast-vlan

该命令用于开启组播 VLAN 功能，它的 no 命令用于禁用该功能。该功能默认禁用。

命令

ipv6 mld snooping multicast-vlan

no ipv6 mld snooping multicast-vlan

模式

全局配置模式

示例

开启组播 VLAN 功能：

```
TL-SG3210(config)# ipv6 mld snooping multicast-vlan
```

29.9 ipv6 mld snooping multicast-vlan vlan-id

该命令用于设置组播 VLAN ID，它的 no 命令用于恢复默认值。

命令

ipv6 mld snooping multicast-vlan vlan-id *vid*

no ipv6 mld snooping multicast-vlan vlan-id

参数

vid —— 组播 VLAN ID。取值范围 1~4094，默认值为 1。

模式

全局配置模式

示例

设置组播 VLAN 为 VLAN 2：

```
TL-SG3210(config)# ipv6 mld snooping multicast-vlan vlan-id 2
```

29.10 ipv6 mld snooping vlan

该命令用于启用指定 VLAN 的 MLD 侦听功能，它的 no 命令用于禁用相应 VLAN 的 MLD 侦听功能。

命令

ipv6 mld snooping vlan *vlan-id*

no ipv6 mld snooping vlan *vlan-id*

参数

vlan-id —— 启用 MLD 侦听功能的 VLAN ID。取值范围 1~4094。

模式

全局配置模式

示例

开启 VLAN 2 的 MLD 侦听功能：

```
TL-SG3210(config)# ipv6 mld snooping vlan 2
```

29.11 ipv6 mld snooping vlan router-aging-time

该命令用于设置指定 VLAN 的路由器端口时间，它的 no 命令用于恢复默认值。

命令

ipv6 mld snooping vlan *vlan-id* router-aging-time *timer*

no ipv6 mld snooping vlan *vlan-id* router-aging-time

参数

vlan-id —— 启用 MLD 侦听功能的 VLAN ID。取值范围 1~4094。

timer —— 指定 VLAN 的路由器端口时间。取值范围 0~1000（秒），默认值为 0，表示使用全局路由器端口时间。

模式

全局配置模式

示例

设置 VLAN 2 的路由器端口时间为 100 秒：

```
TL-SG3210(config)# ipv6 mld snooping vlan 2 router-aging-time 100
```

29.12 ipv6 mld snooping vlan member-aging-time

该命令用于设置指定 VLAN 的成员端口时间，它的 no 命令用于恢复默认值。

命令

ipv6 mld snooping vlan *vlan-id* member-aging-time *timer*

no ipv6 mld snooping vlan *vlan-id* member-aging-time

参数

vlan-id —— 启用 MLD 侦听功能的 VLAN ID。取值范围 1~4094。

timer —— 指定 VLAN 的成员端口时间。取值范围 0 和 200~1000（秒），默认值为 0，表示使用全局成员端口时间。

模式

全局配置模式

示例

设置 VLAN 2 的成员端口时间为 100 秒：

```
TL-SG3210(config)# ipv6 mld snooping vlan 2 member-aging-time 100
```

29.13 ipv6 mld snooping vlan immediate-leave

该命令用于开启指定 VLAN 的快速离开功能，它的 no 命令用于禁用相应 VLAN 的快速离开功能。该功能默认禁用。

命令

```
ipv6 mld snooping vlan vlan-id immediate-leave
```

```
no ipv6 mld snooping vlan vlan-id immediate-leave
```

参数

vlan-id —— 开启快速离开功能的 VLAN ID。取值范围 1~4094。

模式

全局配置模式

示例

开启 VLAN 2 的快速离开功能：

```
TL-SG3210(config)# ipv6 mld snooping vlan 2 immediate-leave
```

29.14 ipv6 mld snooping vlan mrouter

该命令用于设置指定 VLAN 的静态路由器端口，它的 no 命令用于禁用相应 VLAN 的静态路由器端口。

命令

```
ipv6 mld snooping vlan vlan-id mrouter interface gigabitEthernet port
```

```
no ipv6 mld snooping vlan vlan-id mrouter [interface gigabitEthernet port]
```

参数

vlan-id —— 需设置静态路由器端口的 VLAN ID。取值范围 1~4094。

port —— 静态配置的路由器端口。

模式

全局配置模式

示例

设置 VLAN 2 中端口 2 为静态路由器端口：

```
TL-SG3210(config)# ipv6 mld snooping vlan 2 mrouter interface gigabitEthernet  
1/0/2
```

29.15 ipv6 mld snooping vlan static

该命令用于设置静态组播组，它的 no 命令用于禁用静态组播组。

命令

```
ipv6 mld snooping vlan vlan-id static ipv6_multicast_addr interface
gigabitEthernet port

no ipv6 mld snooping vlan vlan-id static ipv6_multicast_addr [interface
gigabitEthernet port]
```

参数

vlan-id —— 组播 IP 对应的 VLAN ID。取值范围 1~4094。

ipv6_multicast_addr —— 静态绑定的组播 IPv6 地址。

port —— 组播 IP 的转发端口。

模式

全局配置模式

示例

设置 VLAN 2 中 IPv6 地址为 ff80::1234 的静态组播组，该组播组的转发端口为端口 2:

```
TL-SG3210(config)# ipv6 mld snooping vlan 2 static ff80::1234 interface
gigabitEthernet 1/0/2
```

29.16 ipv6 mld snooping querier vlan

该命令用于开启指定 VLAN 的 MLD 侦听查询器功能，它的 no 命令用于禁用相应 VLAN 的 MLD 侦听查询器功能。

命令

```
ipv6 mld snooping querier vlan vlan-id

no ipv6 mld snooping querier vlan vlan-id
```

参数

vlan-id —— 开启 MLD 侦听查询器功能的 VLAN ID。取值范围 1~4094。

模式

全局配置模式

示例

开启 VLAN 2 的 MLD 侦听查询器功能:

```
TL-SG3210(config)# ipv6 mld snooping querier vlan 2
```


29.17 ipv6 mld snooping querier vlan max-response-time

该命令用于设置 MLD 侦听查询器的最大响应时间，它的 no 命令用于恢复默认值。

命令

ipv6 mld snooping querier vlan *vlan-id* max-response-time *time*

no ipv6 mld snooping querier vlan *vlan-id* max-response-time

参数

vlan-id —— 开启 MLD 侦听查询器功能的 VLAN ID。取值范围 1~4094。

time —— 最大响应时间。取值范围 1~25（秒），默认值为 10。

模式

全局配置模式

示例

设置 VLAN 2 的 MLD 侦听查询器的最大响应时间为 10 秒：

```
TL-SG3210(config)# ipv6 mld snooping querier vlan 2 max-response-time 10
```

29.18 ipv6 mld snooping querier vlan query-interval

该命令用于设置 MLD 侦听查询器发送通用组查询报文的查询间隔，它的 no 命令用于恢复默认值。

命令

ipv6 mld snooping querier vlan *vlan-id* query-interval *interval*

no ipv6 mld snooping querier vlan *vlan-id* query-interval

参数

vlan-id —— 开启 MLD 侦听查询器功能的 VLAN ID。取值范围 1~4094。

interval —— 通用组查询间隔。取值范围 2~300（秒），默认值为 25。

模式

全局配置模式

示例

设置 VLAN 2 的 MLD 侦听查询器的通用组查询间隔为 10 秒：

```
TL-SG3210(config)# ipv6 mld snooping querier vlan 2 query-interval 10
```

29.19 ipv6 mld snooping querier vlan query-source

该命令用于设置 MLD 侦听查询器发送通用组查询报文的源 IP 地址，它的 no 命令用于恢复默认值。

命令

ipv6 mld snooping querier vlan *vlan-id* query-source *ipv6-addr*

no ipv6 mld snooping querier vlan *vlan-id* query-source

参数

vlan-id —— 开启 MLD 侦听查询器功能的 VLAN ID。取值范围 1~4094。

ipv6-addr —— 通用组源 IPv6 地址，该地址不能设置为组播 IP 地址和广播 IP 地址。默认值为 FE80::02FF:FFFF:FE00:0001。

模式

全局配置模式

示例

设置 VLAN 2 的 MLD 侦听查询器的通用组源 IPv6 地址为 fe80::1234:

```
TL-SG3210(config)# ipv6 mld snooping querier vlan 2 query-source fe80::1234
```

29.20 ipv6 mld snooping filter(global)

该命令用于以地址段格式设置组播组过滤条目，它的 no 命令用于禁用相应过滤条目。

命令

ipv6 mld snooping filter *filter-id* start-ipv6 end-ipv6

no ipv6 mld snooping filter *filter-id*

参数

filter-id —— 设置过滤条目 ID，取值范围 1~30。

start-ipv6 —— 过滤地址段的起始组播 IP 地址。

end-ipv6 —— 过滤地址段的结束组播 IP 地址。

模式

全局配置模式

示例

设置组播组过滤条目 ID 为 2，过滤地址段的起始组播 IP 地址为 ff80::1234，结束组播 IP 地址为 ff80::1235:

```
TL-SG3210(config)# ipv6 mld snooping filter 2 ff80::1234 ff80::1235
```

29.21 ipv6 mld snooping filter(interface)

该命令用于启用端口组播过滤功能，它的 no 命令用于禁用该功能。

命令

ipv6 mld snooping filter

no ipv6 mld snooping filter

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

开启端口 2 的组播过滤功能：

```
TL-SG3210(config)# interface gigabitEthernet 1/0/2
TL-SG3210(config-if)# ipv6 mld snooping filter
```

29.22 ipv6 mld snooping filter-mode

该命令用于设置端口组播过滤功能的过滤模式，它的 no 命令用于恢复默认模式。默认模式为接收。

命令

ipv6 mld snooping filter-mode {accept | refuse}

no ipv6 mld snooping filter-mode

参数

accept —— 当组播地址属于过滤地址范围时，接收该组播组。

refuse —— 当组播地址属于过滤地址范围时，拒绝该组播组。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

设置端口 2 的组播过滤功能过滤模式为 refuse：

```
TL-SG3210(config)# interface gigabitEthernet 1/0/2
TL-SG3210(config-if)# ipv6 mld snooping filter-mode refuse
```

29.23 ipv6 mld snooping filter-id

该命令用于设置端口需要绑定的过滤地址 ID 号，它的 no 命令用于禁用相应配置。

命令

ipv6 mld snooping filter-id *filter-list*

no ipv6 mld snooping filter-id

参数

filter-list —— 设置端口需要绑定的过滤地址 ID 号，一个端口最多只能绑定 15 个过滤地址 ID。输入格式为 1,5,8。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

设置端口 2 绑定的过滤地址 ID 为 1 和 10:

```
TL-SG3210(config)# interface gigabitEthernet 1/0/2
TL-SG3210(config-if)# ipv6 mld snooping filter-id 1,10
```

29.24 ipv6 mld snooping max-group

该命令用于设置端口最多加入组播组数目，它的 no 命令用于恢复默认值。

命令

```
ipv6 mld snooping max-group limit
no ipv6 mld snooping max-group
```

参数

limit —— 端口最多加入组播组数目。取值范围 0~256，默认值为 256。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

设置端口 2 最多加入组播组数目为 128:

```
TL-SG3210(config)# interface gigabitEthernet 1/0/2
TL-SG3210(config-if)# ipv6 mld snooping max-group 128
```

29.25 clear ipv6 mld snooping statistics

该命令用于清除 MLD 报文的统计信息。

命令

```
clear ipv6 mld snooping statistics
```

模式

特权模式和所有配置模式

示例

清除 MLD 报文的统计信息:

```
TL-SG3210(config)# clear ipv6 mld snooping statistics
```

29.26 show ipv6 mld snooping

该命令用于显示 MLD 侦听全局配置。

命令

show ipv6 mld snooping

模式

特权模式和所有配置模式

示例

显示 MLD 侦听全局配置：

```
TL-SG3210(config)# show ipv6 mld snooping
```

29.27 show ipv6 mld snooping vlan

该命令用于显示 MLD 侦听的 VLAN 信息。

命令

show ipv6 mld snooping vlan [vlan-id]

参数

vlan-id —— 要查看信息的 VLAN ID。取值范围 1~4094。

模式

特权模式和所有配置模式

示例

显示所有 VLAN 信息：

```
TL-SG3210(config)# show ipv6 mld snooping vlan
```

29.28 show ipv6 mld snooping static-mcast

该命令用于显示用户设置的静态组播组。

命令

show ipv6 mld snooping static-mcast

模式

特权模式和所有配置模式

示例

显示用户设置的静态组播组：

```
TL-SG3210(config)# show ipv6 mld snooping static-mcast
```

29.29 show ipv6 mld snooping group

该命令用于显示组播组。

命令

```
show ipv6 mld snooping group [ dynamic | static ][ vlan vlan-id ]
```

参数

dynamic —— 显示动态组播组。

static —— 显示静态组播组。

vlan-id —— 要查看信息的 VLAN ID。取值范围 1~4094。

模式

特权模式和所有配置模式

示例

显示所有组播组：

```
TL-SG3210(config)# show ipv6 mld snooping group
```

29.30 show ipv6 mld snooping filter

该命令用于显示过滤条目。

命令

```
show ipv6 mld snooping filter
```

模式

特权模式和所有配置模式

示例

显示过滤条目：

```
TL-SG3210(config)# show ipv6 mld snooping filter
```

29.31 show ipv6 mld snooping interface

该命令用于显示 MLD 侦听的接口信息。

命令

```
show ipv6 mld snooping interface [ gigabitEthernet port ]
```

参数

port —— 要查看信息的接口。

模式

特权模式和所有配置模式

示例

显示所有接口信息：

```
TL-SG3210(config)# show ipv6 mld snooping interface
```

29.32 show ipv6 mld snooping interface filter

该命令用于显示接口绑定的过滤条目号。

命令

show ipv6 mld snooping interface filter [gigabitEthernet *port*]

参数

port —— 要查看信息的接口。

模式

特权模式和所有配置模式

示例

显示所有接口绑定的所有过滤条目号：

```
TL-SG3210(config)# show ipv6 mld snooping interface filter
```

29.33 show ipv6 mld snooping querier

该命令用于显示 VLAN 的查询器设置。

命令

show ipv6 mld snooping querier [vlan *vlan-id*]

参数

vlan-id —— 要查看信息的 VLAN ID。取值范围 1~4094。

模式

特权模式和所有配置模式

示例

显示所有查询器信息：

```
TL-SG3210(config)# show ipv6 mld snooping querier
```

29.34 show ipv6 mld snooping statistics

该命令用于显示 MLD 报文的统计信息。

命令

show ipv6 mld snooping statistics [interface gigabitEthernet *port*]

参数

port —— 要查看信息的接口。

模式

特权模式和所有配置模式

示例

显示 MLD 报文的统计信息：

```
TL-SG3210(config)# show ipv6 mld snooping statistics
```


第30章 SNMP 配置命令

SNMP（Simple Network Management Protocol，简单网络管理协议）功能用于管理网络设备，实现与众多产品的无障碍连接，以便于网络管理员对网络节点的监控和操作。

30.1 snmp-server

该命令用于启用 SNMP 功能，它的 no 命令用于禁用 SNMP 功能。SNMP 功能默认是被禁用的。

命令

snmp-server

no snmp-server

模式

全局配置模式

示例

开启 SNMP 功能：

```
TL-SG3210(config)# snmp-server
```

30.2 snmp-server view

该命令用于添加视图，它的 no 命令用于删除对应视图。在 SNMP 报文中使用管理变量（OID）来描述交换机中的管理对象，MIB（Management Information Base，管理信息库）是所监控网络设备的管理变量的集合。视图用来控制管理变量是如何被管理的。

命令

snmp-server view *name mib-oid* { include | exclude }

no snmp-server view *name mib-oid*

参数

name —— 要添加的视图条目的名称，可输入 1~16 个字符。一个视图可以有多个同名的视图条目。

mib-oid —— MIB 子树 OID，即该视图条目的管理变量（OID）。可输入 1~61 个字符。

include | exclude —— 视图类型，有包括（include）和排除（exclude）两个选项。选择包括时，该 OID 可以被管理软件管理；选择排除时，该 OID 不能被管理软件管理。

模式

全局配置模式

示例

添加视图 view1，并设置其 OID 为 1.3.6.1.6.3.20，该 OID 可以被管理软件管理：

```
TL-SG3210(config)# snmp-server view view1 1.3.6.1.6.3.20 include
```

30.3 snmp-server group

该命令用于添加组管理配置，它的 **no** 命令用于删除对应的组。SNMP v3 提供了 VACM (View-based Access Control Model，基于视图的访问控制模型) 及 USM (User-based Security Model，基于用户的安全模型) 的认证机制。组内的用户通过读、写、通知视图来达到访问控制的目的。同时通过有无认证和有无加密等功能组合，为管理软件和被管理设备之间的通信提供更高的安全性。

命令

```
snmp-server group name [ smode { v1 | v2c | v3 } ] [ slev { noAuthNoPriv | authNoPriv | authPriv } ] [ read read-view ] [ write write-view ] [ notify notify-view ]  
no snmp-server group name smode { v1 | v2c | v3 } slev { noAuthNoPriv | authNoPriv | authPriv }
```

参数

name —— 要添加的组名，可输入 1~16 个字符。组名与“安全模式”和“安全级别”共同组成该组的标识，三项均相同才被认为是同一组。

smode —— 安全模式，有 v1、v2c 和 v3 三个选项，分别表示 SNMP v1、SNMP v2c 和 SNMP v3。其中 SNMP v1 和 SNMP v2c 采用团体名（详见命令 [snmp-server community](#)）认证，SNMP v3 采用 USM 认证。缺省时为 v1。

slev —— SNMP v3 的组安全级别，有 noAuthNoPriv（不认证不加密）、authNoPriv（认证不加密）和 authPriv（认证加密）三个选项，缺省时为 noAuthNoPriv。SNMP v1 和 SNMP v2c 安全模式下不需设置此项。

read-view —— 关联的只读视图名称。只读视图只能被查看不能被编辑。

write-view —— 关联的只写视图名称。只写视图只能被编辑不能被查看。若要对某视图进行读写操作，则需同时将该视图添加为只读视图和只写视图。

notify-view —— 关联的通知视图名称。管理软件可以接收到通知视图发送的异常报警信息。

模式

全局配置模式

示例

添加组 **group1**，并设置其安全模式为 SNMP v3，组安全级别为 **authNoPriv**，组内的用户可对视图 **viewDefault** 进行读写操作，管理软件可以接收到视图 **viewDefault** 发送的异常报警信息：

```
TL-SG3210(config)# snmp-server group group1 smode v3 slev authNoPriv read  
viewDefault write viewDefault notify viewDefault
```

删除组 group1:

```
TL-SG3210(config)# no snmp-server group group1 smode v3 slev authNoPriv
```

30.4 snmp-server user

该命令用于添加用户，它的 no 命令用于删除对应的用户。管理软件可以通过用户的方式对交换机进行管理。用户建立在组之下，与其所属的组具有相同的安全级别和访问控制权限。

命令

```
snmp-server user name { local | remote } group-name [ smode { v1 | v2c | v3 } ] [ slev { noAuthNoPriv | authNoPriv | authPriv } ] [ cmode { none | MD5 | SHA } ] [ cpwd confirm-pwd ] [ emode { none | DES } ] [ epwd encrypt-pwd ]  
no snmp-server user name
```

参数

name —— 要添加的用户名，可输入 1~16 个字符。

local | remote —— 用户类型，分本地（local）和远程（remote）两种。本地用户即建立在本地引擎下的用户，远程用户即建立在远程引擎下的用户。

group-name —— 关联的组名。通过“组名”、“安全模式”和“安全级别”来确定用户所属的组。

smode —— 安全模式，有 v1、v2c 和 v3 三个选项，缺省时为 v1。用户的安全模式必须和其所属组的安全模式相同。

slev —— SNMP v3 的组安全级别，有 noAuthNoPriv（不认证不加密）、authNoPriv（认证不加密）和 authPriv（认证加密）三个选项，缺省时为 noAuthNoPriv。用户的安全级别必须和其所属组的安全级别相同。

cmode —— SNMP v3 用户的认证模式，有 none、MD5 和 SHA 三个选项。其中 none 表示不认证；MD5 为信息摘要算法；SHA 为安全散列算法，比 MD5 的安全性更高。缺省时为 none。

confirm-pwd —— 认证密码，可输入 1~16 个字符。

emode —— SNMP v3 用户的加密模式，有 none 和 DES 两个选项。其中 none 表示不加密，DES 为数据加密标准。缺省时为 none。

encrypt-pwd —— 加密密码，可输入 1~16 个字符。

模式

全局配置模式

示例

将本地用户 admin 添加到组 group2，输入组的安全模式 v3、安全级别 authPriv，并设置用户的认证模式为 MD5、认证密码为 11111、加密模式为 DES、加密密码为 22222：

```
TL-SG3210(config)# snmp-server user admin local group2 smode v3 slev authPriv  
cmode MD5 cpwd 11111 emode DES epwd 22222
```

30.5 snmp-server community

该命令用于添加团体，它的 **no** 命令用于删除对应的团体。SNMP v1 和 SNMP v2c 采用团体名（Community Name）认证，团体名起到了类似于密码的作用。

命令

```
snmp-server community name { read-only | read-write } mib-view  
no snmp-server community name
```

参数

name —— 要添加的团体名称，可输入 1~16 个字符。

read-only | read-write —— 团体对相应视图的权限，有 **read-only**（只读）和 **read-write**（读写）两个选项。

mib-view —— MIB 视图，即团体可访问的视图。

模式

全局配置模式

示例

添加团体 **public**，此团体对视图 **viewDefault** 具有读写权限：

```
TL-SG3210(config)# snmp-server community public read-write viewDefault
```

30.6 snmp-server host

该命令用于添加通知管理条目，它的 **no** 命令用于删除对应条目。通知管理功能是交换机主动向管理软件报告某些视图的重要事件，便于管理软件对交换机的某些事件进行及时监控和处理。

命令

```
snmp-server host ip udp-port user-name [ smode { v1 | v2c | v3 } ] [ slev  
{ noAuthNoPriv | authNoPriv | authPriv } ] [ type { trap | inform } ] [ retries retries ]  
[ timeout timeout ]  
no snmp-server host ip user-name
```

参数

ip —— 管理主机的 IP 地址。支持 IPv4 和 IPv6 地址。例如 IPv4 地址 192.168.0.10，IPv6 地址 fe80::1234。

udp-port —— UDP 端口号，即管理主机上开启供通知过程使用的 UDP 端口号，与 IP 地址共同作用。取值范围为 1~65535，默认值为 162。

user-name —— 配置管理软件的团体名/用户名。

smode —— 用户的安全模式，有 v1、v2c 和 v3 三个选项。缺省时为 v1。

slev —— SNMP v3 的组安全级别，有 noAuthNoPriv（不认证不加密）、authNoPriv（认证不加密）和 authPriv（认证加密）三个选项，缺省时为 noAuthNoPriv。

type —— 通知报文的类型，有 trap 和 inform 两个选项，缺省时为 trap。选择 trap 时，以 Trap 方式发送通知；选择 inform 时，以 Inform 方式发送通知。Inform 具有更高的可靠性，并且需要设置重传次数（*retries*）和超时时间（*timeout*）。v1 安全模式下只能选择 Trap 方式。

retries —— Inform 报文的重传次数，取值范围 1~255。交换机发送 Inform 报文后，若经过超时时间仍没有收到 Inform 回应报文，则会重发 Inform 报文。超过重传次数后，将不再重发 Inform 报文。

timeout —— 超时时间，即交换机等待 Inform 回应报文的时间。超过该时间后，将重新发送 Inform 报文。取值范围为 1~3600（秒）。

模式

全局配置模式

示例

添加通知管理条目，其中管理主机的 IP 地址为 192.168.0.146，其 UDP 端口号为 162，管理软件的用户名为 admin，用户安全模式为 v2c，通知报文以 Inform 的方式发送，Inform 报文的超时时间为 1000 秒，重传次数 100 次：

```
T L-SG3210(config)# snmp-server host 192.168.0.146 162 admin smode v2c type
inform retries 100 timeout 1000
```

添加通知管理条目，其中管理主机的 IP 地址为 fe80::1234，其 UDP 端口号为 162，管理软件的用户名为 admin，用户安全模式为 v2c，通知报文以 Inform 的方式发送，Inform 报文的超时时间为 1000 秒，重传次数 100 次：

```
T L-SG3210(config)# snmp-server host fe80::1234 162 admin smode v2c type
inform retries 100 timeout 1000
```

30.7 snmp-server engineID

该命令用于配置交换机本地和远程的引擎 ID，它的 no 命令用于恢复默认的配置。

命令

```
snmp-server engineID { local local-engineID } { remote remote-engineID }
no snmp-server engineID
```

参数

local-engineID —— 本地引擎 ID，即本地 SNMP 实体的引擎 ID。本地用户建立在本地引擎之下。可输入 10~64 个十六进制字符，且字符的个数必须为偶数。

remote-engineID —— 远程引擎 ID，即 SNMP 管理端的引擎 ID。远程用户建立在远程引擎之下。可输入 10~64 个十六进制字符，且字符个数必须是偶数。

模式

全局配置模式

示例

配置交换机 SNMP 的本地引擎 ID 为 1234567890，远程引擎 ID 为 abcdef123456:

```
T L-SG3210(config)# snmp-server engineID local 1234567890 remote
abcdef123456
```

30.8 snmp-server traps snmp

该命令用于开启所有的标准 traps。它的 no 命令用于关闭标准 traps。

命令

```
snmp-server traps snmp { linkup | linkdown | warmstart | coldstart | auth-failure }
no snmp-server traps snmp { linkup | linkdown | warmstart | coldstart | auth-failure }
```

参数

linkup —— 当端口由断开状态转变为连接状态时，发送 linkup 类型 trap。默认开启。给端口插上连接线可触发此类型 trap。

linkdown —— 当端口由连接状态转变为断开状态时，发送 linkdown 类型 trap。默认开启。断开端口的连接线可触发此类型 trap。

warmstart —— 表示交换机的 SNMP 被重初始化，且该实体的配置没有发生改变。默认开启。在交换机全局 SNMP 功能开启并设置好团体名及通知条目的情况下，先关闭再重新开启全局 SNMP 功能可触发此类型 trap。

coldstart —— 表示因交换机系统的重初始化而导致 SNMP 实体发生初始化。默认开启。重启交换机即可触发此类型 trap。

auth-failure —— 当接收 SNMP 请求未通过认证时，发送此类型 trap。默认开启。

模式

全局配置模式

示例

开启交换机的 SNMP 标准 traps 的 linkup 功能:

```
TL-SG3210(config)# snmp-server traps snmp linkup
```

30.9 snmp-server traps link-status

该命令用于开启指定端口的 SNMP 标准 traps 的端口连接状态监控功能。它的 no 命令用于关闭该功能。

命令

snmp-server traps link-status

no snmp-server traps link-status

模式

接口配置模式（interface gigabitEthernet/ interface range gigabitEthernet）

示例

开启端口 3 的 SNMP 标准 traps 的连接状态监控功能：

```
TL-SG3210(config)# interface gigabitEthernet 1/0/3
```

```
TL-SG3210(config-if)# snmp-server traps link-status
```

30.10 snmp-server traps

该命令用于开启交换机的扩展 traps 功能。 它的 no 命令用于关闭交换机的扩展 traps 功能。

命令

snmp-server traps { bandwidth-control | cpu | flash | ipaddr-change | lldp | loopback-detection | storm-control | spanning-tree | memory }

no snmp-server traps { bandwidth-control | cpu | flash | ipaddr-change | lldp | loopback-detection | storm-control | spanning-tree | memory }

参数

bandwidth-control —— 用于监控端口的速率是否超过了设定的带宽速率。在端口的带宽控制功能开启情况下，以大于所设定速率的速率往该端口发送数据包时，系统会触发此类型 trap。

cpu —— 用于监控 cpu 的负载状况。当 cpu 使用率超过设定的最高阈值时系统会触发此类型 trap。我司交换机的 cpu 使用率最高阈值默认为 80%。

flash —— 用于监控 flash 是否被修改。当 flash 被修改时，如进行保存配置、恢复出厂设置、升级、导入配置等操作时，系统会触发此类型 trap。

ipaddr-change —— 用于监控交换机的 IP 是否更改。当交换机的 IP 地址被修改时，如进行手动修改 IP 地址或通过 DHCP 获取到新的 IP 地址时，系统会触发此类型 trap。

lldp —— 用于 LLDP 监测。当相邻端口发生变化时，系统会触发此类型 trap。

loopback-detection ——用于环路监测。交换机监测到环路时，或是环路被清除时，系统都会触发此类 trap。

storm-control —— 用于监控网络风暴的情况。当广播或者组播的速率达到风暴控制的设定值时系统会触发此类型 trap。

spanning-tree —— 用于监控生成树系统的拓扑状况。以下几种情况会触发此类型 trap：

- a). 交换机端口从非转发态变为转发态或者从转发态变为非转发态；
- b). 交换机端口接收到带 TC flag 的报文或 TCN 报文。

memory —— 用于内存监控。当内存使用率超过80%时，系统会触发此类型trap。

模式

全局配置模式

示例

开启交换机的 SNMP 扩展 traps 的带宽监控功能：

```
TL-SG3210(config)# snmp-server traps bandwidth-control
```

30.11 snmp-server traps mac

该命令用于统一开启交换机中与 MAC 地址表相关的扩展 traps 功能。它的 no 命令用于统一关闭交换机中与 MAC 地址表相关的扩展 traps 功能。与 MAC 地址表相关的 trap 有四种： new、full、learn-mode-change 和 max-learned，可以在后面扩展参数以单独开启其中某一项功能。

命令

snmp-server traps mac [new | full | learn-mode-change | max-learned]

no snmp-server traps mac [new | full | learn-mode-change | max-learned]

参数

new —— 当交换机学习到新地址（包括动态地址、静态地址和过滤地址）时，系统会触发此类型 trap。

full —— 当检测到交换机的地址表满时系统会触发此类型 trap。

learn-mode-change —— 当端口地址学习模式发生变化时系统会触发此类型 trap。

max-learned —— 当端口学习到的 MAC 地址达到指定最大数目（最大数目在开启端口安全的时候指定）时，系统会触发此类型 trap。

模式

全局配置模式

示例

统一开启交换机中与 MAC 地址表相关的扩展 traps 功能：

```
TL-SG3210(config)# snmp-server traps mac
```

单独开启交换机 SNMP 扩展 traps 中的 mac new 功能：

```
TL-SG3210(config)# snmp-server traps mac new
```

30.12 snmp-server traps vlan

该命令用于统一开启交换机中与 VLAN 相关的扩展 traps 功能。它的 no 命令用于统一关闭交换机中与 VLAN 相关的扩展 traps 功能。与 VLAN 相关的 trap 有 vlan create 和 vlan delete 两种，可以在后面扩展参数以单独开启其中某一项功能。

命令

```
snmp-server traps vlan [ create | delete ]
```

```
no snmp-server traps vlan [create | delete ]
```

参数

create —— 当新的 VLAN 被创建成功时系统会触发此类型 trap。

delete —— 当已有 VLAN 被删除成功时系统会触发此类型 trap。

模式

全局配置模式

示例

统一开启交换机中与 vlan 相关的扩展 traps 功能：

```
TL-SG3210(config)# snmp-server traps vlan
```

单独开启交换机 SNMP 扩展 traps 中的 vlan create 功能：

```
TL-SG3210(config)# snmp-server traps vlan create
```

30.13 rmon history

该命令用于配置历史采样条目，它的 no 命令用于恢复默认配置。RMON（Remote Monitoring，远程网络监视）完全基于 SNMP 体系结构，用于监视和管理远程网络设备。历史组是 RMON 的一个组，利用 RMON 的历史采样控制功能，交换机会周期性地收集网络统计信息，从而监视网络的使用情况。

命令

```
rmon history index interface gigabitEthernet port [ interval seconds ] [ owner  
owner-name]
```

```
no rmon history index
```

参数

index —— 采样条目的序号，取值范围 1~12，可输入多条，格式为 1-3,5。

port —— 采样端口。

seconds —— 采样间隔，即端口采样的时间间隔，单位为秒，取值范围 10~3600，默认值为 1800。

owner-name —— 条目的创建者，可输入 1~16 个字符。缺省时为 monitor。

模式

全局配置模式

示例

配置条目 1-3 的采样端口为端口 2，采样间隔为 100 秒，创建者为 owner1：

```
TL-SG3210(config)# rmon history 1-3 interface gigabitEthernet 1/0/2 interval 100  
owner owner1
```

30.14 rmon event

该命令用于配置 SNMP-RMON 事件条目，它的 no 命令用于恢复默认配置。事件组是 RMON 一个组，用来定义事件及其类型，此处定义的事件主要用于在警报配置中触发报警。

命令

```
rmon event index [ user user-name ] [ description descript ] [ type { none | log | notify  
| log-notify } ] [ owner owner-name ]
```

```
no rmon event index
```

参数

index —— 条目序号，取值范围 1~12，每条命令只能输入一个条目。

user-name —— 事件所属的用户名，可输入 1~16 个字符。缺省时为 public。

descript —— 对事件的描述信息，可输入 1~16 个字符，默认为空。

type —— 事件类型，选择 none 时，不做任何操作；选择 log 时，交换机将事件记录在日志表中；选择 notify 时，交换机向管理主机发送报警信息；选择 both 时，交换机将事件记录在日志表中并向管理主机发送报警信息。

owner-name —— 条目的创建者，可输入 1~16 个字符。缺省时为 monitor。

模式

全局配置模式

示例

设置条目 1、2、3、4 的用户名为 user1，事件描述为 description1，事件类型为 log，创建者为 owner1：

```
TL-SG3210(config)# rmon event 1-4 user user1 description description1 type log
owner owner1
```

30.15 rmon alarm

该命令用于配置 SNMP-RMON 警报管理信息，它的 no 命令用于恢复默认配置。警报组是 RMON 的一个组，警报配置是对指定的警报变量进行监视，一旦计数器超过阈值则触发警报，报警方式将按照事件的类型进行相应的处理。

命令

```
rmon alarm index interface gigabitEthernet port [ alarm-variable { drop | revbyte |
revpkt | bpkt | mpkt | crc-lign | undersize | oversize | fragment | jabber | collision | 64 |
65-127 | 128-511 | 512-1023 | 1024-10240 } ] [ s-type { absolute | delta } ]
[ rising-threshold r-hold ] [ rising-event-index r-event ] [ falling-threshold f-hold ]
[ falling-event-index f-event ] [ a-type { rise | fall | all } ] [ owner owner-name ]
[ interval interval ]
no rmon alarm index
```

参数

index —— 警报管理条目的序号，取值范围 1~12，可输入多条，格式为 1-3,5。

port —— 端口号。

alarm-variable —— 警报变量，缺省时为 drop。

s-type —— 样例类型，即为警报变量选择取样，并将取样值与阈值进行比较的方法，有 **absolute**（绝对值）和 **delta**（增量）两个选项。选择 **absolute**，则在一个取样周期结束时将取样结果直接与阈值进行比较；选择 **delta**，则将目前值减去上一次取样值之后的增量与阈值进行比较。默认选项为 **absolute**。

r-hold —— 触发警报的上升阈值，取值范围 1~65535，默认值为 100。

r-event —— 上升事件，即触发上升阈值警报的事件的序号，取值范围 1~12。

f-hold —— 触发警报的下降阈值，取值范围 1~65535，默认值为 100。

f-event —— 下降事件，即触发下降阈值警报的事件的序号，取值范围 1~12。

a-type —— 警报触发的方式，有 **rise**（上升）、**fall**（下降）和 **all**（全部）三个选项。选择 **rise**，则只在触发上升阈值后触发警报；选择 **fall**，则只在触发下降阈值后触发警报；选择 **all**，则触发上升和下降阈值均触发警报。默认选项为 **all**。

owner-name —— 条目的创建者，可输入 1~16 个字符，缺省时为 monitor。

interval —— 时间间隔，取值范围 10~3600，单位为秒，默认值为 1800。

模式

全局配置模式

示例

设置条目 1、2、3 的端口为 3，创建者为 owner1，时间间隔为 100 秒：

```
TL-SG3210(config)# rmon alarm 1-3 interface gigabitEthernet 1/0/2 owner owner1
interval 100
```

30.16 show snmp-server

该命令用于显示 SNMP 全局配置信息。

命令

show snmp-server

模式

特权模式和所有配置模式

示例

显示 SNMP 全局配置信息：

```
TL-SG3210# show snmp-server
```

30.17 show snmp-server view

该命令用于显示视图列表。

命令

show snmp-server view

模式

特权模式和所有配置模式

示例

显示视图列表：

```
TL-SG3210# show snmp-server view
```

30.18 show snmp-server group

该命令用于显示组列表。

命令

show snmp-server group

模式

特权模式和所有配置模式

示例

显示组列表：

```
TL-SG3210# show snmp-server group
```

30.19 show snmp-server user

该命令用于显示用户列表。

命令

```
show snmp-server user
```

模式

特权模式和所有配置模式

示例

显示用户列表：

```
TL-SG3210# show snmp-server user
```

30.20 show snmp-server community

该命令用于显示团体列表。

命令

```
show snmp-server community
```

模式

特权模式和所有配置模式

示例

显示团体列表：

```
TL-SG3210# show snmp-server community
```

30.21 show snmp-server host

该命令用于显示目的主机列表。

命令

```
show snmp-server host
```

模式

特权模式和所有配置模式

示例

显示目的主机列表：

```
TL-SG3210# show snmp-server host
```

30.22 show snmp-server engineID

该命令用于显示 SNMP 的引擎 ID 信息。

命令

```
show snmp-server engineID
```

模式

特权模式和所有配置模式

示例

显示 SNMP 的引擎 ID 信息：

```
TL-SG3210# show snmp-server engineID
```

30.23 show rmon history

该命令用于显示历史采样条目的配置信息。

命令

```
show rmon history [ index ]
```

参数

index —— 要显示配置信息的采样条目序号，取值范围 1~12，可输入多条，格式为 1-3,5。缺省时显示所有历史采样条目的配置信息。

模式

特权模式和所有配置模式

示例

显示所有历史采样条目的配置信息：

```
TL-SG3210# show rmon history
```

30.24 show rmon event

该命令用于显示 SNMP-RMON 事件配置信息。

命令

```
show snmp-rmon event [index]
```

参数

index —— 要显示事件配置信息的条目序号，取值范围 1~12，可输入多条，格式为 1-3，5。缺省时显示所有条目的事件配置信息。

模式

特权模式和所有配置模式

示例

显示条目 1-4 的事件配置信息：

```
T L-SG3210# show rmon event 1-4
```

30.25 show rmon alarm

该命令用于显示警报管理条目的配置信息。

命令

show rmon alarm [*index*]

参数

index —— 要显示配置信息的警报管理条目序号，取值范围 1~12，可输入多条，格式为 1-3，5。缺省时显示所有警报管理条目的配置信息。

模式

特权模式和所有配置模式

示例

显示警报管理条目 1-2 的配置信息：

```
TL-SG3210# show rmon alarm 1-2
```

第31章 LLDP 配置命令



注意：

- 本书所列举的机型中只有 TL-SG3424P 支持 LLDP 功能。

链路层发现协议 LLDP（Link Layer Discovery Protocol）允许网络设备周期性的向处于同一局域网的邻居设备通告自己的设备信息。邻居设备收到信息后将其以标准的 MIB（Management Information Base，管理信息库）形式保存起来，使得网络管理系统可以通过管理协议 SNMP（Simple Network Management Protocol，简单网络管理协议）获取到这些信息。

31.1 lldp

该命令用于全局开启 LLDP 功能，它的 no 命令用于禁用 LLDP 功能。

命令

lldp

no lldp

模式

全局配置模式

示例

使能 LLDP 功能：

```
TL-SG3424P(config)# lldp
```

31.2 lldp hold-multiplier

该命令用于设置 TTL 乘数。TTL 乘数用以控制本地设备发送的 LLDPDU 中 TTL 字段的值，TTL 即为本地信息在邻居设备上的存活时间。 $TTL = TTL \text{ 乘数} \times \text{发送间隔}$ 。它的 no 命令用于恢复默认设置。

命令

lldp hold-multiplier *multiplier*

no lldp hold-multiplier

参数

multiplier —— TTL 乘数，范围为 2~10。默认值为 4。

模式

全局配置模式

示例

设置 TTL 乘数值为 5：


```
TL-SG3424P(config)# lldp hold-multiplier 5
```

31.3 lldp timer

该命令用于设置发送报文的各项时间参数。它的 no 命令用于恢复默认设置。

命令

```
lldp timer { tx-interval tx-interval | tx-delay tx-delay | reinit-delay reinit-delay |  
notify-interval notify-interval | fast-count fast-count }
```

```
no lldp timer { tx-interval | tx-delay | reinit-delay | notify-interval | fast-count }
```

参数

tx-interval——本地设备向邻居设备发送 LLDPDU 的时间间隔，取值范围为 5-32768，默认值为 30 秒。

tx-delay——本地设备向邻居设备发送 LLDPDU 的延迟时间。当本地配置发生变化时，将延迟指定时间再发送 LLDPDU 通知邻居设备，从而可以避免由于本地配置频繁变化而导致 LLDPDU 的频繁发送。取值范围为 1-8192，默认值为 2 秒。

reinit-delay——初始化延迟时间。当端口 LLDP 工作模式改变时，将延迟一段时间再进行初始化，以避免端口 LLDP 工作模式频繁改变导致端口不断执行初始化。取值范围为 1-10，默认值为 3 秒。

notify-interval——本地设备向网络管理系统发送 Trap 信息的时间间隔。通过调整该时间间隔，可以避免由于邻居信息频繁变化而导致 Trap 信息的频繁发送。取值范围为 5-3600，默认值为 5 秒。

fast-count——当端口 LLDP 工作模式从禁用（或只接收）切换为发送接收（或只发送）时，为了让其它设备尽快发现本设备，将启用快速发送机制，即将 LLDP 报文的发送周期缩短为 1 秒，并连续发送指定数量的 LLDPDU 后再恢复为正常的发送周期。取值范围为 1-10，默认值为 3 个。

模式

全局配置模式

示例

设置 LLDPDU 的发送间隔为 45 秒，向网络管理系统发送 trap 信息的发送时间间隔为 120 秒：

```
TL-SG3424P(config)# lldp timer tx-interval 45
```

```
TL-SG3424P(config)# lldp timer notify-interval 120
```

31.4 lldp med-fast-count

该命令用于设置 LLDP-MED 快速发送机制时发送的 LLDP-MED 帧的数目。当 LLDP-MED 的快速发送机制启动时，会连续发送指定个数的包含 LLDP-MED 信息的 LLDPDU，其默认值为 4。它的 no 命令用于恢复默认设置。

命令

lldp med-fast-count count

no lldp med-fast-count

参数

count —— 快速发送报文个数，取值范围为 1~10，默认值为 4。

模式

全局配置模式

示例

设置快速发送报文个数为 5：

```
TL-SG3424P(config)# lldp med-fast-count 5
```

31.5 lldp receive

该命令用于开启指定端口的 LLDPDU 接收功能。它的 no 命令用于禁用该功能。

命令

lldp receive

no lldp receive

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

开启端口 1 的 LLDPDU 接收功能：

```
TL-SG3424P(config)# interface gigabitEthernet 1/0/1
```

```
TL-SG3424P(config-if)# lldp receive
```

31.6 lldp transmit

该命令用于开启指定端口的 LLDPDU 发送功能。它的 no 命令用于禁用该功能。

命令

lldp transmit

no lldp transmit

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

开启端口 1 的 LLDPDU 发送功能：

```
TL-SG3424P(config)# interface gigabitEthernet 1/0/1
TL-SG3424P(config-if)# lldp transmit
```

31.7 lldp snmp-trap

该命令用于启用端口的 SNMP 通知功能。启用此功能时，如果发生 trap 事件，本地设备将会通知 SNMP 服务器。它的 no 命令用于禁用端口的 SNMP 通知功能。

命令

lldp snmp-trap

no lldp snmp-trap

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

启用端口 8 的 SNMP 通知功能：

```
TL-SG3424P(config)# interface gigabitEthernet 1/0/8
TL-SG3424P(config-if)# lldp snmp-trap
```

31.8 lldp tlv-select

该命令用于配置发送的 LLDPDU 中包含的 TLV 类型。LLDPDU 必须顺序包含三个必须的 TLV，然后是可选的 TLV，最后是必须的 END TLV。您可以在此页面选择端口发送 LLDPDU 时包含的可选 TLV 类型。它的 no 命令用于删除 LLDPDU 中包含的相关 TLV 类型。默认情况下，LLDPDU 中包含所有的 TLV 类型。

命令

lldp tlv-select [port-description] [system-capability] [system-description] [system-name] [management-address] [port-vlan-id] [protocol-vlan-id] [vlan-name] [link-aggregation] [mac-phy] [max-frame-size] [power] [all]

no lldp tlv-select [port-description] [system-capability] [system-description] [system-name] [management-address] [port-vlan-id] [protocol-vlan-id] [vlan-name] [link-aggregation] [mac-phy] [max-frame-size] [power] [all]

参数

port-description —— 使 LLDPDU 包含端口描述 TLV，以向邻居发布本端口的 IEEE 802 局域网工作站规定的端口描述。

system-capability —— 使 LLDPDU 包含系统能力 TLV，以向邻居发布本地设备支持的功能和这些功能是否允许的信息。

system-description —— 使 LLDPDU 包含系统描述 TLV，用以向邻居发布本地设备包含系统硬件、软件版本等系统信息的描述。

system-name —— 使 LLDPDU 包含系统名称 TLV，以向邻居发布本地设备的系统名称。

management-address —— 使 LLDPDU 包含管理地址 TLV，以向邻居发布本地设备的管理地址，网络管理协议可以通过该地址对本地设备进行管理。

port-vlan-id —— 使 LLDPDU 包含端口 VLAN ID TLV，以向邻居发布本端口所处 802.1Q VLAN 的 ID。

protocol-vlan-id —— 使 LLDPDU 包含协议 VLAN ID TLV，以向邻居发布本端口所处协议 VLAN 的 ID。

vlan-name —— 使 LLDPDU 包含 VLAN 名称 TLV，以向邻居发布本端口所处 VLAN 被指派的名稱。

link-aggregation —— 使 LLDPDU 包含链路聚合 TLV，以向邻居发布本端口当前的链路聚合信息，包括本端口是否具有链路聚合能力、是否处于聚合状态以及处于链路聚合状态时的端口 ID。

mac-phy —— 使 LLDPDU 包含 MAC/PHY TLV，以向邻居发布本端口的端口属性，包括端口支持的速率双工、当前工作的速率双工以及是手工设置还是自动协商而得到的速率双工。

max-frame-size —— 使 LLDPDU 包含最大帧长度 TLV，以向邻居发布本端口的 MAC 和 PHY 支持的最大帧长度。

power —— 使 LLDPDU 包含供电能力 TLV，以向邻居发布本端口的的基本供电信息。

all —— 使 LLDPDU 包含以上所有的 TLV 类型。

模式

接口配置模式（`interface gigabitEthernet / interface range gigabitEthernet`）

示例

从端口 8 发送的 LLDPDU 中包含的 TLV 类型中删除管理地址 TLV 和端口 VLAN ID TLV：

```
TL-SG3424P(config)# interface gigabitEthernet 1/0/8
```

```
TL-SG3424P(config-if)# no lldp tlv-select management-address port-vlan-id
```

31.9 lldp med-status

该命令用于启用端口的 LLDP-MED 状态。启用端口的 LLDP-MED 功能后，端口的 LLDP 状态会被设置为发送接收。它的 no 命令用于禁用端口的 LLDP-MED 功能。

命令

lldp med-status

no lldp med-status

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

启用端口 2 的 LLDP-MED 功能：

```
TL-SG3424P(config)# interface gigabitEthernet 1/0/2
```

```
TL-SG3424P(config-if)# lldp med-status
```

31.10 lldp med-tlv-select

该命令用于选择发送的 LLDPDU 中包含的 LLDP-MED 的 TLV 类型。默认情况下，LLDPDU 中包含所有的 TLV 类型。它的 no 命令用于删除选中的 TLV 类型。

命令

lldp med-tlv-select { [inventory-management] [location] [network-policy]
[power-management] [all]}

no lldp med-tlv-select { [inventory-management] [location] [network-policy]
[power-management] [all]}

参数

inventory-management —— 使 LLDPDU 包含资产信息 TLV，资产信息中包含七种基本的资产信息 TLV，分别为硬件版本 TLV、固件版本 TLV、软件版本 TLV、序列号 TLV、制造厂商名称 TLV、模块名称 TLV 和资产跟踪 ID TLV。

location —— 使 LLDPDU 包含设备地址 TLV，设备地址 TLV 提供了向相邻设备发布本地设备物理地址信息的能力。

network-policy —— 使 LLDPDU 包含网络策略 TLV，网络策略 TLV 允许网络连接设备和终端设备发布本端口的 VLAN 配置与二层和三层属性。

power-management —— 使 LLDPDU 包含扩展供电能力 TLV，扩展供电能力 TLV 允许 LLDP-MED 连接设备和终端设备之间交互详细的供电信息，例如供电优先级、供电状态等。

all —— 使 LLDPDU 包含以上所有的 TLV 类型。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

从端口 8 发送的 LLDPDU 中包含的 TLV 类型中删除网络策略 TLV 和设备地址 TLV：

```
TL-SG3424P(config)# interface gigabitEthernet 1/0/2
```

```
TL-SG3424P(config-if)# no lldp tlv-select network-policy location
```

31.11 lldp med-location

该命令用于设置端口发送的 LLDPDU 中包含的设备地址 TLV 的信息。

命令

```
lldp med-location {emergency-number identifier | civic-address [language  
language | province-state province-state | county county | city city | street street |  
house-number house-number | name name | postal-zipcode postal-zipcode |  
room-number room-number | post-office-box post-office-box | additional additional |  
country-code country-code | what what]}
```

参数

emergency-number —— 紧急号码是紧急呼叫服务使用的号码，用以呼叫 CAMA 或者 PSAP，字符长度介于 10 到 25 之间。

civic-address —— 普通地址使用 IETF 规定的地址信息格式。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

设置端口 6 发送的 LLDPDU 中设备地址 TLV 类型中的普通地址，设置语言为英语，城市为伦敦：

```
TL-SG3424P(config)# interface gigabitEthernet 1/0/6
```

```
TL-SG3424P(config-if)# lldp med-location civic-address language English city  
London
```

31.12 show lldp

该命令用于显示 LLDP 的全局配置信息。

命令

```
show lldp
```

模式

特权模式和所有配置模式

示例

显示 LLDP 的全局配置信息：

```
TL-SG3424P# show lldp
```

31.13 show lldp interface

该命令用于显示端口的 LLDP 配置信息。

命令

```
show lldp interface [ gigabitEthernet port ]
```

参数

port ——要显示 LLDP 配置信息的端口号。

模式

特权模式和所有配置模式

示例

显示端口 8 的 LLDP 配置信息：

```
TL-SG3424P# show lldp interface gigabitEthernet 1/0/8
```

31.14 show lldp local-information interface

该命令用于显示端口的 LLDP 信息。

命令

```
show lldp local-information interface [ gigabitEthernet port ]
```

参数

port ——要显示 LLDP 信息的端口号,缺省显示所有端口的 LLDP 信息。

模式

特权模式和所有命令模式

示例

显示所有端口的 LLDP 信息：

```
TL-SG3424P# show lldp local-information interface
```

显示端口 8 的 LLDP 信息：

```
TL-SG3424P# show lldp local-information interface gigabitEthernet 1/0/8
```

31.15 show lldp neighbor-information interface

该命令用于显示连接到该端口的邻居信息。

命令

show lldp neighbor-information interface [gigabitEthernet *port*]

参数

port ——要显示邻居信息的本地端口号，缺省显示所有端口的邻居信息。

模式

特权模式和所有命令模式

示例

显示连接到端口 8 的邻居信息：

```
TL-SG3424P# show lldp neighbor-information interface gigabitEthernet 1/0/8
```

31.16 show lldp traffic interface

该命令用于显示连接到该端口的本地设备和邻居设备的 LLDP 统计信息。

命令

show lldp traffic interface [gigabitEthernet *port*]

参数

port ——要显示本地设备和邻居设备的 LLDP 统计信息的端口号，缺省表示显示所有端口的统计信息。

模式

特权模式和所有命令模式

示例

显示连接到端口 1 的 LLDP 统计信息：

```
TL-SG3424P# show lldp traffic interface gigabitEthernet 1/0/1
```


第32章 集群配置命令

集群管理解决了大量分散网络设备的集中管理问题，只需将集群中的一个设备配置为命令交换机，即可通过该命令交换机对集群中的其他设备进行管理和维护。

32.1 cluster ndp

该命令用于拓扑发现全局配置，它的 **no** 命令用于关闭 NDP 功能。NDP（Neighbor Discovery Protocol，邻居发现协议）用于交换机发现与其直接相连的邻居交换机的信息，为集群的建立提供支持。运行 NDP 的交换机周期性地向邻居发送 NDP 报文，NDP 报文包含本设备的信息以及 NDP 信息在接收设备上的老化时间，同时也会接收但不转发邻居设备发送的 NDP 报文。本命令用来设置交换机的 NDP 相关属性。

命令

cluster ndp

cluster ndp timer { [hello *hello-time*] [aging *aging-time*] }

no cluster ndp

no cluster ndp timer { [hello *hello-time*] [aging *aging-time*] }

参数

hello-time ——Hello 定时器，即 NDP 报文发送的时间间隔。取值范围 5~254（秒），缺省时为 60。***hello-time*** 的值必须小于 ***aging-time***。

aging-time ——老化时间，即本交换机发送的 NDP 报文在接收设备上的老化时间。取值范围 5~255（秒），缺省时为 180。

模式

全局配置模式

示例

开启全局 NDP 功能，并设置老化定时器为 120 秒，Hello 定时器为 50 秒：

```
TL-SG3210(config)# cluster ndp
```

```
TL-SG3210(config)# cluster ndp timer hello 50 aging 120
```

老化时间改为 80 秒：

```
TL-SG3210(config)# cluster ndp timer aging 80
```

Hello 定时器改为 80 秒：

```
TL-SG3210(config)# cluster ndp timer hello 80
```

32.2 cluster ntdp

该命令用于拓扑收集全局配置，它的 **no** 命令用于关闭 NTDP 功能。NTDP（Neighbor Topology Discovery Protocol，邻居拓扑发现协议）用来在一定网络范围内收集每个设备的信息以及设备间的连接信息。NTDP 为命令交换机提供可加入集群的设备信息，收集指定跳数内的设备的拓扑信息。

命令

cluster ntdp

cluster ntdp timer { [**interval-time** *time*] [**hop-delay** *hop-delay-value*] [**port-delay** *port-delay-value*] }

cluster ntdp hop *hop-value*

no cluster ntdp

no cluster ntdp timer { [**interval-time** *time*] [**hop-delay** *hop-delay-value*] [**port-delay** *port-delay-value*] }

no cluster ntdp hop *hop-value*

参数

time —— 拓扑收集时间间隔，即本交换机收集拓扑信息的周期。取值范围 1~60（分钟），缺省时为 1。

hop-delay-value —— 请求跳数延迟时间，即本交换机收到拓扑请求报文到第一次转发拓扑请求报文的延时时间。取值范围 1~1000（毫秒），缺省时为 200。

port-delay-value —— 端口跳数延迟时间，即本交换机在相邻端口间转发拓扑请求报文的延时时间。取值范围 1~100（毫秒），缺省时为 20。

hop-value —— 拓扑收集跳数，它决定了本交换机拓扑收集的范围，取值范围 1~16，缺省时为 3。

模式

全局配置模式

示例

开启全局 NTDP 功能，并设置拓扑收集间隔时间为 30 分钟，拓扑收集跳数为 5：

```
TL-SG3210(config)# cluster ntdp
```

```
TL-SG3210(config)# cluster ntdp timer interval-timer 30
```

```
TL-SG3210(config)# cluster ntdp hop 5
```

32.3 cluster explore

该命令用于手动启动拓扑信息收集功能。

命令

cluster explore

模式

全局配置模式

示例

手动启动拓扑信息收集功能：

```
TL-SG3210(config)# cluster explore
```

32.4 cluster

该命令用于集群端口配置，它的 no 命令用于恢复默认配置。

命令

cluster [ndp { disable | enable }] [ntdp { disable | enable }]

no cluster

参数

ndp —— 端口是否启用 NDP 功能，缺省时为启用（enable）。

ntdp —— 端口是否启用 NTDP 功能，缺省时为启用（enable）。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

示例

启用端口 5 的 NDP 和 NTDP 功能：

```
TL-SG3210(config)# interface ethernet 1/0/5
```

```
TL-SG3210(config-if)# cluster ndp enable ntdp enable
```

32.5 cluster candidate

该命令用于指定命令交换机或独立交换机的角色为候选交换机。

命令

cluster candidate

模式

全局配置模式

示例

指定当前交换机角色为候选交换机：

```
TL-SG3210(config)# cluster candidate
```

32.6 cluster individual

该命令用于指定成员交换机或候选交换机的角色为独立交换机。

命令

cluster individual

模式

全局配置模式

示例

指定当前交换机角色为独立交换机：

```
TL-SG3210(config)# cluster individual
```

32.7 show cluster ndp

该命令用于显示指定端口的拓扑发现配置信息。

命令

show cluster ndp [interface [gigabitEthernet port]]

参数

port —— 要显示拓扑发现配置状况的端口号，缺省时显示所有端口的拓扑发现配置状况。

模式

特权模式和所有配置模式

示例

显示拓扑发现全局配置信息：

```
TL-SG3210# show cluster ndp
```

显示所有以太网端口的拓扑发现配置信息：

```
TL-SG3210# show cluster ndp interface
```

显示端口 2 的拓扑发现配置信息：

```
TL-SG3210# show cluster ndp interface gigabitEthernet 1/0/2
```

32.8 show cluster ntdp

该命令用于显示拓扑收集设备信息列表以及本交换机指定端口的拓扑收集配置信息。

命令

show cluster ntdp [interface gigabitEthernet port | device-list]

参数

port —— 要显示拓扑发现配置状况的端口号，缺省时显示所有端口的拓扑发现配置状况。

模式

特权模式和所有配置模式

示例

显示拓扑收集全局配置信息：

```
TL-SG3210# show cluster ntdp
```

显示端口 2 的拓扑收集配置信息：

```
TL-SG3210# show cluster ntdp interface gigabitEthernet 1/0/2
```

显示拓扑收集设备信息列表：

```
TL-SG3210# show cluster ntdp device-list
```

32.9 show cluster neighbour

该命令用于显示集群邻居信息。

命令

```
show cluster neighbour
```

模式

特权模式及所有配置模式

示例

显示集群邻居信息：

```
TL-SG3210# show cluster neighbour
```

32.10 show cluster manage role

该命令用于显示集群管理的全局配置信息。

命令

```
show cluster manage role
```

模式

特权模式和所有配置模式

示例

显示集群管理全局配置信息：

```
TL-SG3210# show cluster manage role
```