# 目　录


1 配置准备 ····· 1
1.1 连接方式 ····· 1
1.2 管理方式 ····· 1
1.3 权限分级和安全保障 ····· 1
1.4 密码保护和忘记密码 ····· 2
1.5 异常恢复 ····· 2
2 CLI 配置 ····· 3
2.1 功能介绍 ····· 3
2.1.1 特性简介 ····· 3
2.1.2 命令格式 ····· 3
2.1.3 视图和命令分类 ····· 3
2.1.4 易用性说明 ····· 3
2.1.5 命令过滤 ····· 4
2.1.6 规格限制 ····· 4
2.2 命令手册 ····· 5
2.2.1 config sysname ····· 5
2.2.2 config system description ····· 5
2.2.3 copy-mode ····· 6
2.2.4 end ····· 6
2.2.5 exit ····· 7
2.2.6 find ····· 7
2.2.7 reboot ····· 8
2.2.8 save ····· 8
2.2.9 screen pager ····· 9
2.2.10 show history-command ····· 9
2.2.11 show hotkey ····· 10
2.2.12 show running-config ····· 11
2.2.13 show saved-config ····· 12
2.2.14 show startup ····· 14
2.2.15 show this ····· 15
2.2.16 startup ····· 15
2.3 配置举例 ····· 16
2.4 常见问题 ····· 16
3 日志管理 ····· 17
3.1 功能介绍 ····· 17
3.2 命令手册 ····· 17
3.2.1 config logbuffer ····· 17
3.2.2 config logfile ····· 18

3.2.3 config loghost ..... 18
3.2.4 diagnostic-information save ..... 19
3.2.5 reset logbuffer ..... 19
3.2.6 show logbuffer ..... 20
3.2.7 show logfile ..... 20
3.2.8 show terminal status ..... 21
3.2.9 terminal debugging ..... 22
3.2.10 terminal monitor ..... 22
3.3 配置举例 ..... 23
3.4 常见问题 ..... 23
4 软件及版本管理 ..... 24
4.1 功能介绍 ..... 24
4.1.1 版本管理 ..... 24
4.1.2 补丁管理 ..... 24
4.2 命令手册 ..... 24
4.2.1 bootfile ..... 24
4.2.2 patch commit ..... 25
4.2.3 patch install ..... 25
4.2.4 patch uninstall ..... 26
4.2.5 restore factory-default ..... 26
4.2.6 show bootfile ..... 27
4.2.7 show patch ..... 27
4.2.8 show version ..... 28
4.3 配置举例 ..... 28
4.4 常见问题 ..... 28
5 时间管理-基础 ..... 29
5.1 功能介绍 ..... 29
5.1.1 NTP 和 SNTP 介绍 ..... 29
5.1.2 时间段 ..... 29
5.2 命令手册 ..... 29
5.2.1 config ntp-client ..... 29
5.2.2 config ntp-server ..... 30
5.2.3 config sntp-client ..... 30
5.2.4 config time-range ..... 31
5.2.5 datetime ..... 31
5.2.6 show clock ..... 32
5.2.7 show ntp state ..... 32
5.2.8 show time-range ..... 33
5.2.9 sync-from ..... 33
5.2.10 timezone ..... 34
5.2.11 time-range ..... 35
5.3 配置举例 ..... 35

5.4 常见问题 ····· 36
6 时间管理-PTP ····· 错误!未定义书签。
6.1 功能介绍 ····· 错误!未定义书签。
6.2 命令手册 ····· 错误!未定义书签。
6.2.1 clock-type ····· 错误!未定义书签。
6.2.2 config ptp ····· 错误!未定义书签。
6.2.3 domain ····· 错误!未定义书签。
6.2.4 priority ····· 错误!未定义书签。
6.2.5 ptp announce-interval ····· 错误!未定义书签。
6.2.6 ptp announce-timeout ····· 错误!未定义书签。
6.2.7 ptp enable ····· 错误!未定义书签。
6.2.8 ptp encap ····· 错误!未定义书签。
6.2.9 ptp min-delayreq-interval ····· 错误!未定义书签。
6.2.10 ptp syn-interval ····· 错误!未定义书签。
6.2.11 show ptp clock ····· 错误!未定义书签。
6.2.12 show ptp correction ····· 错误!未定义书签。
6.2.13 show ptp interface ····· 错误!未定义书签。
6.2.14 show ptp parent ····· 错误!未定义书签。
6.3 配置举例 ····· 错误!未定义书签。
6.4 常见问题 ····· 错误!未定义书签。
7 文件管理 ····· 37
7.1 功能介绍 ····· 37
7.1.1 文件系统介绍 ····· 37
7.1.2 磁盘利用率监控 ····· 37
7.2 命令手册 ····· 37
7.2.1 cd ····· 37
7.2.2 config ftp server ····· 38
7.2.3 cp ····· 38
7.2.4 ftp ····· 39
7.2.5 ls ····· 39
7.2.6 md5sum ····· 40
7.2.7 mkdir ····· 40
7.2.8 more ····· 41
7.2.9 mv ····· 42
7.2.10 pwd ····· 42
7.2.11 rename ····· 43
7.2.12 rm ····· 43
7.2.13 rmdir ····· 44
7.2.14 scp ····· 44
7.2.15 sftp ····· 45
7.2.16 tar ····· 45
7.2.17 tftp ····· 46

7.3 配置举例 ····· 47
7.4 常见问题 ····· 47
8 资源管理 ····· 48
8.1 功能介绍 ····· 48
8.2 命令手册 ····· 48
8.2.1 config memory-threshold ····· 48
8.2.2 monitor process ····· 48
8.2.3 ratio critical ····· 49
8.2.4 show cpu-usage ····· 50
8.2.5 show memory-usage ····· 51
8.2.6 show process ····· 51
8.3 配置举例 ····· 52
8.4 常见问题 ····· 52
9 硬件管理 ····· 53
9.1 功能介绍 ····· 53
9.2 命令手册 ····· 53
9.2.1 config temperature-limit ····· 53
9.2.2 cpld update ····· 53
9.2.3 show device-info ····· 54
9.2.4 show environment ····· 55
9.2.5 show fan ····· 55
9.2.6 show power status ····· 56
9.2.7 show sfp ····· 56
9.2.8 show temperature ····· 57
10 PoE ····· 58
10.1 功能介绍 ····· 58
10.2 命令手册 ····· 58
10.2.1 config poe ····· 58
10.2.2 poe enable ····· 58
10.2.3 poe high-inrush enable ····· 59
10.2.4 poe legacy enable ····· 59
10.2.5 poe max-power ····· 60
10.2.6 poe pd-policy enable ····· 60
10.2.7 poe priority ····· 61
10.2.8 poe threshold ····· 61
10.2.9 poe update ····· 62
10.2.10 show poe device ····· 62
10.2.11 show poe interface ····· 63
11 配置克隆 ····· 64
11.1 功能介绍 ····· 64
11.1.1 配置同步 ····· 64
1.1.2 版本同步 ····· 64

11.2 命令手册 ····· 64
11.2.1 config clone-agent ····· 64
11.2.2 mode ····· 65
11.2.3 start discover ····· 65
11.2.4 start config-clone ····· 66
11.2.5 start software-clone ····· 66
11.2.6 stop clone ····· 67
11.2.7 show clone device ····· 68
11.2.8 show clone status ····· 68
12 智能诊断 ····· 69
12.1 功能介绍 ····· 69
12.2 命令手册 ····· 69
12.2.1 config hig ····· 69
12.2.2 show hig history-alm ····· 70
12.2.3 show hig current-alm ····· 70
12.2.4 show hig current-alm-num ····· 71
12.2.5 show hig policy-alm ····· 71
12.2.6 clear hig alm ····· 71
12.2.7 restory hig alm ····· 72
13 网络诊断 ····· 72
13.1 功能介绍 ····· 72
13.2 命令手册 ····· 73
13.2.1 monitor packet ····· 73
13.2.2 ping ····· 73
13.2.3 ping ipv6 ····· 74
13.2.4 traceroute ····· 74
13.2.5 traceroute ipv6 ····· 75
13.3 配置举例 ····· 75
13.4 常见问题 ····· 76
14 端口镜像 ····· 77
14.1 功能介绍 ····· 77
14.1.1 特性简介 ····· 77
14.2 命令手册 ····· 77
14.2.1 config mirroring group ····· 77
14.2.2 destination-interface ····· 78
14.2.3 remote-vlan ····· 79
14.2.4 reset mirroring configuration ····· 79
14.2.5 show mirroring group ····· 79
14.2.6 source-interface ····· 80
14.3 配置举例 ····· 81
14.4 常见问题 ····· 81

15 SNMP ..... 82
15.1 功能介绍 ..... 82
15.1.1 特性简介 ..... 82
15.2 命令手册 ..... 82
15.2.1 community ..... 82
15.2.2 config snmp ..... 83
15.2.3 contact ..... 83
15.2.4 location ..... 84
15.2.5 system-configuration ..... 84
15.2.6 trap enable ..... 85
15.2.7 trap2sink ..... 85
15.2.8 view ..... 86
15.3 配置举例 ..... 86
15.4 常见问题 ..... 87
16 SNMPv3 ..... 88
16.1 功能介绍 ..... 88
16.2 命令手册 ..... 88
16.2.1 group v3 ..... 88
16.2.2 local-user ..... 89
16.2.3 trapsess ..... 89
16.3 配置举例 ..... 90
16.4 常见问题 ..... 90
17 RMON ..... 91
17.1 功能介绍 ..... 91
17.1.1 特性简介 ..... 91
17.2 命令手册 ..... 91
17.2.1 alarm ..... 91
17.2.2 config rmon ..... 92
17.2.3 event ..... 92
17.2.4 ifmonitor ..... 93
17.2.5 port ifmonitor ..... 94
17.2.6 rmon history ..... 94
17.2.7 rmon statistic ..... 95
17.2.8 show rmon alarm ..... 95
17.2.9 show rmon event ..... 96
17.2.10 show rmon history ..... 96
17.2.11 show rmon statistic ..... 98
17.3 配置举例 ..... 98
17.3.1 统计组配置举例 ..... 98
17.3.2 历史组配置举例 ..... 99
17.3.3 事件组配置举例 ..... 100
17.3.4 告警组配置举例 ..... 100

17.4 常见问题 ····· 100
18 WEB ····· 101
18.1 功能介绍 ····· 101
18.2 命令手册 ····· 101
18.2.1 config web server ····· 101
18.2.2 http-port ····· 101
18.2.3 session timeout ····· 102
18.2.4 show web server ····· 102
19 以太网接口管理 ····· 104
19.1 功能介绍 ····· 104
19.2 命令手册 ····· 104
19.2.1 combo ····· 104
19.2.2 default ····· 104
19.2.3 description ····· 105
19.2.4 duplex ····· 105
19.2.5 eee ····· 106
19.2.6 flow-control ····· 106
19.2.7 interface ····· 107
19.2.8 interface range ····· 107
19.2.9 link-delay ····· 108
19.2.10 loopback ····· 109
19.2.11 reset counters ····· 109
19.2.12 show counters ····· 110
19.2.13 show interface ····· 111
19.2.14 show storm-suppression ····· 112
19.2.15 shutdown ····· 112
19.2.16 speed ····· 113
19.2.17 storm-suppression ····· 114
19.2.18 virtual-cable-test ····· 114
19.3 配置举例 ····· 115
19.4 常见问题 ····· 115
20 MAC ····· 116
20.1 特性简介 ····· 116
20.2 命令手册 ····· 116
20.2.1 blackhole mac-address ····· 116
20.2.2 config mac ····· 116
20.2.3 mac-address security ····· 117
20.2.4 mac-address static ····· 118
20.2.5 mac-learning disable ····· 118
20.2.6 show mac-address ····· 119
20.2.7 timer aging ····· 119
20.2.8 reset mac-address ····· 120

20.3 配置举例 ····· 121
20.4 常见问题 ····· 121
21 VLAN 基础 ····· 122
21.1 特性简介 ····· 122
21.1.1 背景 ····· 122
21.1.2 原理 ····· 122
21.1.3 协议规范 ····· 123
21.2 命令手册 ····· 123
21.2.1 config vlan ····· 123
21.2.2 description ····· 124
21.2.3 name ····· 124
21.2.4 show vlan ····· 125
21.2.5 vlan ····· 126
21.2.6 vlan access ····· 126
21.2.7 vlan hybrid ····· 127
21.2.8 vlan hybrid pvid ····· 127
21.2.9 vlan trunk permit ····· 128
21.2.10 vlan trunk pvid ····· 129
21.2.11 vlan-mode ····· 129
21.3 配置举例 ····· 130
21.4 常见问题 ····· 130
22 动态 VLAN ····· 131
22.1 特性简介 ····· 131
22.2 命令手册 ····· 131
22.2.1 config ip-subnet-vlan ····· 131
22.2.2 config mac-vlan ····· 132
22.2.3 config protocol-vlan ····· 132
22.2.4 ip-subnet-vlan ····· 133
22.2.5 ip-subnet-vlan enable ····· 133
22.2.6 mac-vlan ····· 134
22.2.7 mac-vlan enable ····· 135
22.2.8 protocol-vlan ····· 135
22.2.9 protocol-vlan enable ····· 136
22.2.10 show mac-vlan all ····· 137
23 VLAN Mapping ····· 138
23.1 特性简介 ····· 138
23.2 命令手册 ····· 138
23.2.1 vlan mapping ····· 138
23.2.2 vlan translation ····· 138
23.2.3 show vlan mapping ····· 139
23.3 配置举例 ····· 139
23.4 常见问题 ····· 140

24 Private VLAN ..... 141
24.1 特性简介 ..... 141
24.2 命令手册 ..... 141
24.2.1 config private-vlan ..... 141
24.2.2 principal-vlan ..... 141
24.2.3 secondary-vlan ..... 142
24.3 配置举例 ..... 142
24.4 常见问题 ..... 143
25 QinQ ..... 144
25.1 QinQ 功能 ..... 144
25.1.1 基本 QinQ 功能简介 ..... 144
25.1.2 工作原理 ..... 144
25.2 基于 VLAN 的灵活 QinQ ..... 144
25.3 命令手册 ..... 145
25.3.1 config qinq customer-tpid ..... 145
25.3.2 qinq enable ..... 145
25.3.3 qinq service-tpid ..... 146
25.3.4 qinq service-vlan-id ..... 146
25.3.5 qinq transparent ..... 147
26 Voice VLAN ..... 147
26.1 特性简介 ..... 147
26.2 命令手册 ..... 147
26.2.1 config voice-vlan ..... 147
26.2.2 voice-vlan security enable ..... 148
26.2.3 voice-vlan mac-address ..... 148
26.2.4 voice-vlan enable ..... 149
26.2.5 voice-vlan qos ..... 149
26.2.6 show voice-vlan ..... 150
27 LLDP ..... 151
27.1 功能介绍 ..... 151
27.1.1 特性简介 ..... 151
27.2 命令手册 ..... 151
27.2.1 config lldp ..... 151
27.2.2 interface enable ..... 152
27.2.3 lldp tx-interval ..... 152
27.2.4 lldp tx-hold ..... 153
27.2.5 show lldp ..... 153
27.2.6 reset lldp ..... 157
27.3 配置举例 ..... 157
27.4 常见问题 ..... 159
28 MVRP & GVRP ..... 160
28.1 特性简介 ..... 160

28.2 命令手册 ····· 160
28.2.1 config mvrp ····· 160
28.2.2 mvrp global enable ····· 160
28.2.3 mvrp gvrp-compliance enable ····· 161
28.2.4 mvrp timer leaveall ····· 162
28.2.5 mvrp timer leave ····· 162
28.2.6 mvrp timer join ····· 163
28.2.7 mvrp timer hold ····· 163
28.2.8 mvrp mode ····· 164
28.2.9 mvrp enable ····· 165
28.2.10 show mvrp info ····· 165
28.3 配置举例 ····· 166
28.4 常见问题 ····· 167
29 三层接口管理 ····· 168
29.1 功能介绍 ····· 168
29.2 命令手册 ····· 168
29.2.1 config interface loopback ····· 168
29.2.2 config interface vlan ····· 168
29.2.3 ipv4-address ····· 169
29.2.4 ipv6-address ····· 169
29.2.5 description ····· 170
29.2.6 duplex ····· 171
29.2.7 shutdown ····· 171
29.2.8 speed ····· 172
29.2.9 mtu ····· 172
29.2.10 show interface ····· 173
30 ARP ····· 175
30.1 功能简介 ····· 175
30.2 命令手册 ····· 175
30.2.1 config arp ····· 175
30.2.2 arp timer aging ····· 175
30.2.3 arp static ····· 176
30.2.4 arp-proxy enable ····· 176
30.2.5 reset arp ····· 177
30.2.6 rate-limit ····· 178
30.2.7 rate-limit log enable ····· 178
30.2.8 arp send-gratitous-arp ····· 179
30.2.9 show arp detection ····· 179
30.2.10 show arp ····· 180
30.3 配置举例 ····· 180
30.4 常见问题 ····· 180

31 IPv6 协议栈 ..... 181
31.1 功能简介 ..... 181
31.2 命令手册 ..... 181
31.2.1 config ipv6-neighbor ..... 181
31.2.2 timer aging ..... 181
31.2.3 show ipv6 neighbor ..... 182
31.2.4 reset ipv6 neighbor ..... 182
31.2.5 ipv6 nd ra interval ..... 183
31.2.6 ipv6 nd ra prefix ..... 183
31.2.7 ipv6 nd ra reachable-time ..... 184
31.2.8 ipv6 nd ra router-lifetime ..... 185
31.2.9 ipv6 nd router-preference ..... 185
31.2.10 ipv6 nd autoconfig managed-address-flag ..... 186
31.2.11 ipv6 nd autoconfig other-flag ..... 186
31.2.12 ipv6 nd ra accept ..... 187
31.2.13 ipv6 nd ra halt ..... 187
31.3 配置举例 ..... 188
31.4 常见问题 ..... 188
32 RARP ..... 189
32.1 功能简介 ..... 189
32.2 命令手册 ..... 189
32.2.1 config rarp ..... 189
32.2.2 mac ..... 189
32.3 配置举例 ..... 190
32.4 常见问题 ..... 190
33 DNS ..... 191
33.1 功能简介 ..... 191
33.2 命令手册 ..... 191
33.2.1 config dns server ..... 191
33.2.2 domain ..... 191
33.2.3 server ..... 192
33.2.4 show dns server domain ..... 192
33.2.5 config dns-ipv6 server ..... 193
33.2.6 domain ..... 194
33.2.7 server ..... 194
33.3 配置举例 ..... 195
33.4 常见问题 ..... 195
34 DHCP Server ..... 196
34.1 功能简介 ..... 196
34.2 命令手册 ..... 196
34.2.1 config dhcp-server ..... 196
34.2.2 address-range ..... 196

34.2.3 static-bind ····· 197
34.2.4 option ····· 198
34.2.5 sip-server ····· 198
34.2.6 dns-server ····· 199
34.2.7 dhcp server enable ····· 199
34.2.8 reset dhcp server ip-in-use all ····· 200
34.2.9 show dhcp server ip-in-use ····· 200
34.3 配置举例 ····· 201
34.4 常见问题 ····· 202
35 IPv6 DHCP Server ····· 203
35.1 功能简介 ····· 203
35.2 命令手册 ····· 203
35.2.1 config dhcpv6-server ····· 203
35.2.2 address-range ····· 203
35.2.3 option ····· 204
35.2.4 sip-server ····· 205
35.2.5 static-bind ····· 205
35.2.6 dhcpv6 server enable ····· 206
35.2.7 reset dhcpv6 server ip-in-use all ····· 206
35.2.8 show dhcpv6 server ip-in-use ····· 207
35.2.9 show dhcpv6 duid ····· 207
35.3 配置举例 ····· 208
35.4 常见问题 ····· 208
36 DHCP Relay ····· 209
36.1 功能简介 ····· 209
36.2 命令手册 ····· 209
36.2.1 dhcp relay enable server-ip ····· 209
36.3 配置举例 ····· 209
36.4 常见问题 ····· 209
37 IPv6 DHCP Relay ····· 210
37.1 功能简介 ····· 210
37.2 命令手册 ····· 210
37.2.1 dhcpv6 relay enable ····· 210
37.3 配置举例 ····· 210
37.4 常见问题 ····· 210
38 DHCP Snooping ····· 211
38.1 功能简介 ····· 211
38.1.1 DHCP SNOOPING ····· 211
38.1.2 DHCP SNOOPING 支持 option82 ····· 211
38.2 命令手册 ····· 211
38.2.1 config dhcp snooping ····· 211
38.2.2 dhcp snooping trust ····· 212

38.2.3 max-user-number ····· 212
38.2.4 dhcp snooping max-user-number ····· 213
38.2.5 show dhcp snooping table ····· 213
38.2.6 reset dhcp snooping table ····· 214
38.2.7 dhcp snooping option82 enable ····· 215
38.2.8 dhcp snooping option82 strategy ····· 215
38.2.9 dhcp snooping option82 circuit-id ····· 216
38.2.10 dhcp snooping option82 remote-id ····· 217
38.3 配置举例 ····· 218
38.4 常见问题 ····· 218
39 IPv6 DHCP Snooping ····· 219
39.1 功能简介 ····· 219
39.1.1 dhcpv6 snooping ····· 219
39.1.2 dhcpv6 snooping option ····· 219
39.2 命令手册 ····· 219
39.2.1 config dhcpv6 snooping ····· 219
39.2.2 dhcpv6 snooping trust ····· 220
39.2.3 dhcpv6 snooping max-user-number ····· 220
39.2.4 show dhcpv6 snooping table ····· 221
39.2.5 reset dhcp snooping table ····· 222
39.2.6 dhcpv6 snooping option interface-id ····· 222
39.2.7 dhcpv6 snooping option remote-id ····· 222
39.3 配置举例 ····· 223
39.4 常见问题 ····· 224
40 路由基础 ····· 225
40.1 功能简介 ····· 225
40.2 命令手册 ····· 225
40.2.1 show ip routing-table ····· 225
40.2.2 show ip fib ····· 227
40.2.3 show ipv6 routing-table ····· 228
40.2.4 show ipv6 fib ····· 229
40.2.5 config ip urpf ····· 230
40.2.6 config ipv6 urpf ····· 231
40.2.7 config dlf ····· 231
40.2.8 dlf drop ····· 232
40.3 配置举例 ····· 232
40.4 常见问题 ····· 232
41 静态路由 ····· 233
41.1 功能简介 ····· 233
41.2 命令手册 ····· 233
41.2.1 config ip route-static ····· 233
41.2.2 route ip ····· 233

41.2.3 config ipv6 route-static ····· 234
41.2.4 route ipv6 ····· 235
41.2.5 config ip mroute-static ····· 235
41.2.6 rpf-route-static ····· 236
41.3 配置举例 ····· 236
41.4 常见问题 ····· 237
42 策略路由 ····· 238
42.1 功能介绍 ····· 238
42.2 命令手册 ····· 238
42.2.1 config policy-based-route ····· 238
42.2.2 config ipv6 policy-based-route ····· 238
42.2.3 policy-based-route ····· 239
42.2.4 ipv6 policy-based-route ····· 239
42.2.5 match dst-ip ip ····· 240
42.2.6 match dst-ip ipv6 ····· 240
42.2.7 match dst-port ····· 241
42.2.8 match ip-protocol ····· 241
42.2.9 match src-ip ····· 242
42.2.10 match src-ip ipv6 ····· 243
42.2.11 match src-port ····· 243
42.2.12 set nexthop ····· 244
42.2.13 set nexthop ipv6 ····· 244
42.2.14 show fib policy-based-route nexthop ····· 245
42.2.15 show ipv6 fib policy-based-route nexthop ····· 245
42.2.16 show policy-based-route ····· 246
42.2.17 show ipv6 policy-based-route ····· 247
42.3 配置举例 ····· 248
42.4 常见问题 ····· 248
42.4.1 配置下一跳 show fib policy-based-route nexthop 命令没有显示 ····· 248
43 路由策略 ····· 错误!未定义书签。
43.1 功能简介 ····· 错误!未定义书签。
43.2 命令手册 ····· 错误!未定义书签。
43.2.1 config ip prefix-list ····· 错误!未定义书签。
43.2.2 seq permit or deny ip ····· 错误!未定义书签。
43.2.3 config ipv6 prefix-list ····· 错误!未定义书签。
43.2.4 seq permit or deny ipv6 ····· 错误!未定义书签。
43.2.5 route-map ····· 错误!未定义书签。
43.2.6 route-map-global ····· 错误!未定义书签。
43.2.7 community-list ····· 错误!未定义书签。
43.2.8 as-path-prefix-list ····· 错误!未定义书签。
43.2.9 match interface ····· 错误!未定义书签。
43.2.10 match ip-address ····· 错误!未定义书签。

43.2.11 match ipv6-address ·错误!未定义书签。
43.2.12 match ip-nexthop ·错误!未定义书签。
43.2.13 match as-path ·错误!未定义书签。
43.2.14 match community ·错误!未定义书签。
43.2.15 match extcommunity ·错误!未定义书签。
43.2.16 match local-preference ·错误!未定义书签。
43.2.17 continue ·错误!未定义书签。
43.2.18 set metric ·错误!未定义书签。
43.2.19 set metric-type ·错误!未定义书签。
43.2.20 set tag ·错误!未定义书签。
43.2.21 set community ·错误!未定义书签。
43.2.22 set extcommunity rt ·错误!未定义书签。
43.2.23 set extcommunity soo ·错误!未定义书签。
43.2.24 set extcommunity bandwidth ·错误!未定义书签。
43.2.25 set comm-list ·错误!未定义书签。
43.2.26 set as-path prepend ·错误!未定义书签。
43.2.27 set origin ·错误!未定义书签。
43.2.28 set weight ·错误!未定义书签。
43.2.29 set local-preference ·错误!未定义书签。
43.2.30 set distance ·错误!未定义书签。
43.2.31 show route-map ·错误!未定义书签。
43.2.32 show ip prefix-list ·错误!未定义书签。
43.2.33 show ipv6 prefix-list ·错误!未定义书签。
43.3 配置举例 ·错误!未定义书签。
43.4 常见问题 ·错误!未定义书签。
44 IGMP Snooping · 249
44.1 功能介绍 · 249
44.2 命令手册 · 249
44.2.1 config igmp-snooping · 249
44.2.2 querier enable · 249
44.2.3 robust-count · 250
44.2.4 lastmember-query-interval · 251
44.2.5 query-interval · 251
44.2.6 max-response-time · 252
44.2.7 igmp-snooping enable · 252
44.2.8 igmp-snooping bypass mrouter · 253
44.2.9 igmp-snooping drop-unknown · 253
44.2.10 igmp-snooping query source-ip · 254
44.2.11 igmp-snooping fast-leave · 254
44.2.12 igmp-snooping group deny · 255
44.2.13 igmp-snooping static-group · 256
44.2.14 igmp-snooping static-router-port · 256

44.2.15 reset igmp-snooping router-port ..... 257
44.2.16 reset igmp-snooping group ..... 257
44.2.17 show igmp-snooping ..... 258
44.2.18 show igmp-snooping group ..... 258
44.2.19 show igmp-snooping router-port ..... 259
45 MLD Snooping ..... 260
45.1 功能介绍 ..... 260
45.2 命令手册 ..... 260
45.2.1 config mld-snooping ..... 260
45.2.2 querier enable ..... 260
45.2.3 robust-count ..... 261
45.2.4 lastmember-query-interval ..... 262
45.2.5 query-interval ..... 262
45.2.6 max-response-time ..... 263
45.2.7 mld-snooping enable ..... 263
45.2.8 mld-snooping bypass mrouter ..... 264
45.2.9 mld-snooping drop-unknown ..... 264
45.2.10 mld-snooping query source-ip ..... 265
45.2.11 mld-snooping fast-leave ..... 265
45.2.12 mld-snooping group deny ..... 266
45.2.13 mld-snooping static-group ..... 267
45.2.14 mld-snooping static-router-port ..... 267
45.2.15 reset mld-snooping router-port ..... 268
45.2.16 reset mld-snooping group ..... 268
45.2.17 show mld-snooping ..... 269
45.2.18 show mld-snooping group ..... 269
45.2.19 show mld-snooping router-port ..... 270
46 组播 VLAN ..... 271
46.1 功能简介 ..... 271
46.2 命令手册 ..... 271
46.2.1 config multicast-vlan ..... 271
46.2.2 port multicast-vlan ..... 271
46.2.3 show multicast-vlan ..... 272
47 IGMP ..... 273
47.1 功能简介 ..... 273
47.2 命令手册 ..... 273
47.2.1 config igmp ..... 273
47.2.2 group-limit ..... 273
47.2.3 igmp enable ..... 274
47.2.4 igmp version ..... 274
47.2.5 igmp static ..... 275
47.2.6 igmp query-interval ..... 276

47.2.7 igmp query-max-response-time ..... 276
47.2.8 igmp last-member-query-interval ..... 277
47.2.9 igmp robust-count ..... 277
47.2.10 reset igmp control-messages-counter ..... 278
47.2.11 reset igmp groups ..... 278
47.2.12 show igmp interface ..... 278
47.2.13 show igmp group ..... 280
47.2.14 show igmp static-group ..... 280
47.2.15 show igmp statistics ..... 281
47.3 配置举例 ..... 281
47.4 常见问题 ..... 281
48 MLD ..... 282
48.1 功能简介 ..... 282
48.2 命令手册 ..... 282
48.3 配置举例 ..... 282
48.4 常见问题 ..... 282
49 登录管理 ..... 283
49.1 功能介绍 ..... 283
49.2 命令手册 ..... 283
49.2.1 config console ..... 283
49.2.2 authentication enable ..... 283
49.2.3 config ssh server ..... 284
49.2.4 ssh port ..... 284
49.2.5 re-generate key ..... 285
49.2.6 config telnet server ..... 285
49.2.7 telnet port ..... 286
49.2.8 idle-timeout ..... 286
49.2.9 ssh client ..... 287
49.2.10 telnet client ..... 287
49.2.11 show users ..... 288
49.2.12 free user ..... 289
49.2.13 show ssh2 algorithm ..... 289
49.2.14 show ssl algorithm ..... 290
49.3 配置举例 ..... 291
49.4 常见问题 ..... 291
50 本地用户 ..... 292
50.1 功能简介 ..... 292
50.2 命令手册 ..... 292
50.2.1 config local-user ..... 292
50.2.2 password ..... 292
50.2.3 user-level ..... 293
50.2.4 password-compare ..... 294

50.2.5 config password-control ····· 294
50.2.6 policy-enable ····· 294
50.2.7 sudo ····· 295
50.2.8 sudo password ····· 295
50.2.9 no sudo password ····· 296
50.3 配置举例 ····· 296
50.4 常见问题 ····· 297
51 ISP 域管理 ····· 298
51.1 功能简介 ····· 298
51.2 命令手册 ····· 298
51.2.1 config domain ····· 298
51.2.2 config default domain ····· 298
51.2.3 authentication default radius-scheme ····· 299
51.2.4 authentication default tacacs-scheme ····· 299
51.2.5 authentication default local ····· 300
51.3 配置举例 ····· 300
51.4 常见问题 ····· 300
52 radius ····· 301
52.1 功能简介 ····· 301
52.2 命令手册 ····· 301
52.2.1 config radius scheme ····· 301
52.2.2 primary authentication ····· 301
52.2.3 secondary authentication ····· 302
52.2.4 shared-secret ····· 302
52.2.5 user-name-format with-domain ····· 303
52.2.6 nas-ip ····· 304
52.3 配置举例 ····· 304
52.4 常见问题 ····· 304
53 tacacs ····· 305
53.1 TACACS+简介 ····· 305
53.2 命令手册 ····· 305
53.2.1 config tacacs scheme ····· 305
53.2.2 tacacs primary authentication ····· 305
53.2.3 tacacs secondary authentication ····· 306
53.2.4 tacacs shared-secret ····· 307
53.2.5 tacacs user-name-format with-domain ····· 307
53.3 配置举例 ····· 308
53.4 常见问题 ····· 308
54 802.1x ····· 309
54.1 802.1x 简介 ····· 309
54.1.1 802.1x 的体系结构 ····· 309
54.1.2 802.1x 的工作机制 ····· 310

54.1.3 EAPOL 消息的封装 ····· 310
54.1.4 802.1x 的认证过程 ····· 312
54.1.5 802.1x 支持 guest vlan ····· 315
54.1.6 NOS 802.1X ····· 315
54.2 命令手册 ····· 315
54.2.1 config dot1x enable ····· 315
54.2.2 dot1x enable ····· 315
54.2.3 dot1x mandatory-domain ····· 316
54.2.4 dot1x guest-vlan ····· 316
54.2.5 dot1x re-authenticate ····· 317
54.2.6 reset dot1x session ····· 317
54.2.7 show dot1x connection ····· 318
54.2.8 show dot1x interface ····· 319
54.2.9 show dot1x radius-scheme ····· 319
54.3 配置举例 ····· 319
54.4 常见问题 ····· 320
55 MAC 认证 ····· 321
55.1 功能简介 ····· 321
55.1.1 MAC 地址认证用户的账号格式 ····· 321
55.1.2 MAC 认证支持 Guest vlan ····· 321
55.2 命令手册 ····· 321
55.2.1 config mac-authentication ····· 321
55.2.2 domain ····· 322
55.2.3 fixed account ····· 322
55.2.4 mac-account ····· 323
55.2.5 timer quiet ····· 323
55.2.6 timer re-authentication ····· 324
55.2.7 offline-detect enable ····· 324
55.2.8 mac-authentication guest-vlan re-authentication enable ····· 325
55.2.9 mac-authentication enable ····· 325
55.2.10 mac-authentication domain ····· 326
55.2.11 mac-authentication guest-vlan ····· 326
55.2.12 reset mac-authentication connection ····· 327
55.2.13 show mac-authentication user ····· 327
55.3 配置举例 ····· 328
55.4 常见问题 ····· 328
56 审计日志 ····· 329
56.1 功能简介 ····· 329
56.2 命令手册 ····· 329
56.2.1 config audit log ····· 329
56.2.2 audithost host ····· 329
56.2.3 log file-size ····· 330

56.2.4 log over-action ····· 330
56.2.5 show audit log ····· 331
56.3 配置举例 ····· 331
56.4 常见问题 ····· 331
57 Portal 认证 ····· 332
57.1 功能简介 ····· 332
57.2 命令手册 ····· 332
57.2.1 config portal ····· 332
57.2.2 server ····· 332
57.2.3 web-server ····· 333
57.2.4 url ····· 334
57.2.5 url-parameter ····· 334
57.2.6 portal enable ····· 335
57.2.7 portal domain ····· 335
57.2.8 portal web-server ····· 336
57.2.9 portal mac-authentication enable ····· 336
57.2.10 free-rule ····· 337
57.2.11 max-user ····· 338
57.2.12 reset portal user ····· 338
57.2.13 show portal interface ····· 339
57.2.14 show portal user ····· 339
57.3 配置举例 ····· 340
57.4 常见问题 ····· 342
58 端口安全 ····· 342
58.1 功能简介 ····· 342
58.1.1 端口隔离 ····· 342
58.2 命令手册 ····· 342
58.2.1 port-isolate enable group ····· 342
58.2.2 show port-isolate ····· 343
58.3 配置举例 ····· 344
58.4 常见问题 ····· 344
59 IP Source Guard ····· 345
59.1 功能简介 ····· 345
59.2 命令手册 ····· 345
59.2.1 config ip-source-guard ····· 345
59.2.2 ip-source-guard static ····· 346
59.2.3 ip-source-guard static macv6 ····· 346
59.2.4 ip-source-guard enable ····· 347
59.2.5 show ip-source-guard ····· 348
59.3 配置举例 ····· 348
59.4 常见问题 ····· 349

60 ARP 防攻击 ····· 350
60.1 功能简介 ····· 350
60.1.1 ARP 探测 ····· 350
60.1.2 ARP 源抑制 ····· 350
60.1.3 ARP 限速 ····· 350
60.2 命令手册 ····· 350
60.2.1 config arp-detection ····· 350
60.2.2 arp detection enable ····· 351
60.2.3 arp detection trust ····· 351
60.2.4 validate ····· 352
60.2.5 config arp-source-suppression ····· 352
60.2.6 source-suppression limit ····· 353
60.2.7 rate-limit ····· 353
60.2.8 rate-limit log enable ····· 354
60.3 配置举例 ····· 354
60.4 常见问题 ····· 355
61 DDoS ····· 356
61.1 功能简介 ····· 356
61.2 命令手册 ····· 356
61.2.1 config ddos ····· 356
61.2.2 defense enable ····· 357
61.2.3 defense protocol ····· 357
61.2.4 defense sample ····· 358
61.2.5 defense threshold ····· 358
61.2.6 defense trace-type ····· 359
61.2.7 show ddos config ····· 360
61.2.8 show ddos statistic ····· 360
61.3 配置举例 ····· 361
61.4 常见问题 ····· 362
62 白名单 ····· 363
62.1 功能简介 ····· 363
62.2 命令手册 ····· 363
62.2.1 apply acl ····· 363
62.2.2 apply acl ipv6 ····· 364
62.3 配置举例 ····· 364
62.4 常见问题 ····· 365
63 带内管理 ····· 366
63.1 功能简介 ····· 366
63.2 命令手册 ····· 366
63.2.1 in-band management disable ····· 366
63.3 配置举例 ····· 366
63.4 常见问题 ····· 367

64 CPU 防攻击 ..... 368
64.1 功能简介 ..... 368
64.2 命令手册 ..... 368
64.2.1 config control-plane ..... 368
64.2.2 qos policy inbound ..... 368
64.2.3 show qos policy control-plane ..... 369
64.3 配置举例 ..... 369
64.4 常见问题 ..... 369
65 ACL ..... 370
65.1 功能简介 ..... 370
65.1.1 特性简介 ..... 370
65.1.2 ACL 的编号与分类 ..... 370
65.1.3 ACL 中规则的编号与步长 ..... 370
65.1.4 ACL 的匹配顺序 ..... 371
65.1.5 ACL 规则中的掩码 ..... 371
65.2 命令手册 ..... 371
65.2.1 config acl basic-ipv4 ..... 371
65.2.2 config acl basic-ipv6 ..... 372
65.2.3 config acl advanced-ipv4 ..... 372
65.2.4 config acl advanced-ipv6 ..... 373
65.2.5 config acl mac ..... 373
65.2.6 config acl user-defined ..... 374
65.2.7 rule basic ipv4 ..... 375
65.2.8 rule basic ipv6 ..... 375
65.2.9 rule advanced ipv4 ..... 376
65.2.10 rule advanced ipv6 ..... 377
65.2.11 rule advanced ipv4 tcp ..... 378
65.2.12 rule advanced ipv6 tcp ..... 379
65.2.13 rule advanced ipv4 udp ..... 380
65.2.14 rule advanced ipv6 udp ..... 380
65.2.15 rule mac ..... 381
65.2.16 rule user-defined ..... 382
65.2.17 rule step ..... 383
65.2.18 copy acl ..... 384
65.2.19 config acl global ..... 384
65.2.20 acl apply ..... 385
65.2.21 acl show basic ipv4 ..... 385
65.2.22 acl show basic ipv6 ..... 386
65.2.23 acl show advanced ipv4 ..... 386
65.2.24 acl show advanced ipv6 ..... 387
65.2.25 show acl mac ..... 387
65.2.26 show acl user-defined ..... 388

65.2.27 show acl counters ..... 388
65.3 配置举例 ..... 389
65.4 常见问题 ..... 389
66 QoS 策略 ..... 390
66.1 功能简介 ..... 390
66.1.1 QoS 简介 ..... 390
66.1.2 QoS 策略简介 ..... 390
66.2 命令手册 ..... 390
66.2.1 config qos policy ..... 390
66.2.2 class name ..... 391
66.2.3 match acl (class mode or view) ..... 391
66.2.4 match acl (class mode and view) ..... 392
66.2.5 match mac (class mode and view) ..... 393
66.2.6 Action-set name ..... 394
66.2.7 action permit ..... 394
66.2.8 action deny ..... 395
66.2.9 action mirror ..... 395
66.2.10 action redirect ..... 396
66.2.11 action remark ..... 396
66.2.12 action car ..... 397
66.2.13 **action rate-limit** ..... 398
66.2.14 **action set-queue** ..... 398
66.2.15 policy name ..... 399
66.2.16 sequence ..... 399
66.2.17 config qos global-policy ..... 400
66.2.18 qos policy name ..... 400
66.2.19 qos policy acl ..... 401
66.2.20 show qos policy counters ..... 402
66.2.21 show qos policy car ..... 403
66.3 配置举例 ..... 404
66.4 常见问题 ..... 405
67 优先级映射 ..... 406
67.1 功能简介 ..... 406
67.1.1 优先级映射简介 ..... 406
67.1.2 优先级信任模式 ..... 406
67.2 命令手册 ..... 406
67.2.1 config qos map cos ..... 406
67.2.2 cos lp ..... 407
67.2.3 config qos map dscp ..... 407
67.2.4 dscp lp ..... 408
67.2.5 qos port-priority ..... 409
67.2.6 qos trust (interface view) ..... 409

67.2.7 qos trust dscp(vlan view) ····· 410
67.2.8 show qos map ····· 410
67.3 配置举例 ····· 411
67.4 常见问题 ····· 411
68 队列调度 ····· 412
68.1 功能简介 ····· 412
68.1.1 队列技术简介 ····· 412
68.1.2 队列调度 ····· 412
68.2 命令手册 ····· 412
68.2.1 qos schedule ····· 412
68.2.2 qos bandwidth ····· 413
68.3 配置举例 ····· 414
68.4 常见问题 ····· 414
69 限速与整形 ····· 415
69.1 功能简介 ····· 415
69.1.1 令牌桶技术 ····· 415
69.1.2 流量监管 ····· 416
69.1.3 流量整形 ····· 416
69.1.4 限速 ····· 416
69.2 命令手册 ····· 416
69.2.1 qos shape ····· 416
69.2.2 rate-limit ····· 417
69.2.3 show qos rate-limit ····· 417
69.3 配置举例 ····· 418
69.4 常见问题 ····· 418
70 拥塞避免 ····· 419
70.1 功能简介 ····· 419
70.2 命令手册 ····· 419
70.2.1 config qos wred ····· 419
70.2.2 queue wred ····· 420
70.2.3 qos wred ····· 420
70.3 配置举例 ····· 421
70.4 常见问题 ····· 422
71 链路聚合 ····· 423
71.1 功能介绍 ····· 423
71.1.1 什么是链路聚合 ····· 423
71.1.2 静态聚合 ····· 423
71.1.3 动态聚合 ····· 424
71.2 命令手册 ····· 424
71.2.1 config bridge-aggregation ····· 424
71.2.2 load-balance mode ····· 424
71.2.3 config interface bridge-aggregation ····· 425

71.2.4 member interface ····· 425
71.2.5 description ····· 426
71.2.6 mode ····· 427
71.2.7 lacp period short ····· 427
71.2.8 lacp enable ····· 428
71.2.9 show link-aggregation ····· 428
71.3 配置举例 ····· 429
71.3.1 静态聚合 ····· 429
71.3.2 动态聚合 ····· 430
71.4 常见问题 ····· 431
72 STP ····· 432
72.1 特性简介 ····· 432
72.1.1 MSTP 的功能 ····· 432
72.1.2 MSTP 原理描述 ····· 432
72.1.3 MSTP 对 STP 和 RSTP 的改进 ····· 432
72.1.4 MSTP 基本概念 ····· 432
72.2 命令手册 ····· 437
72.2.1 config stp ····· 437
72.2.2 global enable （STP 视图） ····· 438
72.2.3 timer max-age ····· 438
72.2.4 timer hello ····· 439
72.2.5 timer forward-delay ····· 440
72.2.6 max-hops ····· 440
72.2.7 instance priority ····· 441
72.2.8 mode ····· 441
72.2.9 tc-protection ····· 442
72.2.10 tc-protection threshold ····· 442
72.2.11 region-configuration ····· 443
72.2.12 region-name （STP 域视图） ····· 443
72.2.13 revision-level ····· 444
72.2.14 instance vlan ····· 444
72.2.15 stp instance priority（接口视图） ····· 445
72.2.16 stp external-cost ····· 446
72.2.17 stp internal-cost ····· 446
72.2.18 stp admin-edge ····· 447
72.2.19 stp role-restriction ····· 447
72.2.20 stp tcn-restriction ····· 448
72.2.21 stp mcheck ····· 448
72.2.22 stp bpdu-protection ····· 449
72.2.23 stp enable ····· 449
72.2.24 stp p2p-detect ····· 450
72.2.25 stp loop-protection ····· 450

72.2.26 stp root-protection ····· 451
72.2.27 show stp ····· 451
72.3 配置举例 ····· 455
72.4 常见问题 ····· 459
73 ERPS ····· 460
73.1 特性简介 ····· 460
73.1.1 功能介绍 ····· 460
73.1.2 基本概念 ····· 460
73.2 命令手册 ····· 462
73.2.1 config erps ····· 462
73.2.2 ring ····· 462
73.2.3 ring port ····· 463
73.2.4 ring-type ····· 463
73.2.5 instance ····· 464
73.2.6 instance enable ····· 465
73.2.7 control-vlan ····· 465
73.2.8 protected-vlan ····· 466
73.2.9 node-role ····· 466
73.2.10 switch ····· 467
73.2.11 revertive ····· 468
73.2.12 tc-notify ····· 468
73.2.13 timer guard ····· 469
73.2.14 timer wtr ····· 469
73.2.15 timer hold-off ····· 470
73.2.16 show erps ····· 470
73.3 配置举例 ····· 472
73.4 说明 ····· 474
74 环路检测 ····· 475
74.1 功能介绍 ····· 475
74.1.1 功能简介 ····· 475
74.1.2 原理描述 ····· 475
74.2 命令手册 ····· 475
74.2.1 config loopback-detect ····· 475
74.2.2 detect-interval ····· 476
74.2.3 shutdown-interval ····· 476
74.2.4 loopback-detect enable ····· 477
74.2.5 show loopback-detect ····· 477
74.3 配置举例 ····· 478
74.4 常见问题 ····· 479
75 SRPP ····· 错误!未定义书签。
75.1 特性简介 ····· 错误!未定义书签。
75.1.1 功能介绍 ····· 错误!未定义书签。

75.1.2 基本概念 ····· 错误!未定义书签。
75.2 命令手册 ····· 错误!未定义书签。
75.2.1 config srpp ····· 错误!未定义书签。
75.2.2 ring ····· 错误!未定义书签。
75.2.3 control-vlan ····· 错误!未定义书签。
75.2.4 protected-vlan ····· 错误!未定义书签。
75.2.5 block specified-portid ····· 错误!未定义书签。
75.2.6 preempt ····· 错误!未定义书签。
75.2.7 tc-notify ····· 错误!未定义书签。
75.2.8 ring ····· 错误!未定义书签。
75.2.9 show srpp ring ····· 错误!未定义书签。
75.2.10 show srpp interface ····· 错误!未定义书签。
75.3 配置举例 ····· 错误!未定义书签。
76 Smart link ····· 480
76.1 特性简介 ····· 480
76.2 相关概念 ····· 480
76.2.1 运行机制 ····· 480
76.2.2 控制 VLAN ····· 480
76.2.3 FLUSH 报文 ····· 480
76.2.4 Smart link 角色抢占模式 ····· 480
76.3 命令手册 ····· 480
76.3.1 config smart-link ····· 480
76.3.2 group ····· 481
76.3.3 protected-vlan ····· 481
76.3.4 control-vlan ····· 482
76.3.5 group port ····· 483
76.3.6 revertive ····· 483
76.3.7 timer wtr ····· 484
76.3.8 timer hold-off ····· 484
76.3.9 flush enable ····· 485
76.3.10 show smart-link ····· 485
77 Monitor Link ····· 487
77.1 功能介绍 ····· 487
77.1.1 功能简介 ····· 487
77.1.2 基本概念 ····· 487
77.2 命令手册 ····· 487
77.2.1 config monitor-link group ····· 487
77.2.2 <uplink|downlink> interface ····· 488
77.2.3 show monitor-link group ····· 488
78 BFD ····· 490
78.1 功能简介 ····· 490
78.2 命令手册 ····· 490

78.2.1 config bfd ····· 490
78.2.2 templete ····· 491
78.2.3 detect-multiplier ····· 491
78.2.4 receive-interval ····· 492
78.2.5 transmit-interval ····· 492
78.2.6 show bfd peers ····· 493
78.3 配置举例 ····· 494
78.4 常见问题 ····· 495
79 GLDP ····· 496
79.1 功能介绍 ····· 496
79.1.1 基本概念 ····· 496
79.2 命令手册 ····· 497
79.2.1 config gldp ····· 497
79.2.2 interval ····· 498
79.2.3 gldp enable ····· 498
79.2.4 show gldp ····· 499
79.3 配置举例 ····· 499
79.4 常见问题 ····· 500
80 CID 定制 ····· 501
80.1 功能介绍 ····· 501
80.2 命令手册 ····· 501
80.2.1 banner ····· 501
80.2.2 show banner ····· 502
80.3 配置举例 ····· 502
80.4 常见问题 ····· 502
81 第三方应用管理 ····· 503
81.1 功能介绍 ····· 503
81.1.1 功能简介 ····· 503
81.1.2 API 介绍 ····· 503
81.2 命令手册 ····· 504
81.2.1 config third-party-app ····· 504
81.2.2 daemon ····· 505
81.2.3 data-file ····· 505
81.2.4 exec-file ····· 506
81.3 配置举例 ····· 506
81.4 常见问题 ····· 507

# 1 配置准备

## 1.1 连接方式

目前本系统支持的连接方式有如下几种：

- **Console**：通过将 RJ45 Console 线连接到 Console 口进行管理的方式，默认波特率为 9600。
- **带外管理（管理网口）**：将以太网线连接到专用管理网口（部分设备可能没有管理网口）进行管理的方式。
- **带内管理（业务口）**：将以太网线连接到某个业务口进行管理的方式。

默认管理员账号和密码为 admin/admin，默认情况下通过 Console 连接不需要认证（其他方式都需要认证）。部分产品可能会定制修改上述这些默认信息，具体请以实际产品为准。

由于 Console 传输速率较慢、带内管理可能会受到业务流量冲击，因此推荐优先使用带外管理方式（如果设备有管理网口的话）。

## 1.2 管理方式

目前本系统支持的管理方式有如下几种：

- **Console**：通过 Console 口进行命令行管理。
- **SSH**：通过 SSHv2 方式登录后进行命令行管理，该方式默认开启，且安全性高，推荐优先使用。
- **Telnet**：通过 Telnet 方式登录后进行命令行管理。该方式的安全性低于 SSH 方式，默认是否开启取决于具体产品。
- **Web**:通过浏览器以 HTTP/HTTPS 方式登录后进行 GUI 管理(部分产品可能只支持 HTTPS 方式)。该方式的功能比命令行方式要少，只适合在简单应用场景下使用。
- **SNMP**：通过 SNMP 协议、借用 MIB 信息库对设备进行管理。该方式的功能较少，性能不高，一般不推荐使用。

除 Console 方式外，其他都是通过网络进行管理的方式，如果网络异常，则可能需要使用 Console 方式来恢复管理。

## 1.3 权限分级和安全保障

系统通过三种级别来限制用户操作权限：

- **系统管理员（manage）**：对应管理员级别，拥有所有权限。
- **网络管理员（network）**：具有大部分的网络功能配置和查看权限，但不能进行对系统安全有影响的操作（如账户管理、版本升级等）。
- **访客（guest）**：具有大部分的信息查看和网络诊断权限，但没有配置权限。

如果使用本地账户，则需要在配置本地账户时指定权限级别（具体见用户手册中“本地用户”章节的 user-level 命令），否则默认为 guest 级别。如果使用远程 radius/tacacs 服务器上的账户，则可以通过属性 29（radius）、priv-lvl（tacacs）携带权限级别（guest/network/manage 分别对应 1/2/3），默认为 manage 级别。

对于不同的管理方式，系统提供不同的安全加密机制：

- **Console**：必须是近距离物理连接，因此安全可靠，无加密机制。
- **SSH**：通过 SSH 自身加密机制确保传输安全，且可以按需更新密钥。
- Telnet：无加密。
- **Web**:默认情况下,只能通过 HTTPS 方式登录(HTTP 方式会被强制重定向到 HTTPS),使用 TLSv1.3 加密，使用自签名证书。

- **SNMP**：建议使用 SNMPv3，可以配置认证和加密，确保传输安全，具体请参考用户手册中的“SNMPv3”相关章节。

## 1.4 密码保护和忘记密码

系统中所有的密码信息，均以 AES-256 加密方式存储和显示（在部分安全性要求更高的产品上，密码信息会显示为 6 个*），在系统外不可逆，以确保密码安全。

默认情况下，如果忘记密码，可以通过 Console 登录后再修改密码（不支持找回密码）。但如果 Console 也配置了认证，则需要重启后在 boot 菜单选择“Default config”来临时使用空配置启动（仅本次生效），这样 Console 就会恢复为默认的免认证登录。某些安全性要求较高的产品，默认就开启了 console 的认证，这种情况下如果忘记密码，只能联系售后进行处理（可临时提供免认证版本，通过在 boot 下网络加载 OS 后，再修改并保存密码）。

## 1.5 异常恢复

一般情况下，不管是正常重启还是异常断电，系统都能正常恢复运行。但在低概率的极端情况下，可能会出现以下一些问题：

- **flash 出现坏块**：设备上的 flash 元器件有一定使用寿命限制，虽然软件系统已能尽量做到平衡擦写，但运行时间较长之后，可能会低概率出现坏块。如果是写入数据时生成了新的坏块，则系统会自动使用预留的备用块来替换，不影响运行（除非备用块耗尽）。而如果是其他时机出现坏块，则会导致部分文件数据丢失，可能引起系统运行异常。
- **关键文件损坏**：如果在文件操作过程中异常断电，有可能会损坏文件，从而引起系统运行异常。

如果出现上述异常，一般有如下恢复手段：

- **自动恢复**：如果损坏的是主用版本文件，则系统会自动以备用版本文件启动，然后可以手工更新主用版本文件来恢复。
- **手动恢复**：如果没有备用版本文件、或都启动失败，则可以在 boot 界面下通过网络加载版本启动，然后再更新 flash 上的版本文件。
- **恢复出厂设置**：如果上述方式还是无法正常运行（可能损坏了其他关键文件），则可以在网络加载启动后，执行“restore factory-default” 命令来恢复出厂设置，然后重新更新版本文件。

# 2 CLI 配置

## 2.1 功能介绍

### 2.1.1 特性简介

CLI（Command Line Interface，命令行接口）是用户与设备之间的文本类指令交互界面，类似于 Linux 下的 Shell，用于对设备进行配置和管理，并可以通过查看输出信息确认配置结果。

不同设备支持不同方式进入命令行接口界面，例如通过 Console 口、Telnet 或者 SSH 登录设备。

### 2.1.2 命令格式

所有的命令格式都按照下面的规则在手册中进行描述：

- 关键字用加粗小写单词表示，如“**ping** *DEST*”中的“**ping**”。
- 参数用普通斜体大写单词表示，如“**ping** *DEST*”中的“*DEST*”。
- 可选参数：使用中括号，如：**ping** DEST [**count** *(1-1000)*]
- 整数范围参数：使用小括号，如“**ping** DEST [**count** *(1-1000)*]”中的“*(1-1000)*”。
- 多选一（必选一）：使用尖括号，如：**ping** *DEST* **source** <*IFNAME*|*A.B.C.D*>
- 多选一（可以不选）：组合使用中括号，如：**ping** *DEST* [<**src-if** *IFNAME*|**src-addr** *A.B.C.D*>]
- 多选多（至少一）：使用大括号，如：**ping** *DEST* {**count** *(1-1000)*|**ttl** *TTL*}
- 多选多（可以不选）：组合使用中括号，如：**ping** *DEST* [{**count** *(1-1000)*|**ttl** *TTL*}]
- 可重复参数：使用三个点，如：**ping** *DEST-LIST...*

### 2.1.3 视图和命令分类

为了使命令行界面更简洁清晰，同时也可以降低配置出错可能性，各业务模块的命令行已尽量汇总到各自的配置视图下。另外，进入各模块配置视图的命令，往往同时也控制了该模块的运行与否。

登录设备时，首先进入的是根视图，再通过 config 类命令可以进入各模块的配置视图，通过 exit 命令可以退出到上一级视图，通过 end 命令可以从任意视图直接回到根视图。在根视图下顶格按 TAB 键时，（在配置没有删除的情况下）还可以快速回到上一次的视图。

一般来说，config、show、ping、exit、end 命令可以在任意视图执行，其他命令一般只在特定视图下才有。

根视图下的所有命令行可分为以下几个大类：

- [no] **config** 命令：配置/去配置类命令行，能显示和保存配置信息。
- **show** 命令：显示类命令，不涉及配置显示和保存，可使用别名“display”。
- **reset** 命令：清除类命令，一次性操作，涉及配置显示和保存。
- 其他命令：如 ping、find、ftp 等，属于工具类命令。

除此之外，**startup** 和 **bootfile** 等少量命令行比较特殊，属于独立的配置命令、会保存，但不会生成运行时配置（无法通过 show running-config 查看）。

### 2.1.4 易用性说明

相比 Linux 下的普通 Shell 界面，CLI 界面除了提供正常的文本输入和编辑功能外，还提供了很多便捷操作，例如：

- 当输入的字符足够匹配唯一的关键字时，可以不必输入完整的关键字即可执行。

- 按下问号（?），可以显示接下来的可选输入及帮助信息。
- 按下 TAB 键，可以补全匹配的命令输入，或者列出匹配的可选输入列表。
- 根视图下顶格按下 TAB 键，则会快速进入上次使用 end（或 CTRL_Z）退出的视图。
- 按下向上/向下键，可以填入上一条/下一条命令行。
- 显示类命令可以通过“pipe”管道实现过滤或重定向到文件的功能。
- 其他常用快捷键如下：

```
NOS# show hotkey
 CTRL_A  Move the cursor to the beginning of the line.
 CTRL_B  Move the cursor one character to the left.
 CTRL_C  Stop the current command.
 CTRL_D  Erase the character at the cursor.
 CTRL_E  Move the cursor to the end of the line.
 CTRL_F  Move the cursor one character to the right.
 CTRL_H  Erase the character to the left of the cursor.
 CTRL_L  Clean the screen.
 CTRL_N  Display the next command in the history buffer.
 CTRL_P  Display the previous command in the history buffer.
 CTRL_R  Search backwards through the history.
 CTRL_S  Search forwards through the history.
 CTRL_W  Delete the word to the left of the cursor.
 CTRL_X  Delete all characters from the beginning of the line to the cursor.
 CTRL_Y  Delete all characters from the cursor to the end of the line.
 CTRL_Z  Discard all characters, and return to base view.
 HOME    Same as CTRL_A: Move the cursor to the beginning of the line.
 END     Same as CTRL_E: Move the cursor to the end of the line.
NOS#
```

### 2.1.5 命令过滤

所有显示类命令（show 命令）均支持使用 pipe 过滤或重定向输出信息，格式为：

```
NOS# show xxx pipe PIPE_CMD
```

其中的“PIPE_CMD”必须以管道符“|”（后面接 grep 原生命令）或重定向符“>或>>”（后面接文件名）开始。例如：

- show version pipe | grep Uboot　　*# 只输出结果中包含“Uboot”字符串的行。*
- show running-config pipe > cfg.txt　　*# 将输出信息写入到 cfg.txt 文件。*

### 2.1.6 规格限制

- 单条命令行总长度不能超过 1000 个字符。
- 单条命令行中包含的（以空格分开的）单词数量不能超过 255 个。
- 命令行的单个变参只接受输入可显示 ASCII 字符，且不能包括“?”和所有空白字符。

## 2.2 命令手册

### 2.2.1 config sysname

【功能描述】

**config sysname** 命令用于配置系统名称

【命令格式】

**config sysname** *WORD*

【视图】

根视图

【缺省情况】

不涉及

【参数说明】

*WORD*：系统名称。

【使用举例】

# 将系统名称修改为 SWT1：

```
NOS# config sysname SWT-1
SWT-1#
```

【注意事项】

- 该配置没有 no 命令。
- 配置的系统名称会在命令行提示符里体现。

### 2.2.2 config system description

【功能描述】

**config system description** 命令用于配置系统描述。

【命令格式】

**config system description** *DESC*

**no config system description**

【视图】

根视图

【缺省情况】

不涉及

【参数说明】

*DESC*：系统描述。

【使用举例】

# 将系统描述修改为 NOS：

```
NOS# config system description NOS
```

【注意事项】

LLDP 会使用此处配置的系统描述信息，如果此处未配置，则默认使用“CopyRight，设备名称，版本信息”字符串。

### 2.2.3 copy-mode

【功能描述】

**copy-mode** 命令用于批量配置（常用于拷贝粘贴场景）。

【命令格式】

**copy-mode**

【视图】

根视图

【缺省情况】

不涉及

【参数说明】

无

【使用举例】

```
NOS# copy-mode
You can copy and paste or enter commands now.
Input 'commit' to excute pasted commands or 'quit|exit' to end copy mode.
NOS(copy-mode)# config interface ge1
NOS(copy-mode)# vlan access 100
NOS(copy-mode)# config interface ge2
NOS(copy-mode)# vlan access 100
NOS(copy-mode)# commit
It may take a few seconds to complete
```

【注意事项】

- 在粘贴数据时，不同终端软件会有不同的处理逻辑，部分情况下可能无法正确识别换行，导致配置粘贴失败。为避免配置错误，推荐使用 copy-mode 来粘贴并处理每一行命令。
- 粘贴配置后，输入“commit”来提交批量配置（“quit”或“exit”来取消操作）。
- 如果中途某条命令执行失败，操作不会中断或回退，后面的命令会继续执行。

### 2.2.4 end

【功能描述】

**end** 命令用于从任意视图直接回到根视图

【命令格式】

**end**

【视图】

任意视图

【缺省情况】

不涉及

【参数说明】

无

【使用举例】

# 从 stp 视图切换到根视图：

```
NOS# config stp
NOS(stp)# end
```

【注意事项】

无

### 2.2.5 exit

【功能描述】

**exit** 命令用于退出当前视图，返回上一级视图。如果当前是根视图，则退出登录界面。

【命令格式】

**exit**

【视图】

任意视图

【缺省情况】

不涉及

【参数说明】

无

【使用举例】

```
# 从 stp/region 视图退出到 stp 视图：
NOS# config stp
NOS(stp)# region-configuration
NOS(stp/region)# exit
```

【注意事项】

**quit** 命令（隐藏命令）与 **exit** 命令功能相同。

### 2.2.6 find

【功能描述】

**find** 命令用于查找可用的命令。

【命令格式】

**find** *REGEX* [**excluding-show-cmd**]

【视图】

根视图

【缺省情况】

不涉及

【参数说明】

*REGEX*：正则表达式（POSIX 格式）

**excluding-show-cmd**：不在 show 命令中查找

【使用举例】

```
NOS# find tracer
  (         base) traceroute [{ipv6 | interface ALL_IF}] HOST
NOS#
```

【注意事项】

无

### 2.2.7 reboot

【功能描述】

**reboot** 命令用于重启当前设备。

【命令格式】

**reboot** [**force**]

【视图】

根视图

【缺省情况】

不涉及

【参数说明】

**force**：是否强制重启（不需要输入确认）。

【使用举例】

```
NOS# reboot
System will reboot now, unsaved config will be lost, Continue? [Y/N] y
```

【注意事项】

无

【注意事项】

重启前，请确保配置已保存、启动版本和配置已设置正确。

### 2.2.8 save

【功能描述】

**save** 命令用于保存当前配置。

【命令格式】

**save** [**main**|**backup**|**filename** *FILENAME*]

【视图】

根视图

【缺省情况】

不涉及

【参数说明】

- **main**：保存为主配置文件。
- **backup**：保存为备配置文件。
- **filename** *FILENAME*：保存为指定的配置文件。

【使用举例】

```
NOS# save
The current configuration will be written to /home/startup.conf. Continue? [Y/N] y
NOS#
```

【注意事项】

如果没有使用 **startup** 命令指定设置启动配置文件，**save** 命令将会将会文件配置成设置启动配置文件。

### 2.2.9 screen pager

【功能描述】

screen pager 命令用于设置当前终端显示的分屏功能。

【命令格式】

**screen pager** 〈on|off〉

【视图】

根视图

【缺省情况】

缺省打开分屏功能。

【参数说明】

- **on**：打开分屏功能。
- **off**：关闭分屏功能。

【使用举例】

#关闭分屏功能：

```
NOS# screen pager off
```

【注意事项】

分屏功能仅对 show 命令有效。

### 2.2.10 show history-command

【功能描述】

**show history-command** 命令用于显示历史命令记录。

【命令格式】

**show history-command** [**all**|**last** *COUNT*]

【视图】

任意视图

【缺省情况】

不涉及

【参数说明】

- **all**：显示所有历史命令。
- **last** *COUNT*：显示最后的指定数量的历史命令，范围 1-1000。

【使用举例】

#显示最近 20 条命令行记录：

```
NOS# show history-command
# Last 20 lines:
show device-info
show clock
```

```
show version
show device-info
show history-command
show clock
show version
show device-info
show clock
show version
show device-info
show clock
show version
show device-info
show clock
show version
show device-info
show clock
show version
show device-info
```

【注意事项】

从不同终端登录后，可以查看到所有终端执行过的历史命令。

退出后再次登录，还可以查看到之前的历史记录。

### 2.2.11 show hotkey

【功能描述】

**show hotkey** 命令用于显示当前支持的快捷键情况。

【命令格式】

**show hotkey**

【视图】

任意视图

【缺省情况】

不涉及

【参数说明】

无

【使用举例】

```
NOS# show hotkey
 CTRL_A  Move the cursor to the beginning of the line.
 CTRL_B  Move the cursor one character to the left.
 CTRL_C  Stop the current command.
 CTRL_D  Erase the character at the cursor.
 CTRL_E  Move the cursor to the end of the line.
 CTRL_F  Move the cursor one character to the right.
 CTRL_H  Erase the character to the left of the cursor.
 CTRL_L  Clean the screen.
 CTRL_N  Display the next command in the history buffer.
```

```
CTRL_P  Display the previous command in the history buffer.
CTRL_R  Search backwards through the history.
CTRL_S  Search forwards through the history.
CTRL_W  Delete the word to the left of the cursor.
CTRL_X  Delete all characters from the beginning of the line to the cursor.
CTRL_Y  Delete all characters from the cursor to the end of the line.
CTRL_Z  Discard all characters, and return to base view.
HOME    Same as CTRL_A: Move the cursor to the beginning of the line.
END     Same as CTRL_E: Move the cursor to the end of the line.
```

【注意事项】

无

### 2.2.12 show running-config

【功能描述】

**show running-config** 命令用于显示当前运行的配置情况。

【命令格式】

**show running-config** [**module** *MVIEW*] [**include** *WORD*]

【视图】

任意视图

【缺省情况】

不涉及

【参数说明】

**module** *MVIEW*：只显示指定模块的配置，如不指定则表示显示所有模块的配置。

**include** *WORD*：只显示包含指定单词的配置。

【使用举例】

```
NOS# show running-config
#
version V100R006B07D004
#
config sysname NOS
config coredump enable
config system description NOS
#
config local-user admin
  user-level manage
  password cipher $$5*2Y-mddLLmxtoPnbqu}QT1ZEk1Py{)SV]vvz{ns_i6
#
config domain name system
config default domain system
#
config vlan 1
#
config stp
  region-configuration
```

```
#
config netconf
#
config interface ge1
config interface ge2
config interface ge3
config interface ge4
config interface ge5
config interface ge6
config interface ge7
config interface ge8
config interface ge9
config interface ge10
config interface ge11
config interface ge12
config interface ge13
config interface ge14
config interface ge15
config interface ge16
config interface ge17
config interface ge18
config interface ge19
config interface ge20
config interface ge21
config interface ge22
config interface ge23
config interface ge24
config interface xge25
config interface xge26
config interface xge27
config interface xge28
#
config interface mgt0
  ipv4-address 192.168.1.201/24
#
config ssh server
#
config ftp server
#
config web server
```

【注意事项】

无

### 2.2.13 show saved-config

【功能描述】

**show saved-config** 命令用于显示已保存的配置情况。

【命令格式】

show saved-config [main|backup|*FILENAME*]

【视图】

任意视图

【缺省情况】

不涉及

【参数说明】

**main**：显示主配置文件。

**backup**：显示备配置文件。

*FILENAME*：显示指定的配置文件

【使用举例】

```
NOS# show saved-config
#
version V100R006B07D004
#
config sysname NOS
config coredump enable
#
config local-user admin
  user-level manage
  password cipher $$5*2Y-mddLLmxtoPnbqu}QT1ZEk1Py{)SV]vvz{ns_i6
#
config domain name system
config default domain system
#
config vlan 1
#
config netconf
#
config interface ge1
config interface ge2
config interface ge3
config interface ge4
config interface ge5
config interface ge6
config interface ge7
config interface ge8
config interface ge9
config interface ge10
config interface ge11
config interface ge12
config interface ge13
config interface ge14
config interface ge15
config interface ge16
config interface ge17
```

```
config interface ge18
config interface ge19
config interface ge20
config interface ge21
config interface ge22
config interface ge23
config interface ge24
config interface xge25
config interface xge26
config interface xge27
config interface xge28
#
config interface mgt0
  ipv4-address 192.168.1.201/24
#
config ssh server
#
config ftp server
#
config web server
```

【注意事项】

无

### 2.2.14 show startup

【功能描述】

**show startup** 命令用于显示下次启动时使用的配置文件。

【命令格式】

**show startup** [**json**]

【视图】

任意视图

【缺省情况】

不涉及

【参数说明】

**json**：以 json 格式输出

【使用举例】

```
NOS# show startup
Current startup configuration: NULL.
Next main startup configuration file: startup.conf.
Next backup startup configuration file: NULL.
NOS#
```

【注意事项】

无

### 2.2.15 show this

【功能描述】

**show this** 命令用于显示当前视图下的配置情况。

【命令格式】

**show this**

【视图】

任意视图

【缺省情况】

不涉及

【参数说明】

无

【使用举例】

#显示根视图下的配置情况：

```
NOS# show this
#
version V100R006B07D004
#
config sysname NOS
config coredump enable
config system description NOS
```

【注意事项】

无

### 2.2.16 startup

【功能描述】

**startup** 命令用于指定系统后续启动时使用的配置文件。

**no startup** 命令用于指定后续以空配置启动。

【命令格式】

**startup** *FILENAME* [**main**|**backup**]

**no startup**

【视图】

根视图

【缺省情况】

无

【参数说明】

*FILENAME*：指定的配置文件

**main**：设置为主用配置文件（默认值）。

**backup**：设置为备用配置文件。

【使用举例】

#指定系统后续启动时使用的配置文件为 NOS_config.conf：

```
NOS# startup NOS_config.conf
```

【注意事项】

无

## 2.3 配置举例

配置系统名为 NOS，并增加系统描述。

```
config sysname NOS
config system description NOS
```

## 2.4 常见问题

待补充。

# 3 日志管理

## 3.1 功能介绍

本系统支持四种独立的日志信息输出通道：

- **日志缓冲区**：记录在内存中的日志信息，默认记录 notice 级别及以上，缓冲区大小默认为 16KB，超出则新日志覆盖旧日志。
- **日志文件**：记录在 logfile 目录下的文件里，默认记录 notice 级别及以上，文件大小默认为 10MB，超出则会压缩，最多保存最近的 5 个压缩文件。
- **日志主机**：记录到远程服务器，默认不记录。
- **终端日志**：在当前登录终端实时显示日志信息，默认显示 warning 级别及以上。

这四类信息通道的输出级别都是单独控制，互不影响。

## 3.2 命令手册

### 3.2.1 config logbuffer

【功能描述】

**config logbuffer** 用于配置系统日志记录缓存的过滤等级，低于该等级的不记录。

**no config logbuffer** 用于恢复缺省情况。

【命令格式】

**config logbuffer** {**level** <**error**|**warning**|**notice**|**debugging**> | **size** *SIZE*}

**no config logbuffer** [**level** | **size**]

【视图】

根视图

【缺省情况】

过滤等级为 notice，即 debugging 级别的日志缺省不记录和显示。size 为 16 KB。

【参数说明】

- **error**：记录等级为 error 以及更严重的日志。
- **warning**：记录等级为 warning 以及更严重的日志。
- **notice**：记录等级为 notice 以及更严重的日志。
- **debug**：记录等级为 debugging 以及更严重的日志。
- **size** *SIZE*：日志缓存大小范围(*16-65535*)，单位 KB。

【使用举例】

#记录等级为 error 以及更严重的日志，日志缓存大小为 1024K：

```
NOS# config logbuffer level error size 1024
```

【注意事项】

无

### 3.2.2 config logfile

【功能描述】

**config logfile** 用于配置系统日志写入文件的优先级、文件大小、文件 truncate 频次。

**no config logfile** 用于恢复缺省情况。

【命令格式】

**config logfile** {**level** <**error**|**warning**|**notice**|**debugging**> | **size** *SIZE*}

**no config logfile** {**level**|**size**}

【视图】

根视图

【缺省情况】

缺省等级为 notice。

缺省文件大小为 10Mb。

【参数说明】

- **error**：记录等级为 error 以及更严重的日志。
- **warning**：记录等级为 warning 以及更严重的日志。
- **notice**：记录等级为 notice 以及更严重的日志。
- **debug**：记录等级为 debugging 以及更严重的日志。
- **size** *SIZE*：单个日志文件的大小，单位 Mb，取值范围为 1~100，超过此大小的日志文件会被压缩并生成新的文件。

【使用举例】

#记录等级为 error 以及更严重的日志，单个日志文件大小为 10M：

```
NOS# config logfile level error size 10
```

【注意事项】

为防止频繁写文件，建议日志文件级别不要设置为 debugging 级别。

### 3.2.3 config loghost

【功能描述】

**config loghost** 用于配置系统日志缓存的远程主机信息。

**no config loghost** 用于恢复缺省情况。

【命令格式】

**config loghost** {**host** *HOST* [**port** *(1-65535)*] | **level** <**error**|**warning**|**notice**|**debugging**>}

**no config loghost** [**level**]

【视图】

根视图

【缺省情况】

未配置远程主机，日志缓存在本机。

loghost level 默认为 notice。

【参数说明】

- **host** *HOST*：远程主机的名称或地址。
- **port** *(1-65535)*：远程主机的端口号范围，默认为 syslog 知名端口 514。

- **error**：记录等级为 error 以及更严重的日志。
- **warning**：记录等级为 warning 以及更严重的日志。
- **notice**：记录等级为 notice 以及更严重的日志。
- **debug**：记录等级为 debugging 以及更严重的日志。

【使用举例】

#配置日志缓存远程主机地址为 192.168.201.1，端口号为 514，记录等级为 error 以及更严重的日志：

```
NOS# config loghost host 192.168.201.1 port 514 level error
```

【注意事项】

无

### 3.2.4 diagnostic-information save

【功能描述】

**diagnostic-information save** 命令用于收集设备诊断信息集，以便进一步分析。

【命令格式】

**diagnostic-information save** *FILENAME*

【视图】

任意视图

【缺省情况】

不涉及

【参数说明】

无。

【使用举例】

```
# 收集诊断信息：
NOS# diagnostic-information save dd.log
Please waiting
NOS#
NOS# ls dd*
-rw-r--r--    1 root     root       39.5K Apr  1 12:10 dd.log.tar.gz
 985.2M total, 829.1M free (16% used).
NOS#
```

【注意事项】

- 该命令收集信息较多，可能需要花费较长时间。
- 收集后会生成一个压缩文件，可通过 ftp 等命令传递出来做进一步分析。

### 3.2.5 reset logbuffer

【功能描述】

**reset logbuffer** 命令用于将日志缓冲区清空。

【命令格式】

**reset logbuffer**

【视图】

根视图

【缺省情况】

不涉及

【参数说明】

无

【使用举例】

```
NOS# reset logbuffer
```

【注意事项】

该操作不影响日志文件等其他日志通道。

### 3.2.6 show logbuffer

【功能描述】

**show logbuffer** 命令用于显示日志缓存内容。

【命令格式】

**show logbuffer** [**all**|**last** *LAST_COUNT* |**range** *RANGE_NUM_START RANGE_NUM_END*]

**show logbuffer last** *LAST_COUNT* **json**

【视图】

任意视图

【缺省情况】

不涉及

【参数说明】

- **all**：显示所有日志。
- **last** *LAST_COUNT*：显示最后的指定数量的日志，范围为 1-1000
- **range** *RANGE_NUM_START RANGE_NUM_END*：显示指定范围的日志，其中 *RANGE_NUM_START* 为日志范围的开始，*RANGE_NUM_EMD* 为日志范围的结束，配置范围为 1-1000000。
- **json**：以 json 格式输出。

【使用举例】

```
# 显示所有日志：
NOS# show logbuffer
1970/01/01 08:00:00 [ emerg]
```

【注意事项】

无

### 3.2.7 show logfile

【功能描述】

**show logfile** 命令用于显示日志文件内容，不包括已压缩归档的历史日志。

【命令格式】

**show logfile** [**all**|**last** *LAST_COUNT*]

【视图】

任意视图

【缺省情况】

不涉及

【参数说明】

- **all**：显示所有日志。
- *LAST_COUNT*：显示最后的指定数量的日志，范围为 1-1000。

【使用举例】

# 显示最近 20 条日志信息：

```
NOS# show logfile
# Last 20 lines:
Sat Jan 15 20:28:41 CST 2000 DAEMON.NOTICE minish[7609]: Command: show memory-usage
Sat Jan 15 20:28:45 CST 2000 DAEMON.NOTICE minish[7609]: Command: show cpu-usage
Sat Jan 15 20:29:07 CST 2000 DAEMON.NOTICE minish[7609]: Command: show process
Sat Jan 15 20:29:22 CST 2000 DAEMON.NOTICE minish[7609]: Command: show process sort-by cpu
Sat Jan 15 20:29:38 CST 2000 DAEMON.NOTICE minish[7609]: Command: show process sort-by memory
Sat Jan 15 20:30:05 CST 2000 DAEMON.NOTICE minish[7609]: Command: show process sort-by memory
Sat Jan 15 20:30:10 CST 2000 DAEMON.NOTICE minish[7609]: Command: show process sort-by memory
Sat Jan 15 20:46:11 CST 2000 DAEMON.NOTICE minish[7661]: Command: config telemetry
Sat Jan 15 20:46:12 CST 2000 DAEMON.NOTICE minish[7661]: Command: dis th
Sat Jan 15 20:46:16 CST 2000 DAEMON.NOTICE minish[7661]: Command: no subscription s1
Sat Jan 15 20:47:05 CST 2000 DAEMON.NOTICE minish[7661]: Command: no sensor-group s1
Sat Jan 15 20:47:06 CST 2000 DAEMON.NOTICE minish[7661]: Command: dis th
Sat Jan 15 20:47:12 CST 2000 DAEMON.NOTICE minish[7661]: Command: sensor-group s1
Sat Jan 15 20:47:55 CST 2000 DAEMON.NOTICE minish[7661]: Command: sensor path
/openconfig-acl:acl
Sat Jan 15 20:47:56 CST 2000 DAEMON.NOTICE minish[7661]: Command: dis th
Sat Jan 15 20:47:59 CST 2000 DAEMON.NOTICE minish[7661]: Command: qu
Sat Jan 15 20:48:00 CST 2000 DAEMON.NOTICE minish[7661]: Command: dis th
Sat Jan 15 20:48:02 CST 2000 DAEMON.NOTICE minish[7661]: Command: subscription s1
Sat Jan 15 20:48:05 CST 2000 DAEMON.NOTICE minish[7661]: Command: sensor-group s1
sample-interval 5
Sat Jan 15 20:48:07 CST 2000 DAEMON.NOTICE minish[7661]: Command: destination-group d1
```

【注意事项】

无

### 3.2.8 show terminal status

【功能描述】

**show terminal status** 命令用于显示当前终端日志通道的开关状态。

【命令格式】

**show terminal status**

【视图】

任意视图

【缺省情况】

不涉及

【参数说明】

无

【使用举例】

```
# 查看当前终端日志通道的开关状态：
NOS# show terminal status
Monitor status: ON
Debugging status: OFF
NOS#
```

【注意事项】

无

### 3.2.9 terminal debugging

【功能描述】

**terminal debugging** 用于将当前终端的日志信息显示级别调整为 debugging。

**no terminal debugging** 用于恢复缺省情况。

【命令格式】

**terminal debugging**

**no terminal debugging**

【视图】

根视图

【缺省情况】

缺省显示级别为 Warning。

【参数说明】

无

【使用举例】

```
NOS# terminal debugging
```

【注意事项】

该功能需要同时打开“terminal monitor”才能输出到当前终端。

### 3.2.10 terminal monitor

【功能描述】

**terminal monitor** 用于打开当前终端的实时日志输出功能。

**no terminal monitor** 用于恢复缺省情况。

【命令格式】

**terminal monitor**

**no terminal monitor**

【视图】

根视图

【缺省情况】

该功能缺省为打开状态。

【参数说明】

无

【使用举例】

```
NOS# terminal monitor
```

【注意事项】

如果输出信息较多，推荐在 SSH 或 Telnet 终端上开启该功能。串口传输带宽较小，大量日志的打印可能会影响命令行操作。

## 3.3 配置举例

设置日志缓存 1000kb，日志文件大小 5M，并配置远程日志主机 ip

```
config logbuffer level error size 1000
config logfile level error size 5
config loghost host 192.168.1.123
```

## 3.4 常见问题

待补充。

# 4 软件及版本管理

## 4.1 功能介绍

### 4.1.1 版本管理

软件版本可以通过“show version”查看，里面的“Product version”就是指该产品当前运行的软件版本号，“Build date”则表示该版本的发布日期。

### 4.1.2 补丁管理

补丁包括三种类型：

- **内核补丁**：用于修复 kernel 的问题，目前内核态业务很少，大部分都是在用户态。
- **用户态冷补丁**：冷补丁是指通过更换和重启指定业务进程来解决问题的补丁。由于进程重启很快，一般对业务影响较小。但若涉及设备间的配合、需要重新学习对端状态，则可能会对业务有一定影响。
- **用户态热补丁**：热补丁是指不重启进程、直接在线修复 bug 的补丁方式，对业务影响最小，但补丁间的依赖关系比较复杂，维护比较困难。

目前本系统只支持用户态补丁（包括冷补丁和热补丁），不支持内核补丁。发布和安装补丁时，按补丁包（.bin 文件）为粒度，一个补丁包里可能会包含多个补丁。

一些规则和限制如下：

- 系统最多可支持 32 个补丁包。
- 补丁包前后存在依赖关系，因此载时只能从最后一个开始。
- 系统重启时，会自动安装所有 commit 过的补丁。
- 补丁包跟软件版本绑定，版本号不匹配的不能安装。

## 4.2 命令手册

### 4.2.1 bootfile

【功能描述】

bootfile 命令用于指定系统下次启动时使用的版本文件。

【命令格式】

**bootfile** *IMAGE* <**main**|**backup**>

【视图】

根视图

【缺省情况】

不涉及

【参数说明】

*IMAGE*：文件名。

**main**：指定为主用启动版本。

**backup**：指定为备用启动版本。

【使用举例】

# 指定 NOS_sc3331_debug.image 为主启动文件：

```
NOS# bootfile NOS_sc3331_debug.image main
Verifying image...
Verified OK
```

【注意事项】

### 4.2.2 patch commit

【功能描述】

**patch commit** 用于提交补丁操作（包括安装和卸载），只有 commit 之后的补丁在重启后才会继续生效。

【命令格式】

**patch commit**

【缺省情况】

不涉及

【参数说明】

无

【使用举例】

```
NOS# patch commit
```

【注意事项】

- 建议在补丁验证无误后再执行 commit，防止出现因补丁异常导致设备脱管、后续重启后无法卸载补丁的情况出现。
- commit 后的补丁文件不能删除，否则设备重启后会因找不到文件而安装失败。

### 4.2.3 patch install

【功能描述】

**patch install** *FILE* 用于安装补丁文件

【命令格式】

**patch install** *FILE* [**verbose**] [**description** *TEXT*]

【缺省情况】

不涉及

【参数说明】

- *FILE*:补丁文件名。
- **verbose**：输出详细的安装过程信息。
- **description**：补丁描述信息，在 show patch 时会显示出来。

【使用举例】

# 加载装备补丁：

```
NOS# patch install switch_equip_patch.bin description equip
NOS# show patch
 Idx  Committed  File                            Description      Installed
 ---  ---------  ------------------------------  ---------------  ---------
```

```
 1    No       switch_equip_patch.bin          equip          Yes
```

【注意事项】

安装的补丁仅当前生效，如果需要在设备重启后仍然生效，需要再执行 commit 命令确认。

### 4.2.4 patch uninstall

【功能描述】

**patch uninstall** 用于卸载补丁操作

【命令格式】

**patch uninstall** [{**all**|**verbose**}]

【缺省情况】

不涉及

【参数说明】

- **verbose**：输出详细的卸载过程信息。
- **all**：卸载所有补丁。如果不选择 all，则表示只卸载最后一个补丁。

【使用举例】

```
# 卸载所有补丁：
NOS# patch uninstall all
NOS# show patch
 Idx  Committed  File                          Description      Installed
```

【注意事项】

无

### 4.2.5 restore factory-default

【功能描述】

**restore factory-default** 命令用于将设备恢复成出厂设置（但仍使用当前的版本文件）。

【命令格式】

**restore factory-default**

【视图】

根视图

【缺省情况】

不涉及

【参数说明】

无

【使用举例】

```
# 恢复出厂设置：
NOS# restore factory-default
This command will restore the system to the factory default configuration and clear the
operation data. Continue [Y/N]:y
Please wait ......
Please reboot the system.
```

【注意事项】

本命令不可回退，请谨慎使用。

### 4.2.6 show bootfile

【功能描述】

**show bootfile** 命令用于查看系统下次启动时使用的版本文件。

【命令格式】

**show bootfile**

【视图】

任意视图

【缺省情况】

不涉及

【参数说明】

无

【使用举例】

```
# 查看下次启动版本文件：
NOS# show bootfile
Main:NOS_sc3331_debug.image
Backup:
```

【注意事项】

无

### 4.2.7 show patch

【功能描述】

**show patch** 用于显示当前已安装的补丁信息。

【命令格式】

**show patch**

【缺省情况】

不涉及

【参数说明】

无。

【使用举例】

```
# 查看当前安装的补丁：
NOS# show patch
 Idx  Committed  File                          Description      Installed
 ---  ---------  ------------------------------  ---------------  ---------
1    Yes        patch_01_stp.bin               stp_bug_1       Yes
2    No         patch_02_mstp.bin (NOT found)   mstp_bug_2       No
```

【注意事项】

无

### 4.2.8 show version

【功能描述】

**show version** 命令用于显示当前运行版本信息。

【命令格式】

**show version**

【视图】

任意视图

【缺省情况】

不涉及

【参数说明】

无

【使用举例】

```
# 显示当前版本信息：
NOS# show version
Copyright (c) 2020-2026 Co., Ltd.
Device name     :
Build date      : 2025/03/28 13:48:10 UTC
Uptime          : 0day 0h 12min 17s
Product version : V100R006B07D001-r101
Uboot version   :
Reboot cause    :
```

【注意事项】

无

## 4.3 配置举例

这些命令都是实时操作，不是具体的配置。

## 4.4 常见问题

待补充。

# 5 时间管理-基础

## 5.1 功能介绍

### 5.1.1 NTP和SNTP介绍

NTP（Network Time Protocol，网络时间协议）是一种可以在服务器和客户端之间进行时间同步的协议，一般可以达到毫秒级别的精度。NTP 采用的传输层协议为 UDP，使用的 UDP 端口号为 123，对应协议为 RFC 5905。

SNTP（Simple NTP，简单 NTP）是由 RFC 4330 定义的简化版 NTP，仅涉及客户端（服务端仍采用 NTP 服务器）。大致原理跟 NTP 相同，但同步速度较快、精度稍低、配置简单。

### 5.1.2 时间段

时间段定义了一个时间范围。当一个功能只需在某个特定的时间范围内生效时，可以先配置好这个时间段，然后在配置该功能时引用该时间段，这样该模块就只能在该时间段定义的时间范围内生效。时间段可分为以下两种类型：

- 周期时间段：表示以一周为周期（如每周三的 9 至 18 点）循环生效的时间段。
- 绝对时间段：表示在指定时间范围内（如 2023 年 3 月 1 日 7 点至 2023 年 4 月 1 日 12 点）生效的时间段。

每个时间段都以一个名称来标识，用户最多可创建 128 个不同名称的时间段。

当一个时间段内既包含有周期时间段也包含有绝对时间段时，系统将取它们的交集作为该时间段最终生效的时间范围。

无法修改已创建的时间段。

## 5.2 命令手册

### 5.2.1 config ntp-client

【功能描述】

**config ntp-client** 命令用于开启 NTP 客户端功能，即使用 NTP 协议对本地时间进行校准。

**no config ntp-client** 命令用于恢复确实情况。

【命令格式】

[no] **config ntp-client**

【视图】

根视图

【缺省情况】

未启用 NTP 客户端

【参数说明】

无

【使用举例】

#配置启用 NTP 客户端，并配置 10.1.1.1 为同步时钟源。

```
NOS# config ntp-client
NOS(ntp-client)#
```

【注意事项】

无

### 5.2.2 config ntp-server

【功能描述】

**config ntp-server** 命令用于开启 NTP 服务端功能，即可做为 Server 给其他 Client 同步时钟。

【命令格式】

**config ntp-server**

**no config ntp-server**

【视图】

根视图

【缺省情况】

未启用 NTP 服务端

【参数说明】

无。

【使用举例】

#启用 NTP 服务端。

```
NOS# config ntp-server
NOS(ntp-server)#
```

【注意事项】

无。

### 5.2.3 config sntp-client

【功能描述】

**config sntp-client** 命令用于开启 SNTP 客户端，即使用 SNTP 协议对本地时间进行校准。

**no config sntp-client** 命令用于关闭 SNTP 客户端。

【命令格式】

[no] **config sntp-client**

【视图】

根视图

【缺省情况】

未启用 SNTP 客户端

【参数说明】

无

【使用举例】

#配置启用 SNTP 客户端

```
NOS# config sntp-client
NOS(sntp-client)#
```

【注意事项】

无

### 5.2.4 config time-range

【功能描述】

**config time-range** 命令用于进入 timerange 视图。

**no config time-range** 命令用于退出 timerange 视图及删除视图下的所有配置。

【命令格式】

[no] config time-range

【视图】

根视图

【缺省情况】

无。

【参数说明】

无。

【使用举例】

```
NOS# config acl time-range
NOS(time-range)#
```

【注意事项】

无。

### 5.2.5 datetime

【功能描述】

**datetime** 命令用于配置当前时间。

【命令格式】

**datetime** *DATE* [*TIME*]

【视图】

根视图

【缺省情况】

不涉及

【参数说明】

- *DATE*：要设置的日期，支持 YYYY/MM/DD 和 YYYY-MM-DD 两种格式。
- *TIME*：要设置的时间，格式为 hh:mm:ss。

【使用举例】

```
NOS# datetime 2024/01/01 13:00:00
NOS# show clock
2024/01/01 13:00:03 CST(Asia/Shanghai), Monday
```

【注意事项】

如果配置了 NTP 客户端功能，则会自动按 NTP 时间调整本地时钟。

### 5.2.6 show clock

【功能描述】

**show clock** 命令用于显示当前时间及时区。

【命令格式】

**show clock** [**json**]

【缺省情况】

不涉及

【参数说明】

**json**：以 json 格式输出

【使用举例】

#显示当前时间。

```
NOS# show clock
2020/02/14 12:14:00 CST(Asia/Shanghai), Tuesday
```

【注意事项】

无。

### 5.2.7 show ntp state

【功能描述】

**show ntp state** 命令用于显示当前 NTP 状态。

【命令格式】

**show ntp state**

【缺省情况】

不涉及

【参数说明】

无。

【使用举例】

#显示当前 NTP 状态。

```
NOS# show ntp state
  Client state : Disabled (Unsynced)
  Selected peer: (offset: 0.000000s, stratum: 1)
  Poll interval: 1s
  Send requests: 0
  Recv replys  : 0
Server state   : Enabled
  Recv requests: 0
  Send replys  : 0
```

【注意事项】

无。

### 5.2.8 show time-range

【功能描述】

**show time-range** 命令用于查看指定时间段的信息。

【命令格式】

**show time-range** [*NAME*]

【视图】

任意视图

【缺省情况】

无。

【参数说明】

NAME：指定时间段的名称，长度（1-31）不允许包含字母、数字以外的字符。

【使用举例】

```
NOS(time-range)# show time-range

Current time: 2021/09/01 06:37:02 Wednesday

Total timerange count: 5

  Time-range a1:
    State: Active
    daily

  Time-range a2:
    State: InActive
    00:00 to 24:00 Mon Tue Wed Thu Sat from 00:00 1970/01/02 to 06:30 2021/09/01

  Time-range a3:
    State: Active
    00:00 to 24:00 off-day Mon Wed

  Time-range a4:
    State: Active
    from 24:00 2021/08/31 to 08:00 2021/09/01

  Time-range a7:
    State: Active
from 00:00 1970/01/02 to 24:00 2021/09/01
```

【注意事项】

无。

### 5.2.9 sync-from

【功能描述】

**sync-from** 命令用于配置 NTP 客户端使用的时钟源。

【命令格式】

**sync-from** *SERVER*

**no sync-from** 〈*SERVER* | **all**〉　　# NTP 客户端视图

**no sync-from**　　# SNTP 客户端视图

【视图】

NTP 客户端视图

SNTP 客户端视图

【缺省情况】

未配置 NTP/SNTP 时钟源服务器。

【参数说明】

*SERVER*：使用的时钟源，支持地址和主机名两种格式。NTP 支持配置多个（会根据 NTP 协议自动选择最佳时钟源），SNTP 只支持配置一个。

【使用举例】

#配置 10.1.1.1 为同步时钟源。

```
NOS# config ntp-client
NOS(ntp-client)# sync-from 10.1.1.1
```

【注意事项】

NTP 和 SNTP 不能同时运行。

### 5.2.10　timezone

【功能描述】

**timezone** 命令用于配置系统使用的时区。

**no timezone** 命令用于将时区配置为默认时区。

【命令格式】

**timezone** {*TZ_AREA TZ_COUNTRY* | **utc**}

**no timezone**

【视图】

根视图

【缺省情况】

缺省使用亚洲/上海时区。

【参数说明】

- *TZ_AREA*：时区对应的地区。
- *TZ_COUNTRY*：时区对应的城市。
- **utc**：配置为 0 时区，即使用 UTC 时间。

【使用举例】

# 配置时间，时区为上海（亚洲）。

```
NOS# timezone Asia Shanghai
```

【注意事项】

系统目前只支持亚洲地区的时区。

### 5.2.11 time-range

【功能描述】

**time-range** 命令用于创建时间段。

**no time-range** 命令用于删除指定名称的时间段。

【命令格式】

**time-range** *NAME* <**infinite** | {**period** *START-TIME* **to** *END-TIME* {**Sun** | **Mon** | **Tue** | **Wed** | **Thu** | **Fri** | **Sat** | **daily** | **off-day** | **working-day**} | **from** *TIME-FROM DATE-FROM* | **to** *TIME-TO DATE-TO*}>

**no time-range** [*NAME*]

【视图】

timee-range 视图

【缺省情况】

未创建时间段。

【参数说明】

- NAME：指定时间段的名称，长度（1-31）不允许包含字母、数字以外的字符。
- **infinite**：生效时间为永远生效。
- **period**：设置周期时间段，具体如下：
  - *START-TIME*：指定周期时间段的开始时间，格式 hh:mm。
  - *END-TIME*：指定周期时间段的结束时间，格式 hh:mm。
  - Sun Mon Tue Wed Thu Fri Sat：指定周期时间段在每周周几生效。
  - **daily**：指定周期时间段每天都生效。
  - **off-day**：指定周期时间段在周末生效。
  - **working-day**：指定周期时间段在工作日生效。
- **from** *TIME-FROM DATE-FROM*：指定绝对时间段的开始时间（格式 hh:mm）和开始日期（格式 yyyy/mm/dd），未指定则默认为 1970/01/02 00:00。
- **to** *TIME-TO DATE-TO*：指定绝对时间段的结束时间(格式 hh:mm)和结束日期(格式 yyyy/mm/dd)，未指定则默认为永远。

【使用举例】

# 创建名为 learn 的时间段，其时间范围为 2023 年 9 月 1 日 6 点到 9 月 20 日 20 点内每周周一和周三的 8 点到 18 点

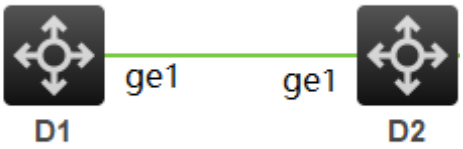
```
NOS(time-range)#time-range learn period 8:00 to 18:00 Mon Wed from 6:00 2023/9/1 to 20:00 2023/9/20
```

【注意事项】

- 最终生效时间按配置的交集计算。
- 周期时间段和绝对时间段的开始时间不能晚于结束时间。
- 绝对时间段的开始日期最早可设置为 1970/1/2。
- 绝对时间段开始时间配置为当日 24：00，结束时间配置为次日 0：0 属于非法配置。

## 5.3 配置举例

配置亚洲时区，在 D1 设备上开启 NTP 服务端功能，在 D2 设备上开启客户端功能。




D1 设备

```
timezone Asia Singapore
config ntp-server
```

D2 设备

```
timezone Asia Singapore
config ntp-client
```

## 5.4 常见问题

无。

# 6 文件管理

## 6.1 功能介绍

### 6.1.1 文件系统介绍

本系统使用标准的 Linux EXT4 文件系统，用户所有可操作都只能在/home/flash 之下（所有操作在断电重启后仍然生效），这个目录就是用户文件系统的根目录，其他外层目录不可操作。

如果设备有双 flash（或硬盘），则在根目录下会存在一个 hdd 的子目录，表示备用存储。如果插入了 USB 存储（目前仅支持 FAT32 文件系统），则会在根目录下动态创建一个 usb 子目录，拔出时会自动删除。

根目录下的如下几个子目录为系统目录，不可删除：

- corefile：保存进程异常信息的目录。
- hdd：备用 flash（或硬盘）存储路径。
- logfile：保存日志文件的目录，其中的 system.log 文件也不可删除。
- usb：动态拔插 USB 存储对应的目录。
- usrapp：第三方应用程序使用的目录。

### 6.1.2 磁盘利用率监控

当磁盘用满后，很多功能会收到影响，因此本系统在磁盘使用率超过 95%、且持续超 10 秒后，会输出告警日志：Disk usage is too high(xx.xx%)。

回落到 90%以下、且持续超 10 秒后会输出告警恢复日志：Disk usage is recoverd(xx.xx%)。

## 6.2 命令手册

### 6.2.1 cd

【功能描述】

cd 命令用于修改当前工作路径。

【命令格式】

cd [*PATH*]

【视图】

根视图

【缺省情况】

不涉及

【参数说明】

*PATH*：要更改的目的路径，如果为空，则显示当前工作路径。

【使用举例】

#更改工作路径到 logfile。

```
NOS# cd logfile/
```

【注意事项】

无

### 6.2.2 config ftp server

【功能描述】

**config ftp server** 命令用于开启 ftp 服务。

**no config ftp server** 命令用于关闭 ftp 服务。

【命令格式】

[no] **config ftp server**

【视图】

根视图

【缺省情况】

默认开启了 ftp 服务

【参数说明】

无

【使用举例】

#启动 ftp 服务

```
NOS# config ftp server
NOS(ftp)#
```

【注意事项】

ftp 服务的根目录为/home/flash。

### 6.2.3 cp

【功能描述】

**cp** 命令用于复制文件或文件夹。

【命令格式】

**cp** *SRC DST*

【视图】

根视图

【缺省情况】

不涉及

【参数说明】

- *SRC*：要拷贝的源文件或源目录。
- *DST*：要拷贝的目的文件或目的目录，如果目标已存在，会强制覆盖。

【使用举例】

#备份 system.log 文件。

```
NOS# cp logfile/system.log logfile/system_bak.log
```

【注意事项】

使用前请先确认目标是否存在，防止被误覆盖。

### 6.2.4 ftp

【功能描述】

**ftp** 命令用于跟 FTP 服务器上传或下载文件。

【命令格式】

**ftp** <**get**|**put**> *FILE SERVER USER PASSWD*

【视图】

根视图

【缺省情况】

不涉及

【参数说明】

- **get**：从服务器下载文件。
- **put**：上传文件到服务器。
- *FILE*：要上传或下载的文件名。
- *USER*：FTP 账户的用户名。
- *PASSWD*：FTP 账户的密码。

【使用举例】

#ftp 获取 system.log 文件。

```
NOS# ftp get system.log 192.168.56.1 aaa 123456
```

【注意事项】

无

### 6.2.5 ls

【功能描述】

**ls** 命令用于显示文件和文件夹，**dir** 是命令别名。

【命令格式】

<**ls**|**dir**> [*PATH*]

【视图】

根视图

【缺省情况】

不涉及

【参数说明】

*PATH*：显示指定目录下的文件。

【使用举例】

#显示 logfile 目录下的文件信息。

```
NOS# ls logfile
-rwxrwxrwt    1 admin    admin     803.0K Feb 14 11:13 system.log
-rwxrwxrwt    1 admin    admin     803.0K Feb 14 11:13 system_bak.log
NOS#
```

【注意事项】

无

### 6.2.6 md5sum

【功能描述】

**md5sum** 命令用于计算文件的 MD5 值。

【命令格式】

**md5sum** *FILE*

【视图】

根视图

【缺省情况】

不涉及

【参数说明】

FILE：要计算的文件。

【使用举例】

#计算 log 文件 md5 值。

```
NOS# md5sum system.log
256c9f5cb5e659af5a43cd7d93be8f7e
```

【注意事项】

无

### 6.2.7 mkdir

【功能描述】

**mkdir** 命令用于创建文件夹。

【命令格式】

**mkdir** [ *PATH* ]

【视图】

根视图

【缺省情况】

不涉及

【参数说明】

*PATH*：要创建的文件夹。

【使用举例】

```
NOS# mkdir NOS_log
NOS# ls
drwxr-xr-x    2 root     root          160 Jan  1 13:06 NOS_log
-rw-r--r--    1 logd     root        6.2M Jan 15  2000 system.log
-rw-r--r--    1 logd     root      349.2K Jan  9  2000 system1.log.tar.gz
-rw-r--r--    1 logd     root      245.9K Jan  9  2000 system2.log.tar.gz
-rw-r--r--    1 logd     root      270.3K Jan  9  2000 system3.log.tar.gz
```

```
-rw-r--r--    1 logd     root      439.4K Jan 15  2000 system4.log.tar.gz
-rw-r--r--    1 logd     root      275.1K Jan 16  2000 system5.log.tar.gz

 452.0M total, 366.2M free (18% used).
```

【注意事项】

如果文件夹已经存在，则不会执行任何动作。

### 6.2.8 more

【功能描述】

**more** 命令用于显示文件内容。

【命令格式】

**more** *FILE*

【视图】

根视图

【缺省情况】

不涉及

【参数说明】

*FILE*：要显示的文件。

【使用举例】

#显示 system.log 文件:

```
NOS# more system.log
Sun Jan 16 03:21:02 CST 2000 DAEMON.ERR grpc[4944]: 947964059, grpc_get_sensor_path_data:320
Sun Jan 16 03:21:02 CST 2000 DAEMON.ERR grpc[4944]: 947964059, grpc_get_sensor_path_data:328
Sun Jan 16 03:21:02 CST 2000 DAEMON.ERR grpc[4944]: 947964059, grpc_get_sensor_path_data:331
Sun Jan 16 03:21:02 CST 2000 DAEMON.ERR grpc[4944]: 947964059, grpc_get_sensor_path_data:339
Sun Jan 16 03:21:04 CST 2000 DAEMON.ERR grpc[4944]: 947964064, grpc_get_sensor_path_data:320
Sun Jan 16 03:21:04 CST 2000 DAEMON.NOTICE minish[4340]: Command: show clock
Sun Jan 16 03:21:04 CST 2000 DAEMON.NOTICE minish[4340]: Command: show version
Sun Jan 16 03:21:04 CST 2000 DAEMON.NOTICE minish[4340]: Command: show device-info
Sun Jan 16 03:21:04 CST 2000 DAEMON.ERR grpc[4944]: 947964064, grpc_get_sensor_path_data:328
Sun Jan 16 03:21:04 CST 2000 DAEMON.ERR grpc[4944]: 947964064, grpc_get_sensor_path_data:331
Sun Jan 16 03:21:04 CST 2000 DAEMON.ERR grpc[4944]: 947964064, grpc_get_sensor_path_data:339
Sun Jan 16 03:21:04 CST 2000 DAEMON.ERR grpc[4944]: 947964064, grpc_get_sensor_path_data:320
Sun Jan 16 03:21:04 CST 2000 DAEMON.NOTICE minish[4340]: Command: show clock
Sun Jan 16 03:21:04 CST 2000 DAEMON.NOTICE minish[4340]: Command: show version
Sun Jan 16 03:21:05 CST 2000 DAEMON.NOTICE minish[4340]: Command: show device-info
Sun Jan 16 03:21:05 CST 2000 DAEMON.ERR grpc[4944]: 947964065, grpc_get_sensor_path_data:328
Sun Jan 16 03:21:05 CST 2000 DAEMON.ERR grpc[4944]: 947964065, grpc_get_sensor_path_data:331
Sun Jan 16 03:21:05 CST 2000 DAEMON.ERR grpc[4944]: 947964065, grpc_get_sensor_path_data:339
Sun Jan 16 03:21:05 CST 2000 DAEMON.ERR grpc[4944]: 947964065, grpc_get_sensor_path_data:320
Sun Jan 16 03:21:05 CST 2000 DAEMON.ERR grpc[4944]: 947964065, grpc_get_sensor_path_data:328
Sun Jan 16 03:21:05 CST 2000 DAEMON.ERR grpc[4944]: 947964065, grpc_get_sensor_path_data:331
Sun Jan 16 03:21:05 CST 2000 DAEMON.ERR grpc[4944]: 947964065, grpc_get_sensor_path_data:339
Sun Jan 16 03:21:05 CST 2000 DAEMON.ERR grpc[4944]: 947964065, grpc_get_sensor_path_data:320
```

```
--More--
```

【注意事项】

该操作支持分屏，且不可关闭。

### 6.2.9 mv

【功能描述】

**mv** 命令用于移动文件或文件夹。

【命令格式】

**mv** *SRC DST*

【视图】

根视图

【缺省情况】

不涉及

【参数说明】

- *SRC*：要移动的源文件或源目录。
- *DST*：要移动的目的文件或目的目录，如果目标已存在，会强制覆盖。

【使用举例】

```
NOS# mv NOS_log/ NOS_log1
NOS# ls
drwxr-xr-x    2 root     root         160 Jan  1 13:06 NOS_log1
-rw-r--r--    1 logd     root        6.2M Jan 15  2000 system.log
-rw-r--r--    1 logd     root      349.2K Jan  9  2000 system1.log.tar.gz
-rw-r--r--    1 logd     root      245.9K Jan  9  2000 system2.log.tar.gz
-rw-r--r--    1 logd     root      270.3K Jan  9  2000 system3.log.tar.gz
-rw-r--r--    1 logd     root      439.4K Jan 15  2000 system4.log.tar.gz
-rw-r--r--    1 logd     root      275.1K Jan 16  2000 system5.log.tar.gz

 452.0M total, 366.2M free (18% used).
```

【注意事项】

使用前请先确认目标是否存在，防止被误覆盖。

### 6.2.10 pwd

【功能描述】

**pwd** 命令用于显示当前的工作路径。

【命令格式】

**pwd**

【视图】

根视图

【缺省情况】

不涉及

【参数说明】

无

【使用举例】

```
NOS# pwd
/home/flash/logfile
```

【注意事项】

无

### 6.2.11 rename

【功能描述】

**rename** 命令用于重命名文件或文件夹。

【命令格式】

**rename** *SRC DST*

【视图】

根视图

【缺省情况】

不涉及

【参数说明】

- *SRC*：要重命名的源文件或源目录。
- *DST*：要重命名的目的文件或目的目录，如果目标已存在，会强制覆盖。

【使用举例】

```
NOS# rename NOS_log1/ NOS_log
NOS# ls
drwxr-xr-x    2 root     root         160 Jan  1 13:06 NOS_log
-rw-r--r--    1 logd     root        6.2M Jan 15  2000 system.log
-rw-r--r--    1 logd     root      349.2K Jan  9  2000 system1.log.tar.gz
-rw-r--r--    1 logd     root      245.9K Jan  9  2000 system2.log.tar.gz
-rw-r--r--    1 logd     root      270.3K Jan  9  2000 system3.log.tar.gz
-rw-r--r--    1 logd     root      439.4K Jan 15  2000 system4.log.tar.gz
-rw-r--r--    1 logd     root      275.1K Jan 16  2000 system5.log.tar.gz

 452.0M total, 366.2M free (18% used).
```

【注意事项】

使用前请先确认目标是否存在，防止被误覆盖。

### 6.2.12 rm

【功能描述】

**rm** 命令用于删除文件。

【命令格式】

**rm** FILE

【视图】

根视图

【缺省情况】

不涉及

【参数说明】

FILE：要删除的文件。

【使用举例】

#删除 system.log 文件。

```
NOS# rm logfile/system.log
Deleted file could not be restored, continue? [y/N] y
NOS#
```

【注意事项】

删除后无法恢复，请谨慎使用。

### 6.2.13 rmdir

【功能描述】

**rmdir** 命令用于删除文件夹。

【命令格式】

**rmdir** [ *PATH* ]

【视图】

根视图

【缺省情况】

不涉及

【参数说明】

PATH：要删除的文件夹。

【使用举例】

#删除 system.log 文件。

```
NOS# rmdir logfile
Deleted folder could not be restored, continue? [y/N] y
NOS#
```

【注意事项】

该操作会强制删除指定文件夹（及所有子文件夹），不可恢复。

### 6.2.14 scp

【功能描述】

**scp** 命令用来与远程 SCP 服务器建立连接，并进行文件传输。

【命令格式】

**scp** *SERVER* [*PORT*] [*USER*] <**get**|**put**> *FILE1* [*FILE2*]

【视图】

根视图

【缺省情况】

不涉及

【参数说明】

- *SERVER*：服务器 IPv4/IPv6 地址或主机名称。
- *PORT*：服务器端口号，取值范围为 1~65535，缺省值为 22。
- *USER*：指定用户名。
- **get**：指定下载文件操作。
- **put**：指定上传文件操作。
- *FILE1*：源文件名称，默认工作路径是/home/flash/。
- *FILE2*：目的文件名称，默认工作路径是/home/flash/。

【使用举例】

#获取 system.log 文件。

```
NOS# scp 192.168.56.100 22 aaa get system.log
```

【注意事项】

当指定了用户名，未指定端口号时，用户名不能是数字。

### 6.2.15 sftp

【功能描述】

**sftp** 命令用来与远程 SFTP 服务器建立连接，并进入 SFTP 客户端视图。

【命令格式】

**sftp** *SERVER* [*PORT*]

【视图】

根视图

【缺省情况】

不涉及

【参数说明】

- *SERVER*：服务器 IPv4/IPv6 地址或主机名称。
- *PORT* ：服务器端口号，取值范围为 1~65535，缺省值为 22。

【使用举例】

```
NOS# sftp 192.168.56.100
User name: aaa
```

【注意事项】

无

### 6.2.16 tar

【功能描述】

**tar** 命令用于压缩/解压/显示功能。

【命令格式】

**tar** <**create** *TARFILE* **source** *SRC...*| **extract** *TARFILE* [**to** *DST*] | **list** *TARFILE*>

【视图】

根视图

【缺省情况】

不涉及

【参数说明】

- *TARFILE*：压缩文件，使用 gzip 压缩方式，后缀名一般建议为“.tar.gz”。
- **source** *SRC...*：要添加到压缩文件的源文件或文件夹列表。
- **to** *DST*：要解压的目的文件夹（不存在时会自动创建），如不指定表示当前文件夹。

【使用举例】

```
NOS# tar create system.log source NOS_log/
NOS_log/
```

【注意事项】

无

### 6.2.17 tftp

【功能描述】

**tftp** 命令用于跟 TFTP 服务器上传或下载文件。

【命令格式】

**tftp** <**get**|**put**> [**packet-size** *(256-65535)*] *FILE SERVER*

【视图】

根视图

【缺省情况】

不涉及

【参数说明】

- **get**：从服务器下载文件。
- **put**：上传文件到服务器。
- **packet-size** *(256-65535)*：指定报文传输大小，默认为 512（RFC 1350）。
- *FILE*：要上传或下载的文件名。
- *SERVER*：要上传或下载的 TFTP 服务器 IP 或名称。

【使用举例】

```
NOS# tftp get switch_equip_patch.bin 192.168.56.1
switch_equip_patch.b 100%
|*******************************************************************************
**********************************************************************| 3439k  0:00:00
ETA
NOS#
```

【注意事项】

增加报文传输大小可以提高传输速度，从而加快整体速度；但如果设备性能较弱，反而可能会因为需要分片重组而降低整体速度。

## 6.3 配置举例

这些命令都是实时操作，不是具体的配置。

## 6.4 常见问题

待补充。

# 7 资源管理

## 7.1 功能介绍

资源管理主要包括 CPU、内存、业务进程等软硬件资源，可以对其使用状态进行查看、监控。

当 CPU 使用率超过 95%且持续 60 秒以上，会产生告警日志“CPU usage is too high(xx.xx%)” 、并打印占用 CPU 靠前的业务进程信息。当降低到 80%以下并持续 60 秒以上，则打印恢复信息“CPU usage is recoverd”。

当内存使用率超过 90%，会立即产生告警日志“Memory usage is too high(xx.xx%)”、并打印占用内存靠前的业务进程信息。当降低到 80%以下并持续 60 秒以上，则打印恢复信息“Memory usage is recoverd”。

内存使用率除了上述固定阈值的监控外，还支持内存门限功能：当超过用户指定的门限值后，会主动尝试终止部分非关键业务来尝试让系统继续运行，如果还无法恢复到门限值以内，则会自动重启系统。

对磁盘资源的监控，请参考“文件管理”章节。

## 7.2 命令手册

### 7.2.1 config memory-threshold

【功能描述】

**config memory-threshold** 用于开启内存门限功能，并进入内存门限视图。

**no config memory-threshold** 用于退出内存门限视图，并关闭内存门限功能。

【命令格式】

[no] **config memory-threshold**

【视图】

根视图

【缺省情况】

内存门限功能默认开启。

【参数说明】

无

【使用举例】

```
NOS# config memory-threshold
NOS(memory-threshold)#
```

【注意事项】

该功能默认开启

### 7.2.2 monitor process

【功能描述】

**monitor process** 命令用于动态显示当前进程信息，动态更新周期为 1 秒。

【命令格式】

**monitor process** [**sort-by** <**cpu**|**memory**|**time**>]

【视图】

根视图

【缺省情况】

不涉及

【参数说明】

- **sort-by**：按指定方式排序，缺省为按进程 ID 降序排列。
- **cpu**：按当前 CPU 占用率降序排列。
- **memory**：按当前内存占用率降序排列。
- **time**：按总 CPU 使用时间降序排列。

【使用举例】

```
NOS# monitor process

Mem: 798556K used, 214164K free, 1668K shrd, 69976K buff, 287632K cached
CPU:  1.4% usr  0.8% sys  0.0% nic 97.6% idle  0.0% io  0.0% irq  0.0% sirq
Load average: 0.01 0.03 0.00 1/131 8087
  PID  PPID USER     STAT   VSZ %VSZ %CPU COMMAND
 8087  8085 root     R     4824  0.4  0.1 top -d 3 -
 8085  8015 root     S     4688  0.4  0.0 sh -c echo "N" | top -d 3 - 2>&1
 8081     2 root     IW       0  0.0  0.0 [kworker/0:0-eve]
 8052     2 root     IW       0  0.0  0.0 [kworker/0:1-mm_]
 8019     2 root     IW       0  0.0  0.0 [kworker/0:2-mm_]
 8015   892 root     S     108m 10.9  0.0 minish
 7935     1 root     S     2928  0.2  0.1 /sbin/logread -f -h NOS -r 192.168.201
 7934     1 logd     S     4932  0.4  0.0 /sbin/logd -S 1024 -l 3 -M 10 -F 3
 7755     2 root     IW       0  0.0  0.0 [kworker/u4:0-ev]
```

【注意事项】

- 此命令只显示前 20 个进程，如果需要查看所有进程信息，请使用 show process 命令。
- 如要退出显示，可使用“Ctrl^c”断开。

### 7.2.3 ratio critical

【功能描述】

**ratio critical** 用于设置内存门限阈值。

**no ration critical** 用于恢复缺省值。

【命令格式】

**ratio critical** *MEMORY_RATIO*

**no ratio critical**

【视图】

内存门限视图

【缺省情况】

缺省情况各产品不同

【参数说明】

*MEMORY_RATIO*：内存占用率阈值百分比，各产品的可选范围不同。内存使用率大于等于这个值会启动内存门限功能。首先会重启 logd 日志进程；如果内存使用率没有下降到配置值以下，会强制登录用户退出；如果内存使用率仍然没有下降到配置值以下，将会重启设备。

【使用举例】

# 将内存门限阈值设置为 66%：

```
NOS#(memory-threshold)# ratio critical 66
```

【注意事项】

请根据配置情况合理配置内存门限阈值。

### 7.2.4 show cpu-usage

【功能描述】

**show cpu-usage** 命令用于显示 CPU 占用情况。

【命令格式】

**show cpu-usage** [**history**] [**json**]

【视图】

任意视图

【缺省情况】

不涉及

【参数说明】

- **history**：如果指定该参数，表示显示历史数据，包括最近 5 秒、最近 1 分钟、最近 5 分钟的 CPU 平均占用率。如果不指定该参数，表示显示当前实时的 CPU 占用率情况。
- **json**：以 json 格式输出。

【使用举例】

#显示当前 CPU 占用率。

```
NOS# show cpu-usage
 CPU    User    Kernel  IOWait  HardIRQ  SoftIRQ  Idle
 -----  ------  ------  ------  -------  -------  ------
  Total   1.0%    1.0%    0.0%     0.0%     0.0%   98.0%
   cpu0   1.0%    1.0%    0.0%     0.0%     0.0%   98.0%
```

#显示历史 CPU 占用率。

```
NOS# show cpu-usage history
 Total:
     0%  in last 5 seconds
     0%  in last 60 seconds
     0%  in last 300 seconds
 cpu0:
     0%  in last 5 seconds
     0%  in last 60 seconds
     0%  in last 300 seconds
```

【注意事项】

无

### 7.2.5 show memory-usage

【功能描述】

show memory-usage 命令用于显示设备内存占用情况。

【命令格式】

show memory-usage [history][json]

【视图】

任意视图

【缺省情况】

不涉及

【参数说明】

- history：如果指定该参数，表示显示历史数据，包括最近 5 秒、最近 1 分钟、最近 5 分钟的 CPU 平均占用率。如果不指定该参数，表示显示当前实时的 CPU 占用率情况。
- json：以 json 格式输出。

【使用举例】

#显示当前内存占用率。

```
NOS# show memory-usage
MemTotal:       4037616 kB
MemFree:        3779120 kB
MemAvailable:    3872448 kB
Buffers:          39392 kB
Cached:          101968 kB
```

#显示历史内存占用率。

```
NOS# show memory-usage history
   2%  in last 5 seconds
   2%  in last 60 seconds
   2%  in last 300 seconds
```

【注意事项】

无

### 7.2.6 show process

【功能描述】

show process 命令用于显示当前运行的进程情况（包括内核线程）。

【命令格式】

show process [{sort-by <cpu|memory>}]

【视图】

任意视图

【缺省情况】

不涉及

【参数说明】

- sort-by：按指定方式排序，缺省为按进程 ID 升序排列。
- cpu：按当前 CPU 占用率降序排列。

- **memory**：按当前内存占用率降序排列。

【使用举例】

#显示当前进程占用率。

```
NOS# show process
Mem: 798384K used, 214336K free, 1668K shrd, 69976K buff, 287632K cached
CPU:  0.0% usr  4.5% sys  0.0% nic 95.4% idle  0.0% io  0.0% irq  0.0% sirq
Load average: 0.08 0.04 0.01 1/133 8094
  PID  PPID USER     STAT   VSZ %VSZ %CPU COMMAND
    1     0 root     S     3932  0.3  0.0 /sbin/procd
    2     0 root     SW       0  0.0  0.0 [kthreadd]
    3     2 root     IW<      0  0.0  0.0 [rcu_gp]
    4     2 root     IW<      0  0.0  0.0 [rcu_par_gp]
    6     2 root     IW<      0  0.0  0.0 [kworker/0:0H-kb]
    8     2 root     IW<      0  0.0  0.0 [mm_percpu_wq]
    9     2 root     SW       0  0.0  0.0 [ksoftirqd/0]
   10     2 root     IW       0  0.0  0.0 [rcu_preempt]
   11     2 root     SW       0  0.0  0.0 [migration/0]
   12     2 root     SW       0  0.0  0.0 [cpuhp/0]
   13     2 root     SW       0  0.0  0.0 [cpuhp/1]
   14     2 root     SW       0  0.0  0.0 [migration/1]
   15     2 root     SW       0  0.0  0.0 [ksoftirqd/1]
   17     2 root     IW<      0  0.0  0.0 [kworker/1:0H-kb]
   18     2 root     IW<      0  0.0  0.0 [netns]
   21     2 root     SW       0  0.0  0.0 [rcu_tasks_kthre]
   24     2 root     IW       0  0.0  0.0 [kworker/1:1-eve]
  217     2 root     SW       0  0.0  0.0 [oom_reaper]
  218     2 root     IW<      0  0.0  0.0 [writeback]
--More--
```

【注意事项】

该命令显示的各业务进程占用的内存信息为虚拟内存，并不是真实占用的物理内存大小，后者一般会小于前者。

## 7.3 配置举例

设置内存门限阈值为百分之 80。

```
config memory-threshold
  ratio critical 80
```

## 7.4 常见问题

待补充。

# 8 硬件管理

## 8.1 功能介绍

除了 CPU/内存/磁盘外，交换机或路由器设备一般还有电源、风扇、温度传感器、光模块、指示灯、业务口、网管口。对这些硬件单元的运行状态可以进行监控和配置。

## 8.2 命令手册

### 8.2.1 config temperature-limit

【功能描述】

**config temperature-limit** 命令用于配置 mac 芯片温度的监控阈值

**no config temperature-limit** 命令用于取消 mac 芯片温度监控

【命令格式】

**config temperature-limit** *LOW_LIMIT WARNING_LIMIT ALARM_LIMIT*

**no config temperature-limit**

【视图】

根视图

【缺省情况】

取决于实际产品类型

【参数说明】

- *LOW_LIMIT*：指定温度限制的最低限度，取值范围为(-50-50)。如果温度低于该值，会打印 Warning 级别的日志。
- *WARNING_LIMIT*：指定温度限制的警告限度，取值范围为(31-140)。如果温度高于该值，会打印 Warning 级别的日志。
- *ALARM_LIMIT*：指定温度限制的报警限度，取值范围为(51-140)。如果温度高于该值，会打印 Alert 级别的日志。

【使用举例】

#设置温度最低，告警，报警限度为-50，50，100。

```
NOS# config temperature-limit -50 50 100
NOS# 2024/01/01 13:19:14 [  warn] diagd: Temperature is greater than the high-temperature warning threshold on sensor(55 C).
```

【注意事项】

无

### 8.2.2 cpld update

【功能描述】

**cpld update** *FILE* 命令用于在线升级 CPLD 逻辑固件。

【命令格式】

**cpld update** *FILE INDEX*

【视图】

根视图

【缺省情况】

无

【参数说明】

*INDEX*：选择 CPLD 逻辑槽位为第几片逻辑，范围为（1-2）。

【使用举例】

```
NOS# cpld update YLSP8FTCPUA_08.pef 1
System will reboot after cpld update successful, Continue? [Y/N]y
```

【注意事项】

升级逻辑文件会触发设备自动重启。

### 8.2.3 show device-info

【功能描述】

**show device-info** 命令用于显示设备信息，包括硬件、电子标签、制造信息等。

【命令格式】

**show device-info**

【视图】

任意视图

【缺省情况】

不涉及

【参数说明】

无。

【使用举例】

#显示当前设备信息。

```
NOS# show device-info
FLASH size      : 7.9M
DRAM size       : 484.82M
Vendor          :
Device name     :
Device ID       :
Device MAC      :
Manufacture date:
Product version : r101
Platform version: V100R006B07D001
Additional infor:
```

【注意事项】

无

### 8.2.4 show environment

【功能描述】

**show environment** 命令用于显示 mac 芯片温度及阈值信息

【命令格式】

**show environment**

【视图】

任意视图

【缺省情况】

无

【参数说明】

无

【使用举例】

#显示当前设备的温度信息。

```
NOS# show environment
Temperature        Lower         Warning       Alarm
-------------------------------------------------------------------
  74               -40           99            102
NOS#
```

【注意事项】

无

### 8.2.5 show fan

【功能描述】

**show fan** 命令用于显示风扇状态

【命令格式】

**show fan status**

【视图】

任意视图

【缺省情况】

无

【参数说明】

无

【使用举例】

#显示当前设备的风扇状态信息。

```
NOS# show fan status
Fan 0 State: Invalid
Fan 1 State: Invalid
Fan 2 State: Normal
Set PWM Fan Frame 2 Rate is 30
NOS#
```

【注意事项】

无

### 8.2.6 show power status

【功能描述】

**show power status** 命令用于显示电源状态

【命令格式】

**show power status**

【视图】

任意视图

【缺省情况】

无

【参数说明】

无

【使用举例】

#显示当前设备的电源状态信息。

```
NOS# show power status
Power 1 is Absent
Power 2 is Normal
```

【注意事项】

无

### 8.2.7 show sfp

【功能描述】

**show sfp information** 命令用来显示光模块的基础信息和诊断信息（DDM）。

**show sfp temperature** 命令用来显示光模块当前的温度。

【命令格式】

**show sfp** <**information**|**temperature**> **interface** <*SWITCH_IF*|**all**>

【视图】

任意视图

【缺省情况】

无

【参数说明】

*SWITCH_IF*：指定显示接口号的以太接口名称，**all** 表示所有接口。

【使用举例】

#显示当前设备的光模块信息。

```
NOS# show sfp information interface all

Current interface : ge1/0/25
Current state     : absent
```

```
Current interface : ge1/0/26
Current state     : absent

Current interface : ge1/0/27
Current state     : absent

Current interface : ge1/0/28
Current state     : absent

Current interface : ge1/0/29
Current state     : absent
```

【注意事项】

无

### 8.2.8 show temperature

【功能描述】

**show temperature** 命令用来显示设备上各关键部件的温度信息。

【命令格式】

**show temperature**

【视图】

任意视图

【缺省情况】

无

【参数说明】

无

【使用举例】

#显示当前设备上的温度信息：

```
NOS# show temperature
Current CPU temperature: 78 (degree centigrade)
Current MAC temperature: 81 (degree centigrade)
Current system temperature: 56 (degree centigrade)
```

【注意事项】

无

# 9 PoE

## 9.1 功能介绍

PoE(Power over Ethernet)即以太网供电、远程供电。是通过网线传输电力的一种技术，借助现有以太网通过网线同时为 IP 终端设备进行传输和供电。

PoE 供电系统包括两个设备角色：

- 供电设备 PSE(Power-sourcing Equipment):通过以太网给受电设备供电的 PoE 设备。
- 受电设备 PD(Powered Device)：受电方设备，分为标准 PD 和非标准 PD。

## 9.2 命令手册

### 9.2.1 config poe

【功能描述】

**config poe** 命令用于开启 PoE 功能并进入 poe 视图。

【命令格式】

[no] **config poe**

【视图】

根视图

【缺省情况】

PoE 功能默认开启

【参数说明】

无

【使用举例】

#启动 poe 功能：

```
NOS# config poe
NOS(poe)#
```

【注意事项】

无

### 9.2.2 poe enable

【功能描述】

**poe enable** 命令用于开启接口的 PoE 功能。

**no poe enable** 命令用于关闭接口的 PoE 功能。

【命令格式】

**poe enable** [**time-range** *NAME*]

**no poe enable**

【视图】

二层物理接口视图

【缺省情况】

接口下 PoE 功能默认开启

【参数说明】

**time-range** *NAME*：指定时间段的名称，用于按时间段生效 PoE，长度（1～31）不允许包含字母、数字以外的字符。

【使用举例】

# 在名称为 night 的时间段内使能接口 ge2 的 poe 功能。

```
NOS# config interface  ge2
NOS(if-ge2)# poe enable time-range night
```

【注意事项】

无

### 9.2.3 poe high-inrush enable

【功能描述】

**poe high-inrush enable** 命令用于配置允许高冲击电流通过。

**no poe high-inrush enable** 用来恢复默认情况。

【命令格式】

**poe high-inrush enable**

**no poe high-inrush enable**

【视图】

二层物理接口视图

【缺省情况】

默认禁止高冲击电流通过

【参数说明】

无

【使用举例】

# 接口 ge1 配置允许高冲击电流通过。

```
NOS# config interface ge1
NOS(if-ge1)# poe high-inrush enable
```

【注意事项】

- PD 上电瞬间、或 PD 受电过程中可能产生高冲击电流，该电流会导致 PSE 自我保护并对 PD 断电。这时如果仍然需要为 PD 供电，则需要配置该命令允许 PD 的高冲击电流。
- 高冲击电流可能会损坏设备元器件，请谨慎配置该功能。

### 9.2.4 poe legacy enable

【功能描述】

**poe legacy enable** 命令用于使能非标供电。

**no poe legacy enable** 命令用来关闭非标供电。

【命令格式】

[no] **poe legacy enable**

【视图】

PoE 视图

【缺省情况】

未开启非标供电功能

【参数说明】

无

【使用举例】

```
NOS# config poe
NOS(poe)# poe legacy enable
```

【注意事项】

非标供电即不做 class 分级直接供电，有可能会损坏 PD，请谨慎使用。

### 9.2.5 poe max-power

【功能描述】

**poe max-power** 命令用于修改接口的 PoE 最大供电功率。

【命令格式】

**poe max-power** *MAX_POWER*

【视图】

二层物理接口视图

【缺省情况】

缺省情况接口最大供电功率为 30000 毫瓦（即 30 瓦）。

【参数说明】

*MAX_POWER*：取值范围(1000～30000)，接口的最大供电功率，单位为毫瓦(mW)。

【使用举例】

配置接口 ge2 的最大供电功率为 15000 毫瓦（即 15 瓦）。

```
NOS# config interface ge2
NOS(if-ge2)# poe max-power 15000
```

【注意事项】

无

### 9.2.6 poe pd-policy enable

【功能描述】

**poe pd-policy enable** 命令用于使能 POE 系统根据端口实际供电功率和端口配置的供电优先级进行动态电源管理模式

**no poe pd-policy enable** 命令用于恢复 PoE 系统默认电源管理模式

【命令格式】

[no] **poe pd-policy enable**

【视图】

PoE 视图

【缺省情况】

PoE 系统根据端口实际供电功率进行动态电源管理

【参数说明】

无

【使用举例】

```
NOS# config poe
NOS(poe)# poe pd-policy enable
NOS(poe)#
```

【注意事项】

默认所有端口的供电优先级都是 low

### 9.2.7 poe priority

【功能描述】

**poe priority** 命令用于修改 PoE 接口供电优先级，以便在 PSE 过载时决定是否给 PD 供电。

【命令格式】

**poe priority** <**low**|**high**|**critical**>

【视图】

二层物理接口视图

【缺省情况】

缺省情况接口优先级为低（**low**）。

【参数说明】

- **low**：设置该接口的供电优先级为低。
- **high**：设置该接口的供电优先级为高。
- **critical**：设置该接口的供电优先级为最高。

【使用举例】

```
NOS# config interface ge1
NOS(if-ge1)# poe priority high
```

【注意事项】

各优先级下的供电原则如下：

- 如果某个 PD 功率增大导致 PSE 功率过载，则停止对该 PD 供电。
- 如果新接入 PD 时导致 PSE 功率过载，则优先级高的 PD 优先供电；如果优先级相同，则先接入的优先供电。
- 如果多个 PoE 接口优先级相同，接口编号小的优先供电。

### 9.2.8 poe threshold

【功能描述】

**poe threshold** 命令用于配置 POE 设备整机正常供电功率水线，防止超过整机最大供电功率

**no poe threshold** 命令用于恢复 PSE 设备的功率水线为缺省配置。

【命令格式】

**poe threshold** *THRESHOLD*

**no poe threshold**

【视图】

PoE 视图

【缺省情况】

PSE 设备的功率水线为 90%。

【参数说明】

*THRESHOLD*：取值范围(1～99)，PSE 设备的功率水线，单位为百分比。

【使用举例】

```
NOS# config poe
NOS(poe)# poe threshold 60
```

【注意事项】

无

### 9.2.9 poe update

【功能描述】

**poe update** 命令用于在线升级 PoE 固件。

【命令格式】

**poe update** *FILE*

【视图】

PoE 视图

【缺省情况】

无

【参数说明】

*FILE*：版本文件名称，文件必须在/home/flash 目录下，必须是 bin 文件，文件名称长度小于 128。

【使用举例】

#在线升级 PoE 固件。

```
NOS# config poe
NOS(poe)# poe update poe_update.bin
Update poe pse, waiting.....
```

【注意事项】

无

### 9.2.10 show poe device

【功能描述】

**show poe device** 命令用于查看 PSE 设备的版本信息及相关配置信息。

【命令格式】

**show poe device**

【视图】

任意视图

【缺省情况】

无

【参数说明】

无

【使用举例】

# 查看 PoE 设备及配置信息：

```
NOS# show poe device
PSE Version:                        10-10
PSE PD-policy:                      enable
PSE Curent Power:                   0mW
PSE Max Power:                      780000mW
PSE Legacy Detection:               disable
PSE Utilization-threshold:          90%
NOS#
```

【注意事项】

无

### 9.2.11 show poe interface

【功能描述】

**show poe interface** 命令用于查看 POE 接口配置信息。

【命令格式】

**show poe interface** [*L2_ETH_IF*]

【视图】

任意视图

【缺省情况】

无

【参数说明】

*L2_ETH_IF*：二层物理接口，如果不选则显示所有。

【使用举例】

# 查看 PoE 接口配置信息：

```
NOS# show poe interface ge1
Interface  Enable  Priority  CurPower(mW)  MaxPower(mW) Class Status State
ge1        enable   low       0             30000        0     Searching
NOS#
```

【注意事项】

无

# 10 配置克隆

## 10.1 功能介绍

通过二层私有协议，在当前设备上广播配置到网络中的所有设备（强制接受、或空配置才接受），方便快速批量配置，甚至 OS 版本。

### 10.1.1 配置同步

所有设备应默认开启该功能，然后要能在 Master 上将配置同步到所有 slave 设备，同时能看到进展。具体如下：

- 在 master 上能看到所有 slave 列表，包括 slave 编号、接入端口名、系统 MAC（最好还能显示设备型号、当前软件版本、SN）。其中 slave 编号从 1 开始，要按接入端口排序（同一端口下的多个 slave 按 MAC 排序）。
- 能在 master 上主动发起配置同步过程（异步执行），随时查看各 slave 的同步进展和状态（包括：未开始、同步中、同步成功、同步失败），能按状态筛选（支持多选）。
- 同步成功的 slave 设备，自动 save 并设置为下次启动。
- 为支持给不同 slave 配置不同的 IP 或设备名称等需求，支持在配置中含变量 i（i 为 slave 编号），建议按 shell 风格，如“$((i + 100)) ”。
- 支持一些扩展控制选项，例如：同步成功后是否要自动重启、是否只在 slave 为空配置启动时才需要同步。

### 1.1.2 版本同步

具体功能类似配置同步，但发起命令行不同，具体如下：

- 在 master 上能看到所有 slave 列表，同配置同步一致。
- 能在 master 上主动发起版本同步过程（异步执行），同配置同步一致。
- 同步成功的 slave 设备，自动设置为主启动文件。
- 支持一些扩展控制选项，例如：同步成功后是否要自动重启、如果 flash 不够是否自动覆盖旧版本文件、同步成功后是否要恢复出厂设置。

## 10.2 命令手册

### 10.2.1 config clone-agent

【功能描述】

**config clone-agent** 命令用于启动配置克隆进程，进入 clone-agent 视图

**no config clone-agent** 命令用于关闭配置克隆进程，退出 clone-agent 视图

【命令格式】

[no] **config clone-agent**

【视图】

根视图

【缺省情况】

默认开启该特性

【参数说明】

无

【使用举例】

```
NOS# config clone-agent
NOS(clone-agent)#
```

【注意事项】

无

### 10.2.2 mode

【功能描述】

**mode** 命令用于配置当前克隆模式

**no mode** 命令用于恢复成默认模式

【命令格式】

**mode** < *master* | *slave* >

【视图】

clone-agent 视图

【缺省情况】

默认为 slave

【参数说明】

**master**：配置为主模式，向 slave 发送数据

**slave**：从模式，接受 master 发来的配置文件等

【使用举例】

```
NOS(clone-agent)#
NOS(clone-agent)# mode master
```

### 10.2.3 start discover

【功能描述】

start **discover** 命令用于发现下游 slave 设备。

【命令格式】

**start discover** [**timeout** *(3 - 180)*]

【视图】

clone-agent 视图

【缺省情况】

默认发现时间为 10 秒

【参数说明】

**timeout**：在指定时间内进行设备发现，超时后即使有新设备接入，也不进行传输，需要重新进行发现

【使用举例】

```
NOS(clone-agent)# start discover
NOS(clone-agent)# show clone status
```

```
Current clone file :
Idx Interface MAC             Model          Status
--- --------- ----------------- -------------- ----------
1   ge1/0/1   50:d3:3b:2e:15:01               INIT
2   ge1/0/4   50:d3:3b:2e:15:01               INIT
```

【注意事项】

有新设备接入后可通过 log 查看设备信息，也可通过 show clone devive 查看设备信息

### 10.2.4 start config-clone

【功能描述】

**start config-clone** 命令用于启动配置克隆。

【命令格式】

**start config-clone [advance] file CONFIG-FILE [{reboot-after-complete | only-for-initial-device}][slave** *SLAVE*] **user-name** *USER-NAME* **user-password** *USER-PASSWORD*

【视图】

clone-agent 视图

【缺省情况】

不涉及

【参数说明】

- **advance**：高级模式，该模式下可支持在配置文件中使用变量 i（目标设备编号）、以及数学运算（加、减、乘、除、取余），表达式为 bash 风格，例如“$((i + 100))”。
- *CONFIG-FILE*：配置模板文件。如果选择了 **advance** 模式，则会对其中包含变量 i 的表达式进行运算和替换；否则不会进行解析处理，按完全相同的配置进行同步。
- **reboot-after-complete**：设置在同步完成后自动重启目标设备（以新配置启动）。默认不会自动重启（但会设置下次以新配置启动）。
- **only-for-initial-device**：设置只针对初始状态的设备，未指定启动文件（即当前配置为空）进行配置同步。默认针对所有目标设备。
- **user-name**：指定 slave 的用户名。
- **user-password**：指定 slave 的密码。
- **slave**：向指定 slave 传输配置（slave 编号可在 show clone device 查看）。

【使用举例】

```
NOS(clone-agent)# start config-clone file startup.conf user-name root user-password 123456
NOS(clone-agent)#
```

【注意事项】

- 该命令会以异步方式启动同步过程，可使用 **show clone status** 查看同步状态。
- 配置同步和版本同步不能同时进行，也不能在上一次同步未结束时开启新同步。
- 配置同步前，请先使用 **show clone device** 查看设备情况。
- 指定用户名和密码需要和 slave 上一致才能通过认证进行传输。

### 10.2.5 start software-clone

【功能描述】

**start software-clone** 命令用于启动软件版本克隆。

【命令格式】

start software-clone *IMAGE-FILE* [{reboot-after-complete | overwrite-while-no-space | restore-factory-after-complete}] [slave *SLAVE*] user-name *USER-NAME* user-password *USER-PASSWORD*

【视图】

clone-agent 视图

【缺省情况】

不涉及

【参数说明】

- IMAGE-FILE：软件版本文件。
- **reboot-after-complete**：设置在同步完成后自动重启目标设备（以新版本启动）。默认不会自动重启。
- **overwrite-while-no-space**：设置在目标设备 flash 空间不足时，自动删除旧版本文件以释放空间。默认不会自动删除。（传输时把版本大小传到 slave，slave 进行判断空间是否充足）
- **restore-factory-after-complete**：设置在同步完成后自动将目标设备恢复到出厂设置状态。默认保持状态不变。
- **user-name**：指定 slave 的用户名。
- **user-password**：指定 slave 的密码。
- **slave**：向指定 slave 传输配置（slave 编号可在 show clone device 查看）。

【使用举例】

```
NOS(clone-agent)# start software-clone cnos.image user-name root user-password 123456
NOS(clone-agent)#
```

【注意事项】

- 该命令会以异步方式启动同步过程，可使用 **show clone status** 查看同步状态。
- 配置同步和版本同步不能同时进行，也不能在上一次同步未结束时开启新同步。
- 目标设备在同步成功后，会设置新版本为主启动版本。
- 版本同步前，建议先使用 **show clone device** 查看设备情况。
- 指定用户名和密码需要和 slave 上一致才能通过认证进行传输。

### 10.2.6 stop clone

【功能描述】

**stop clone** 命令用于终止当前进行中的配置或软件版本克隆。

【命令格式】

stop clone

【视图】

clone-agent 视图

【缺省情况】

不涉及

【参数说明】

无

【使用举例】

```
NOS(clone-agent)# stop clone
NOS(clone-agent)#
```

【注意事项】

终止克隆时，不会对已完成的克隆进行回退。

### 10.2.7 show clone device

【功能描述】

**show clone device** 命令用于显示可以参与克隆的目标设备列表。

【命令格式】

**show clone device**

【视图】

clone-agent 视图

【缺省情况】

不涉及

【参数说明】

无

【使用举例】

```
# 查看设备列表：
NOS(clone-agent)# show clone device
Current clone file : /home/flash/startup.conf
Idx Interface MAC             Model          Version            SN
--- --------- ----------------- ---------------- -------------------- ----------------
1   ge1/0/1   50:d3:3b:2e:15:01               trunk
2   ge1/0/4   50:d3:3b:2e:15:01               trunk
NOS(clone-agent)#
```

【注意事项】

无

### 10.2.8 show clone status

【功能描述】

**show clone status** 命令用于显示当前克隆状态。

【命令格式】

**show clone status [include {init | sync | success | failed | skip | stop}]**

【视图】

根视图

【缺省情况】

不涉及

【参数说明】

无

【使用举例】

# 查看同步状态：

```
NOS(clone-agent)# show clone status
Current clone file : /home/flash/startup.conf
Idx Interface MAC            Model          Status
--- --------- ---------------- --------------- ----------
1   ge1/0/1   50:d3:3b:2e:15:01               CONFIG_SUCCESS
2   ge1/0/4   50:d3:3b:2e:15:01               SKIP
NOS(clone-agent)#
```

Status 说明：

- Init：初始状态（未开始同步）。
- Skip：跳过。
- Sync：同步中。
- Success：同步结束并成功。(同步结束并成功，用户可以安全移除)
- Failed：同步失败。
- stop：同步停止。

【注意事项】

此命令显示的是最近一次同步的结果，如果 master 重启，则所有状态信息都会被清除。

# 11 智能诊断

## 11.1 功能介绍

由 HIG（Health Intelligent Guidance，健康智能运维）模块实时监听各模块异常信息。出现异常时，HIG 模块收集展示告警信息，并进行异常处理或给出处理建议。可展示当前告警和历史告警。

## 11.2 命令手册

### 11.2.1 config hig

【功能描述】

**config hig** 命令用于开启 hig 功能并进入 hig 视图。

【命令格式】

[no] **config hig**

【视图】

根视图

【缺省情况】

hig 功能默认开启

【参数说明】

无

【使用举例】

#启动 hig 功能：

```
NOS# config hig
```

```
NOS(hig)#
```

【注意事项】

无

### 11.2.2 show hig history-alm

【功能描述】

展示历史告警信息。

【命令格式】

**show hig history-alm <id** *ID*> [**offset** *OFFSET*] [**json** *JSON*]

【视图】

任意视图

【缺省情况】

无

【参数说明】

- id：打印该 id 类型的历史告警
- offset：按照偏移量打印历史告警
- json：以 json 格式打印

【使用举例】

```
NOS# show hig history-alm id 1
```

【注意事项】

无

### 11.2.3 show hig current-alm

【功能描述】

展示当前告警信息

【命令格式】

**show hig current-alm** [**json** *JSON*]

【视图】

任意视图

【缺省情况】

无

【参数说明】

json:以 json 格式打印

【使用举例】

```
NOS# show hig current-alm
```

【注意事项】

无

### 11.2.4 show hig current-alm-num

【功能描述】

展示当前告警信息数量。

【命令格式】

**show hig current-alm-num** [**json** *JSON*]

【视图】

任意视图

【缺省情况】

无

【参数说明】

json:以 json 格式打印

【使用举例】

```
NOS# show hig current-alm-num
```

【注意事项】

无

### 11.2.5 show hig policy-alm

【功能描述】

显示智能诊断告警策略。

【命令格式】

show hig policy-alm

【视图】

任意视图

【缺省情况】

无

【参数说明】

无

【使用举例】

#启动 hig 功能:

```
NOS# show hig policy-alm
```

【注意事项】

无

### 11.2.6 clear hig alm

【功能描述】

清除当前告警信息。

【命令格式】

**clear hig alm** <**id** *ID*> <**option** *OPTION* | **interface** *L2_IF*>

【视图】

hig 视图

【缺省情况】

无

【参数说明】

- id：清除该 id 类型的当前告警。
- option：按照偏移量清除当前告警。
- interface：清除该端口当前告警。

【使用举例】

```
NOS# clear hig alm id 1
```

【注意事项】

无

### 11.2.7 restory hig alm

【功能描述】

清除告警信息。

【命令格式】

**restory hig alm <id** *ID*> **<option** *OPTION* | **interface** *L2_IF*>

【视图】

hig 视图

【缺省情况】

无

【参数说明】

- id：清除该 id 类型的告警。
- option：按照偏移量清除告警。
- interface：清除该端口告警。

【使用举例】

```
NOS# restory hig alm id 1
```

【注意事项】

无

# 12 网络诊断

## 12.1 功能介绍

通过网络诊断相关工具，可以快速检测网络是否可达、链路是否通畅，辅助问题定位。

## 12.2 命令手册

### 12.2.1 monitor packet

【功能描述】

**monitor packet** 命令用于实时监控并打印当前设备上收发的网络报文。

【命令格式】

**monitor packet** [{**interface** *IFNAME* | **direction** <**in**|**out**> | **protocol** <**arp**|**stp**|**lldp**|**lacp**|**ip**|**icmp**|**tcp**|**udp**|**ssh**|**dns**|**dhcp**|**telnet**|**igmp**|**ospf**|**ip6**|**pim**|**isis**|**rip**|**snmp**|**ntp**|**ptp**|**mvrp**|**dot1x**> | **verbose** | **dump**}] [**to-file** *FILE*]

【视图】

任意视图

【缺省情况】

不涉及

【参数说明】

- **interface** *IFNAME*：要捕获的接口名称，默认为所有接口。
- **direction** <**in**|**out**>：数据包流向，默认为双向监控。
- **protocol**：只监控指定协议类型的报文，默认为所有协议类型。
- **verbose**：输出详细的报文信息，默认只输出简要信息。
- **dump**：显示报文 16 进制内容。
- **to-file** *FILE*：将监控的报文保存为文件（不打印到屏幕）。

【使用举例】

# 监控 ge1 接口流量信息：

```
NOS# monitor packet interface ge1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ge1, link-type EN10MB (Ethernet), capture size 262144 bytes
```

【注意事项】

- 此功能仅对上 CPU 的报文生效（一般是协议报文、或从网管口传输的报文），纯硬件转发的过路报文无法监控。
- 使用 Ctrl^C 结束监控。

### 12.2.2 ping

【功能描述】

**ping** 命令用于检测指定 IP 地址是否可达，并输出相应的统计信息。

【命令格式】

**ping** [<**interface** *IF_NAME* | **source** *A.B.C.D*>] [{**count** *COUNT* | **size** *SIZE* }] *HOST*

【缺省情况】

不涉及。

【参数说明】

- **interface** *IF_NAME*：指定出接口名称，同时使用该接口 IP 做为报文源 IP。
- **source** *A.B.C.D*：指定报文源 IPv4 地址。

- **count** *COUNT*：要发送的报文数量，取值范围为(1～65535)，默认不限数量，即持续发送。
- **size** *SIZE*：报文数据填充部分的字节数（不含协议头），取值范围为(1～65535)，默认 56。
- *HOST*：目标地址，支持 IP 地址格式和主机名格式。

【使用举例】

```
# 检测 192.168.1.77 地址是否可达：
NOS# ping 192.168.1.77
PING 192.168.1.77 (192.168.1.77): 56 data bytes
64 bytes from 192.168.1.77: seq=0 ttl=128 time=1.037 ms
64 bytes from 192.168.1.77: seq=1 ttl=128 time=1.028 ms
64 bytes from 192.168.1.77: seq=2 ttl=128 time=1.002 ms
^C
--- 192.168.1.77 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 1.002/1.022/1.037 ms
```

【注意事项】

无

### 12.2.3 ping ipv6

【功能描述】

**ping ipv6** 命令用于检测指定 IPv6 地址是否可达，并输出相应的统计信息。

【命令格式】

**ping ipv6** [<**interface** *IF_NAME* | **source** *X:X::X:X*>] [{**count** *COUNT* | **size** *SIZE* }] *HOST*

【缺省情况】

不涉及。

【参数说明】

- **interface** *IF_NAME*：指定出接口名称，同时使用该接口 IPv6 地址做为报文源地址。
- **source** *X:X::X:X*：指定报文源 IPv6 地址。
- **count** *COUNT*：要发送的报文数量，取值范围为(1～65535)，默认不限数量，即持续发送。
- **size** *SIZE*：报文数据填充部分的字节数（不含协议头），取值范围为(1～65535)，默认 56。
- *HOST*：目标地址，支持 IPv6 地址格式和主机名格式。

【使用举例】

```
NOS# ping ipv6 11:22::33:44
PING 11:22::33:44 (11:22::33:44): 56 data bytes
```

【注意事项】

无

### 12.2.4 traceroute

【功能描述】

**traceroute** 命令用于查看报文经过的路径。

【命令格式】

**traceroute** [**interface** *L3_IF*] *HOST*

【缺省情况】

不涉及

【参数说明】

**interface** *L3_IF*：指定源接口。

*HOST*：目标地址，支持 IP 地址格式和主机名格式。

【使用举例】

```
NOS# traceroute 192.168.1.77
traceroute to 192.168.1.77 (192.168.1.77), 30 hops max, 46 byte packets
 1  192.168.1.77 (192.168.1.77)  0.861 ms  *  0.822 ms
```

【注意事项】

无

### 12.2.5 traceroute ipv6

【功能描述】

**traceroute ipv6** 命令用于查看 IPv6 报文经过的路径。

【命令格式】

**traceroute ipv6** [**interface** *L3_IF*] *HOST*

【缺省情况】

不涉及

【参数说明】

- **interface** *L3_IF*：指定源接口。
- *HOST*：目标地址，支持 IPv6 地址格式和主机名格式。

【使用举例】

```
NOS# traceroute ipv6 11:22::33:44
```

【注意事项】

如果指定的目标地址是 IPv6 的 LinkLocal 地址，则必须指定源接口。

## 12.3 配置举例

(1) 实时监控并打印 ge1 接口上收发的网络报文

(2) 检测 192.168.1.77 的 IP 地址是否可达，并输出相应的统计信息

(3) 查看报文经过 192.168.1.77 的路径

```
NOS# monitor packet interface ge1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ge1, link-type EN10MB (Ethernet), capture size 262144 bytes
21:47:50.443062 IP 192.168.1.77 > 192.168.1.201: ICMP echo request, id 1, seq 106, length
40
21:47:50.443280 IP 192.168.1.201 > 192.168.1.77: ICMP echo reply, id 1, seq 106, length 40
21:47:51.444717 IP 192.168.1.77 > 192.168.1.201: ICMP echo request, id 1, seq 107, length
40
21:47:51.444937 IP 192.168.1.201 > 192.168.1.77: ICMP echo reply, id 1, seq 107, length 40
21:47:52.447331 IP 192.168.1.77 > 192.168.1.201: ICMP echo request, id 1, seq 108, length
40
```

```
21:47:52.447551 IP 192.168.1.201 > 192.168.1.77: ICMP echo reply, id 1, seq 108, length 40
21:47:53.451074 IP 192.168.1.77 > 192.168.1.201: ICMP echo request, id 1, seq 109, length
40
21:47:53.451290 IP 192.168.1.201 > 192.168.1.77: ICMP echo reply, id 1, seq 109, length 40
21:48:06.823852 IP6 fe80::9016:b22a:a231:83f2.dhcpv6-client > ff02::1:2.dhcpv6-server:
dhcp6 solicit

NOS# ping 192.168.1.77
PING 192.168.1.77 (192.168.1.77): 56 data bytes
64 bytes from 192.168.1.77: seq=0 ttl=128 time=2.247 ms
64 bytes from 192.168.1.77: seq=1 ttl=128 time=1.552 ms
64 bytes from 192.168.1.77: seq=2 ttl=128 time=2.235 ms
64 bytes from 192.168.1.77: seq=3 ttl=128 time=1.638 ms
64 bytes from 192.168.1.77: seq=4 ttl=128 time=1.628 ms
64 bytes from 192.168.1.77: seq=5 ttl=128 time=1.297 ms
^C
--- 192.168.1.77 ping statistics ---
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max = 1.297/1.766/2.247 ms

NOS# traceroute 192.168.1.77
traceroute to 192.168.1.77 (192.168.1.77), 30 hops max, 46 byte packets
 1  192.168.1.77 (192.168.1.77)  2.258 ms  *  1.966 ms
```

## 12.4 常见问题

无。

# 13 端口镜像

## 13.1 功能介绍

端口镜像通过将指定端口的报文复制到与数据监测设备相连的端口，使用户可以利用数据监测设备分析这些复制过来的报文，以进行网络监控和故障排除。

### 13.1.1 特性简介

**镜像源：**

镜像源是指被监控的报文源端口，经过镜像源收发的报文会被复制一份到镜像目的端口，这样用户就可以对这些报文（称为镜像报文）进行监控和分析了。

**源设备：**

镜像源所在的设备称为源设备。

**镜像目的：**

镜像目的是指镜像报文所要到达的目的地，即与数据监测设备相连的端口，该端口称为目的端口。目的端口会将镜像报文转发给与之相连的数据监测设备。

由于一个目的端口可以同时监控多个镜像源（反过来，一个镜像源不能复制到多个目的端口），因此在某些组网环境下，目的端口可能收到对同一报文的多份拷贝。例如，目的端口 Port A 同时监控同一台设备上的源端口 Port B 和 Port C 收发的报文，如果某报文从 Port B 进入该设备后又从 Port C 发送出去，那么该报文将被复制两次给 Port A。

**目的设备：**

镜像目的所在的设备称为目的设备。

**镜像方向：**

镜像方向是指在镜像源上可复制哪些方向的报文：

- 入方向：是指仅复制镜像源收到的报文。
- 出方向：是指仅复制镜像源发出的报文。
- 双向：是指对镜像源收到和发出的报文都进行复制。

**镜像组：**

镜像组是一个逻辑上的概念，镜像源和镜像目的都要属于某一个镜像组。根据具体的实现方式不同，镜像组可分为本地镜像组、远程源镜像组和远程目的镜像组。本地镜像组的镜像源和目的为同一台设备，远程镜像组的镜像源和目的为不同设备。

## 13.2 命令手册

### 13.2.1 config mirroring group

【功能描述】

**config mirroring group** 命令创建镜像组并进入镜像组配置视图。

**no config mirroring group** 命令用于删除镜像组。

【命令格式】

**config mirroring group** *GROUP* <**local**|**remote-source**|**remote-destination**>

**no config mirroring group** *GROUP*

【视图】

根视图

【缺省情况】

未配置镜像组

【参数说明】

- *GROUP*：镜像组编号，各产品的范围有所不同。
- **local**：表示本地镜像组。
- **remote-destination**：表示远程目的镜像组。
- **remote-source**：表示远程源镜像组。

【使用举例】

# 配置本地镜像组 1，其中 ge1 和 ge2 为镜像源，ge3 为镜像目的：

```
NOS# config mirroring group 1 local
NOS(mirror-group-1)#
NOS(mirror-group-1)# source-interface ge1 both
NOS(mirror-group-1)# source-interface ge2 both
NOS(mirror-group-1)# destination-interface ge3
```

【注意事项】

部分产品不支持远程镜像配置。

### 13.2.2 destination-interface

【功能描述】

**destination-interface** 命令用于配置镜像组的目的端口。

**no destination-interface** 命令用于删除镜像组目的端口配置。

【命令格式】

**destination-interface** *L2_ETH_IF*

**no destination-interface** *L2_ETH_IF*

【视图】

镜像组视图

【缺省情况】

镜像组不存在目的端口。

【参数说明】

*L2_ETH_IF*：指定镜像目的端口，只能是二层以太口。

【使用举例】

# 配置本地镜像组 1，镜像组的目的端口为 ge3：

```
NOS# config mirroring group 1 local
NOS(mirror-group-1)# destination-interface ge3
```

【注意事项】

镜像组源端口和目的端口不能相同。

### 13.2.3 remote-vlan

【功能描述】

**remote-vlan** 命令用于配置专用的远程镜像 vlan 来传输远程镜像的报文。

**no remote-vlan** 命令用于取消配置远程镜像 vlan。

【命令格式】

**remote-vlan** *VLANID* [**force**]

**no remote-vlan**

【视图】

镜像组视图

【缺省情况】

未配置远程镜像 vlan。

【参数说明】

*VLANID*：专用的远程镜像 vlan id，vlan 范围(1～4094)，该 vlan 不能再做其他用途，以免干扰。

**force**：强制配置，无需用户确认该 vlan 是否有冲突。

【使用举例】

```
NOS(mirror-group-1)# remote-vlan 1
```

【注意事项】

本地镜像组无法下发此配置。

### 13.2.4 reset mirroring configuration

【功能描述】

**reset mirroring configuration** 命令用于删除所有镜像组配置。

【命令格式】

**reset mirroring configuration**

【视图】

任意视图

【缺省情况】

不涉及。

【参数说明】

无。

【使用举例】

```
NOS# reset mirroring configuration
```

【注意事项】

该命令会删除所有镜像配置、且无需确认，请谨慎使用。

### 13.2.5 show mirroring group

【功能描述】

**show mirroring group** 命令用于显示镜像组的配置。

【命令格式】

show mirroring group <all|*GROUP*> [json]

【视图】

任意视图

【缺省情况】

不涉及

【参数说明】

- all：显示所有的镜像组。
- *GROUP*：镜像组的数量，取值范围 1～8。
- json：以 json 格式输出。

【使用举例】

```
# 显示当前所有镜像组的配置：
NOS# show mirroring group all
Mirroring group 1:
Type: Local
Status: Active
Source port:
        ge1 both
        ge2 both
Dest port: ge3
NOS#
```

【注意事项】

无

### 13.2.6 source-interface

【功能描述】

source-interface 命令用于启用配置镜像源端口与镜像组绑定。

no source-interface 命令用于恢复默认配置。

【命令格式】

source-interface *L2_ETH_IF* <both|inbound|outbound>

no source-interface *L2_ETH_IF*

【视图】

镜像组视图

【缺省情况】

镜像组不存在源端口配置。

【参数说明】

- *L2_ETH_IF:* 指定镜像源端口，只能选择二层以太口。
- both：同时监控镜像源端口的发送及接收报文。
- inbound：仅监控镜像源端口接收的报文。
- outbound：仅监控镜像源端口发送的报文。

【使用举例】

# 指定镜像源端口 ge1：

```
NOS# config mirroring group 1 local
NOS(mirror-group-1)# source-interface ge1 both
NOS(mirror-group-1)#
```

【注意事项】

镜像组源端口和目的端口不能相同。

## 13.3 配置举例

(1) 创建本地镜像组

```
NOS# config mirroring group 1 local
```

(2) 将 ge1 ge2 配置为镜像源端口，对出入报文进行镜像

```
NOS(mirror-group-1)#
NOS(mirror-group-1)# source-interface ge1 both
NOS(mirror-group-1)# source-interface ge2 both
```

(3) 配置 ge3 为镜像目的端口

```
NOS(mirror-group-1)# destination-interface ge3
```

# 显示当前所有镜像组的配置：

```
NOS# show mirroring group all
Mirroring group 1:
Type: Local
Status: Active
Source port:
        ge1 both
        ge2 both
Dest port: ge3
```

## 13.4 常见问题

略。

# 14 SNMP

## 14.1 功能介绍

### 14.1.1 特性简介

SNMP（Simple Network Management Protocol）协议也称简单网络管理协议，是 TCP/IP 协议簇的一个应用层协议。在 1988 年被制定，并被 Internet 体系结构委员会（IAB）采纳作为一个短期的网络管理解决方案，依次有 v1/v2c/v3 供三个版本，只有网管和设备的 SNMP 版本号相同时才能互相通信。

- SNMPv1 采用团体名（Community Name）的认证机制，团体名类似于密码，用于网管平台和设备之间的认证配对。
- SNMPv2c 对 SNMPv1 的功能进行了扩展：支持更多的数据类型，提供了更多的操作类型，以及更丰富的错误代码。
- SNMPv3 采用 USM（User-Based Security Model，基于用户的安全模型）认证机制，可以通过配置认证和加密功能，提供更高的安全性。

一套完整的 SNMP 系统主要包括管理信息库（MIB）、管理信息结构（SMI）及 SNMP 报文协议。

## 14.2 命令手册

### 14.2.1 community

【功能描述】

**community** 命令用于配置共同体名称。

**no community** 命令用于恢复缺省情况。

【命令格式】

**community** <**read**|**write**> *COM_NAME*

**no community** <**read**|**write**> *COM_NAME*

【视图】

snmp 视图

【缺省情况】

未配置共同体信息

【参数说明】

- **read**：配置只读权限的共同体
- **write**：配置可读可写权限的共同体。
- *COM_NAME*：共同体名称，最大长度为 31 个字符，只支持字母和数字。

【使用举例】

```
# 配置读写共同体名称为 admin
NOS# config snmp
NOS(snmp)# community write admin
NOS(snmp)#
```

【注意事项】

无。

### 14.2.2 config snmp

【功能描述】

**config snmp** 命令用于启用 SNMP 服务，并进入 SNMP 配置视图。

**no config snmp** 命令用于禁用 SNMP 服务并删除所有 SNMP 配置。

【命令格式】

[no] **config snmp**

【视图】

根视图

【缺省情况】

未启用 SNMP 服务。

【参数说明】

无

【使用举例】

```
# 开启 snmp 功能
NOS# config snmp
NOS(snmp)#
```

【注意事项】

无。

### 14.2.3 contact

【功能描述】

**contact** 命令用于配置 SNMP 中系统维护联系信息。

**no contact** 命令用于恢复 SNMP 中系统维护联系信息为缺省情况。

【命令格式】

**contact** *CONTACT*

**no contact**

【视图】

SNMP 系统配置视图

【缺省情况】

缺省未配置联系信息。

【参数说明】

*CONTACT*：系统维护联系信息。

【使用举例】

```
#配置系统维护联系信息为 10086。
NOS# config snmp
NOS(snmp)# system-configuration
NOS(snmp/system)# contact 10086
```

【注意事项】

无。

### 14.2.4 location

【功能描述】

**location** 命令用于配置 SNMP 中系统物理位置信息。

**no location** 命令用于恢复 SNMP 中系统物理位置信息为缺省情况。

【命令格式】

**location** *LOCAT*

**no location**

【视图】

SNMP 系统配置视图

【缺省情况】

缺省未配置物理位置信息。

【参数说明】

*LOCAT*：系统物理位置信息。

【使用举例】

#配置系统物理位置信息为 HangZhou。

```
NOS# config snmp
NOS(snmp)# system-configuration
NOS(snmp/system)# location HangZhou
```

【注意事项】

无。

### 14.2.5 system-configuration

【功能描述】

**system-configuration** 命令用于进入 SNMP 系统配置视图。

【命令格式】

**system-configuration**

【视图】

SNMP 视图

【缺省情况】

不涉及。

【参数说明】

无

【使用举例】

```
NOS# config snmp
NOS(snmp)#
NOS(snmp)# system-configuration
NOS(snmp/system)#
```

【注意事项】

无。

### 14.2.6 trap enable

【功能描述】

**trap enable** 命令用于使能指定模块的 trap 功能。

**no trap enable** 命令用于去使能指定模块的 trap 功能。

【命令格式】

**trap enable <ospf <nbrstatechange|ifstatechange>|vrrp newmaster|interface <linkup|linkdown>|standrd <coldstart|warmstart>>**

**no trap enable <ospf <nbrstatechange|ifstatechange>|vrrp newmaster|interface <linkup|linkdown>|standrd <coldstart|warmstart>>**

【视图】

SNMP 视图

【缺省情况】

**coldstart** 的 trap 默认开启，其余模块默认关闭。

【参数说明】

- ospf <nbrstatechange|ifstatechange>：OSPF 邻居状态改变、接口状态改变的 trap。
- vrrp newmaster：VRRP 接口成为 master 的 trap。
- interface <linkup|linkdown>：接口 up、down 的 trap。
- standard：SNMP 标准 trap。
- coldstart：设备冷重启触发的 trap。
- warmstart：设备热重启触发的 trap。

【使用举例】

#使能 ospf 模块邻居状态变化的 trap。

```
NOS# config snmp
NOS(snmp)# trap enable ospf nbrstatechange
```

【注意事项】

无。

### 14.2.7 trap2sink

【功能描述】

**trap2sink** 命令用于配置发送 SNMPv2 版本的 Trap 的目的地址和共同体名称。

**no trap2sink** 命令用于删除已配置的 SNMPv2 版本的 trap。

【命令格式】

**trap2sink host** *<A.B.C.D/X:X::X:X>* **community** *COM_NAME* [**port** *PORT*]

**no trap2sink** [**community** *COM_NAME* [**ipv4**|**ipv6**]]

【视图】

SNMP 视图

【缺省情况】

未配置该信息

【参数说明】

- **host** *<A.B.C.D/X:X::X:X>*：指定 trap 发送的目的 IPv4/IPv6 地址信息。

- **community** *COM_NAME*：指定发送 trap 的共同体名称，该共同体需存在，否则无法配置。
- **port** *PORT*：指定 trap 发送的端口，取值范围(1～65535)，默认为 162。

【使用举例】

#配置共同体 public 从端口 8888 向 10.1.1.1 发送 trap。

```
NOS# config snmp
NOS(snmp)# trap2sink host 10.1.1.1 community public port 8888
```

【注意事项】

对同一共同体的多次配置视为修改。

### 14.2.8 view

【功能描述】

**view** 命令创建 MIB 视图并设置对 MIB 节点的访问权限。

**no view** 命令用来删除指定 MIB 视图。

【命令格式】

**view** *VIEW_NAME* <**included**|**excluded**> **oid** <**all**|*OID*>

**no view** [*VIEW_NAME*]

【视图】

SNMP 视图

【缺省情况】

不存在 view 配置。

【参数说明】

- *VIEW_NAME*：MIB 视图名，长度限制为 1～31 个字符，只支持字母和数字。
- **included**：包含设置的 MIB 节点。
- **excluded**：不包含设置的 MIB 节点。
- **all**：指定 MIB 节点为所有节点。
- *OID*：指定具体的 MIB 节点。

【使用举例】

#创建名为 sys 的 MIB 视图，包含 all，不包含 MIB 节点.1.3.6.1.2.1.1.2。

```
NOS# config snmp
NOS(snmp)# view sys excluded oid .1.3.6.1.2.1.1.2
NOS(snmp)# view sys included oid all
```

【注意事项】

- 对于任意 MIB 视图，必须要有 included 的 MIB 节点，否则无法访问任何 MIB 节点。
- 对于同一 MIB 视图，如果同一 MIB 节点既 included 又 excluded，则视为 included。

## 14.3 配置举例

(1) 配置读写共同体名称为 aaa

(2) 配置系统维护联系信息为 abc@bc，物理位置信息为 hangzhou

(3) 使能 trap 功能

(4) 用于开启带宽利用率 Trap 告警上报功能

(5) 开启 CPU 利用率 Trap 告警上报功能

(6) 配置带宽利用率 Trap 告警门限最低为 1 最高为 100

```
NOS# config snmp
NOS(snmp)# system-configuration
NOS(snmp/system)# location hangzhou contact abc@bc
NOS(snmp/system)# qu
NOS(snmp)# community write aaa
NOS(snmp)# trap2sink host 192.1.1.155 community aaa
NOS(snmp)# in-band management disable
NOS(snmp)# trap enable cpu-usage
NOS(snmp)# trap enable in-usage
NOS(snmp)# trap enable memory-usage
NOS(snmp)# trap enable out-usage
NOS(snmp)# trap enable interface linkdown
NOS(snmp)# trap enable interface linkup
NOS(snmp)# trap enable ospf ifstatechange
NOS(snmp)# trap enable ospf nbrstatechange
NOS(snmp)# ifmonitor in-usage low-threshold 1 high-threshold 100
```

## 14.4 常见问题

不涉及。

# 15 SNMPv3

## 15.1 功能介绍

SNMPv3 主要在安全性方面进行了增强，提供了基于 USM（User Security Module）的认证加密和基于 VACM（View-based Access Control Model）的访问控制。SNMPv3 版本支持的操作和 SNMPv2c 版本支持的操作一样。

注意：使用 walk 操作时，对于要开启子代理才能访问的 MIB 节点：开启子代理后，若网管端对应的 MIB 模块中存在本系统不支持的节点，会 walk 失败（支持的节点需配置对应功能才能访问）。例如：开启子代理后，未配置 RMON，walk 包含 RMON 的节点，则 walk 会在 RMON 前一个 MIB 模块的最后一个节点报错。

对于 MG-SOFT MIB-Browser 软件，若系统重启，该软件也需重启，才可正常与 Agent 通信。

## 15.2 命令手册

### 15.2.1 group v3

【功能描述】

**group v3** 命令用于创建 SNMPv3 用户组，并指定是否需要对报文进行认证、加密以及指定 NMS 对 MIB 视图的访问权限。

**no group v3** 命令用来删除指定 SNMPv3 用户组，并删除所有加入该组的所有用户。

【命令格式】

**group v3** *GROUP_NAME* [**auth**|**priv**] [{**read** *VIEW_NAME*|**write** *VIEW_NAME*}]

**no group v3** [*GROUP_NAME*]

【视图】

SNMP 视图

【缺省情况】

不存在 SNMPv3 用户组。

【参数说明】

- *GROUP_NAME*：SNMPv3 用户组名，长度限制为 1～31 个字符，只支持字母和数字。
- **auth**：对报文进行认证但不加密。
- **priv**：对报文进行认证和加密。若 auth 和 priv 均未配置，则既不认证也不加密。
- **read**：指定 NMS 具有读权限的 MIB 视图，若不指定则默认为对所有节点可读。
- **write**：指定 NMS 具有写权限的 MIB 视图，若不指定则默认无节点可写。
- *VIEW_NAME*：MIB 视图名，长度限制为 1～31 个字符，只支持字母和数字。

【使用举例】

#创建名为 grp 的 SNMPv3 用户组,对报文进行认证和加密,指定 NMS 具有读权限的 MIB 视图为 sys1，具有写权限的 MIB 视图为 sys2。

```
NOS# config snmp
NOS(snmp)# group v3 grp priv read sys1 write sys2
```

【注意事项】

- 若指定网管具有读权限和写权限的为同一视图则视为读写权限。

- 若不指定可访问的视图，则使用默认视图：对所有节点只读。

### 15.2.2 local-user

【功能描述】

**local-user** 命令创建 SNMPv3 用户，指定要加入的 SNMPv3 用户组，以及对报文是否需要认证、加密并设置对应密码。

**no local-user** 命令用来删除指定 SNMPv3 用户。

【命令格式】

**local-user** *USER_NAME* **group** *GROUP_NAME* [**auth-mode** [**cipher**] <**md5** *AUTH_PASSWORD* [**priv-mode des** *PRIV_PASSWORD*] | **sha** *AUTH_PASSWORD* [**priv-mode aes** *PRIV_PASSWORD*]>

**no local-user** [*USER_NAME*]

【视图】

SNMP 视图

【缺省情况】

不存在 SNMPv3 用户。

【参数说明】

- *USER_NAME*：SNMPv3 用户名，长度限制为 1～31 个字符，只支持字母和数字。
- *GROUP_NAME*：SNMPv3 用户组名，长度限制为 1～31 个字符，只支持字母和数字。
- **auth-mode**：指定认证和加密参数。若未指定，则表示既不认证也不加密。
- **cipher**：以密文方式设置认证密码和加密密码。若未指定，则表示明文方式。
- **md5** *AUTH_PASSWORD* [**priv-mode des** *PRIV_PASSWORD*]：设置认证算法为 MD5，并设置认证密码，同时设置 DES 加密密码（可选）。
- **sha** *AUTH_PASSWORD* [**priv-mode aes** *PRIV_PASSWORD*]：设置认证算法为 SHA，并设置认证密码，同时设置 AES 加密密码（可选）。

【使用举例】

#创建名为 u1 的 SNMPv3 用户，加入名为 g1 的 SNMPv3 用户组，对报文需要 MD5 认证和 DES 加密，且明文认证密码为 12345678，加密密码为 12345678。

```
NOS# config snmp
NOS(snmp)# group v3 g1 priv
NOS(snmp)# local-user u1 group g1 auth-mode md5 12345678 priv-mode des 12345678
```

【注意事项】

- 需先配置具有相同认证、加密方式的 SNMPv3 组，然后再配置用户。
- 需确保 NMS 网管平台的认证和加密一致，否则 NMS 无法和 Agent 通信。

### 15.2.3 trapsess

【功能描述】

**trapsess** 命令用于配置发送 SNMPv3 版本的 Trap 的目的地址和 SNMPv3 用户名称。

**no trapsess** 命令用于删除已配置的 SNMPv3 版本的 trap。

【命令格式】

**trapsess local-user** *USER_NAME* **host** <*A.B.C.D/X:X::X:X*> [**port** *PORT*]

**no trapsess** [**local-user** *USER_NAME*]

【视图】

SNMP 视图

【缺省情况】

未配置相关信息

【参数说明】

- *USER_NAME*：发送 trap 的 SNMPv3 用户名称，该用户需存在，若不存在，则无法配置。
- **host** *<A.B.C.D/X:X::X:X>*：指定 trap 发送的目的 IPv4/IPv6 地址信息。
- **port** *PORT*：指定 trap 发送的端口，取值范围(1～65535)，默认为 162。

【使用举例】

#配置 SNMPv3 用户 user1 从端口 8888 向 10.1.1.1 发送 trap。

```
NOS# config snmp
NOS(snmp)# trapsess local-user user1 host 10.1.1.1 port 8888
```

【注意事项】

对同一 SNMPv3 用户的多次配置视为修改。

## 15.3 配置举例

(1) 创建 MIB 视图并设置对 MIB 节点的访问权限为全部 oid 节点

(2) 创建 SNMPv3 用户组 bc，

(3) 创建 SNMPv3 用户 aaa，指定要加入的 SNMPv3 用户组 bc

(4) 配置发送 SNMPv3 版本的 Trap 的目的地址为 192.1.1.155，SNMPv3 用户名称为 aaa

```
NOS# config snmp
NOS(snmp)# view abc included oid all
NOS(snmp)# group v3 bc write abc
NOS(snmp)# local-user aaa group bc
NOS(snmp)# trapsess local-user aaa host 192.1.1.155
```

## 15.4 常见问题

无。

# 16 RMON

## 16.1 功能介绍

### 16.1.1 特性简介

RMON（Remote Network Monitoring，远程网络监视）主要实现了统计和告警功能，用于网络中管理设备对被管理设备的远程监控和管理。统计功能指的是被管理设备可以按周期或者持续跟踪统计其端口所连接的网段上的各种流量信息，比如某段时间内某网段上收到的报文总数，或收到的超长报文的总数等。告警功能指的是被管理设备能监控指定 MIB 变量的值，当该值达到告警阈值时（比如端口速率达到指定值，或者广播报文的比例达到指定值），能自动记录日志、向管理设备发送 Trap 消息。

SNMP 是 RMON 实现的基础，RMON 是 SNMP 功能的增强。RMON 使用 SNMP Trap 报文发送机制向管理设备发送 Trap 消息告知告警变量的异常。虽然 SNMP 也定义了 Trap 功能，但通常用于告知被管理设备上某功能是否运行正常、接口物理状态的变化等，两者监控的对象、触发条件以及报告的内容均不同。

RMON 使 SNMP 能更有效、更积极主动地监测远程网络设备，为监控子网的运行提供了一种高效的手段。RMON 协议规定达到告警阈值时被管理设备能自动发送 Trap 信息，所以管理设备不需要多次去获取 MIB 变量的值进行比较，从而能够减少管理设备同被管理设备的通讯流量，达到简便而有力地管理大型互连网络的目的。

## 16.2 命令手册

### 16.2.1 alarm

【功能描述】

**alarm** 命令用来在告警表中添加一个表项。

**no alarm** 用来删除指定的告警表项。

【命令格式】

**alarm** *ALARM_INDEX* **OID** *INTERVAL* <**absolute**|**delta**> **rising-threshold** *VALUE EVENTIDX* **falling-threshold** *VALUE EVENTIDX* [**owner** *NAME*]

**no alarm** [*ALARM_INDEX*]

【视图】

RMON 视图

【缺省情况】

未在告警表中添加表项。

【参数说明】

- *ALARM_INDEX*：告警表项索引，表项索引范围(1～65535)。删除时如不指定，则表示删除所有。
- **OID**：点分格式的告警节点 ID
- *INTERVAL*：告警监控对象采样的时间间隔，范围为(5～65535)，单位为秒。
- **absolute**：指定采样类型为绝对值。
- **delta**：指定采样类型为变化值。

- **rising-threshold** *VALUE EVENTIDX*：指定采样值的上限阈值（范围为(-2147483648～2147483647)）和对应的事件索引号（范围是(1～65535)）。
- **falling-threshold** *VALUE EVENTIDX*：指定采样值的下限阈值（范围为(-2147483648～2147483647)）和对应的事件索引号（范围是(1～65535)），注意下限阈值必须小于上限阈值。
- **owner** *NAME*：表项创建者名称。

【使用举例】

# 配置节点的上限阈值为 9、下限阈值为 5，采样类型为绝对值：

```
NOS# config rmon
NOS(rmon)# alarm 1 .1.3.6.1.2.1.16.3 60 absolute rising-threshold 9 1 falling-threshold 5
2
```

【注意事项】

配置指定对象的阈值告警功能前，需要通过 rmon event 命令定义好告警所引用的事件。否则，虽然会存在告警功能，但是不能触发事件。

### 16.2.2 config rmon

【功能描述】

**config rmon** 命令用于进入 RMON 视图。

**no config rmon** 用来删除 RMON 视图及所有相关配置。

【命令格式】

**config rmon**

**no config rmon**

【视图】

根视图

【缺省情况】

无 RMON 相关配置。

【参数说明】

无

【使用举例】

# 进入 rmon 视图

```
NOS# config rmon
NOS(rmon)#
```

【注意事项】

无。

### 16.2.3 event

【功能描述】

**event** 命令用来在事件表中添加一个表项。

**no event** 用来删除事件表中的指定表项。

【命令格式】

**event** *EVENT_INDEX* <**trap**|**log**|**trap-log**|**none**> [**owner** *NAME*] [**description** *STRING*]

**no event** [*EVENT_INDEX*]

【视图】

RMON 视图

【缺省情况】

未在事件表中添加表项。

【参数说明】

- *EVENT_INDEX*：事件表项索引，表项索引范围为(1～65535)。删除时如不指定，则表示删除所有。
- **Trap**：对事件的处理方式是向网管发送 trap 消息。
- **log**：对事件的处理方式是记录日志。
- **trap-log**：对事件的处理方式是记录日志，并同时向网管发送 trap 消息。
- **none**：事件触发时，系统不做任何处理。
- **owner** *NAME*：表项创建者名称。
- **description** *STRING*：事件的描述信息。

【使用举例】

# 配置事件 1，动作是发送 trap 消息：

```
NOS# config rmon
NOS(rmon)# event 1 trap
```

【注意事项】

配置指定事件及处理方式后，需要通过 alarm 命令配置告警对象与之关联，否则，不会触发此事件。

### 16.2.4 ifmonitor

【功能描述】

**ifmonitor** 命令用来配置全局生效的接口带宽使用率监控门限。

**no ifmonitor** 用来恢复默认情况。

【命令格式】

**ifmonitor** <**in-usage**|**out-usage**> **low-threshold** *(1-100)* **high-threshold** *(1-100)*

**no ifmonitor** <**in-usage**|**out-usage**> **low-threshold** *(1-100)* **high-threshold** *(1-100)*

【视图】

RMON 视图

【缺省情况】

未配置监控门限。

【参数说明】

- **in-usage**|**out-usage**：监控入方向带宽利用率还是出方向。
- **low-threshold** *(1-100)*：门限百分比的低限值，从高于该值降到低于该值，则恢复 trap 告警。
- **high -threshold** *(1-100)*：门限百分比的高限值，从低于该值升到高于该值，则触发 trap 告警。

【使用举例】

# 配置接口带宽使用率监控门限最低为 20%，最高为 80%：

```
NOS(snmp)# ifmonitor in-usage low-threshold 20 high-threshold 80
```

【注意事项】

无

### 16.2.5 port ifmonitor

【功能描述】

**port ifmonitor** 命令用来配置指定接口下生效的接口带宽使用率监控门限。

**no port ifmonitor** 用来恢复默认情况。

【命令格式】

**port ifmonitor** <**in-usage**|**out-usage**> **low-threshold** *(1-100)* **high-threshold** *(1-100)*

**no port ifmonitor** <**in-usage**|**out-usage**> **low-threshold** *(1-100)* **high-threshold** *(1-100)*

【视图】

二层以太网接口视图

【缺省情况】

未配置监控门限。

【参数说明】

- **in-usage**|**out-usage**：监控入方向带宽利用率还是出方向。
- **low-threshold** *(1-100)*：门限百分比的低限值，从高于该值降到低于该值，则恢复 trap 告警。
- **high -threshold** *(1-100)*：门限百分比的高限值，从低于该值升到高于该值，则触发 trap 告警。

【使用举例】

# 配置接口下生效的接口带宽使用率监控门限最低为 20%，最高为 80%：

```
NOS(snmp)# ifmonitor in-usage low-threshold 20 high-threshold 80
```

【注意事项】

如果在接口下配置了监控门限，则以接口下配置为准，否则以全局配置为准。

### 16.2.6 rmon history

【功能描述】

**rmon history** 命令用来在历史表中为当前接口添加一个表项。

**no rmon history** 用来删除历史表中的指定表项。

【命令格式】

**rmon history** *HIS_INDEX* **buckets** *BUCKETS* **interval** *INTERVAL* [**owner** *NAME*]

**no rmon history** [*HIS_INDEX*]

【视图】

二层接口视图

【缺省情况】

未在历史表中添加表项。

【参数说明】

- *HIS_INDEX*：历史表项索引，取值范围为(1～65535)。删除时如不指定，则表示删除所有。
- **buckets** *BUCKETS*：最大采样记录数，取值范围为 1～10。

- **interval** *INTERVAL*：采样间隔时间，取值范围(5～3600)，单位为秒。
- **owner** *NAME*：表项创建者名称。

【使用举例】

# 为接口 ge1 创建历史表项，最大记录个数为 10 个，采样间隔 60 秒：

```
NOS# config interface ge1
NOS(if-ge1)# rmon history 1 buckets 10 interval 60
```

【注意事项】

- 创建历史表项后，系统会按指定周期统计当前接口的报文收发情况，并将统计值保存在 etherHistoryEntry 表的叶子节点下。可保存的统计值个数由 buckets number 参数决定，当历史表的容量达到最大值时，系统会删除最早的记录来保存新的统计值。
- 一个接口下可以创建多个历史表项，用于按不同采样间隔进行统计。

### 16.2.7 rmon statistic

【功能描述】

**rmon statistic** 命令用来在统计表中添加一个表项。当需要统计某个接口的累加数据时，可以创建此统计表，然后通过 show rmon statistics 命令来查看统计结果。

**no rmon statistic** 用来删除当前接口下的统计表表项。

【命令格式】

**rmon statistic** *STAT_INDEX* [**owner** *NAME*]

**no rmon statistic**

【视图】

二层接口视图

【缺省情况】

未在统计表中添加表项。

【参数说明】

- *STAT_INDEX*：统计表项索引，取值范围(1～65535)，必须全局唯一。
- **owner** *NAME*：表项创建者名称。

【使用举例】

```
NOS# config interface ge1
NOS(if-ge1)# rmon statistic 2
```

【注意事项】

每个接口下只能定义一个统计表项。

### 16.2.8 show rmon alarm

【功能描述】

**show rmon alarm** 命令用于查看告警表信息。

【命令格式】

**show rmon alarm** [*ALARM_INDEX*]

【视图】

任意视图

【缺省情况】

不涉及

【参数说明】

*ALARM_INDEX*：指定查看的告警表表项索引，范围为(1～65535)。

【使用举例】

```
NOS(rmon)# show rmon alarm 2
Alarm table 2 owned by creator is valid.
  Samples type     : absolute
  Variable formula  : .1.3.6.1.2.1.2.2.1.3.21
  Sampling interval : 30(sec)
  Rising threshold  : 500 (linked with event 1)
  Falling threshold : 100 (linked with event 2)
```

【注意事项】

无。

### 16.2.9 show rmon event

【功能描述】

**show rmon event** 命令用于查看事件表信息。

【命令格式】

**show rmon event** [*EVENT_INDEX*]

【视图】

任意视图

【缺省情况】

不涉及

【参数说明】

*EVENT_INDEX*：指定查看的事件表表项索引，范围为(1～65535)。

【使用举例】

```
NOS# show rmon event 5
Event table 5 owned by user is valid.
  Description: none
  Will cause trap when triggered, last triggered at 0
```

【注意事项】

无。

### 16.2.10 show rmon history

【功能描述】

**show rmon history** 命令用于查看历史表信息。

【命令格式】

**show rmon history** [*HIS_INDEX*|**interface** *L2_ETH_IF*]

【视图】

任意视图

【缺省情况】

无

【参数说明】

*HIS_INDEX*：指定查看的历史表表项，索引范围(1～65535)。

**interface** *L2_ETH_IF*：指定查看的历史表的接口名称。

【使用举例】

```
NOS# show rmon history interface ge4

Total rmon history count: 5

HistoryControlEntry 1 owned by user is valid.
  Samples interface         :   ge4
  Sampling interval         :   5(sec) with 5 buckets max
  Sampled values of record 5 :
    dropevents       :  0      ,  octets             : 0
    packets          :   0      ,  broadcast packets    : 0
    multicast packets : 0      , CRC alignment errors : 0
    undersize packets : 0      , oversize packets    : 0
    fragments        : 0      , jabbers            : 0
    collisions       : 0      , utilization         : 0
  Sampled values of record 6 :
    dropevents       : 0      , octets             : 0
    packets          :  0      , broadcast packets    : 0
    multicast packets :0      , CRC alignment errors : 0
    undersize packets :0      , oversize packets    : 0
    fragments        :  0      , jabbers            : 0
    collisions       :  0      , utilization         : 0
  Sampled values of record 7 :
    dropevents       :  0      , octets             : 0
    packets          :   0      , broadcast packets    : 0
    multicast packets : 0      , CRC alignment errors : 0
    undersize packets : 0      , oversize packets    : 0
    fragments        :   0      , jabbers            : 0
    collisions       :   0      , utilization         : 0
  Sampled values of record 8 :
    dropevents       :   0      , octets             : 0
    packets          :    0      , broadcast packets    : 0
    multicast packets :  0      , CRC alignment errors : 0
    undersize packets :  0      , oversize packets    : 0
    fragments        :    0      , jabbers            : 0
    collisions       :    0      , utilization         : 0
  Sampled values of record 9 :
    dropevents       :    0      , octets             : 0
    packets          :     0      , broadcast packets    : 0
    multicast packets :   0      , CRC alignment errors : 0
    undersize packets :   0      , oversize packets    : 0
    fragments        :    0      , jabbers            : 0
```

```
collisions       :        0       , utilization         : 0
```

【注意事项】

无

### 16.2.11 show rmon statistic

【功能描述】

**show rmon statistic** 命令用于查看统计表信息。

【命令格式】

**show rmon statistic** [*STAT_INDEX* |**interface** *L2_ETH_IF*]

【视图】

任意视图

【缺省情况】

无

【参数说明】

- *STAT_INDEX*：指定查看的统计表表项索引，范围为(1～65535)。
- **interface** *L2_ETH_IF*：指定查看统计表的接口名称。

【使用举例】

```
NOS# show rmon statistics interface ge1
Statistics entry 1 owned by user is valid.
  Interface : ge1
  octets             :   0          , packets          :   0
  broadcast packets    : 0          , multicast packets : 0
  undersize packets    : 0          , oversize packets  :  0
  fragments packets     : 0          , jabbers packets   :   0
  CRC alignment errors :0          ,  collisions       :   0
  Dropped packet (insufficient resources): 0
  Packets received according to length (octets):
  64     :  0          , 65-127  :   0          , 128-255  :  0
  256-511: 0           , 512-1023: 0          , 1024-1518: 0
```

【注意事项】

无

## 16.3 配置举例

### 16.3.1 统计组配置举例

配置 RMON 对接口 ge1 进行流量统计，创建者为 user：

```
NOS# config interface ge1
NOS(if-ge1)# rmon statistic 1 owner user
```

配置验证：

```
NOS# show rmon statistics interface ge1
Statistics entry 1 owned by user is valid.
```

```
Interface : ge1
octets             : 0          , packets         : 0
broadcast packets    : 0          , multicast packets : 0
undersize packets    : 0          , oversize packets  : 0
fragments packets     : 0          , jabbers packets   : 0
CRC alignment errors : 0          , collisions       : 0
Dropped packet (insufficient resources): 0
Packets received according to length (octets):
64     : 0          , 65-127  : 0          , 128-255  : 0
256-511: 0          , 512-1023: 0          , 1024-1518: 0
```

### 16.3.2 历史组配置举例

配置 RMON 对接口 ge4 进行周期性流量统计，创建者为 user：

```
NOS# config interface ge4
NOS(if-fe4)# rmon history 1 buckets 5 interval 5 owner user
```

配置验证：

```
NOS# show rmon history interface ge4
Total rmon history count: 5
HistoryControlEntry 1 owned by user is valid.
  Samples interface         : ge4
  Sampling interval         : 5(sec) with 5 buckets max
  Sampled values of record 5 :
    dropevents       : 0      , octets             : 0
    packets          : 0      , broadcast packets    : 0
    multicast packets : 0      , CRC alignment errors : 0
    undersize packets : 0      , oversize packets     : 0
    fragments        : 0      , jabbers            : 0
    collisions       : 0      , utilization         : 0
  Sampled values of record 6 :
    dropevents       : 0      , octets             : 0
    packets          : 0      , broadcast packets    : 0
    multicast packets : 0      , CRC alignment errors : 0
    undersize packets : 0      , oversize packets     : 0
    fragments        : 0      , jabbers            : 0
    collisions       : 0      , utilization         : 0
  Sampled values of record 7 :
    dropevents       : 0      , octets             : 0
    packets          : 0      , broadcast packets    : 0
    multicast packets : 0      , CRC alignment errors : 0
    undersize packets : 0      , oversize packets     : 0
    fragments        : 0      , jabbers            : 0
    collisions       : 0      , utilization         : 0
  Sampled values of record 8 :
    dropevents       : 0      , octets             : 0
    packets          : 0      , broadcast packets    : 0
    multicast packets : 0      , CRC alignment errors : 0
    undersize packets : 0      , oversize packets     : 0
    fragments        : 0      , jabbers            : 0
```

```
    collisions       : 0      , utilization        : 0
  Sampled values of record 9 :
    dropevents       : 0      , octets             : 0
    packets          : 0      , broadcast packets    : 0
    multicast packets : 0      , CRC alignment errors : 0
    undersize packets : 0      , oversize packets     : 0
    fragments        : 0      , jabbers            : 0
collisions       : 0      , utilization        : 0
```

### 16.3.3 事件组配置举例

配置事件 5 为发送 trap 信息的事件，创建者为 user，描述为 none：

```
NOS# config rmon
NOS(rmon)# event 5 trap owner user description none
```

配置验证：

```
NOS# show rmon event 5
Event table 5 owned by user is valid.
  Description: none
  Will cause trap when triggered, last triggered at 0
```

### 16.3.4 告警组配置举例

配置 snmp：

```
NOS# config snmp
NOS(snmp)# agentx enable
NOS(snmp)# community write public
```

配置告警阈值触发事件：

```
NOS# config rmon
NOS(rmon)# event 1 log owner public
NOS(rmon)# event 2 trap owner public
```

配置对告警监控对象 ifType.21（对应的告警 OID 为.1.3.6.1.2.1.2.2.1.3.21）进行告警阈值监控，以 30 秒的采样间隔进行绝对值采样，当采样值大于等于 500 的上限阈值触发事件 1，小于等于下限阈值 100 时触发事件 2，创建者为 creator：

```
NOS(rmon)# alarm 2 .1.3.6.1.2.1.2.2.1.3.21 30 absolute rising-threshold 500 1
falling-threshold 100 2 owner creator
```

配置验证

```
NOS(rmon)# show rmon alarm 2
Alarm table 2 owned by creator is valid.
  Samples type     : absolute
  Variable formula  : .1.3.6.1.2.1.2.2.1.3.21
  Sampling interval : 30(sec)
  Rising threshold  : 500 (linked with event 1)
  Falling threshold : 100 (linked with event 2)
```

## 16.4 常见问题

无。

# 17 WEB

## 17.1 功能介绍

Web 是指通过 HTTP/HTTPS 协议进行设备管理的一种方式，相比 CLI 命令行，Web 更简单易用，但功能完整度不及命令行，一般只用于基础配置管理。

## 17.2 命令手册

### 17.2.1 config web server

【功能描述】

**config web server** 命令用于启用 web 管理服务。

**no config web server** 命令用于禁用 web 管理服务并删除所有 web 配置。

【命令格式】

[no] **config web server**

【视图】

根视图

【缺省情况】

未启用 web 服务。

【参数说明】

无

【使用举例】

# 启用 web 管理服务：

```
NOS# config web server
```

【注意事项】

无

### 17.2.2 http-port

【功能描述】

**http-port** 命令用于修改 web 管理服务的 TCP 端口号。

**no http-port** 命令用于恢复 web 管理服务的 TCP 端口号为缺省值。

【命令格式】

**http-port** *(1-65535)*

**no http-port**

【视图】

web 配置视图

【缺省情况】

缺省为知名端口 80。

【参数说明】

*(1-65535)*：要设置的 TCP 端口号，注意不要与已使用的端口冲突。

【使用举例】

# 配置 web 管理服务端口号为 200：

```
NOS# config web server
NOS(web)# http-port 200
Change port may cause connection lost, continue? [Y/N] y
```

【注意事项】

修改端口号会导致当前 web 会话断开连接，请谨慎使用。

### 17.2.3 session timeout

【功能描述】

**session timeout** 命令用于修改 web 管理服务的闲置超时时间。

**no session timeout** 命令用于恢复 web 管理服务的闲置超时时间为缺省值。

【命令格式】

**session timeout** *(60-1000000)*

**no session timeout**

【视图】

web 配置视图

【缺省情况】

缺省为 300 秒。

【参数说明】

*(60-1000000)*：要设置的闲置超时时间，单位为秒。

【使用举例】

# 配置 web 超时时间为 1000：

```
NOS# config web server
NOS(web)# session timeout 1000
```

【注意事项】

修改后仅对新接入的 web 会话有效。

### 17.2.4 show web server

【功能描述】

**show web server** 命令用于查看当前 web 服务状态。

【命令格式】

**show web server** [json]

【视图】

任意视图

【缺省情况】

不涉及

【参数说明】

json：以 json 格式显示

【使用举例】

# 查看当前 web 服务状态

```
NOS# show web server
web server : enabled
  session timeout 300
NOS#
```

【注意事项】

无

# 18 以太网接口管理

## 18.1 功能介绍

接口管理用于维护端口、接口、虚接口、VLAN 等网络接口相关的配置。

## 18.2 命令手册

### 18.2.1 combo

【功能描述】

combo 命令用于进行光电接口切换，只有支持 combo 接口的设备才能执行该命令。

【命令格式】

combo enable <auto|copper|fiber>

【视图】

二层以太网接口视图

【缺省情况】

取决于具体产品

【参数说明】

- auto：自动模式，在该模式下会自动选择可用的接口（如果都可用，优先选择光口）。
- copper：强制使用电口模式。
- fiber：强制使用光口模式。

【使用举例】

#将 xge49 口切换为电口

```
NOS# interface xge49
NOS(if-xge49)# combo enable copper
```

【注意事项】

无

### 18.2.2 default

【功能描述】

default 命令用于将接口配置恢复到默认值（空配置）。

【命令格式】

default [force]

【视图】

物理接口视图

【缺省情况】

不涉及

【参数说明】

**force**：无需确认，直接执行。若不带该参数，则会用用户确认后再执行。

【使用举例】

```
NOS# interface ge1
NOS(if-ge1)# default
All configuration on this interface will be removed. Continue? [Y/N]y
NOS(if-ge1)#
```

【注意事项】

- 该命令会将该接口下的配置逐条删除，如果配置较多，则可能需要较长时间。
- 接口默认不会被 shutdown，因此 default 操作时需要注意避免引发环路。

### 18.2.3 description

【功能描述】

**description** 命令用于给接口设置描述信息，方便区分业务。

**no description** 命令用于清除接口的描述信息。

【命令格式】

**description** *DESC*

**no description**

【视图】

二层以太网接口视图

聚合接口视图

【缺省情况】

无描述信息

【参数说明】

*DESC*：描述信息字符串，不长于 255 字符。

【使用举例】

```
# 设置 ge1 接口的描述信息为“port_to_dev1_p1”：
NOS# config interface ge1
NOS(if-ge1)# description port_to_dev1_p1
```

【注意事项】

无

### 18.2.4 duplex

【功能描述】

**duplex** 命令用来配置接口的双工模式。

**no duplex** 命令用来恢复缺省情况。

【命令格式】

**duplex** <**full**|**half**>

**no duplex**

【视图】

二层以太网接口视图

【缺省情况】

接口缺省为全双工模式。

【参数说明】

- full：全双工模式，可以同时发送和接收数据包。
- half：半双工模式，只有速率低于 1000M 的以太电口才支持。

【使用举例】

# 设置 ge3 接口为半双工模式：

```
NOS# interface ge3
NOS(if-ge3)# duplex half
NOS(if-ge3)#
```

【注意事项】

无

### 18.2.5 eee

【功能描述】

eee 命令用来使能端口节能功能。

no eee 命令用来取消使能端口节能功能。

【命令格式】

```
eee
no eee
```

【视图】

二层以太网接口视图

【缺省情况】

未使能端口节能功能。

【参数说明】

无

【使用举例】

# 开启 ge1 端口节能功能：

```
NOS# interface ge1
NOS(if-ge1)# eee
```

【注意事项】

无

### 18.2.6 flow-control

【功能描述】

flow-control 命令用来开启接口的流量控制功能。

no flow-control 命令用来关闭接口的流量控制功能。

【命令格式】

**flow-control**

**no flow-control**

【视图】

二层以太网接口视图

【缺省情况】

未开启接口的流量控制功能。

【参数说明】

无

【使用举例】

# 开启 ge1 流量控制功能：

```
NOS# interface ge1
NOS(if-ge1)# flow-control
NOS(if-ge1)#
```

【注意事项】

无

### 18.2.7 interface

【功能描述】

**interface** 命令用于进入接口配置视图

【命令格式】

[**config**] **interface** *IF-NAME*

【视图】

根视图

【缺省情况】

不涉及

【参数说明】

*IF-NAME*：接口名称，包括物理口和虚拟口。

【使用举例】

# 进入接口 ge1 视图：

```
NOS# interface ge1
NOS(if-ge1)#
```

【注意事项】

带 config 关键字和不带该关键字的效果完全相同，可兼容业界配置风格。

### 18.2.8 interface range

【功能描述】

**interface range** 命令用于进入接口批量配置视图

【命令格式】

[config] interface range *IF-NAME...*

[config] interface range *IF-NAME-FROM* to *IF-NAME-TO*

【视图】

根视图

【缺省情况】

不涉及

【参数说明】

- *IF-NAME*：接口名称，包括物理口和虚拟口。
- *IF-NAME-FROM*：起始接口名称。
- *IF-NAME-TO*：结束接口名称，必须和起始接口的类型相同。

【使用举例】

# 批量配置 ge1-ge10：

```
NOS# interface range ge1 to ge10
NOS(if-range)#
```

【注意事项】

带 config 关键字和不带该关键字的效果完全相同，可兼容业界配置风格。

### 18.2.9 link-delay

【功能描述】

**link-delay** 命令用于设置端口 up/down 时的响应时延。

**no link-delay** 命令用于取消设置端口 up/down 时的响应时延。

【命令格式】

**link-delay** <**up**|**down**> *TIME*

**no link-delay** [**up**|**down**|**all**]

【视图】

二层以太网接口视图

【缺省情况】

没有响应时延，即时延为 0

【参数说明】

- *TIME*：延迟时间，取值范围(0～20000)，单位为毫秒。
- **up**：端口 up 时的响应延迟。
- **down**：端口 down 时的响应延迟。
- **all**：取消所有的延时配置。

【使用举例】

# 设置 ge1 接口的 UP 时延为 50 毫秒，DOWN 的时延为 100 毫秒：

```
NOS# interface ge1
NOS(if-ge1)# link-delay up 50
NOS(if-ge1)# link-delay down 100
```

【注意事项】

配置较大的时延，可以有效避免因链路故障可能导致的高频震荡，但也会延长链路切换的时间，请根据实际网络情况合理配置。

### 18.2.10 loopback

【功能描述】

**loopback** 命令用于设置端口内环/外环功能。

**no loopback** 命令用于取消设置端口环回。

【命令格式】

**loopback** <**internal**|**external**>

**no loopback**

【视图】

二层以太网接口视图

【缺省情况】

没有设置自环

【参数说明】

- **internal**：设置以太网的内部环回。配置内部环回后，接口会将需要转发出去的报文返回给设备内部，一般用于定位设备是否故障。
- **external**：设置以太网的外部环回。配置外部环回后，接口会将来自对端设备的报文返回给对端设备，一般用于定位设备间链路是否故障。

【使用举例】

# 设置 ge1 为内部环回接口：

```
NOS# interface ge1
NOS(if-ge1)# loopback internal
```

【注意事项】

开启环回功能后，接口将不能正常转发数据包，请按需配置，使用完后及时取消配置。

### 18.2.11 reset counters

【功能描述】

**reset counters** 命令用于清除接口的报文统计信息。

【命令格式】

**reset counters interface** [*IF_NAME*]

【视图】

根视图

【缺省情况】

不涉及

【参数说明】

*IF_NAME*：指定要清除统计信息的接口，如果不指定，表示清除所有接口。

【使用举例】

# 清除 ge1 的接口统计信息：

```
NOS# reset counters interface ge1
NOS#
```

【注意事项】

无

### 18.2.12 show counters

【功能描述】

**show counters** 命令用于显示计数统计，包括错误统计信息、流量统计、指定端口计数统计。

【命令格式】

**show counters** [<**error**|**rate**|**interface** [*L2_ETH_IF*]>] [**json**]

【视图】

任意视图

【缺省情况】

不涉及

【参数说明】

- **error**：显示所有接口的报文转发错误统计信息。
- **rate**：显示所有接口的报文收发速率统计信息。
- **interface** *L2_ETH_IF*：指定单个接口显示，如果不指定，则表示显示所有接口。
- **json**：以 json 格式输出。

【使用举例】

# 显示报文收发速率统计信息：

```
NOS# show counters rate

            Rate(Pps)           Usage(%)
Name     Inbound   Outbound    InUsage   OutUsage
----- ---------- ---------- ---------- ----------
ge1            0          0          0          0
ge2            0          0          0          0
ge3            0          0          0          0
ge4            0          0          0          0
ge5            0          0          0          0
ge6            0          0          0          0
ge7            0          0          0          0
ge8            0          0          0          0
```

【注意事项】

无

### 18.2.13 show interface

【功能描述】

show interface 命令用来显示接口信息。

【命令格式】

show interface [<*IF_NAME*|layer2|layer3>] [status <up|down>] [json]

show interface *IF_NAME* detail [json]

【缺省情况】

不涉及

【视图】

任意视图

【参数说明】

*IF_NAME*：只显示指定的接口，如果不指定则表示所有接口。

layer2：只显示二层接口。

layer3：只显示三层接口。

status <up|down>：只显示当前状态为 UP 或 DOWN 的接口。

detail：显示详细信息。

json：以 json 格式输出。

【使用举例】

#显示所有接口信息：

```
NOS# show interface
 *[State] A-Down: Administratively down
L3-interface list:
 Name       State     Proto           UpTime       Address
 ----------  -------    ------------     ------------
-------------------------------------
 mgt0       Up        static/static    08:20:54     192.168.5.107/16
 vlan10     Down      static/static    00:00:00     10.1.1.1/24
L2-interface list:
 Name        State             Speed    Duplex    PVID   MAC
 ----------   -----------------   -------   -------   ----   -----------------
 ge1         Down              --       --       10     50:d3:3b:f8:92:02
 ge2         Down              --       --       1      50:d3:3b:f8:92:03
 ge3         Down              --       --       1      50:d3:3b:f8:92:04
 ge4         Down              --       --       1      50:d3:3b:f8:92:05
 ge5         Down              --       --       1      50:d3:3b:f8:92:06
 ge6         Down              --       --       1      50:d3:3b:f8:92:07
 ge7         Down              --       --       1      50:d3:3b:f8:92:08
 ge8         Down              --       --       1      50:d3:3b:f8:92:09
```

#显示单个二层接口的详细信息：

```
NOS# show interface ge1 detail
  IfIndex                    : 24
  State                      : down
  MAC                        : 50:d3:3b:f8:92:02
```

```
  Description                : ge1(Layer2 interface)
```
#显示单个三层接口的详细信息：
```
NOS# show interface mgt0 detail
  IfIndex                    : 2
  State                      : up
  MAC                        : 08:00:27:b6:70:c4
  Description                : mgt0(Layer3 interface)
  IPv4 address               : 192.168.5.107/16 (primary)

  Mtu                        : 1500
  IPV6 address               : 19
    fe80::a00:27ff:feb6:70c4/64 Scope:Linklocal
  Multicast address:
    ff02::1:ff00:0
    ff02::1:ffb6:70c4
    ff05::2
    ff02::2
    ff02::1
```

### 18.2.14 show storm-suppression

【功能描述】

show storm-suppression 命令用来显示所有接口的风暴抑制配置情况。

【命令格式】

show storm-suppression [json]

【缺省情况】

不涉及

【视图】

任意视图

【参数说明】

json：以 json 格式输出。

【使用举例】

#显示所有接口的风暴抑制配置情况：
```
NOS# show storm-suppression
 Ifname         Type              Unit              Value
 --------       ----              ----              ----
 ge1            broadcast          100               pps
 ge2            unknown-unicast    1000              kbps
                unknown-multicast  1000              kbps
                broadcast          1000              kbps
```

### 18.2.15 shutdown

【功能描述】

shutdown 命令用来强制关闭接口。

no shutdown 命令用来恢复缺省情况。

【命令格式】

shutdown

no shutdown

【缺省情况】

接口缺省处于启用状态。

【参数说明】

无

【视图】

接口视图

【使用举例】

#强制关闭 ge1 接口：

```
NOS# interface ge1
NOS(if-ge1)# shutdown
```

【注意事项】

本命令会导致该端口链路中断，影响数据通信，请谨慎使用。

### 18.2.16 speed

【功能描述】

speed 命令用来配置以太端口速率。

no speed 命令用来恢复缺省情况。

【命令格式】

speed *SPEED*

no speed

【视图】

二层以太网接口视图

【缺省情况】

自动协商速率。

【参数说明】

*SPEED*：速率值，取值范围取决于接口类型，单位为 Mbps。

【使用举例】

#在端口 ge1 上配置速率为 100M：

```
NOS# config interface ge1
NOS (if-ge1)# speed 100
```

【注意事项】

速率配置需要确保两端一致，一般情况下，建议不要手工修改速率，使用默认的自动协商即可。

### 18.2.17 storm-suppression

【功能描述】

storm-suppression 命令用于端口风暴抑制，包括广播、未知多播和未知单播风暴抑制。

no storm-suppression 命令用于取消设置端口风暴抑制。

【命令格式】

storm-suppression <all|broadcast|unknown-multicast|unknown-unicast> <kbps *RATE* |pps *VALUE*>

no storm-suppression <all|broadcast|unknown-multicast|unknown-unicast>

【视图】

二层以太网接口视图

【缺省情况】

未配置风暴抑制

【参数说明】

- all：端口上抑制所有类型风暴，包括广播、未知多播和未知单播风暴抑制。
- broadcast：广播风暴抑制类型。
- unknown-multicast：未知多播风暴抑制类型。
- unknown-unicast：未知单播风暴抑制类型。
- kbps *RATE*：按流量设置风暴抑制，单位为每秒千比特（kbps），取值范围取决于实际产品。
- pps *VALUE*：按报文数量设置风暴抑制，单位为每秒的数据包数量（pps），取值范围取决于实际产品。

【使用举例】

#在端口 ge1 上抑制所有类型风暴，按照 100kbps 进行风暴抑制：

```
NOS# interface ge1
NOS(if-ge1)# storm-suppression all kbps 100
NOS(if-ge1)#
```

【注意事项】

无。

### 18.2.18 virtual-cable-test

【功能描述】

virtual-cable-test 命令用来进行以太网连接电缆检测，检测内容包括电缆的状态以及一些物理参数，同时可以检测出故障线缆的长度。

【命令格式】

virtual-cable-test

【视图】

二层以太网接口视图

【缺省情况】

无

【参数说明】

无

【使用举例】

#检测 ge1 的电缆连接状态：

```
NOS# config interface ge1
NOS(if-ge1)# virtual-cable-test
VCT result:
Pair_A: open at length 1
Pair_B: open at length 1
Pair_C: open at length 0
Pair_D: open at length 1
NOS(if-ge1)#
```

【注意事项】

检测过程可能会使接口自动 DOWN/UP 一次，在有业务流量的时候请谨慎使用。

## 18.3 配置举例

(1) 进入接口 ge1 后，将接口配置为默认值
(2) 设置接口描述信息为 port_ge1
(3) 设置接口为半双工模式
(4) 设置 ge1 接口的 UP 时延为 50 毫秒，DOWN 的时延为 100 毫秒
(5) 配置接口速率为 100M
(6) 抑制所有类型风暴，按照 100kbps 进行风暴抑制

```
NOS# config interface ge1
NOS(if-ge1)# default
All configuration on this interface will be removed. Continue? [Y/N]y
NOS(if-ge1)#
NOS(if-ge1)# description port_ge1
NOS(if-ge1)# duplex half
NOS(if-ge1)# link-delay up 50
NOS(if-ge1)# link-delay down 100
NOS(if-ge1)# speed 100
NOS(if-ge1)# storm-suppression all kbps 100
```

## 18.4 常见问题

略。

# 19 MAC

## 19.1 特性简介

MAC（Media Access Control，媒体访问控制）地址表记录了 MAC 地址与接口的对应关系，以及接口所属的 VLAN 等信息。设备在转发报文时，根据报文的目的 MAC 地址查询 MAC 地址表，如果 MAC 地址表中包含与报文目的 MAC 地址对应的表项，则直接通过该表项中的出接口转发该报文；如果 MAC 地址表中没有包含报文目的 MAC 地址对应的表项时，设备将采取广播方式通过对应 VLAN 内除接收接口外的所有接口转发该报文。

## 19.2 命令手册

### 19.2.1 blackhole mac-address

【功能描述】

**blackhole mac-address** 用于配置黑洞 MAC。

**no blackhole mac-address** 用于删除已配置的黑洞 MAC。

【命令格式】

**blackhole mac-address** *X:X:X:X:X:X* **vlan** *VLANID*

**no blackhole mac-address** *X:X:X:X:X:X* **vlan** *VLANID*

【视图】

MAC 配置视图

【缺省情况】

未配置黑洞 MAC

【参数说明】

- *X:X:X:X:X:X*：设置为黑洞 mac 的 mac 地址。
- *VLANID*：指定黑洞 mac 对应的 VLAN ID，取值范围为(1～4094)。

【使用举例】

#配置黑洞 mac 地址为 12:22:33:44:55:66，对应 vlan id 为 1：

```
NOS# config mac
NOS(mac)# blackhole mac-address 12:22:33:44:55:66 vlan 1
NOS(mac)#
```

【注意事项】

不能使用特殊 mac（广播，全 0mac 等）。

### 19.2.2 config mac

【功能描述】

**config mac** 用于进入 MAC 配置视图。

**no config mac** 用于删除 MAC 配置视图下的所有配置、并退出视图。

【命令格式】

**config mac**

**no config mac**

【视图】

根视图

【缺省情况】

无 MAC 视图下相关配置

【参数说明】

无

【使用举例】

#进入 mac 视图：

```
NOS# config mac
NOS(mac)#
```

【注意事项】

无

### 19.2.3 mac-address security

【功能描述】

**mac-address security** 用于打开 mac 地址学习数量限制功能。

**no mac-address security** 用于关闭 mac 地址学习数量限制功能。

【命令格式】

**mac-address security** {**max-count** *COUNT*|**disable-forwarding**}

**no mac-address security**

【视图】

二层以太网接口视图。

【缺省情况】

未开启 MAC 地址学习数量限制功能。

【参数说明】

- **max-count** *COUNT*：设置 mac 地址学习数量限制值，范围为(0～65535)，为 0 时表示禁止学习。
- **disable-forwarding**：mac 地址学习数量达到上限后禁止转发新 MAC 的流量，如果不指定，则会转发（但不学习 mac 地址）。

【使用举例】

#设置 ge1 接口 mac 地址学习数量上限为 100：

```
NOS# interface ge1
NOS(if-ge1)# mac-address security max-count 100
NOS(if-ge1)#
```

【注意事项】

无

### 19.2.4 mac-address static

【功能描述】

**mac-address static** 用于配置静态 mac 地址。

**no mac-address static** 用于删除配置的静态 mac 地址。

【命令格式】

**mac-address static** *X:X:X:X:X:X* **vlan** *VLANID*

[no] **mac-address static** *X:X:X:X:X:X* **vlan** *VLANID*

【视图】

二层以太网接口视图

以太网聚合接口视图

【缺省情况】

无静态 MAC

【参数说明】

*X:X:X:X:X:X*：需要设置为静态 mac 的 mac 地址，不能是特殊 mac（广播，全 0mac 等）。

**vlan** *VLANID*：指定对应的 VLAN ID，取值范围为 1～4094。

【使用举例】

#设置 ge1 接口静态 mac 地址为 22:33:44:55:77:11，对应 vlan1：

```
NOS# interface ge1
NOS(if-ge1)# mac-address static 22:33:44:55:77:11 vlan 1
NOS(if-ge1)#
```

【注意事项】

删除 vlan 或所属接口时，会将对应的静态 mac 自动删除。

### 19.2.5 mac-learning disable

【功能描述】

**mac-learning disable** 用于关闭 VLAN 内的 MAC 学习功能。

**no mac-learning disable** 用于恢复默认情况。

【命令格式】

**mac-learning disable**

**no mac-learning disable**

【视图】

VLAN 视图

【缺省情况】

默认开启 MAC 学习功能

【参数说明】

无

【使用举例】

#关闭 vlan1 的 mac 学习功能

```
NOS# config vlan 1
```

```
NOS(vlan-1)# mac-learning disable
```

【注意事项】

关闭 MAC 学习功能后可能会导致广播，影响正常转发，请谨慎使用。

### 19.2.6 show mac-address

【功能描述】

**show mac-address** 命令用于显示 MAC 地址信息。

【命令格式】

**show mac-address** [**dynamic**|**static**] [{**vlan** *VLANID*|*X:X:X:X:X:X*|*L2_IF*}] [**json**]

**show mac-address blackhole** [{**vlan** *VLANID*|*X:X:X:X:X:X*}] [**json**]

【缺省情况】

不涉及。

【参数说明】

- [**dynamic**|**static**]：显示动态学习或静态配置的 mac 转发表项，如果都不指定，表示显示所有 MAC 表项（动态、静态及黑洞 MAC）。
- **blackhole**：显示黑洞 MAC 表项。
- **vlan** *VLANID*：显示指定 VLAN 内的 mac 转发表项，取值范围为 1～4094。
- *X:X:X:X:X:X*：显示指定 MAC 地址的 MAC 转发表项。
- *L2_IF*：显示指定二层以太网接口下的 MAC 转发表项。
- **json**：以 json 格式输出。

【使用举例】

```
# 显示所有 MAC 地址：
NOS# show mac-address
Totally count 2 entries.

Address           Vlan    Interface         Type
-----------------------------------------------------------
00:00:00:11:11:11   1       -               blackhole
00:00:00:11:11:22   1       ge1              static
```

【注意事项】

无。

### 19.2.7 timer aging

【功能描述】

用于配置动态 mac 的老化时间。

【命令格式】

**timer aging** *TIME*

**no timer aging**

【视图】

mac 配置视图。

【缺省情况】

默认老化时间 300s。

【参数说明】

*TIME*：动态 mac 老化时间（单位：秒），具体范围取决于实际产品。

【使用举例】

# 配置动态 mac 老化时间为 100 秒：

```
NOS# config mac
NOS(mac)# timer aging 100
NOS(mac)#
```

【注意事项】

如果配置较短的老化时间，可能会增加老化的概率、从而增加系统的负荷。

### 19.2.8 reset mac-address

【功能描述】

**reset mac-address** 命令用于重置设备学习到的动态 MAC 地址表项。

【命令格式】

**reset mac-address all**

**reset mac-address interface** *L2_IF* [**vlan** *VLANID*]

**reset mac-address** *X:X:X:X:X:X* [**vlan** *VLANID*]

**reset mac-address vlan** *VLANID* [**interface** *L2_IF*]

【视图】

MAC 配置视图。

【缺省情况】

不涉及。

【参数说明】

- **all**：重置所有动态学习的 MAC 表项。
- **interface** *L2_IF* [**vlan** *VLANID*]：重置指定二层以太网接口下（可同时指定 VLAN）的动态 MAC 表项。
- *X:X:X:X:X:X* [**vlan** *VLANID*]：重置指定 MAC 地址（可同时指定 VLAN）的动态 MAC 表项。
- **vlan** *VLANID* [**interface** *L2_IF*]：重置指定 VLAN 内（可同时指定二层以太网接口）的动态 MAC 表项，取值范围为 1～4094。

【使用举例】

# 重置所有动态 MAC 地址：

```
NOS# show mac-address
Totally count 3 entries.

Address           Vlan    Interface         Type
-----------------------------------------------------------
00:00:00:00:00:20   1      ge1/0/1           static
00:00:00:00:00:30   1      ge1/0/1           dynamic
00:00:00:00:00:40   1      ge1/0/1           dynamic
NOS# reset mac-address all
```

```
NOS# show mac-address
Totally count 1 entries.

Address           Vlan    Interface         Type
-----------------------------------------------------------
00:00:00:00:00:20   1      ge1/0/1           static
```

【注意事项】

无。

## 19.3 配置举例

(1) 进入 mac 视图，配置黑洞 mac 地址为 12:22:33:44:55:66，对应 vlan id 为 1

(2) 设置 ge1 接口 mac 地址学习数量上限为 100

(3) 设置 ge1 接口静态 mac 地址为 22:33:44:55:77:11，对应 vlan1

(4) 配置动态 mac 老化时间为 100 秒

```
NOS# config mac
NOS(mac)# blackhole mac-address 12:22:33:44:55:66 vlan 1
NOS(if-ge1)# mac-address security max-count 100
NOS(if-ge1)# mac-address static 22:33:44:55:77:11 vlan 1
NOS(mac)# timer aging 100
```

(5) 显示所有 MAC 地址：

```
NOS# show mac-address
Totally count 2 entries.

Address           Vlan    Interface         Type
-----------------------------------------------------------
12:22:33:44:55:66   1      -                blackhole
22:33:44:55:77:11   1      ge1              static
```

## 19.4 常见问题

待补充。

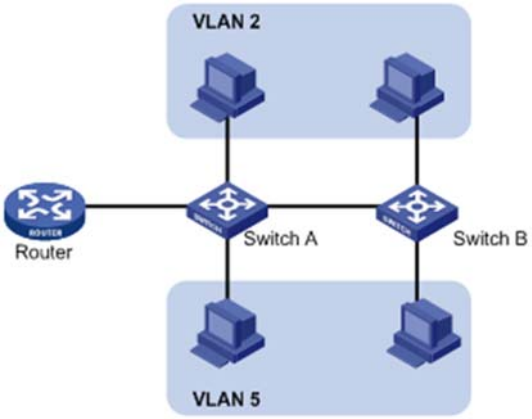
# 20 VLAN 基础

## 20.1 特性简介

### 20.1.1 背景

以太网是一种基于 CSMA/CD（Carrier Sense Multiple Access/Collision Detect，带冲突检测的载波侦听多路访问）技术的共享通讯介质。采用以太网技术构建的局域网，既是一个冲突域，又是一个广播域。当网络中主机数目较多时会导致冲突严重、广播泛滥、性能显著下降，甚至网络不可用等问题。通过在以太网中部署网桥或二层交换机，可以解决冲突严重的问题，但仍然不能隔离广播报文。在这种情况下出现了 VLAN（Virtual Local Area Network，虚拟局域网）技术，这种技术可以把一个物理 LAN 划分成多个逻辑的 LAN——VLAN。处于同一 VLAN 的主机能直接互通，而处于不同 VLAN 的主机则不能直接互通。这样，广播报文被限制在同一个 VLAN 内，即每个 VLAN 是一个广播域。如下图所示，VLAN 2 内的主机可以互通，但与 VLAN 5 内的主机不能互通。

图20-1 图示




VLAN 的划分不受物理位置的限制：物理位置不在同一范围的主机可以属于同一个 VLAN；一个 VLAN 包含的主机可以连接在同一个交换机上，也可以跨越交换机，甚至可以跨越路由器。

VLAN 根据划分方式不同可以分为不同类型。基于端口静态划分 VLAN 是其中最简单、最有效的 VLAN 划分方式。它按照设备端口来定义 VLAN 成员，将指定端口加入到指定 VLAN 中之后，端口就可以转发该 VLAN 的报文。本章将介绍基于端口的 VLAN。

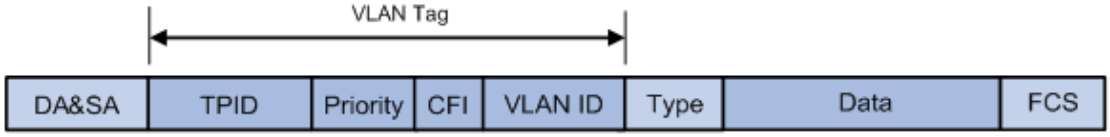
VLAN 的优点如下：

- 限制广播域。广播域被限制在一个 VLAN 内，节省了带宽，提高了网络处理能力。
- 增强局域网的安全性。VLAN 间的二层报文是相互隔离的，即一个 VLAN 内的主机不能和其他 VLAN 内的主机直接通信，如果不同 VLAN 要进行通信，则需通过路由器或三层交换机等三层设备。
- 灵活构建虚拟工作组。通过 VLAN 可以将不同的主机划分到不同的工作组，同一工作组的主机可以位于不同的物理位置，网络构建和维护更方便灵活。

### 20.1.2 原理

要使网络设备能够分辨不同 VLAN 的报文，需要在报文中添加标识 VLAN 的字段。IEEE 802.1Q 协议规定，在以太网报文的目的 MAC 地址和源 MAC 地址字段之后、协议类型字段之前加入 4 个字节的 VLAN Tag，用以标识 VLAN 的相关信息。

图20-2 VLAN Tag 的组成字段




如上图所示，VLAN Tag 包含四个字段，分别是 TPID（Tag Protocol Identifier，标签协议标识符）、Priority、CFI（Canonical Format Indicator，标准格式指示位）和 VLAN ID。

- TPID：协议规定 TPID 取值为 0x8100 时表示报文带有 VLAN Tag，但各设备厂商可以自定义该字段的值。当邻居设备将 TPID 值配置为非 0x8100 时，为了能够识别这样的报文，实现互通，必须在本设备上修改 TPID 值，确保和邻居设备的 TPID 值配置一致。如果报文的 TPID 值为配置值或 0x8100，则该报文被认为带有 VLAN Tag。
- Priority：用来表示报文的 802.1p 优先级，长度为 3 比特，相关内容请参见“ACL 和 QoS 配置指导/QoS”中的“附录”。
- CFI：用来表示 MAC 地址在不同的传输介质中是否以标准格式进行封装，长度为 1 比特。取值为 0 表示 MAC 地址以标准格式进行封装，为 1 表示以非标准格式封装。在以太网中，CFI 取值为 0。
- VLAN ID：用来表示该报文所属 VLAN 的编号，长度为 12 比特。由于 0 和 4095 为协议保留取值，所以 VLAN ID 的取值范围为 1～4094。

网络设备根据报文是否携带 VLAN Tag 以及携带的 VLAN Tag 信息，来对报文进行处理，利用 VLAN ID 来识别报文所属的 VLAN。

- 以太网支持 Ethernet II、802.3/802.2 LLC、802.3/802.2 SNAP 和 802.3 raw 封装格式，本文以 Ethernet II 型封装为例。802.3/802.2 LLC、802.3/802.2 SNAP 和 802.3 raw 封装格式添加 VLAN Tag 字段的方式请参见相关协议规范。
- 对于携带有多层 VLAN Tag 的报文，设备会根据其最外层 VLAN Tag 进行处理，而内层 VLAN Tag 会被视为报文的普通数据部分。

### 20.1.3 协议规范

与 VLAN 相关的协议规范有：

- IEEE 802.1Q：IEEE Standard for Local and Metropolitan Area Networks-Virtual Bridged Local Area Networks。

## 20.2 命令手册

### 20.2.1 config vlan

【功能描述】

**config vlan** 命令用来创建 vlan，若指定单个 vlan 会进入 vlan 视图。

**no config vlan** 命令用来删除创建的 vlan 和 vlan 下的所有配置。

【命令格式】

**config vlan** *VLAN_LIST...*

**no config vlan** *VLAN_LIST...*

【视图】

根视图

【缺省情况】

缺省只存在 vlan 1。

【参数说明】

*VLAN_LIST*：vlan ID，范围 1-4094，VLAN_LIST 支持单个 vlan 输入（如：1）、多个 vlan 输入（如：1 3 5 7，多个 VLAN 之间用空格分隔），或 vlan 范围（如：1 3 5 10-20 30-50）。

【使用举例】

#创建 ID 为 10、20，以及 31 到 40 共 12 个 vlan：

```
NOS# config vlan 10 20 31-40
VLAN creating... OK!
NOS#
```

【注意事项】

同时创建多个 vlan 时只会创建不会进入 VLAN 配置视图，配置单个 VLAN 时才会进入视图。

### 20.2.2 description

【功能描述】

**description** 命令用于给 VLAN 设置描述信息，方便区分业务。

**no description** 命令用于清除 VLAN 的描述信息。

【命令格式】

**description** *DESC*

**no description**

【视图】

VLAN 配置视图

【缺省情况】

无描述信息

【参数说明】

*DESC*：描述信息字符串，不长于 255 字符

【使用举例】

#设置 vlan1 的描述信息为 vlan_1：

```
NOS# vlan 1
NOS(vlan-1)# description vlan_1
NOS(vlan-1)#
```

【注意事项】

无

### 20.2.3 name

【功能描述】

**name** 命令用于给 VLAN 设置名称，可用于 SNMP。

**no name** 命令用于清除 VLAN 名称。

【命令格式】

**name** *NAME*

**no name**

【视图】

VLAN 配置视图

【缺省情况】

未配置名称，在 SNMP 中显示为 vlan<id>

【参数说明】

*NAME*：名称字符串，不长于 255 字符

【使用举例】

#设置 vlan1 的名称为 vlan_1：

```
NOS# vlan 1
NOS(vlan-1)# name vlan_1
NOS(vlan-1)#
```

【注意事项】

无

### 20.2.4 show vlan

【功能描述】

**show vlan** 命令用于显示设备上的 VLAN 信息。

【命令格式】

**show vlan** [<**interface** *SWITCH_IF* | **vid** *VLANID* | **static** | **dynamic**>]

【视图】

任意视图

【缺省情况】

不涉及

【参数说明】

- **interface** *SWITCH_IF*：显示指定接口的详细 VLAN 信息。
- **vid** *VLANID*：显示指定 VLANID 的详细信息。
- **static**：显示所有静态配置的 VLAN 简要信息。
- **dynamic**：显示所有由 MVRP 协议动态创建的 VLAN 简要信息。

【使用举例】

# 显示所有 VLAN 的简要信息：

```
NOS# show vlan
Static Vlan(s):
  1 10 20 31-40
Dynamic Vlan(s):
  NONE
NOS#
```

# 显示指定 VLAN 的详细信息：

```
NOS# show vlan vid 10
VLAN ID:          10
VLAN NAME:     vlan10
```

```
VLAN TYPE:     Static
Total Port Count:   3
---------------------
Tagged Port(s):
   ge2
Untagged Port(s):
   ge1    ge3
NOS#
```

【注意事项】

如果不指定任何参数，表示显示所有静态和动态的 VLAN 简要信息。

### 20.2.5 vlan

【功能描述】

**vlan** 命令用来创建单个 VLAN 并进入 VLAN 配置视图。

【命令格式】

**vlan** *VLANID*

【视图】

根视图

【缺省情况】

缺省只存在 VLAN 1。

【参数说明】

*VLANID*：VLAN ID，范围 1～4094，只支持单个 vlan 输入（如：1）。

【使用举例】

#创建 vlan100 并进入 vlan100 视图：

```
NOS# vlan 100
NOS(vlan-100)#
```

【注意事项】

如需要一次创建多个 VLAN，可使用 **config vlan** 命令。

### 20.2.6 vlan access

【功能描述】

**vlan access** 用于 Access 端口加入到指定的 VLAN 中。

**no vlan access** 用于恢复默认情况。

【命令格式】

**vlan access** *VLANID*

**no vlan access**

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省情况】

所有 Access 端口都属于 VLAN 1。

【参数说明】

*VLANID*：指定 VLAN ID，取值范围(1～4094)。

【使用举例】

#将接口 ge10 加入到 vlan100 中：

```
NOS# interface ge10
NOS(if-ge10)# vlan access 100
NOS(if-ge10)#
```

【注意事项】

接口加入二层聚合口后，不再支持单独配置 VLAN（需要转到聚合口上去配置）。

### 20.2.7 vlan hybrid

【功能描述】

**vlan hybrid** 用于在接口上将指定的 VLAN 通过当前 Hybrid 端口。

**no vlan hybrid** 用于禁止指定的 VLAN 通过当前 Hybrid 端口。

【命令格式】

**vlan hybrid** <**tagged**|**untagged**> *VLAN_LIST...*

**no vlan hybrid** *VLAN_LIST...*

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省情况】

默认仅允许 VLAN 1 以 Untagged 方式通过。

【参数说明】

*VLAN_LIST*：vlan ID，范围 1～4094，VLAN_LIST 支持单个 vlan 输入（如：1）、多个 vlan 输入（如：1 3 5 7，多个 VLAN 之间用空格分隔），或 vlan 范围（如：1 3 5 10-20 30-50）。

【使用举例】

#在接口 ge5 中仅允许 vlan 1 以 tagged 方式通过：

```
NOS# interface ge5
NOS(if-ge5)# vlan hybrid tagged 1
```

【注意事项】

- 只有在 vlan-mode 为 hybrid 的时候才允许进行此配置。
- 接口加入二层聚合口后，不再支持单独配置 VLAN（需要转到聚合口上去配置）。
- 多次配置本命令后，会合并所有配置进行生效，如有冲突则以最新配置为准。

### 20.2.8 vlan hybrid pvid

【功能描述】

**vlan hybrid pvid** 用于配置该 Hybrid 端口的缺省 VLAN。

**no vlan hybrid pvid** 用于将该 Hybrid 端口的缺省 VLAN 设置为默认值 1。

【命令格式】

**vlan hybrid pvid** *VLANID*

**no vlan hybrid pvid**

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省情况】

默认为 1。

【参数说明】

*VLANID*：vlan ID，范围 1～4094。

【使用举例】

#配置接口 ge5 的缺省 vlan 为 100：

```
NOS# interface ge5
NOS(if-ge5)# vlan hybrid pvid 100
```

【注意事项】

- 只有在 vlan-mode 为 hybrid 的时候才允许进行此配置。
- 接口加入二层聚合口后，不再支持单独配置 VLAN（需要转到聚合口上去配置）。

### 20.2.9 vlan trunk permit

【功能描述】

**vlan trunk permit** 用于配置允许指定的 VLAN 通过当前 Trunk 端口。

**no vlan trunk permit** 用于禁止指定的 VLAN 通过当前 Trunk 端口。

【命令格式】

**vlan trunk permit** *VLAN_LIST...*

**no vlan trunk permit** *VLAN_LIST...*

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省情况】

Trunk 端口只允许 VLAN 1 通过。

【参数说明】

*VLAN_LIST*：vlan ID，范围 1～4094，VLAN_LIST 支持单个 vlan 输入（如：1）、多个 vlan 输入（如：1 3 5 7，多个 VLAN 之间用空格分隔），或 vlan 范围（如：1 3 5 10-20 30-50）。

【使用举例】

#配置接口 ge5 为 Trunk 端口并允许 vlan 1 100 通过：

```
NOS# interface ge5
NOS(if-ge5)# vlan-mode trunk
NOS(if-ge5)# vlan trunk permit 1 100
NOS(if-ge5)#
```

【注意事项】

- 只有在 vlan-mode 为 trunk 的时候才允许进行此配置。
- 接口加入二层聚合口后，不再支持单独配置 VLAN（需要转到聚合口上去配置）。
- 多次配置本命令后，会合并所有配置进行生效，如有冲突则以最新配置为准。

### 20.2.10 vlan trunk pvid

【功能描述】

**vlan trunk pvid** 用于配置该 Trunk 端口的缺省 VLAN。

**no vlan trunk pvid** 用于恢复默认值。

【命令格式】

**vlan trunk pvid** *VLANID*

**no vlan trunk pvid**

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省情况】

Trunk 端口的缺省 VLAN 为 VLAN 1。

【参数说明】

*VLANID*：vlan ID，范围 1～4094。

【使用举例】

#配置接口 ge5 为 Trunk 端口并设置缺省 vlan 为 50：

```
NOS# interface ge5
NOS(if-ge5)# vlan-mode trunk
NOS(if-ge5)# vlan trunk pvid 50
NOS(if-ge5)#
```

【注意事项】

- 只有在 vlan-mode 为 trunk 的时候才允许进行此配置。
- 接口加入二层聚合口后，不再支持单独配置 VLAN（需要转到聚合口上去配置）。

### 20.2.11 vlan-mode

【功能描述】

**vlan-mod** 命令用设置端口 vlan 模式。

**no vlan-mode** 命令用来恢复默认情况。

【命令格式】

**vlan-mode** <**access**|**hybrid**|**trunk**>

**no vlan-mode**

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省情况】

缺省为 access 模式。

【参数说明】

- **access**：接口 vlan 为 access 模式。
- **hybrid**：接口 vlan 为 hybrid 模式。
- **trunk**：接口 vlan 为 trunk 模式。

【使用举例】

#配置接口 ge5 接口 vlan 为 hybrid 模式：

```
NOS# interface ge5
NOS(if-ge5)# vlan-mode hybrid
NOS(if-ge5)#
```

【注意事项】

切换模式会将该接口下原来的 vlan 配置全部清除。

## 20.3 配置举例

(1) 设置 vlan1 的描述信息为 vlan_1

(2) 设置 vlan1 的名称为 vlan_1

(3) 将接口 ge5 加入到 vlan1 中

(4) 配置接口 ge2 为 hybrid 接口，pvid 为 10，允许 VLAN 1 以 Untagged 方式通过

(5) 配置接口 ge3 为 trunk 接口，pvid 为 20，允许 vlan1 通过当前 Trunk 端口

```
NOS(vlan-1)# description vlan_1
NOS(vlan-1)# name vlan_1
NOS(vlan-1)# interface ge5
NOS(if-ge5)# vlan access 1
NOS(if-ge5)# quit
NOS# interface ge2
NOS(if-ge2)# vlan-mode hybrid
NOS(if-ge2)# vlan hybrid pvid 10
NOS(if-ge2)# vlan hybrid untagged 1
NOS(if-ge2)# interface ge3
NOS(if-ge3)# vlan-mode trunk
NOS(if-ge3)# vlan trunk permit 1
NOS(if-ge3)# vlan trunk pvid 20
```

## 20.4 常见问题

待补充。

# 21 动态 VLAN

## 21.1 特性简介

动态 VLAN 是一种根据报文信息（例如端口、MAC 地址、IP 子网地址、网络协议等）进行 VLAN 划分的功能，目前支持的类型和优先级为：MAC VLAN > IP 子网 VLAN > 协议 VLAN > 静态 VLAN。

**基于 MAC 地址的 vlan：**

根据报文携带的 MAC 地址信息进行对应的 vlan tag 编辑。在实现中，本设备使用源 MAC 地址作为规则匹配的对象，对本身不存在 vlan tag 的二层报文和三层报文添加 vlan tag，而对于已有 vlan tag 的报文，则根据端口 vlan 规则进行操作。

**基于 IP 子网的 vlan：**

根据报文携带的 IP 地址信息进行 vlan tag 编辑。本设备使用源 IP 地址作为规则匹配的对象，对本身不存在 vlan tag 的三层报文添加 vlan tag，而对于已有 vlan tag 的报文，则根据端口 vlan 规则进行操作。由于 IP 报文在数据交流时的特点，在下发 IP-VLAN 匹配规则的同时也会下发一条相同 IP 地址的 ARP 匹配规则。

**基于网络协议的 vlan：**

根据报文携带的网络协议封装方式和协议号进行 vlan tag 的编辑。对于本身已经存在 vlan tag 的报文(假设协议为以太网 II、协议号 8100)，即使添加了匹配类型为以太网 II、协议号为 8100 的规则，交换机依然会将该报文视作已经存在 vlan tag 的报文，根据端口 vlan 规则操作；但是，若设置交换机用于分辨报文是否携带 vlan tag 的 tpid 值为其他合法参数，则将协议号为 8100 的报文视为本身不存在 vlan tag 的报文，添加 vlan tag。

## 21.2 命令手册

### 21.2.1 config ip-subnet-vlan

【功能描述】

**config ip-subnet-vlan** 命令用来进入 ip-subnet-vlan 视图。

**no config ip-subnet-vlan** 命令用来删除 ip-subnet-vlan 视图和该视图下的所有配置。

【命令格式】

[no] **config ip-subnet-vlan**

【视图】

根视图

【缺省情况】

缺省不存在 ip-subnet-vlan 视图和配置。

【参数说明】

无

【使用举例】

#进入 ip-subnet-vlan 视图：

```
NOS# config ip-subnet-vlan
NOS(ip-subnet-vlan)#
```

【注意事项】

无

### 21.2.2 config mac-vlan

【功能描述】

**config mac-vlan** 命令用来进入 mac-vlan 视图。

**no config mac-vlan** 命令用来删除 mac-vlan 视图和该视图下的所有配置。

【命令格式】

[no] **config mac-vlan**

【视图】

根视图。

【缺省情况】

缺省不存在 mac-vlan 视图。

【参数说明】

无

【使用举例】

#进入 mac-vlan 视图：

```
NOS# config mac-vlan
NOS(mac-vlan)#
```

【注意事项】

无

### 21.2.3 config protocol-vlan

【功能描述】

**config protocol-vlan** 命令用来进入 protocol-vlan 视图。

**no config protocol-vlan** 命令用来删除 protocol-vlan 视图和该视图下的所有配置。

【命令格式】

[no] **config protocol-vlan**

【视图】

根视图

【缺省情况】

不存在 protocol-vlan 视图。

【参数说明】

无。

【使用举例】

#进入 protocol-vlan 视图：

```
NOS# config protocol-vlan
NOS(protocol-vlan)#
```

【注意事项】

无

### 21.2.4 ip-subnet-vlan

【功能描述】

**ip-subnet-vlan** 用于添加一条基于 ip 地址或 ip 子网的 vlan 匹配规则。

**no ip-subnet-vlan** 用于删除基于 ip 地址或 ip 子网的 vlan 匹配规则。

【命令格式】

**ip-subnet-vlan** <*A.B.C.D* | *A.B.C.D/M*> **vlan** *VLANID*

**no ip-subnet-vlan**<*A.B.C.D* | *A.B.C.D/M* | **all**>

【视图】

ip-subnet-vlan 视图

【缺省情况】

不存在 ip 子网 vlan 规则。

【参数说明】

*A.B.C.D*：指定要匹配的 ip 地址，不允许 127 开头、全 0、掩码为 0 的 ip 地址。

*A.B.C.D/M*：指定要匹配的 ip 子网，不允许 127 开头、全 0、掩码为 0 的 ip 地址。

**vlan** *VLANID*：指定匹配成功后添加的 VLAN ID，范围(1-4094)。

**all**：删除所有已配置的匹配规则，删除时如果不指定任何参数，默认为 all。

【使用举例】

# 为属于 IP 子网 192.168.5.0/24 的报文添加 vlan-id 为 10 的 vlan tag，为属于 IP 地址 192.168.1.120 的报文添加 vlan-id 为 20 的 vlan tag。

```
NOS# config vlan 10-20
NOS# config ip-subnet-vlan
NOS(ip-subnet-vlan)# ip-subnet-vlan 192.168.5.24/24 vlan 10
NOS(ip-subnet-vlan)# ip-subnet-vlan 192.168.1.120 vlan 20
```

【注意事项】

- 若要使 ip-subnet-vlan 配置生效，须创建好对应的 vlan，在端口下使能 ip-subnet-vlan 并允许该 vlan 报文通过。建议使用端口的 hybrid 模式并将对应 vlan 添加到 hybrid 的 tagged 列表。
- ip 子网之间不允许有任何重叠，不允许 127 开头、全 0、掩码为 0 的 ip 地址。

### 21.2.5 ip-subnet-vlan enable

【功能描述】

**ip-subnet-vlan enable** 用于在接口下使能 ip-subnet-vlan 功能。

**no ip-subnet-vlan enable** 用于在接口下取消 ip-subnet-vlan 功能的使能。

【命令格式】

[**no**] **ip-subnet-vlan enable**

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省情况】

接口未使能 ip-subnet-vlan 功能。

【参数说明】

无。

【使用举例】

# 在接口 ge4 下使能 ip-subnet-vlan 功能。

```
NOS# interface ge4
NOS(if-ge4)# ip-subnet-vlan enable
NOS(if-ge4)#
```

【注意事项】

二层接口加入二层聚合口后，聚合口的成员接口的 ip-subnet-vlan enable 行为会同步为与聚合口保持一致；二层接口退出聚合口后，ip-subnet-vlan enable 配置将被清空。

### 21.2.6 mac-vlan

【功能描述】

**mac-vlan** 用于添加一条基于 mac 地址的 vlan 匹配规则。

**no mac-vlan** 用于删除基于 mac 地址的 vlan 匹配规则。

【命令格式】

**mac-vlan** *X:X:X:X:X:X* **vlan** *VLANID* [**priority** *PRIORITY*]

**no mac-vlan** <*X:X:X:X:X:X*|**all**>

【视图】

mac-vlan 视图

【缺省情况】

不存在 mac-vlan 规则。

【参数说明】

*X:X:X:X:X:X*：指定要匹配的 mac 地址，不允许组播和全 0 的 mac 地址。

**vlan** *VLANID*：指定匹配成功后添加的 VLAN ID，范围(1-4094)。

**priority** *PRIORITY*：指定匹配成功后要修改成的 802.1 优先级，缺省值为 0，范围 0-7。

**all**：删除所有已配置的匹配规则。

【使用举例】

```
NOS# config mac-vlan
NOS(mac-vlan)# mac-vlan 12:22:22:33:33:44 vlan 100
NOS(mac-vlan)#
```

【注意事项】

- 若要使 mac-vlan 配置生效，须创建好对应的 vlan，在端口下使能 mac-vlan 并允许该 vlan 报文通过。建议使用端口的 hybrid 模式并将对应 vlan 添加到 hybrid 的 tagged 列表。
- 不允许配置重复 mac 地址的表项，替换前请先删除原表项。

### 21.2.7 mac-vlan enable

【功能描述】

**mac-vlan enable** 用于在端口或聚合口下使能 mac vlan 功能。

**no mac-vlan enable** 用于在端口或聚合口下取消 mac vlan 功能的使能。

【命令格式】

[no] **mac-vlan enable**

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省情况】

mac vlan 功能未使能。

【参数说明】

无。

【使用举例】

# 在接口 ge4 下使能 mac vlan 功能。

```
NOS# interface ge4
NOS(if-ge4)# mac-vlan enable
NOS(if-ge4)#
```

【注意事项】

二层接口加入二层聚合口后，聚合口的成员接口的 mac vlan enable 行为会同步为与聚合口保持一致；二层接口退出聚合口后，mac vlan enable 配置将被清空。

### 21.2.8 protocol-vlan

【功能描述】

**protocol-vlan** 用于添加一条基于报文封装类型和协议类型的 vlan 匹配规则。

**no protocol-vlan** 用于删除基于报文封装类型和协议类型的 vlan 匹配规则。

【命令格式】

**protocol-vlan** *INDEX* <**ethernetii** <**ipv4**|**ipv6**|**etype** *TYPEID*>|**llc dsap** *DSAPID* **ssap** *SSAPID*|**snap type** *TYPEID*|**raw ipx**> **default-vlan** *VLANID*

**no protocol-vlan** <*INDEX*|**all**>

【视图】

protocol-vlan 视图

【缺省情况】

不存在 protocol-vlan 规则。

【参数说明】

- *INDEX*：由用户指定的协议 VLAN 模板的索引值，取值范围取决于实际产品。
- **ethernetii** <**ipv4**|**ipv6**|**etype** *TYPEID*>：指定匹配的协议类型，*TYPEID* 取值范围为 16 进制数 0600~ffff，ipv4 代表 type 0800，ipv6 代表 type 86dd。
- **llc dsap** *DSAPID* **ssap** *SSAPID*：LLC 的目的服务接入点和源服务接入点，*SSAPID* 的取值范围为 16 进制数 00~ff。

- **snap type** *TYPEID*：匹配 SNAP 封装格式及相应的协议类型值，取值范围为十六进制数 600～ffff。
- **raw ipx**：基于 IPX 协议的 VLAN，RAW 封装类型。
- **default-vlan** *VLANID*：协议模板默认绑定的 vlan-id，范围 1-4094，当端口使能了对应的协议模板时，匹配成功的报文会被打上对应的 vlan tag。
- **all**：删除所有已配置的匹配规则，如果删除时不指定任何参数，默认为 all。

【使用举例】

# 创建一条索引值为 1，匹配协议类型为 ipv4 的规则绑定到 vlan100 上。

```
NOS# config protocol-vlan
NOS(protocol-vlan)# protocol-vlan 1 ethernetii ipv4 default-vlan 100
NOS(protocol-vlan)#
```

【注意事项】

若要使 protocol-vlan 配置生效，须创建好对应的 vlan，在端口下使能 protocol-vlan 并允许该 vlan 报文通过。建议使用端口的 hybrid 模式并将对应 vlan 添加到 hybrid 的 tagged 列表。

协议类型为 ipv4 与 type 0800 视作同一类型；ipv6 与 type 86dd 视作同一类型；相同的协议类型或相同的 pidx 都不允许使用。

### 21.2.9 protocol-vlan enable

【功能描述】

**protocol-vlan enable** 用于在端口或聚合口下使能 protocol vlan 功能。

**no protocol-vlan enable** 用于在端口或聚合口下取消 protocol vlan 功能的使能。

【命令格式】

[no] **protocol-vlan enable** <*INDEX*|**all**>

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省情况】

接口未使能 protocol vlan 功能。

【参数说明】

- *INDEX*：配置或取消指定的协议 VLAN 配置项，取值范围取决于实际产品。
- **all**：配置或取消所有协议 VLAN 配置项。

【使用举例】

# 在接口 ge4 下使能 protocol vlan 功能。

```
NOS# interface ge4
NOS(if-ge4)# protocol-vlan enable all
NOS(if-ge4)#
```

【注意事项】

二层接口加入二层聚合口后，聚合口的成员接口的 protocol-vlan enable 行为会同步为与聚合口保持一致；二层接口退出聚合口后，protocol-vlan enable 配置将被清空。

### 21.2.10 show mac-vlan all

【功能描述】

**show mac-vlan all** 命令用来查看 mac-vlan 表项。

【命令格式】

**show mac-vlan all**

【视图】

所有视图

【缺省情况】

不涉及

【参数说明】

无

【使用举例】

#查看所有 mac-vlan 表项。

```
NOS# show mac-vlan all
Totally count 1 entries.

Address           Vlan    Pri     Static
-----------------------------------------------------------
12:22:22:33:33:44   100     0       YES
NOS#
```

【注意事项】

无

# 22 VLAN Mapping

## 22.1 特性简介

VLAN 映射（VLAN Mapping）也叫做 VLAN 转换（VLAN Translation），用于修改报文携带的 VLAN Tag，以实现不同 VLAN ID 之间的相互转换。目前支持的类型如下：

- 1:1 VLAN 映射：将来自某一特定 VLAN 的报文所携带的 VLAN ID 替换为新的 VLAN ID。
- N:1 VLAN 映射：将来自某一范围内 VLAN 的报文所携带的 VLAN ID 替换为新的 VLAN ID。

## 22.2 命令手册

### 22.2.1 vlan mapping

【功能描述】

**vlan mapping** 命令用来在创建 N:1 VLAN 映射。

**no vlan mapping** 命令用来删除 N:1 VLAN 映射。

【命令格式】

**vlan mapping** *VLANLIST* **remark** *VLANID*

**no vlan mapping** <*VLANLIST* **remark** *VLANID* | **all**>

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省情况】

未创建 N:1 VLAN 映射。

【参数说明】

*VLANLIST*：原始 VLAN ID，可以时单个 VLAN 也可以是一个 VLAN 列表，范围为(1～4094)。

*VLANID*：转换后 VLAN ID，范围为 1～4094，原始 VLAN ID 和转换后的 VLAN ID 不允许相同。

**all**：删除接口上配置的所有 N:1 VLAN 映射。

【使用举例】

```
NOS# interface ge5
NOS(if-ge5)# vlan mapping 1-100 remark 200
NOS(if-ge5)#
```

【注意事项】

无

### 22.2.2 vlan translation

【功能描述】

**vlan translation** 命令用来在创建 1:1 VLAN 映射。

**no vlan translation** 命令用来删除 1:1 VLAN 映射。

【命令格式】

**vlan translation** *VLANID* **remark** *VLANID*

**no vlan translation** <*VLANID* **remark** *VLANID* | **all**>

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省情况】

未创建 1:1 VLAN 映射。

【参数说明】

*VLANID*：原始 VLAN ID 及转换后 VLAN ID，取值范围为(1～4094)。

**all**：删除接口上配置的所有 1:1 VLAN 映射。

【使用举例】

```
NOS# interface ge5
NOS(if-ge5)# vlan translation 100 remark 200
```

【注意事项】

无

### 22.2.3 show vlan mapping

【功能描述】

**show vlan mapping** 命令用来查看 VLAN 映射信息。

【命令格式】

**show vlan mapping** [**interface** *SWITCH_IF*]

【视图】

任意视图

【缺省情况】

不涉及

【参数说明】

**interface** *SWITCH_IF*：查看指定二层接口下的 VLAN 映射信息。

【使用举例】

#查看 vlan 映射关系。

```
NOS# show vlan mapping
Port              Src Vlan Id    Mapped Vlan Id
----------------    ----------     ------------
ge1/0/1            10          20
```

【注意事项】

无

## 22.3 配置举例

(1) xge1/0/2 中 vlan10 映射为 vlan20

(2) xge1/0/1 中 vlan10 映射为 vlan20

```
NOS# config interface xge1/0/2
NOS(if-xge1/0/2)# vlan mapping 10 remark 20
NOS# config interface xge1/0/1
NOS(if-xge1/0/1)# vlan translation 10 remark 20
```

(3) 查看 vlan 映射关系。

```
NOS# show vlan mapping
Port              Src Vlan Id    Mapped Vlan Id
----------------    ----------     ------------
xge1/0/1           10          20
xge1/0/2           10          20
```

## 22.4 常见问题

待补充。

# 23 Private VLAN

## 23.1 特性简介

私有 VLAN（Private VLAN）是指采用两层 VLAN 划分的一种 VLAN 隔离方法，第二层的从 VLAN 对外不可见，因此叫私有 VLAN。通过配置主从两级 VLAN，既能够保证接入用户之间相互隔离，又能将接入的 VLAN ID 屏蔽掉，从而节省了 VLAN 资源。

- 主 VLAN：也叫 Principal VLAN，用于连接上行设备，一个主 VLAN 可以和多个从 VLAN 相对应。上行设备只需知道主 VLAN，不必关心从 VLAN（不可见）。
- 从 VLAN：也叫 Secondary VLAN，用于连接用户，从 VLAN 之间二层报文互相隔离。如果需要互通，可通过走三层实现。

## 23.2 命令手册

### 23.2.1 config private-vlan

【功能描述】

[no] **config private-vlan** 用于进入私有 vlan 视图或删除所有私有 vlan。

【命令格式】

[no] **config private-vlan**

【视图】

根视图

【缺省情况】

不存在私有 vlan 视图。

【参数说明】

无

【使用举例】

#进入私有 vlan 视图。

```
NOS# config private-vlan
NOS(private-vlan)#
```

【注意事项】

无

### 23.2.2 principal-vlan

【功能描述】

**principal-vlan** 用于配置主 vlan id 并进入主 VLAN 配置视图。

**no principal-vlan** 用于删除主 VLAN 配置视图及下面的所有从 VLAN 配置。

【命令格式】

**principal-vlan** *VLANID*

**no principal-vlan** *VLANID*

【视图】

私有 vlan 视图

【缺省情况】

不存在私有 vlan 主 vlan 配置。

【参数说明】

*VLANID*：配置主 vlan id，vlan 范围为(1-4094)。

【使用举例】

#进入私有 vlan 视图并配置主 vlan id 为 100。

```
NOS# config private-vlan
NOS(private-vlan)# principal-vlan 100
NOS(private-vlan/principal-vlan-100)#
```

【注意事项】

无

### 23.2.3 secondary-vlan

【功能描述】

**secondary-vlan** 用于配置从 vlan id。

**secondary-vlan** 用于删除从 vlan id 配置。

【命令格式】

**secondary-vlan** *VLANID*

**no secondary-vlan** *VLANID*

【视图】

主 vlan 视图

【缺省情况】

不存在私有 vlan 从 vlan 配置。

【参数说明】

*VLANID*：配置从 vlan id，id 范围为(1-4094)。

【使用举例】

#进入私有 vlan 视图并配置从 vlan id 为 200。

```
NOS# config private-vlan
NOS(private-vlan)# principal-vlan 100
NOS(private-vlan/principal-vlan-100)# secondary-vlan 200
NOS(private-vlan/principal-vlan-100)#
```

【注意事项】

该命令可以配置多条，表示多个从 VLAN 对应同一个主 VLAN

## 23.3 配置举例

(1) 进入私有 vlan 视图并配置主 vlan id 为 100。

(2) 配置从 vlan id 为 200

```
NOS# config private-vlan
```

```
NOS(private-vlan)# principal-vlan 100
NOS(private-vlan/principal-vlan-100)# secondary-vlan 200
NOS(private-vlan/principal-vlan-100)#
```

## 23.4 常见问题

待补充。

# 24 QinQ

## 24.1 QinQ功能

### 24.1.1 基本QinQ功能简介

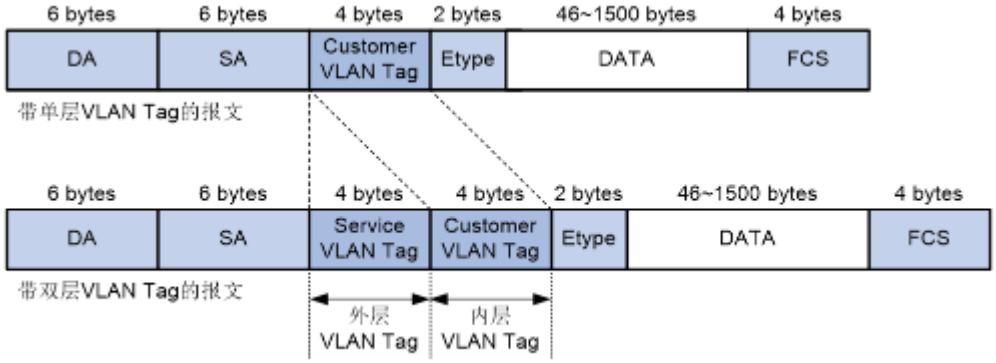
QinQ 是 802.1Q in 802.1Q 的简称，是基于 IEEE 802.1Q 技术的一种比较简单的二层 VPN（Virtual Private Network，虚拟专用网络）协议。QinQ 通过将一层 VLAN Tag 封装到私网报文上，使其携带两层 VLAN Tag 穿越运营商的骨干网络（又称公网），从而使运营商能够利用一个 VLAN 为包含多个 VLAN 的用户网络提供服务。QinQ 最多可以提供 4094 x 4094 个 VLAN，满足了城域网对 VLAN 数量的需求。

### 24.1.2 工作原理

如图所示，QinQ 报文在运营商网络中传输时带有双层 VLAN Tag：

- 内层 VLAN Tag：为用户的私网 VLAN Tag，对应图中的 Customer VLAN Tag（简称 CVLAN）。设备依靠该 Tag 在私网中传送报文。
- 外层 VLAN Tag：为运营商分配给用户的公网 VLAN Tag，对应图中的 Service VLAN Tag（简称 SVLAN）。设备依靠该 Tag 在公网中传送 QinQ 报文。

图24-1 QinQ 的报文结构




## 24.2 基于VLAN的灵活QinQ

灵活 QinQ 是对 QinQ 的一种更灵活的实现，又叫 VLAN Stacking 或 QinQ Stacking。它是基于接口和 VLAN 相结合的方式实现的，对于同一个接口可以根据报文携带 VLAN 的不同添加不同的外层 VLAN Tag。

灵活 QinQ 功能是对基本 QinQ 功能的扩展，它比基本 QinQ 的功能更灵活。二者主要区别是：

基本 QinQ：对进入二层 QinQ 接口的所有帧都加上相同的外层 Tag。

灵活 QinQ：对进入二层 QinQ 接口的帧，可以根据不同的 VLAN Tag 而加上不同的外层 VLAN Tag，对于 VLAN 的划分更细致。

需要实现的功能：基于 VLAN ID 的灵活 QinQ，为具有不同 VLAN ID 的报文添加不同的外层 VLAN Tag。

## 24.3 命令手册

### 24.3.1 config qinq customer-tpid

【功能描述】

**config qinq customer-tpid** 命令用于配置全局内层 VLAN Tag 的 TPID 值。

**no config qinq customer-tpid** 命令用于恢复全局内层 VLAN Tag 的 TPID 值为 0x8100。

【命令格式】

**config qinq customer-tpid** *HEX_VALUE*

**no config qinq customer-tpid**

【视图】

根视图

【缺省情况】

缺省情况下，内层 VLAN Tag 的 TPID 值为 0x8100。

【参数说明】

*HEX_VALUE*：TPID 值，16 进制形式（不需要 0x 前缀），范围 1～FFFF。

【使用举例】

#配置全局内层 VLAN Tag 的 TPID 值为 8200。

```
NOS# config qinq customer-tpid 8200
```

【注意事项】

第三方厂商的设备可能将 QinQ 报文外层 VLAN Tag 的 TPID 设为不同的值。为了与这些厂商的设备兼容，用户可以通过修改 TPID 值，使发送的 QinQ 报文携带的 TPID 值与第三方厂商的相同，从而实现与这些厂商的设备互通。

### 24.3.2 qinq enable

【功能描述】

**qinq enable** 命令用于开启该接口下 QinQ 功能。

**no qinq enable** 命令关闭该接口 QinQ 功能。

【命令格式】

**qinq enable**

**no qinq enable**

【视图】

二层接口视图

【缺省情况】

接口未开启 QinQ 功能。

【参数说明】

无

【使用举例】

#开启接口 ge1 下 QinQ 功能。

```
NOS# interface ge1
NOS(if-ge1)# qinq enable
```

【注意事项】

无

### 24.3.3 qinq service-tpid

【功能描述】

**qinq service-tpid** 命令用于配置该接口下外层 VLAN Tag 的 TPID 值。

**no qinq service-tpid** 命令用于恢复该接口下外层 VLAN Tag 的 TPID 值为 0x8100。

【命令格式】

**qinq service-tpid** *HEX_VALUE*

**no qinq service-tpid**

【视图】

二层接口视图

【缺省情况】

缺省情况下，外层 VLAN Tag 的 TPID 值为 0x8100。

【参数说明】

*HEX_VALUE*：TPID 值，16 进制形式，范围 1～FFFF，一个端口下同时只支持配置一个。

【使用举例】

#配置接口 ge1 下外层 VLAN Tag 的 TPID 值为 8200。

```
NOS# interface ge1
NOS(if-ge1)# qinq service-tpid 8200
```

【注意事项】

外层 VLAN Tag 的 TPID 值应在设备的运营商侧的接口上进行配置。

### 24.3.4 qinq service-vlan-id

【功能描述】

**qinq service-vlan-id** 命令用于配置一条基于用户 VLAN ID 添加外层 VLAN ID 的灵活 QinQ。

**no qinq service-vlan-id** 命令用于删除一条基于用户 VLAN ID 添加外层 VLAN ID 的灵活 QinQ 配置。

【命令格式】

**qinq service-vlan-id** *VLANID* **customer-vlan-id** *VLANLIST...*

**no qinq service-vlan-id** *VLANID* **customer-vlan-id** *VLANLIST...*

【视图】

二层接口视图

【缺省情况】

接口下未配置。

【参数说明】

**service-vlan-id** *VLANID*：需要叠加到报文外层的外层 VLAN ID（运营商 VLAN），取值范围（1-4094）。

**customer-vlan-id** *VLANLIST*：需要匹配的用户 VLAN ID 范围。

【使用举例】

#配置接口 ge1 下叠加到报文外层的外层 VLAN ID 为 100，需要匹配的用户 VLAN ID 为 200。

```
NOS# interface ge1
```

```
NOS(if-ge1)# qinq service-vlan-id 100 customer-vlan-id 200
```

【注意事项】

无

### 24.3.5 qinq transparent

【功能描述】

**qinq transparent** 命令用于配置 QinQ 下的 VLAN 透传功能。

**no qinq transparent** 命令用于恢复默认情况。

【命令格式】

**qinq transparent** *VLANLIST...*

**no qinq transparent** *VLANLIST...*

【视图】

二层接口视图

【缺省情况】

接口下未配置 VLAN 透传。

【参数说明】

*VLANLIST*：需要透传的用户 VLAN ID 范围。

【使用举例】

#配置接口 ge1 下需要透传的用户 VLAN ID 为 1，100。

```
NOS# config interface ge1
NOS(if-ge1)# qinq transparent 1 100
```

【注意事项】

- 端口上使能了 QinQ 功能后，从该端口收到的报文就会被打上额外 Tag。而 VLAN 透传功能则可以指定对某些用户 VLAN 不做该操作。
- 多次执行本命令，按 VLAN 合集生效。

# 25 Voice VLAN

## 25.1 特性简介

Voice VLAN 是为用户的语音数据流专门划分的 VLAN。通过划分 Voice VLAN 并将连接语音设备的端口加入 Voice VLAN，系统自动为语音报文修改 QoS（Quality of Service，服务质量）参数，来提高语音数据报文优先级、保证通话质量。

## 25.2 命令手册

### 25.2.1 config voice-vlan

【功能描述】

[no] **config voice-vlan** 用于进入语音 vlan 视图或删除全局所有语音 vlan 配置。

【命令格式】

[no] **config voice-vlan**

【视图】

根视图

【缺省情况】

不存在语音 vlan 视图。

【参数说明】

无

【使用举例】

#进入语音 vlan 视图。

```
NOS# config voice-vlan
NOS(voice-vlan)#
```

【注意事项】

无

### 25.2.2 voice-vlan security enable

【功能描述】

[no] **voice-vlan security enable** 用于开启或关闭全局语音 vlan 安全模式。

【命令格式】

[no] **voice-vlan security enable**

【视图】

语音 vlan 视图

【缺省情况】

关闭语音 vlan 安全模式。

【参数说明】

无

【使用举例】

#开启语音 vlan 安全模式。

```
NOS# config voice-vlan
NOS(voice-vlan)# voice-vlan security enable
```

【注意事项】

无

### 25.2.3 voice-vlan mac-address

【功能描述】

**voice-vlan mac-address** 用于添加全局 oui 地址。

**no voice-vlan mac-address** 用于删除全局 oui 地址。

【命令格式】

[no] **voice-vlan mac-address** *X:X:X:X:X:X* **mask** *X:X:X:X:X:X*

【视图】

语音 vlan 视图

【缺省情况】

没有配置 OUI mac 地址。

【参数说明】

*X:X:X:X:X:X*：需要设置为 OUI 地址。

*X:X:X:X:X:X*：需要设置为 OUI 地址的掩码。

【使用举例】

#添加 OUI mac 地址为 00:00:00:00:00:20。

```
NOS# config voice-vlan
NOS(voice-vlan)# voice-vlan mac-address 00:00:00:00:00:20 mask ff:ff:ff:ff:ff:ff
```

【注意事项】

无

### 25.2.4 voice-vlan enable

【功能描述】

**voice-vlan enable** 用于使能接口下 voicevlan 功能。

**no voice-vlan enable** 用于关闭接口下 voicevlan 功能。

【命令格式】

[no] **voice-vlan enable** *VLANID*

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省情况】

接口未开启 voicevlan 功能。

【参数说明】

*VLANID*：配置主 vlan id，vlan 范围为(2-4094)。

【使用举例】

#使能端口下 vlan 为 10 的 voicevlan。

```
NOS# config interface ge1/0/1
NOS(if-ge1/0/1)# voice-vlan 10 enable
```

【注意事项】

无

### 25.2.5 voice-vlan qos

【功能描述】

**voice-vlan qos** 用于设置接口 voice vlan cos 和 dscp 的值。

**no voice-vlan qos** 用于删除接口 voice vlan cos 和 dscp 的值

【命令格式】

[no] **voice-vlan** *dscp* [*cos*]

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省情况】

接口未配置 voicevlan qos 值。

【参数说明】

*dscp:* dscp 范围为（0-63）

*cos:* cos 范围为（0-7）

【使用举例】

#设置端口下 voicevlan dscp 为 10。

```
NOS# config interface ge1/0/1
NOS(if-ge1/0/1)# voice-vlan qos 10
```

【注意事项】

无

### 25.2.6 show voice-vlan

【功能描述】

**show voice-vlan** 用于显示 voicevlan 的配置信息

【命令格式】

**show voice-vlan** [**interface** *SWITCH_IF*]

【视图】

任意视图

【缺省情况】

不涉及

【参数说明】

**interface** *SWITCH_IF*: 查看指定二层接口下的 VLAN 映射信息。

【使用举例】

#查看当前配置的 voivevlan 信息。

```
NOS# show voice-vlan
Global Voice VLAN Security Mode: Disabled

Interface         Voice VLAN ID  Status    CoS   DSCP
----------------    ----------    ------------------------

Voice VLAN OUI MAC Addresses:
MAC Address        Mask
------------------- ------------------
```

【注意事项】

无

# 26 LLDP

## 26.1 功能介绍

### 26.1.1 特性简介

#### 1. 协议概述

随着网络技术的发展，接入网络的设备的种类越来越多，配置越来越复杂，来自不同设备厂商的设备也往往会增加自己特有的功能，这就导致在一个网络中往往会有很多具有不同特性的、来自不同厂商的设备，为了方便对这样的网络进行管理，就需要使得不同厂商的设备能够在网络中相互发现并交互各自的系统及配置信息。

LLDP（Link Layer Discovery Protocol，链路层发现协议）就是用于这个目的的协议。LLDP 定义在 802.1ab 中,它是一个二层协议，它提供了一种标准的链路层发现方式。LLDP 协议使得接入网络的一台设备可以将其主要的能力，管理地址，设备标识，接口标识等信息发送给接入同一个局域网络的其它设备。当一个设备从网络中接收到其它设备的这些信息时，它就将这些信息以 MIB 的形式存储起来。

这些 MIB 信息可用于发现设备的物理拓扑结构以及管理配置信息。需要注意的是 LLDP 仅仅被设计用于进行信息通告,它被用于通告一个设备的信息并可以获得其它设备的信息,进而得到相关的 MIB 信息。它不是一个配置、控制协议，无法通过该协议对远端设备进行配置，它只是提供了关于网络拓扑以及管理配置的信息，这些信息可以被用于管理、配置的目的，如何用取决于信息的使用者。

#### 2. 应用场景

**LLDP 产生背景**

由于网络设备生产厂商众多，造成网络设备的种类繁多。儿各个厂商的网络设备的配置即其他信息各不相同，为了使不同厂商的设备能够在网络中相互发现并交互各自的系统配置信息，需要有一个标准的信息交流平台。LLDP 协议就是 在这样的背景下产生的。

**LLDP 的存在意义**

现在存在很多网络管理系统，该系统可以直接获取网络的拓扑，各设备的描述等有用信息。当然，根据该系统也就很方便的进行查询即判断链路的通信状况等工作，而网络管理系统时以 LLDP 协议为支撑，其所获取的数据也是由 LLDP 收集、组织并提供的，由此可见其存在意义。

**应用场景**

当存在网络管理系统，可以的获取网络的拓扑信息；

当网络链路出现故障时，更方便快捷地获得链路的通信状况，根据链路状况可以迅速地找到链路故障所在，避免人工排查的麻烦及效率低下。LLDP 支持配置 TLV，可以实现自主决定和邻居交互那些 TLV 信息。

## 26.2 命令手册

### 26.2.1 config lldp

【功能描述】

no config lldp 命令用于禁用 lldp 服务。

config lldp 命令用于启用 lldp 服务。

【命令格式】

config lldp

no config lldp

【视图】

根视图

【缺省情况】

未启用 lldp 服务。

【参数说明】

无

【使用举例】

```
NOS# config lldp
NOS(lldp)#
```

【注意事项】

无

### 26.2.2 interface enable

【功能描述】

**no interface lldp enable** 命令用于移除接口上的 lldp 配置并停止侦听接口上的 LLDP 报文。

**interface lldp enable** 用于将接口加入 LLDP 协议，以侦听接口上的 LLDP 报文。

【命令格式】

**no lldp enable**

**lldp enable**

【视图】

接口视图

【缺省情况】

接口未使能 LLDP 协议

【参数说明】

无

【使用举例】

在接口 ge1 上使能 LLDP 协议。

```
NOS# config interface ge1
NOS(if-ge1)# lldp enable
```

【注意事项】

无

### 26.2.3 lldp tx-interval

【功能描述】

**no tx-interval** 命令用于恢复 LLDP 报文发送间隔默认配置。

**tx-interval** 命令用于配置 LLDP 报文发送间隔。

【命令格式】

**no tx-interval**

**tx-interval** *INTERVAL*

【视图】

LLDP 视图

【缺省情况】

缺省为系统默认值 30（单位：秒）

【参数说明】

*INTERVAL*：LLDP 报文发送频率，单位秒。

【使用举例】

```
NOS# config lldp
NOS(lldp)# tx-interval  1
```

【注意事项】

无

### 26.2.4 lldp tx-hold

【功能描述】

**no tx-hold** 命令用于恢复 LLDP TTL 乘数默认配置。

**tx-hold** 命令用于配置 LLDP TTL 乘数。

【命令格式】

**no tx-hold**

**tx-hold** *INTERVAL*

【视图】

LLDP 视图

【缺省情况】

缺省为系统默认值 4

【参数说明】

*INTERVAL*：TTL 乘数，设置范围 1～10。

【使用举例】

```
NOS# config lldp
NOS(lldp)# tx-hold 2
```

【注意事项】

TTL 时间=TTL 乘数×LLDP 报文发送间隔.

### 26.2.5 show lldp

【功能描述】

- show lldp configuration 命令用来显示 LLDP 会话全局配置信息。
- show lldp statistics 命令用来显示 LLDP 报文统计信息。
- show lldp chassis 命令用来显示 LLDP 本机设备基本信息。
- show lldp interfaces 命令用来显示接口 LLDP 基本配置信息。
- show lldp neighbors 命令用来显示接口 LLDP 邻居信息。

【命令格式】

- show lldp configuration [json]

- show lldp statistics [{ports *L2_ETH_IF* |summary}]
- show lldp chassis [<details|summary>]
- show lldp interfaces [{ports *L2_ETH_IF* |details}][ json]
- show lldp neighbors [<details|summary>[{hidden|ports *L2_ETH_IF* |protocol *PROTO*}]][ json]

【视图】

所有视图

【缺省情况】

无

【参数说明】

- *L2_ETH_IF*：二层以太接口名字。
- *PROTO*：协议类型。
- **json**：以 json 格式输出

【使用举例】

显示 lldp 配置信息

```
NOS# show lldp configuration
--------------------------------------------------------------------------------
Global configuration:
--------------------------------------------------------------------------------
Configuration:
  Transmit delay: 30
  Transmit delay in milliseconds: 30000
  Transmit hold: 4
  Maximum number of neighbors: 32
  Receive mode: no
  Pattern for management addresses: (none)
  Interface pattern: ge3,ge4
  Permanent interface pattern: (none)
  Interface pattern for chassis ID: (none)
  Override chassis ID with: (none)
  Override description with: trunk-r101
  Override platform with: Linux
  Override system name with: NOS
  Override system capabilities: no
  Advertise version: yes
  Update interface descriptions: no
  Promiscuous mode on managed interfaces: no
  Disable LLDP-MED inventory: no
  LLDP-MED fast start mechanism: yes
  LLDP-MED fast start interval: 1
  Source MAC for LLDP frames on bond slaves: local
  Port ID TLV subtype for LLDP frames: ifname
  Agent type:   unknown
--------------------------------------------------------------------------------
NOS#
```

显示 lldp 接口报文统计信息

```
NOS# show lldp statistics
--------------------------------------------------------------------------------
LLDP statistics:
--------------------------------------------------------------------------------
Interface:   ge3
  Transmitted:  7
  Received:    87
  Discarded:   0
  Unrecognized: 0
  Ageout:      0
  Inserted:    1
  Deleted:     0
--------------------------------------------------------------------------------
Interface:   ge4
  Transmitted:  7
  Received:    87
  Discarded:   0
  Unrecognized: 0
  Ageout:      0
  Inserted:    1
  Deleted:     0
--------------------------------------------------------------------------------
NOS#
```

显示 lldp chassis 简要信息

```
NOS# show lldp chassis
--------------------------------------------------------------------------------
Local chassis:
--------------------------------------------------------------------------------
Chassis:
  ChassisID:   mac 50:d3:3b:cb:22:01
  SysName:     NOS
  SysDescr:    trunk-r101
  MgmtIP:      192.168.32.17
  MgmtIface:   2
  MgmtIP:      fe80::a00:27ff:fec8:5ad
  MgmtIface:   2
  Capability:  Bridge, on
  Capability:  Router, on
  Capability:  Wlan, off
  Capability:  Station, off
--------------------------------------------------------------------------------
```

显示 lldp 接口信息

```
NOS# show lldp interfaces ports ge3
--------------------------------------------------------------------------------
LLDP interfaces:
--------------------------------------------------------------------------------
Interface:   ge3
  Administrative status: RX and TX
```

```
  Chassis:
    ChassisID:    mac 50:d3:3b:cb:22:01
    SysName:      NOS
    SysDescr:     trunk-r101
    MgmtIP:       192.168.32.17
    MgmtIface:    2
    MgmtIP:       fe80::a00:27ff:fec8:5ad
    MgmtIface:    2
    Capability:   Bridge, on
    Capability:   Router, on
    Capability:   Wlan, off
    Capability:   Station, off
  Port:
    PortID:       ifname ge3
    PortDescr:    ge3
    Status:       RX and TX
  TTL:         120
------------------------------------------------------------------------------
NOS#
```

显示 lldp 邻居的简要信息

```
NOS# show lldp neighbors
------------------------------------------------------------------------------
LLDP neighbors:
------------------------------------------------------------------------------
Interface:    ge3, via: LLDP, RID: 1, Time: 0 day, 00:00:00
  Chassis:
    ChassisID:    mac 50:d3:3b:94:34:01
    SysName:      dut1
    SysDescr:     trunk-r101
    MgmtIP:       192.168.32.16
    MgmtIface:    2
    MgmtIP:       fe80::a00:27ff:fec1:797f
    MgmtIface:    2
    Capability:   Bridge, on
    Capability:   Router, on
    Capability:   Wlan, off
    Capability:   Station, off
  Port:
    PortID:       ifname ge3
    PortDescr:    ge3
    TTL:         2
------------------------------------------------------------------------------
Interface:    ge4, via: LLDP, RID: 1, Time: 0 day, 00:00:41
  Chassis:
    ChassisID:    mac 50:d3:3b:94:34:01
    SysName:      dut1
    SysDescr:     trunk-r101
    MgmtIP:       192.168.32.16
```

```
    MgmtIface:    2
    MgmtIP:       fe80::a00:27ff:fec1:797f
    MgmtIface:    2
    Capability:   Bridge, on
    Capability:   Router, on
    Capability:   Wlan, off
    Capability:   Station, off
  Port:
    PortID:       ifname ge4
    PortDescr:    ge4
    TTL:          2
------------------------------------------------------------------------------
NOS#
```

【注意事项】

无

### 26.2.6 reset lldp

【功能描述】

reset lldp 命令用于重新启动 lldp 服务。

【命令格式】

**reset lldp**

【视图】

根视图

【缺省情况】

不涉及。

【参数说明】

不涉及

【使用举例】

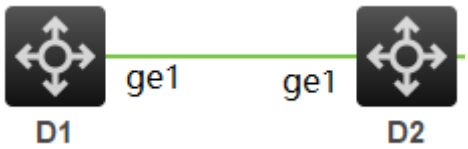
```
NOS#reset lldp
Restarting lldpd please wating...
LLDP loading configuration, please wating... ... ... ...end!!
```

【注意事项】

无

## 26.3 配置举例

图26-1 配置举例




按照如上图所示组网，在 D1/D2 上分别做如下配置：

```
NOS# config lldp
NOS(lldp)# interface ge1
NOS(if-ge1)# lldp enable
```

在 D1 上查看邻居关系:

```
NOS(if-ge1)# show lldp neighbors
------------------------------------------------------------------------------
LLDP neighbors:
------------------------------------------------------------------------------
Interface: ge1, via: LLDP, RID: 3, Time: 0 day, 00:00:20
  Chassis:
    ChassisID:    mac 50:d3:3b:20:2c:01
    SysName:      NOS
    SysDescr:     trunk-r101
    MgmtIP:       192.168.56.3
    MgmtIface:    2
    MgmtIP:       fe80::a00:27ff:fe5e:7dd2
    MgmtIface:    2
    Capability:   Bridge, on
    Capability:   Router, on
    Capability:   Wlan, off
    Capability:   Station, off
  Port:
    PortID:       ifname ge1
    PortDescr:    ge1
    TTL:          120
------------------------------------------------------------------------------
```

在 D2 上查看邻居关系

```
NOS# show lldp neighbors
------------------------------------------------------------------------------
LLDP neighbors:
------------------------------------------------------------------------------
Interface:    ge1, via: LLDP, RID: 2, Time: 0 day, 00:12:15
  Chassis:
    ChassisID:    mac 50:d3:3b:e3:42:01
    SysName:      NOS
    SysDescr:     trunk-r101
    MgmtIP:       192.168.56.2
    MgmtIface:    2
    MgmtIP:       fe80::a00:27ff:fe1d:6dd4
    MgmtIface:    2
    Capability:   Bridge, on
    Capability:   Router, on
    Capability:   Wlan, off
    Capability:   Station, off
  Port:
    PortID:       ifname ge1
    PortDescr:    ge1
    TTL:          120
```

---

## 26.4 常见问题

无。

# 27 MVRP & GVRP

## 27.1 特性简介

GARP（Generic Attribute Registration Protocol，通用属性注册协议）是一种基于协议类型为0x0001，封装方式为 IEEE 802.3 Ethernet 的协议报文进行设备间属性的传播和注册的协议；

GVRP（GARP Vlan Registration Protocol）基于 GARP 协议实现了设备间 VLAN 信息的交流和注册。当一个 GARP 报文的 type 字段取值为 0x01 时表示 GVRP 应用。

MRP 和 MVRP 是 GARP 和 GVRP 的优化升级版本，用于实现 GARP 和 GVRP 相同的功能，但能够克服一些 GARP 和 GVRP 限制，特别是在具有大量 VLAN 的大型网络中涉及带宽使用和融合时间的限制。

MVRP 功能在全局使能 GVRP 兼容后，可以处理 GVRP 消息的接收、解析、封装和发送。

## 27.2 命令手册

### 27.2.1 config mvrp

【功能描述】

**config mvrp** 命令进入 mvrp 视图。

**no config mvrp** 命令退出 mvrp 视图并删除视图下面的所有配置。

【命令格式】

**config mvrp**

**no config mvrp**

【视图】

根视图

【缺省情况】

未配置 mvrp 视图。

【参数说明】

无

【使用举例】

配置并进入 mvrp 视图。

```
NOS# config mvrp
NOS(mvrp)#
```

删除 mvrp 视图和该视图下所有配置。

```
NOS# no config mvrp
```

【注意事项】

no config mvrp 命令会删除该视图下所有全局 mvrp 配置并停止 mvrp 进程，但二层端口下的其他 mvrp 配置信息不会被删除。

### 27.2.2 mvrp global enable

【功能描述】

**mvrp global enable** 命令配置 mvrp 全局使能。

**no mvrp global enable** 命令配置 mvrp 全局去使能。

【命令格式】

**mvrp global enable**

**no mvrp global enable**

【视图】

mvrp 视图

【缺省情况】

未全局使能。

【参数说明】

无

【使用举例】

全局使能/去使能 mvrp 功能。

```
NOS# config mvrp
NOS(mvrp)# mvrp global enable
NOS(mvrp)# no mvrp global enable
```

【注意事项】

**no mvrp global enable** 会停止 mvrp 进程，但二层端口下的 mvrp 配置信息不会被删除。

### 27.2.3 mvrp gvrp-compliance enable

【功能描述】

**mvrp gvrp-compliance enable** 命令配置 mvrp 全局使能 gvrp 兼容模式，mvrp 可以兼容处理 gvrp 报文。

**mvrp gvrp-compliance enable** 命令配置 mvrp 全局去使能 gvrp 兼容模式。

【命令格式】

**mvrp gvrp-compliance enable**

**no mvrp gvrp-compliance enable**

【视图】

mvrp 视图

【缺省情况】

未全局使能 gvrp 兼容模式。

【参数说明】

无

【使用举例】

全局使能/去使能 gvrp 兼容模式。

```
NOS# config mvrp
NOS(mvrp)# mvrp gvrp-compliance enable
NOS(mvrp)# no mvrp gvrp-compliance enable
```

【注意事项】

没有开启 gvrp 兼容模式使能前，mvrp 进程不会接收、解析、封装和发送 gvrp 报文。

开启 gvrp 兼容模式后，mvrp 进程可以接收和解析 gvrp 报文，并且在发送 mvrp 报文的同时封装一份包含相同信息的 gvrp 报文从相同端口发送出去。

### 27.2.4 mvrp timer leaveall

【功能描述】

**mvrp timer leaveall** 命令设置 mvrp 模块的 leaveall 定时器时长。

**no mvrp timer leaveall** 命令设置 mvrp 模块的 leaveall 定时器时长恢复缺省值。

【命令格式】

**mvrp timer leaveall** *TIME*

**no mvrp timer leaveall**

【视图】

mvrp 视图

【缺省情况】

缺省 1000 厘秒

【参数说明】

*TIME:* leaveall 定时器时长,取值范围<20-32740>，至少 20 厘秒，至多 32740 厘秒。

【使用举例】

设置 leaveall 定时器为 2000 厘秒。

```
NOS# config mvrp
NOS(mvrp)# mvrp timer leaveall 2000
```

恢复 leaveall 定时器默认设置（1000 厘秒）。

```
NOS# config mvrp
NOS(mvrp)# no mvrp timer leaveall
```

【注意事项】

为了保证 mvrp 正常运行，建议将 leaveall 定时器的时间配置大于 leave 定时器。

为了防止设备在同一时间发送 leaveall 消息，leaveall 定时器会有小于 1 秒的随机延迟。

### 27.2.5 mvrp timer leave

【功能描述】

**mvrp timer leave** 命令设置 mvrp 模块的 leave 定时器时长。

**no mvrp timer leave** 命令设置 mvrp 模块的 leave 定时器时长恢复缺省值。

【命令格式】

**mvrp timer leave** *TIME*

**no mvrp timer leave**

【视图】

mvrp 视图。

【缺省情况】

缺省 60 厘秒。

【参数说明】

*TIME:* leaveall 定时器时长,取值范围<20-32740>，至少 20 厘秒，至多 32740 厘秒。

【使用举例】

设置 leave 定时器为 100 厘秒。

```
NOS# config mvrp
```

```
NOS(mvrp)# mvrp timer leave 100
```

恢复 leave 定时器默认设置（60 厘秒）。

```
NOS# config mvrp
NOS(mvrp)# no mvrp timer leave
```

【注意事项】

为了保证 mvrp 正常运行，建议将 leave 定时器的时间配置小于 leaveall 定时器并大于 join 定时器的两倍。

### 27.2.6 mvrp timer join

【功能描述】

**mvrp timer join** 命令设置 join 定时器时长。

**no mvrp timer join** 命令设置 join 定时器时长恢复缺省值。

【命令格式】

**mvrp timer join** *TIME*

**mvrp timer join**

【视图】

mvrp 视图

【缺省情况】

缺省 20 厘秒。

【参数说明】

*TIME*：join 定时器时长，取值范围为<20-16360>，至少 20 厘秒，至多 16360 厘秒。

【使用举例】

设置 join 定时器为 50 厘秒。

```
NOS# config mvrp
NOS(mvrp)# mvrp timer join 100
```

恢复 join 定时器默认设置（20 厘秒）。

```
NOS# config mvrp
NOS(mvrp)# no mvrp timer join
```

【注意事项】

为了保证 mvrp 正常运行，建议将 join 定时器的时间配置小于 leave 定时器的一半。

### 27.2.7 mvrp timer hold

【功能描述】

**mvrp timer hold** 命令设置 hold 定时器。

**no mvrp timer hold** 命令设置 hold 定时器恢复缺省值。

【命令格式】

**mvrp timer hold** *TIME*

**no mvrp timer hold**

【视图】

mvrp 视图

【缺省情况】

缺省 100 厘秒。

【参数说明】

*TIME*：hold 定时器时间，取值范围<100-1000>，至少 100 厘秒，至多 1000 厘秒。

【使用举例】

设置 hold 定时器为 500 厘秒。

```
NOS# config mvrp
NOS(mvrp)# mvrp timer hold 500
```

恢复 hold 定时器默认设置（100 厘秒）。

```
NOS# config mvrp
NOS(mvrp)# no mvrp timer hold
```

【注意事项】

无。

### 27.2.8 mvrp mode

【功能描述】

**mvrp mode** 命令设置 mvrp 和 gvrp 在二层端口下的工作模式。

**no mvrp mode** 命令设置 mvrp 和 gvrp 在二层端口下的工作模式恢复缺省值。

【命令格式】

**mvrp mode** <**normal**|**fix**|**forbidden**>

**no mvrp mode**

【视图】

二层端口视图。

【缺省情况】

mvrp 在二层端口视图下工作在 normal 模式。

【参数说明】

- **normal**：不作限制。
- **fix**：禁止端口接收 mvrp 报文，已经注册的动态 vlan 不会被注销，端口向外发送的 vlan 信息包括所有静态 vlan、动态 vlan 和来自其他端口收到的注册信息。
- **forbidden**：禁止端口接收 mvrp 报文，删除端口全部动态 vlan，端口向外发送的 vlan 信息仅包括所有静态 vlan 和来自其他端口收到的注册信息。

【使用举例】

配置端口工作在 fix 模式。

```
NOS# config interface ge1
NOS(if-ge1)# mvrp mode fix
```

恢复端口工作模式到默认模式

```
NOS# config interface ge1
NOS(if-ge1)# no mvrp mode
```

【注意事项】

若同时全局使能了 gvrp 兼容模式，gvrp 和 mvrp 共用二层端口下的模式配置，但在表现上略有不同，具体体现在：

- **normal**：不作限制。

- **fix**：禁止端口接收 gvrp 报文，已经注册的动态 vlan 不会被注销，端口向外发送的 vlan 信息仅包括所有静态 vlan。
- **forbidden**：禁止端口接收 gvrp 报文，删除端口全部动态 vlan，端口向外发送的 vlan 信息仅包括 vlan1。

### 27.2.9 mvrp enable

【功能描述】

**mvrp enable** 命令在二层端口下使能 mrvp。

**no mvrp enable** 命令在二层端口下去使能 mrvp。

【命令格式】

**mvrp enable**

**no mvrp enable**

【视图】

二层端口视图

【缺省情况】

未在二层端口使能

【参数说明】

无

【使用举例】

在二层端口下使能/去使能 mvrp 功能。

```
NOS# config interface ge1
NOS(if-ge1)# vlan trunk
NOS(if-ge1)# vlan trunk permit 1-4094
NOS(if-ge1)# mvrp enable
NOS(if-ge1)# no mvrp enable
```

【注意事项】

mvrp 的二层使能支持二层聚合口。

若成员口在添加到聚合口前配置了 mvrp 二层使能，加入聚合口时原本的配置信息会被删除。

### 27.2.10 show mvrp info

【功能描述】

**show mvrp info** 命令显示 mvrp 信息。

【命令格式】

**show mvrp info**

【视图】

所有视图。

【缺省情况】

无

【参数说明】

无

【使用举例】

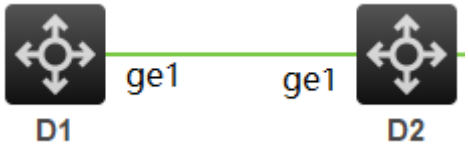
```
NOS(if-bagg1)# show mvrp info
Totally count 1 entries.

----[interface bagg1]----
Registered VLANs:
  1 10 20 30 40
Declared  VLANs:
  1 10 20 30 40
```

【注意事项】

无

## 27.3 配置举例

图27-1 配置举例




按照如上图所示组网，在 D1 上分别做如下配置：

```
NOS# config mvrp
NOS(mvrp)# mvrp global enable
NOS(mvrp)#
NOS# config interface bridge-aggregation 1
NOS(if-bagg1)# member interface ge1
NOS(if-bagg1)# vlan-mode trunk
NOS(if-bagg1)# vlan tr per 1-4094
NOS(if-bagg1)# mvrp enable
NOS# config vlan 1 10 20 30 40
```

按照如上图所示组网，在 D2 上分别做如下配置：

```
NOS# config mvrp
NOS(mvrp)# mvrp global enable
NOS(mvrp)#
NOS# config interface bridge-aggregation 1
NOS(if-bagg1)# member interface ge1
NOS(if-bagg1)# vlan-mode trunk
NOS(if-bagg1)# vlan tr per 1-4094
NOS(if-bagg1)# mvrp enable
NOS# config vlan 1 10 20 30 40 50
```

在 D1 查看 mvrp info

```
NOS# show mvrp info
Totally count 1 entries.
----[interface bagg1]----
Registered VLANs:
  1 10 20 30 40 50
```

```
Declared   VLANs:
  1 10 20 30 40
NOS#
```

在 D2 查看 mvrp info

```
NOS# show mvrp info
Totally count 1 entries.
----[interface bagg1]----
Registered VLANs:
  1 10 20 30 40
Declared   VLANs:
  1 10 20 30 40 50
```

## 27.4 常见问题

无。

# 28 三层接口管理

## 28.1 功能介绍

LoopBack 接口是一种虚拟接口们需要用户手工创建。除非手动关闭 LoopBack 物理层和链路层协议永远处于 up 状态。该接口的地址常被配置为设备产生的 IP 报文的源地址，但是 LoopBack 接口地址用于 IP 报文源地址时，需配置路由来确保 LoopBack 接口到对端的路由可达。另外，任何送到 LoopBack 接口的 IP 报文都会被认为是送往设备本身的，设备将不再转发这些报文。

## 28.2 命令手册

### 28.2.1 config interface loopback

【功能描述】

**config interface loopback** 命令用来创建 LoopBack 接口。

**no config interface loopback** 命令用来删除 LoopBack 接口。

【命令格式】

**config interface loopback** *NUM*

**no config interface loopback** *NUM*

【视图】

根视图

【缺省情况】

不存在 LoopBack 接口。

【参数说明】

*NUM*：LoopBack 接口的编号，取值范围(0～1023)。

【使用举例】

#在设备配置 LoopBack 接口 loopback10

```
NOS# config interface loopback 10
NOS(if-loopback10)#
```

【注意事项】

无

### 28.2.2 config interface vlan

【功能描述】

**config interface vlan** 命令用来创建 VLAN 接口。

**no config interface vlan** 命令用来删除 VLAN 接口。

【命令格式】

**config interface vlan** *VLANID*

**no config interface vlan** *VLANID*

【视图】

系统视图/根视图

【缺省情况】

不存在 VLAN 接口。

【参数说明】

*VLANID*：接口 VLAN ID，范围 1～4094。

【使用举例】

#在设备配置 VLAN 接口 vlan100。

```
NOS# config interface vlan 100
```

【注意事项】

删除 VLAN 接口，对应的地址等配置也会被删除。

### 28.2.3 ipv4-address

【功能描述】

**ipv4-address** 命令用来配置接口 IP 地址。

**no ipv4-address** 命令用来恢复缺省情况。

【命令格式】

**ipv4-address** <*A.B.C.D/M*|*A.B.C.D MASK_LENGTH*> [**sub**]

**ipv4-address dhcp**

**no ipv4-address**

【视图】

三层接口视图

【缺省情况】

缺省没有配置任何 IP 地址。

【参数说明】

- **dhcp**：配置使用 DHCP 方式分配 IPv4 地址。
- *A.B.C.D/M*：配置静态 IPv4 地址。
- *A.B.C.D*： 静态 IPv4 地址。
- *MASK_LENGTH*：静态 IPv4 地址掩码长度。
- sub：配置 IPv4 从地址。

【使用举例】

#在接口 vlan10 上配置地址为 10.1.1.10/24。创建 vlan 和 vlan-interface 省略

```
NOS# config interface vlan10
NOS(if-vlan10)# ipv4-address 10.1.1.10/24
```

【注意事项】

LoopBack 接口不支持 dhcp 方式配置 IP 地址。

### 28.2.4 ipv6-address

【功能描述】

**Ipv6-address** 命令用来配置接口 IPv6 地址。

**no ipv6-address** 命令用来恢复缺省情况。

【命令格式】

**ipv6-address** <**dhcp**|*X:X::X:X/M*|*X:X::X:X MASK_LENGTH*>

**no ipv6-address**

【视图】

三层接口视图

【缺省情况】

缺省没有配置任何 IPV6 地址。

【参数说明】

**dhcp**：配置使用 DHCP 方式分配 IPv6 地址。

*X:X::X:X/M*：配置静态 IPv6 地址。

*X:X::X:X*： 静态 IPv6 地址

*MASK_LENGTH*: 静态 IPv6 地址掩码长度

【使用举例】

#在接口 vlan10 上配置地址为 2001::2/64。创建 vlan 和 vlan-interface 省略。

```
NOS# config interface vlan10
NOS(if-vlan10)# ipv6-address 2001::2/64
```

【注意事项】

LoopBack 接口不支持 dhcp 方式配置 IP 地址。

### 28.2.5 description

【功能描述】

**description** 命令用于给接口设置描述信息，方便区分业务。

**no description** 命令用于清除接口的描述信息。

【命令格式】

**description** *DESC*

**no description**

【视图】

三层接口视图

Vlan 接口视图

LoopBack 接口视图

【缺省情况】

无描述信息

【参数说明】

*DESC*：描述信息字符串，不长于 255 字符

【使用举例】

# 设置 vlan10 接口的描述信息为“port_to_dev1_p1”：

```
NOS# config interface vlan 10
NOS(if-ge1)# description port_to_dev1_p1
```

【注意事项】

无

### 28.2.6 duplex

【功能描述】

duplex 命令用来配置接口的双工模式。

no duplex 命令用来恢复缺省情况。

【命令格式】

duplex <auto|full|half>

no duplex

【视图】

三层接口视图

【缺省情况】

接口缺省为全双工模式。

【参数说明】

auto：自动协商模式。

full：全双工模式，可以同时发送和接收数据包。

half：半双工模式，只有速率低于 1000M 的以太电口才支持。

【使用举例】

#在端口 ge1/0/1 上配置全双工模式：

```
NOS# config interface ge1/0/1
NOS(if-ge1/0/1)# port-link-mode router
NOS(if-ge1/0/1)# duplex full
```

【注意事项】

无

### 28.2.7 shutdown

【功能描述】

shutdown 命令用来强制关闭接口。

no shutdown 命令用来恢复缺省情况。

【命令格式】

shutdown

no shutdown

【缺省情况】

接口缺省处于启用状态。

【参数说明】

无

【视图】

三层接口视图

【使用举例】

#在端口 ge1/0/1 上配置接口 shutdown：

```
NOS# config interface ge1/0/1
NOS(if-ge1/0/1)# port-link-mode router
```

```
NOS(if-ge1/0/1)# shutdown
```

【注意事项】

本命令会导致该端口链路中断，影响数据通信，请谨慎使用。

### 28.2.8 speed

【功能描述】

**speed** 命令用来配置以太端口速率。

**no speed** 命令用来恢复缺省情况。

【命令格式】

**speed** *SPEED*

**no speed**

【视图】

三层接口视图

【缺省情况】

自动协商速率。

【参数说明】

*SPEED*：速率值，取值范围取决于接口类型，单位为 Mbps。

【使用举例】

#在端口 ge1 上配置速率为 100M：

```
NOS# config interface fe1
NOS(if-fe1)# speed 100
```

【注意事项】

速率配置需要确保两端一致，一般情况下，建议不要手工修改速率，使用默认的自动协商即可。

### 28.2.9 mtu

【功能描述】

**mtu** 命令用来配置接口的最大传输单元 MTU（Maximum Transmission Unit，MTU）。

**no mtu** 命令用来恢复缺省值(1500)。

【命令格式】

**mtu** *NUM*

**no mtu**

【视图】

三层接口视图

【缺省情况】

接口缺省 MTU *NUM* 为 1500。

【参数说明】

*NUM*：配置的最大传输单元 MTU（Maximum Transmission Unit，MTU）值(576-9200)。

【使用举例】

#在接口 vlan10 上配置 MTU 为 2000。创建 vlan 和 vlan-interface 省略

```
NOS# config interface vlan10
```

```
NOS(if-vlan10)# mtu 2000
```

【注意事项】

无

### 28.2.10 show interface

【功能描述】

**show interface** 命令用来显示接口信息。

【命令格式】

**show interface** [*INTERFACE*|**status** {**up**|**down**}]

【视图】

任意视图

【缺省情况】

不涉及

【参数说明】

- *INTERFACE*：接口名称。可以是二层或者三层。
- **status**：如果输入 status，回显以 status 状态展示。
- **up**：显示 up 的接口。
- **down**：显示 down 的接口。

【使用举例】

#显示所有接口信息。

```
<NOS># show interface
*[State] A-Down: Administratively down
L3-interface list:
 Name       State    Proto    UpTime       IPv4 address
 ----------  -------  -------  ------------  ------------------
 mgt0       Up      static   04:27:40     192.168.2.101/16
 vlan10     Down     static   00:00:00
L2-interface list:
 Name       State    Speed    Duplex   MAC
 ----------  -------  -------  -------  -----------------
 fe1       A-Down      10M  Half    08:00:27:2d:c6:02
 fe2       Up         10M  Half    08:00:27:2d:c6:03
 fe3       A-Down      10M  Half    08:00:27:2d:c6:04
 fe4       Up         10M  Half    08:00:27:2d:c6:05
 ge5       Down        10M  Full    08:00:27:2d:c6:06
 ge6       Down        10M  Full    08:00:27:2d:c6:07
 ge7       Down        10M  Full    08:00:27:2d:c6:08
 ge8       Down        10M  Full    08:00:27:2d:c6:09
 ge9       Down        10M  Full    08:00:27:2d:c6:0a
 ge10      Down        10M  Full    08:00:27:2d:c6:0b
 ge11      Down        10M  Full    08:00:27:2d:c6:0c
 ge12      Down        10M  Full    08:00:27:2d:c6:0d
 ge13      Down        10M  Full    08:00:27:2d:c6:0e
 ge14      Down        10M  Full    08:00:27:2d:c6:0f
```

```
ge15      Down        10M  Full    08:00:27:2d:c6:10
ge16      Down        10M  Full    08:00:27:2d:c6:11
ge17      Down        10M  Full    08:00:27:2d:c6:12
ge18      Down        10M  Full    08:00:27:2d:c6:13
ge19      Down        10M  Full    08:00:27:2d:c6:14
ge20      Down        10M  Full    08:00:27:2d:c6:15
ge21      Down        10M  Full    08:00:27:2d:c6:16
ge22      Down        10M  Full    08:00:27:2d:c6:17
ge23      Down        10M  Full    08:00:27:2d:c6:18
ge24      Down        10M  Full    08:00:27:2d:c6:19
xge25      Down        10M  Full    08:00:27:2d:c6:1a
xge26      Down        10M  Full    08:00:27:2d:c6:1b
xge27      Down        10M  Full    08:00:27:2d:c6:1c
xge28      Down        10M  Full    08:00:27:2d:c6:1d
```

表28-1 show interface 命令显示详细信息描述表

| 字段 | 描述 |
| --- | --- |
| Name | 接口名称 |
| State | 接口状态<br>• Up：接口状态是 up 状态<br>• Down：接口状态时 down 状态<br>• A-Down：接口状态是 admindown |
| Proto | 三层接口地址配置方式<br>• static：静态配置地址<br>• dhcp：dhcp 客户端方式配置地址 |
| UpTime | 三层接口Up时间 |
| IPv4 address | 三层接口配置的IP地址 |
| MAC | MAC地址 |
| Speed | 接口速率 |
| Duplex | 接口双工模式：<br>• Full：全双工<br>• Half：半双工 |

【注意事项】

无。

# 29 ARP

## 29.1 功能简介

ARP（Address Resolution Protocol，地址解析协议）是将 IP 地址解析为以太网 MAC 地址（或称物理地址）的协议。

在网络中，当主机或其它网络设备有数据要发送给另一个主机或设备时，它必须知道对方的网络层地址（即 IP 地址）。但是仅仅有 IP 地址是不够的，因为 IP 数据报必须封装成帧才能通过物理网络发送，因此发送站还必须有接收站的物理地址，所以需要一个从 IP 地址到物理地址的映射。ARP 就是实现这个功能的协议。

## 29.2 命令手册

### 29.2.1 config arp

【功能描述】

**config arp** 命令用来进入 arp 配置视图。

**no config arp** 命令用来删除 arp 配置视图下的所有配置。

【命令格式】

**config arp**

**no config arp**

【视图】

根视图

【缺省情况】

缺省不存在 arp 配置视图。

【参数说明】

无

【使用举例】

#进程 arp 配置视图。

```
NOS# config arp
NOS(arp)#
```

【注意事项】

无

### 29.2.2 arp timer aging

【功能描述】

**arp timer aging** 命令用于配置 arp 老化时间。

**no arp timer aging** 命令恢复缺省情况。

【命令格式】

**timer aging** *SECTIMENUM*

**no timer aging**

【视图】

arp 视图

【缺省情况】

arp 缺省老化时间是 1200 秒即 20 分钟。

【参数说明】

*SECTIMENUM*:需要配置的 arp 老化时间(60-86400)，单位秒（s）。

【使用举例】

#在 arp 视图下配置老化时间 5 分钟

```
NOS# config arp
NOS(arp)# timer aging 300
```

【注意事项】

无

### 29.2.3 arp static

【功能描述】

**arp static** 命令用来配置静态 arp。

**no arp static** 命令用来恢复到缺省配置。

【命令格式】

**arp static** *A.B.C.D X:X:X:X:X:X*

**no arp static** *A.B.C.D*

【视图】

三层接口视图

【缺省情况】

缺省没有配置静态 arp。

【参数说明】

- *A.B.C.D*: 配置 arp 所对应的 ip 地址。
- *X:X:X:X:X:X*: 配置 arp 所对应的 mac 地址。

【使用举例】

#在虚接口 vlan4 上

```
NOS# config interface vlan4
NOS(if-vlan4)# arp static 192.168.2.83 08:00:5e:42:06:43
```

【注意事项】

无

### 29.2.4 arp-proxy enable

【功能描述】

**arp-proxy enable** 命令用来开启 arp 代理功能，接口可以使用本地 MAC 地址回复和本接口同网段地址的 arp 请求。

**no arp-proxy enable** 命令用来关闭 arp 代理功能。

【命令格式】

**arp-proxy enable**

【视图】

三层接口视图

【缺省情况】

接口 arp 代理功能处于关闭状态。

【参数说明】

无。

【使用举例】

```
# 开启接口 vlan10 的 arp 代理功能。
NOS# config interface vlan 10
NOS(if-vlan10)# arp-proxy enable
```

【注意事项】

无

### 29.2.5 reset arp

【功能描述】

**reset arp** 命令用来重置动态、静态或者学习到的某一 ip 对应的 arp。

【命令格式】

**reset arp** <**all**|**static**|**dynamic** [*A.B.C.D*]>

【视图】

根视图

【缺省情况】

无

【参数说明】

- **all**：清除所有 arp 条目。
- **static**：清除静态 arp 条目。
- **dynamic**：清除动态 arp 条目。
- *A.B.C.D*：需要被删除的某一个动态 arp 对应的 ip。

【使用举例】

```
# 删除静态 arp：
NOS# reset arp static
You may lost static arp, Are you sure? [y/n]
# 重置动态 arp：
NOS# reset arp dynamic
#删除 192.168.2.84 对应的 arp：
NOS# reset arp dynamic 192.168.2.84
#删除所有 arp：
NOS# reset arp all
You may lost all arp, Are you sure? [y/n]
```

【注意事项】

无

### 29.2.6 rate-limit

【功能描述】

**rate-limit** 命令用来开启 ARP 限速功能。

**no rate-limit** 命令用来关闭 ARP 限速功能。

【命令格式】

**rate-limit** *PPSNUM*

**no rate-limit**

【视图】

arp 视图。

【缺省情况】

未开启 ARP 限速功能。

【参数说明】

*PPSNUM*：速率限制值(1-500)，单位为 pps。

【使用举例】

```
NOS(arp)# rate-limit 200
```

【注意事项】

无

### 29.2.7 rate-limit log enable

【功能描述】

**rate-limit log enable** 命令用来开启 ARP 限速日志。

**no rate-limit log enable** 命令用来关闭 ARP 限速日志。

【命令格式】

**rate-limit log enable**

**no rate-limit log enable**

【视图】

arp 视图。

【缺省情况】

未开启开启 ARP 限速日志。

【参数说明】

无。

【使用举例】

```
NOS(arp)# rate-limit log enable
```

【注意事项】

无

### 29.2.8 arp send-gratitous-arp

【功能描述】

**arp send-gratitous-arp** 命令配置接口进行免费 arp 报文发送功能。

**no arp send-gratitous-arp** 命令用来恢复接口缺省配置。

【命令格式】

**arp send-gratitous-arp interval** *MSECTIME*

**no arp send-gratitous-arp**

【视图】

三层接口视图。

【缺省情况】

未开启免费 arp 报文发送功能。

【参数说明】

*MSECTIME*: 接口进行免费 arp 发送的周期(1000-20000)，单位为毫秒。

【使用举例】

#配置接口 vlan 20 以 5 秒为周期进行免费 arp 报文发送。

```
NOS(if-vlan20)# arp send-gratuitous-arp interval 5000
```

【注意事项】

(1) 修改发送免费 arp 发送周期后，需要等待下次发送后才会生效。

(2) 只有已经配置了 ipv4 地址的三层接口使能本功能且接口处于 up 状态才能够正常进行免费 arp 的发送。

### 29.2.9 show arp detection

【功能描述】

**show arp detection** 命令用于显示配置了 ARP Detection 功能的 VLAN。

【命令格式】

**show arp detection**

【视图】

任意视图

【缺省情况】

无

【参数说明】

无

【使用举例】

#显示 arp detection 表项。

```
<NOS> show arp detection
```

【注意事项】

无。

### 29.2.10 show arp

【功能描述】

**show arp** 命令用于显示 ARP 表项。

【命令格式】

**show arp** [**dynamic**|**static**] [*A.B.C.D*]

【视图】

任意视图

【缺省情况】

无

【参数说明】

- **static**：显示静态 arp 条目。
- **dynamic**：显示动态 arp 条目。
- *A.B.C.D*：显示某一个 ip 的 arp 条目。

【使用举例】

#显示路由。

```
NOS# timer aging
IPv4 address       Interface     Mac Address        Type
---------------    ------------  -----------------  ----------
192.168.2.1        eth0          0a:00:27:00:00:11  Static
```

表29-1 show arp 命令显示详细信息描述表

| 字段 | 描述 |
| --- | --- |
| IPv4 address | IPv4地址 |
| Interface | ARP表项对应的出接口 |
| Mac Address | MAC地址 |
| Type | 当前ARP表项的状态<br>• Static：静态 ARP 表项<br>• Dynamic：静态 |

【注意事项】

无。

## 29.3 配置举例

无。

## 29.4 常见问题

无。

# 30 IPv6 协议栈

## 30.1 功能简介

IPv6（Internet Protocol Version 6，互联网协议版本 6）是网络层协议的第二代标准协议，也被称为 IPng(IP Next Generation,下一代互联网协议),它是 IETF(Internet Engineering Task Force，互联网工程任务组）设计的一套规范，是 IPv4 的升级版本。IPv6 和 IPv4 之间最显著的区别为：IP 地址的长度从 32 比特增加到 128 比特。

其中，IPv6 ND（IPv6 Neighbor Discovery，IPv6 邻居发现）协议使用五种类型的 ICMPv6 消息，实现下面一些功能：地址解析、验证邻居是否可达、重复地址检测、路由器发现/前缀发现、地址自动配置和重定向等功能

## 30.2 命令手册

### 30.2.1 config ipv6-neighbor

【功能描述】

**config ipv6-neighbor** 命令用来进入 ipv6-neighbor 配置视图。

**no config ipv6-neighbor** 命令用来删除 ipv6-neighbor 配置视图下的所有配置。

【命令格式】

**config ipv6-neighbor**

**no config ipv6-neighbor**

【视图】

根视图

【缺省情况】

缺省不存在 ipv6-neighbor 配置视图。

【参数说明】

无

【使用举例】

#进程 ipv6-neighbor 配置视图。

```
NOS# config ipv6-neighbor
NOS(ipv6-neighbor)#
```

【注意事项】

无

### 30.2.2 timer aging

【功能描述】

**timer aging** 命令用于配置 nd 老化时间。

**no timer aging** 命令恢复缺省情况。

【命令格式】

**timer aging** *SECTIMENUM*

**no timer aging**

【视图】

ipv6-neighbor 视图

【缺省情况】

ipv6-neighbor 缺省老化时间是 1200 秒即 20 分钟。

【参数说明】

*SECTIMENUM*:需要配置的 nd 老化时间(60-86400)，单位秒（s）。

【使用举例】

#在 ipv6-neighbor 视图下配置老化时间 5 分钟

```
NOS# config ipv6-neighbor
NOS(ipv6-neighbor)# timer aging 300
```

【注意事项】

无

### 30.2.3 show ipv6 neighbor

【功能描述】

**show ipv6 neighbor** 命令用于显示 ND 表项。

【命令格式】

**show ipv6 neighbor** [**all**|**dynamic**|**static**] [*X:X::X:X*]

【视图】

任意视图

【缺省情况】

无

【参数说明】

**static**：显示静态 nd 条目。

**dynamic**：显示动态 nd 条目。

*X:X::X:X*：显示某一个 ip 的 nd 条目。

【使用举例】

```
NOS# show ipv6 neighbor
Total ipv6 neighbor count: 1
Ageing Timer: 1200
IPv6 address                          Interface         Mac Address        State
------------------------              ---------------    ---------------    ----------
2001:10::30                            vlan10           50:d3:3b:19:31:01   Reachable
```

【注意事项】

无。

### 30.2.4 reset ipv6 neighbor

【功能描述】

**reset ipv6 neighbor** 命令用于显示 ND 表项。

【命令格式】

**show ipv6 neighbor** [**dynamic**|**static**] [*X:X::X:X*]

【视图】

任意视图

【缺省情况】

无

【参数说明】

**static**：显示静态 nd 条目。

**dynamic**：显示动态 nd 条目。

*X:X::X:X*：显示某一个 ip 的 nd 条目。

【使用举例】

```
NOS# reset ipv6 neighbor dynamic
```

【注意事项】

无。

### 30.2.5 ipv6 nd ra interval

【功能描述】

**ipv6 nd ra interval** 命令用来配置 RA 消息发布的最大时间间隔和最小时间间隔。

**no ipv6 nd ra interval** 命令用来恢复缺省情况。

【命令格式】

**ipv6 nd ra interval max** *MAX-INTERVAL* **min** *MIN-INTERVAL*

**no ipv6 nd ra interval**

【视图】

三层接口视图

【缺省情况】

无

【参数说明】

- *MAX-INTERVAL*：指定 RA 消息发布的最大时间间隔，取值范围是 4～1800，单位为秒。
- *MIN-INTERVAL*：指定 RA 消息发布的最小时间间隔，取值范围是 3～（max-interval＊3/4），单位为秒。

【使用举例】

#在三层接口视图下配置

```
NOS(if-vlan10)# ipv6 nd ra interval max 5 min 3
```

【注意事项】

无。

### 30.2.6 ipv6 nd ra prefix

【功能描述】

**ipv6 nd ra prefix** 命令用来配置 RA 消息中的前缀信息。

**no ipv6 nd ra prefix** 命令用来恢复缺省情况。

【命令格式】

**ipv6 nd ra prefix** *X:X::X:X/M* [{**no-autoconfig** | **off-link** | **valid-lifetime** *TIME* **preferred-lifetime** *TIME*}]

**no ipv6 nd ra interval**

【视图】

三层接口视图

【缺省情况】

无

【参数说明】

- X:X::X:X/M：IPv6 地址。
- **no-autoconfig**：定前缀不用于无状态地址配置。如果不选择该参数，则指定前缀用于无状态地址配置。
- **off-link**：指定前缀不是该链路上直连可达的。如果不选择该参数，则表示指定前缀是直连可达的。
- **valid-lifetime** *TIME*：指定前缀信息的有效存活时间，整数形式，取值范围是 0～4294967295，单位是秒。
- **preferred-lifetime** *TIME*：指定前缀信息的首选存活时间，整数形式，取值范围是 0～4294967295，单位是秒。首选存活时间不能大于有效存活时间。

【使用举例】

#在三层接口视图下配置

```
NOS(if-vlan10)# ipv6 nd ra prefix 2001:10::10/24 no-autoconfig
```

【注意事项】

无。

### 30.2.7 ipv6 nd ra reachable-time

【功能描述】

**ipv6 nd ra reachable-time** 命令用来配置接口保持邻居可达状态的时间。

**no ipv6 nd ra reachable-time** 命令用来恢复缺省情况。

【命令格式】

**ipv6 nd ra reachable-time** *TIME*

**no ipv6 nd ra reachable-time**

【视图】

三层接口视图

【缺省情况】

无

【参数说明】

**reachable-time** *TIME*：保持邻居可达状态的时间，取值范围为 100-3600000,单位为毫秒。

【使用举例】

#在三层接口视图下配置

```
NOS(if-vlan10)# ipv6 nd ra reachable-time 200
```

【注意事项】

无。

### 30.2.8 ipv6 nd ra router-lifetime

【功能描述】

**ipv6 nd ra router-lifetime** 命令用来配置 RA 消息中路由器的生存时间。

**no ipv6 nd ra router-lifetime** 命令用来恢复缺省情况。

【命令格式】

**ipv6 nd ra router-lifetime** *TIME*

**no ipv6 nd ra router-lifetime**

【视图】

三层接口视图

【缺省情况】

RA 消息中路由器的生存时间为 RA 消息发布的最大时间间隔的 3 倍。

【参数说明】

**router-lifetime** *TIME*：RA 消息中路由器的生存时间，取值范围为 0～9000，单位为秒。当配置为 0 时，表示本设备不作为默认路由器。

【使用举例】

#在三层接口视图下配置

```
NOS(if-vlan10)# ipv6 nd ra router-lifetime 200
```

【注意事项】

无。

### 30.2.9 ipv6 nd router-preference

【功能描述】

**ipv6 nd router-preference** 命令用来配置 RA 消息中路由器的生存时间。

**no ipv6 nd router-preference** 命令用来恢复缺省情况。

【命令格式】

**ipv6 nd router-preference** <**high**|**low**|**medium**>

**no ipv6 nd router-preference**

【视图】

三层接口视图

【缺省情况】

设备发送的 RA 消息中的路由器优先级为 medium。

【参数说明】

**high**：设置发布 RA 的路由器为高优先级。

**low**：设置发布 RA 的路由器为低优先级。

**medium**：设置发布 RA 的路由器为中优先级。

【使用举例】

#在三层接口视图下配置

```
NOS(if-vlan10)# ipv6 nd router-preference high
```

【注意事项】

无。

### 30.2.10 ipv6 nd autoconfig managed-address-flag

【功能描述】

**ipv6 nd autoconfig managed-address-flag** 命令用来设置 RA 报文中的有状态自动配置地址的标志位。

**no ipv6 nd autoconfig managed-address-flag** 命令用来清除 RA 报文中的有状态自动配置地址的标志位。

【命令格式】

**ipv6 nd autoconfig managed-address-flag**

**no ipv6 nd autoconfig managed-address-flag**

【视图】

三层接口视图

【缺省情况】

管理地址的配置标志位为 0，即主机可以通过无状态自动配置获取 IPv6 地址。

【参数说明】

无。

【使用举例】

#在三层接口视图下配置

```
NOS(if-vlan10)# ipv6 nd autoconfig managed-address-flag
```

【注意事项】

无。

### 30.2.11 ipv6 nd autoconfig other-flag

【功能描述】

**ipv6 nd autoconfig other-flag** 命令用来配置其他信息配置标志位为 1，即主机通过有状态自动配置（例如 DHCPv6 服务器）获取除 IPv6 地址外的其他信息。

**no ipv6 nd autoconfig other-flag** 命令用来恢复该缺省情况。

【命令格式】

**ipv6 nd autoconfig other-flag**

**no ipv6 nd autoconfig other-flag**

【视图】

三层接口视图

【缺省情况】

其他信息配置标志位为 0，即主机可以通过无状态自动配置获取其他信息。

【参数说明】

无。

【使用举例】

#在三层接口视图下配置

```
NOS(if-vlan10)# ipv6 nd autoconfig other-flag
```

【注意事项】

无。

### 30.2.12 ipv6 nd ra accept

【功能描述】

**ipv6 nd ra accept** 命令用来配置其他信息配置标志位为 1，即主机通过有状态自动配置（例如 DHCPv6 服务器）获取除 IPv6 地址外的其他信息。

**no ipv6 nd ra accept** 命令用来恢复该缺省情况。

【命令格式】

**ipv6 nd autoconfig other-flag**

**no ipv6 nd autoconfig other-flag**

【视图】

三层接口视图

【缺省情况】

其他信息配置标志位为 0，即主机可以通过无状态自动配置获取其他信息。

【参数说明】

无。

【使用举例】

#在三层接口视图下配置

```
NOS(if-vlan10)# ipv6 nd autoconfig other-flag
```

【注意事项】

无。

### 30.2.13 ipv6 nd ra halt

【功能描述】

**ipv6 nd ra halt** 命令用来去使能系统发布 RA 报文功能。

**no ipv6 nd ra halt** 命令用来使能系统发布 RA 报文功能。

【命令格式】

**ipv6 nd ra halt**

**no ipv6 nd ra halt**

【视图】

三层接口视图

【缺省情况】

抑制发布 RA 消息。

【参数说明】

无。

【使用举例】

#在三层接口视图下配置

```
NOS(if-vlan10)# ipv6 nd ra halt
```

【注意事项】

无。

## 30.3 配置举例

无。

## 30.4 常见问题

无。

# 31 RARP

## 31.1 功能简介

RARP（Reverse Address Resolution Protocol，反向地址解析协议）用于获得已知 MAC 地址的 IP 地址。

RARP 以与 ARP 相反的方式工作。RARP 发出要反向解析的物理地址并希望返回其对应的 IP 地址，应答包括由能够提供所需信息的 RARP 服务器发出的 IP 地址。虽然发送方发出的是广播信息，RARP 规定只有 RARP 服务器能产生应答。

## 31.2 命令手册

### 31.2.1 config rarp

【功能描述】

**config rarp** 命令用来进入 rarp 配置视图。

**no config rarp** 命令用来删除 rarp 配置视图下的所有配置。

【命令格式】

**config rarp**

**no config rarp**

【视图】

根视图

【缺省情况】

缺省不存在 rarp 配置视图。

【参数说明】

无

【使用举例】

#进程 arp 配置视图。

```
NOS# config rarp
NOS(rarp)#
```

【注意事项】

无

### 31.2.2 mac

【功能描述】

**mac** 命令用于配置指定 vlan 接口下，mac 与 ip 的静态。

**no mac** 命令恢复缺省情况。

【命令格式】

**mac** *X:X:X:X:X:X* **vlan** *VLANIDNUM* **ip** *A.B.C.D*

**no mac** *X:X:X:X:X:X* **vlan** *VLANIDNUM* [**ip** *A.B.C.D*]

【视图】

rarp 视图

【缺省情况】

没有配置 mac 与 ip 静态映射条目。

【参数说明】

- X:X:X:X:X:X：客户端 mac 地址。
- VLANIDNUM：客户端从属的 vlan 号(1-4094)。
- A.B.C.D：要解析的客户端 ip。

【使用举例】

#在 rarp 视图下配置 vlan11 接口下，00:00:00:00:00:a0 物理地址的 ip 映射条目。

```
NOS# config rarp
NOS(rarp)# mac 00:00:00:00:00:a0 vlan 11 ip 100.0.0.66
```

【注意事项】

无。

## 31.3 配置举例

无。

## 31.4 常见问题

无。

# 32 DNS

## 32.1 功能简介

DNS（Domain Name System，域名系统）是一种用于 TCP/IP 应用程序的分布式数据库，提供域名与 IP 地址之间的转换。通过域名系统，用户进行某些应用时，可以直接使用便于记忆的、有意义的域名，而由网络中的域名解析服务器将域名解析为正确的 IP 地址。

域名解析分为静态域名解析和动态域名解析。在解析域名时，首先采用静态域名解析，查找静态域名解析表，如果静态域名解析不成功，再采用动态域名解析。动态解析是 DNS 服务器会向上游 DNS 服务器转发域名解析请求。

## 32.2 命令手册

### 32.2.1 config dns server

【功能描述】

**config dns server** 命令用来进入 dns-server 视图。

**no config dns server** 命令用来删除 dns-server 视图及视图下的所有配置。

【命令格式】

**config dns server**

**no config dns server**

【视图】

根视图

【缺省情况】

不存在 dns-server 视图。

【参数说明】

无。

【使用举例】

#配置 dns server 并进去 dns-server 视图。

```
NOS# config dns server
NOS(dns-server)#
```

【注意事项】

无。

### 32.2.2 domain

【功能描述】

**domain** 命令配置静态域名解析表，配置域名对应的 IP 地址。

**no domain** 命令用来删除域名对应的 IP 地址。

【命令格式】

**domain** *DOMAIN A.B.C.D*

**no domain** *DOMAIN*

【视图】

dns-server 视图

【缺省情况】

不存在域名对应的 IP 地址。

【参数说明】

- DOMAIN：域名。
- A.B.C.D：域名对应的 IP 地址。

【使用举例】

#配置域名 aa.abc.com 对应的 IP 地址是 100.1.1.2。

```
NOS# config dns server
NOS(dns-server)# domain abc.com ip-address 100.1.1.2
```

【注意事项】

同一个域名配置多个 IP 地址，最新的配置生效。

### 32.2.3 server

【功能描述】

**server** 命令用来配置上游 DNS 服务器 IP 地址、静态域名解析表。

**no server** 命令用来上游 DNS 服务器 IP 地址、静态域名解析表。

【命令格式】

**server** *A.B.C.D* [*DOMAIN*]

**no server** *A.B.C.D* [*DOMAIN*]

【视图】

dns-server 视图

【缺省情况】

不存在域名上游 DNS 服务器 IP 地址。

【参数说明】

- *A.B.C.D*：上游 DNS 服务器 IP 地址。
- *DOMAIN*：域名。

【使用举例】

#配置 DNS 服务器上游 DNS 服务器的 IP 地址为 100.10.10.1。

```
NOS# config dns server
NOS(dns-server)# server server-ip 100.10.10.1
```

【注意事项】

可以重复命令配置多个上游 DNS 服务器地址

### 32.2.4 show dns server domain

**show dns server domain** 命令显示已经配置的静态域名映射。

【命令格式】

**show dns server domain**

【视图】

任意视图

【缺省情况】

无。

【参数说明】

无。

【使用举例】

#显示已经配置的域名映射表

```
<NOS> show dns server domain
Hostname                        Ip Address
--------------------            ---------------
www.mydomain.com                100.233.10.1
```

表32-1 show dns server domain 命令显示详细信息描述表

| 字段 | 描述 |
| --- | --- |
| Hostname | 主机名称 |
| Ip Address | 对应的IP地址 |

## 32.2.5 config dns-ipv6 server

【功能描述】

**config dns-ipv6 server** 命令用来进入 dns-ipv6-server 视图。

**no config dns-ipv6 server** 命令用来删除 dns-ipv6-server 视图及视图下的所有配置。

【命令格式】

**config dns-ipv6 server**

**no config dns-ipv6 server**

【视图】

根视图

【缺省情况】

不存在 dns-ipv6-server 视图。

【参数说明】

无。

【使用举例】

#配置 dns-ipv6 server 并进去 dns-ipv6-server 视图。

```
NOS# config dns-ipv6 server
NOS(dns-ipv6-server)#
```

【注意事项】

无。

### 32.2.6 domain

【功能描述】

**domain** 命令配置静态域名解析表，配置域名对应的 IPv6 地址。

**no domain** 命令用来删除域名对应的 IPv6 地址。

【命令格式】

**domain** *DOMAIN X:X::X:X*

**no domain** *DOMAIN*

【视图】

dns-ipv6-server 视图

【缺省情况】

不存在域名对应的 IPv6 地址。

【参数说明】

- DOMAIN：域名。
- X:X::X:X：域名对应的 IPv6 地址。

【使用举例】

#配置域名 aa.abc.com 对应的 IP 地址是 100.1.1.2。

```
NOS# config dns server
NOS(dns-ipv6-server)# domain abc.com 2001:10::20
```

【注意事项】

同一个域名配置多个 IPv6 地址，最新的配置生效。

### 32.2.7 server

【功能描述】

**server** 命令用来配置上游 DNS 服务器 IPv6 地址、静态域名。

**no server** 命令用来上游 DNS 服务器 IPv6 地址、静态域名。

【命令格式】

**server-ip** *X:X::X:X* [*DOMAIN*]

**no server-ip** *X:X::X:X* [*DOMAIN*]

【视图】

dns-ipv6-server 视图

【缺省情况】

不存在域名上游 DNS 服务器 IP 地址。

【参数说明】

- *X:X::X:X*：上游 DNS 服务器 IP 地址。
- *DOMAIN*：域名。

【使用举例】

#配置 DNS 服务器上游 DNS 服务器的 IPv6 地址为 2001:10::20。

```
NOS# config dns-ipv6 server
NOS(dns-ipv6-server)# server 2001:10::20
```

【注意事项】

可以重复命令配置多个上游 DNS 服务器地址。

## 32.3 配置举例

配置域名 abc.com 的 ip 地址为 100.200.22.11，并配置 DNS 上游服务器的地址 10.200.1.1。客户端查询域名 abc.com 的 IP 地址时，可以直接查找返回 100.200.22.11，查询其余域名则把查询请求转发至上游服务器。

(1) 配置域名 abc.com 的 ip 地址为 100.200.22.11。

```
NOS# config dns server
NOS(dns-server)# domain abc.com ip-address 100.200.22.11
```

(2) 配置 DNS 上游服务器的地址 10.200.1.1

```
NOS(dns-server)# server-ip 10.200.1.1
```

## 32.4 常见问题

无。

# 33 DHCP Server

## 33.1 功能简介

DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）是一个局域网的网络协议。指的是由服务器控制一段 IP 地址范围，客户机登录服务器时就可以自动获得服务器分配的 IP 地址和子网掩码。DHCP 通常被应用在大型的局域网络环境中，主要作用是集中的管理、分配 IP 地址，使网络环境中的主机动态的获得 IP 地址、Gateway 地址、DNS 服务器地址等信息，并能够提升地址的使用率。

针对客户端的不同需求，DHCP 提供两种 IP 地址分配策略：

- 静态分配地址：由管理员为少数特定客户端（如 WWW 服务器等）静态绑定固定的 IP 地址。通过 DHCP 将配置的固定 IP 地址分配给客户端。
- 动态分配地址：DHCP 为客户端分配具有一定有效期限的 IP 地址，到达使用期限后，客户端需要重新申请地址。绝大多数客户端得到的都是这种动态分配的地址。

## 33.2 命令手册

### 33.2.1 config dhcp-server

【功能描述】

**config dhcp-server** 命令用来进入 dhcp-server 视图。

**no config dhcp-server** 命令用来删除 dhcp-server 视图及视图下的所有配置。

【命令格式】

**config dhcp-server**

**no config dhcp-server**

【视图】

根视图

【缺省情况】

缺省不存在 dhcp-server 视图。

【参数说明】

无。

【使用举例】

#配置 dhcp server 并进去 dhcp-server 视图。

```
NOS# config dhcp-server
NOS(dhcp-server)#
```

【注意事项】

无。

### 33.2.2 address-range

【功能描述】

**address-range** 命令配置接口作为 DHCP 服务器分配地址范围。

**no address-range** 命令用来恢复缺省情况。

**leasetime** 命令配置接口作为 DHCP 服务器分配 IP 地址的租期。

【命令格式】

**address-range** *A.B.C.D A.B.C.D A.B.C.D* [**leasetime day** *NUM* [**hour** *NUM* [**minute** *NUM*]]]

**no address-range** *A.B.C.D A.B.C.D A.B.C.D*

【视图】

dhcp-server 视图

【缺省情况】

接口地址池的租期为 12 小时。

【参数说明】

- *A.B.C.D*: dhcp 配置范围的最小地址。
- *A.B.C.D*: dhcp 配置范围的最大地址。
- *A.B.C.D*: dhcp 配置范围的网络掩码。
- **day** *NUM*:配置租期的天数(0-365)。
- **hour** *NUM*: 配置租期的小时数(0-23)。
- **minute** *NUM*: 配置租期的分钟数(0-59)。

【使用举例】

#在接口 vlan10 上配置地址范围为 10.1.1.10-10.1.1.100.并配置该地址租期时间 5 天。

```
NOS# config dhcp-server
NOS(dhcp-server)# address-range 10.1.1.10 10.1.1.100 255.255.255.0 leasetimeday 5
```

【注意事项】

(1) 接口必须配置地址，配置的地址必须和接口地址在同一网段。配置的地址范围最大地址必须不小于最小地址。

(2) 配置租期时间不能小于 2 分钟。

### 33.2.3 static-bind

【功能描述】

**static-bind** 命令用于配置客户端 MAC 和要分配的地址静态绑定。

**no static-bind** 命令用于恢复缺省行为。

【命令格式】

**static-bind** *A.B.C.D X:X:X:X:X:X*

**no static-bind** *A.B.C.D*

【视图】

dhcp-server 配置视图

【缺省情况】

缺省情况下，没有配置静态绑定的 IP 地址。

【参数说明】

*A.B.C.D*: 要绑定的地址。

*X:X:X:X:X:X*: 要绑定的客户端 mac。

【使用举例】

#为 mac 地址为 08:00:04:00:00:64 的交换机配置静态绑定到 10.1.1.64 地址池。

```
NOS# config dhcp server
NOS(dhcp-server)# static-bind 10.1.1.64 08:00:04:00:00:64
```

【注意事项】

静态绑定的 IP 地址不能是 DHCP 服务器的接口 IP 地址，否则会导致 IP 地址冲突，被绑定的客户端将无法正常获取到 IP 地址。

### 33.2.4 option

【功能描述】

**option** 命令用于配置 DHCP option 自定义内容。

**no option** 命令用于恢复缺省行为。

【命令格式】

**option** *CODENUM* <**ascii** *STR*|**hex** *STR*|**ipv4** *A.B.C.D...*>

**no option** *CODENUM* [<**ascii** *STR*|**hex** *STR*|**ipv4** *A.B.C.D...*>]

【视图】

dhcp-server 配置视图

【缺省情况】

缺省情况下，没有配置相应 option 选项自定义内容。

【参数说明】

- *CODENUM*：需要配置的 option 选项号(2-254)。
- **ascii** *STR*：选项内容以 ascii 字符串形式配置（1-128）。
- **hex** *STR*：选项内容以 hex 十六进制形式配置（2-256）。
- *A.B.C.D*：选项内容配置为 ipv4 地址，最多配置 8 个。

【使用举例】

#在 dhcp-server 视图配置十六进制内容的 option 选项

```
NOS# config dhcp-server
NOS(dhcp-server)# option 77 hex ffeeddccbbaa99887766554433221100
```

【注意事项】

(1) 部分 option 选项不支持自定义配置，命令行已做限制。

(2) option 自定义功能属于低优先级，如遇 option 专属配置下发，自定义功能不生效，专属功能优先生效。

### 33.2.5 sip-server

【功能描述】

**sip-server** 命令用于配置 DHCP 的 sip server 选项内容，即 DHCP option 120 的专属命令。

**no sip-server** 命令用于恢复缺省行为。

【命令格式】

**sip-server** <**address** *A.B.C.D* |**domain** *DOMAIN* >

**no sip-server** <**address** *A.B.C.D* |**domain** *DOMAIN* >

【视图】

dhcp-server 配置视图

【缺省情况】

缺省情况下，没有配置 sip-server 选项内容。

【参数说明】

- *A.B.C.D*：配置 sip-server 选项内容为 ipv4 地址，最多配置 2 个。
- *DOMAIN*：配置 sip-server 选项内容为 domain 字符串（1-63），最多配置 2 个。

【使用举例】

#在 dhcp-server 视图配置 domain 字符串内容的 sip server 选项

```
NOS# config dhcp-server
NOS(dhcp-server)# sip-server domain abaaba.com
```

【注意事项】

- dhcpv4 的 sip-server 仅支持 domain 和 address 之一。
- 存在 dhcpv4 自定义 option 命令时，该命令优先生效。

### 33.2.6 dns-server

【功能描述】

**dns-server** 命令用于配置 DHCP 的 domain name server 选项内容，即 DHCP option 6 的专属命令。

**no dns-server** 命令用于恢复缺省行为。

【命令格式】

**dns-server** *A.B.C.D*

**no dns-server** [*A.B.C.D*]

【视图】

dhcp-server 配置视图

【缺省情况】

缺省情况下，没有配置 dns-server 选项内容。

【参数说明】

*A.B.C.D*：配置 dns-server 选项内容为 ipv4 地址，最多配置 8 个。

【使用举例】

#在 dhcp-server 视图配置 dns-server 选项内容

```
NOS# config dhcp-server
NOS(dhcp-server)# dns-server 100.0.0.1
```

【注意事项】

存在 dhcpv4 自定义 option 命令时，该命令优先生效。

### 33.2.7 dhcp server enable

【功能描述】

**dhcp server enable** 命令在接口开启 DHCP 服务。

**no dhcp server enable** 命令在接口关闭 DHCP 服务。

【命令格式】

**dhcp server enable**

**no dhcp server enable**

【视图】

三层接口视图

【缺省情况】

接口不开启 DHCP 服务。

【参数说明】

*IFNAME*：接口名称。

【使用举例】

#在接口 vlan10 上开启 DHCP 服务器。

```
NOS# config interface vlan10
NOS(if-vlan10)# dhcp server enable
```

【注意事项】

接口不能同时作为 DHCP 服务器和 DHCP 客户端使用。

### 33.2.8 reset dhcp server ip-in-use all

【功能描述】

reset dhcp server ip-in-use all 命令用于清除 dhcpv4 server 的用户租约表项。

【命令格式】

**reset dhcp server ip-in-use all**

【视图】

根视图

【缺省情况】

无。

【参数说明】

无。

【使用举例】

#清除用户租约表项。

```
NOS# reset dhcp server ip-in-use all
You will lost all dhcpv4 lease, Are you sure? [Y/N]
```

【注意事项】

无

### 33.2.9 show dhcp server ip-in-use

【功能描述】

**show dhcp server ip-in-use** 命令显示已经分配的地址。

【命令格式】

**show dhcp server ip-in-use**

【视图】

任意视图

【缺省情况】

无。

【参数说明】

无。

【使用举例】

#显示租约。

```
NOS# show dhcp server ip-in-use
Hostname          MAC address        IPv4 address       Expire
------------     ------------       ------------       ------------
rscu             08:00:27:2D:C6:01   10.1.2.165         11h59m43s
```

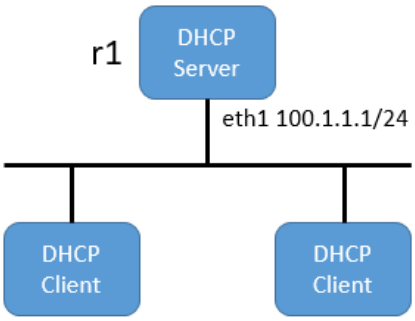
图33-1 show dhcp server lease 命令显示详细信息描述表

| 字段 | 描述 |
| --- | --- |
| Hostname | 客户端主机名称 |
| MAC address | 客户端MAC地址 |
| IPv4 address | 分配的IPv4地址 |
| Expire | 租约到期剩余时间 |

## 33.3 配置举例

配置DHC服务器通过接口fe1为DHCP客户端分配IP地址，分配地址范围为100.1.1.20-100.1.1.100，租期为10天。

图33-2 组网图




(2) 配置vlan10接口的IP地址

a. 配置vlan 10

```
r1# config vlan 10
```

b. 将端口加入vlan10

```
r1# config interface fe1
r1(if-fe1)# vlan trunk permit 10
```

(3) 在虚接口vlan10上启用dhcp server

```
r1# config vlan-interface 10
r1(if-vlan10)# ip-address 100.1.1.1/24
```

```
r1(if-vlan10)# dhcp server enable
```

(4) 配置分配地址范围和租期。

```
r1# config dhcp-server
r1(dhcp-server)#
r1(dhcp-server)# address-range 100.1.1.20 100.1.1.100 255.255.255.0 leasetime day 10
```

(5) 配置客户端通过 DHCP 分配地址（通过网络配置，略）。

(6) 配置验证

a. DHCP 客户端有正确的地址配置，DHCP 服务器端能显示分配的 IP 地址。

```
r1# show dhcp server ip-in-use
Hostname          MAC address        IPv4 address       Expire
------------      ------------       ------------       ------------
rscu              08:00:27:2D:C6:01   100.1.1.115       11h59m52s
```

## 33.4 常见问题

无。

# 34 IPv6 DHCP Server

## 34.1 功能简介

DHCPv6（Dynamic Host Configuration Protocol for IPv6，IPv6 动态主机配置协议）是针对 IPv6 编址方案设计的协议，用于为主机分配 IPv6 地址、前缀和其他网络配置参数的一种有状态协议。DHCPv6 的主要目的是在 IPv6 网络环境中合理高效地分配 IP 地址，它不仅能够分配 IPv6 地址，还能够分配 IPv6 前缀和一些网络配置参数，如 DNS 服务器地址、域名等。通过 DHCPv6，可以更好地控制地址的分配，记录为主机分配的地址/前缀，并为特定主机分配特定的地址/前缀，以便于网络管理。

DHCPv6 具有以下优点：

- 更好地控制地址的分配。通过 DHCPv6 不仅可以记录为主机分配的地址，还可以为特定主机分配特定的地址，以便于网络管理。
- 为客户端分配前缀，以便于全网络的自动配置和管理。
- 除了 IPv6 前缀、IPv6 地址外，还可以为主机分配 DNS 服务器、域名后缀等网络配置参数。

## 34.2 命令手册

### 34.2.1 config dhcpv6-server

【功能描述】

**config dhcpv6-server** 命令用来进入 dhcpv6-server 视图。

**no config dhcpv6-server** 命令用来删除 dhcpv6-server 视图及视图下的所有配置。

【命令格式】

**config dhcpv6-server**

**no config dhcpv6-server**

【视图】

根视图

【缺省情况】

缺省不存在 dhcpv6-server 视图。

【参数说明】

无。

【使用举例】

#配置 dhcpv6 server 并进去 dhcpv6-server 视图。

```
NOS# config dhcpv6-server
NOS(dhcpv6-server)#
```

【注意事项】

无。

### 34.2.2 address-range

【功能描述】

**address-range** 命令配置接口作为 DHCPv6 服务器分配地址范围。

**no address-range** 命令用来恢复缺省情况。

**leasetime** 命令配置接口作为 DHCPv6 服务器分配 IP 地址的租期。

【命令格式】

**address-range** *X:X::X:X X:X::X:X MASK_LENGTH* [**leasetime day** *NUM* [**hour** *NUM* [**minute** *NUM*]]]

**no address-range** *X:X::X:X X:X::X:X MASK_LENGTH*

【视图】

dhcpv6-server 视图

【缺省情况】

接口地址池的租期为 24 小时。

【参数说明】

- *X:X::X:X*：dhcpv6 配置范围的最小地址。
- *X:X::X:X*：dhcpv6 配置范围的最大地址。
- *MASK_LENGTH*：dhcpv6 配置的前缀长度。
- **day** *NUM*:配置租期的天数(0-365)。
- **hour** *NUM*：配置租期的小时数(0-23)。
- **minute** *NUM*：配置租期的分钟数(0-59)。

【使用举例】

#在接口 vlan10 上配置地址范围为 2001:20::10-2001:20::99.并配置该地址租期时间 5 天。

```
NOS# config dhcpv6-server
NOS(dhcpv6-server)# address-range 2001:20::10 2001:20::99 64 leasetime day 5
```

【注意事项】

(1) 配置的地址范围最大地址必须不小于最小地址。

(2) 配置租期时间不能小于 2 分钟。

### 34.2.3 option

【功能描述】

**option** 命令用于配置 DHCPv6 option 自定义内容。

**no option** 命令用于恢复缺省行为。

【命令格式】

**option** *CODENUM* <**ascii** *STR*|**hex** *STR*|**ipv6** *X:X::X:X...*>

**no option** *CODENUM* [<**ascii** *STR*|**hex** *STR*|**ipv6** *X:X::X:X...*>]

【视图】

dhcpv6-server 配置视图

【缺省情况】

缺省情况下，没有配置相应 option 选项自定义内容。

【参数说明】

- *CODENUM*：需要配置的 option 选项号(21-65535)。
- **ascii** *STR*：选项内容以 ascii 字符串形式配置(1-128)。
- **hex** *STR*：选项内容以 hex 十六进制形式配置(2-256)。
- *X:X::X:X*：选项内容配置为 ipv6 地址，最多配置 8 个。

【使用举例】

#在 dhcpv6-server 视图配置 ipv6 地址内容的 option 选项

```
NOS# config dhcpv6-server
NOS(dhcpv6-server)# option 88 ipv6 2001:10::1 2001:10::2 2001:10::3
```

【注意事项】

(1) 部分 option 选项不支持自定义配置，命令行已做限制。

(2) option 自定义功能属于低优先级，如遇 option 专属配置下发，自定义功能不生效，专属功能优先生效。

### 34.2.4 sip-server

【功能描述】

**sip-server** 命令用于配置 DHCPv6 的 sip server 选项内容，即 DHCP option 120 的专属命令。

**no sip-server** 命令用于恢复缺省行为。

【命令格式】

**sip-server** <**address** *X:X::X:X* |**domain** *DOMAIN* >

**no sip-server** <**address** *X:X::X:X* |**domain** *DOMAIN* >

【视图】

dhcpv6-server 配置视图

【缺省情况】

缺省情况下，没有配置 sip-server 选项内容。

【参数说明】

- *X:X::X:X*：配置 sip-server 选项内容为 ipv6 地址，最多配置 2 个。
- *DOMAIN*：配置 sip-server 选项内容为 domain 字符串(1-63)，最多配置 2 个。

【使用举例】

#在 dhcpv6-server 视图配置 ipv6 地址内容的 sip server 选项

```
NOS# config dhcpv6-server
NOS(dhcpv6-server)# sip-server address 2001:10::2
```

【注意事项】

- dhcpv6 支持 address 和 domain 同时下发。
- 存在 dhcpv6 自定义 option 命令时，该命令优先生效。

### 34.2.5 static-bind

【功能描述】

**static-bind** 命令用于配置客户端 DUID 和要分配的 ipv6 地址静态绑定。

**no static-bind** 命令用于恢复缺省行为。

【命令格式】

**static-bind** *X:X::X:X DUID*

**no static-bind** *X:X::X:X*

【视图】

dhcpv6-server 配置视图。

【缺省情况】

缺省情况下，没有配置静态绑定的 IPv6 地址。

【参数说明】

- *X:X::X:X*：要绑定的地址。
- *DUID*：要绑定的客户端标识符。

【使用举例】

#为 duid 为 0003000150d33b7abd01 的交换机配置静态绑定到 2001:20::66 地址池。

```
NOS# config dhcpv6 server
NOS(dhcp-server)# static-bind 2001:20::66 0003000150d33b7abd01
```

【注意事项】

静态绑定的 IPv6 地址不能是 DHCPv6 服务器的接口 IPv6 地址，否则会导致 IPv6 地址冲突，被绑定的客户端将无法正常获取到 IPv6 地址。

### 34.2.6 dhcpv6 server enable

【功能描述】

**dhcpv6 server enable** 命令在接口开启 DHCPv6 服务。

**no dhcpv6 server enable** 命令在接口关闭 DHCPv6 服务。

【命令格式】

**dhcpv6 server enable**

**no dhcpv6 server enable**

【视图】

三层接口视图

【缺省情况】

接口不开启 DHCPv6 服务

【参数说明】

*IFNAME*：接口名称。

【使用举例】

#在接口 vlan10 上开启 DHCPv6 服务器。

```
NOS# config interface vlan10
NOS(if-vlan10)# dhcpv6 server enable
```

【注意事项】

接口不能同时作为 DHCPv6 服务器和 DHCPv6 客户端使用。

### 34.2.7 reset dhcpv6 server ip-in-use all

【功能描述】

**reset dhcpv6 server ip-in-use all** 命令用于清除 dhcpv6 server 的用户租约表项。

【命令格式】

**reset dhcpv6 server ip-in-use all**

【视图】

根视图

【缺省情况】

无。

【参数说明】

无。

【使用举例】

#清除用户租约表项。

```
NOS# reset dhcpv6 server ip-in-use all
You will lost all dhcpv6 lease, Are you sure? [Y/N]
```

【注意事项】

无

### 34.2.8 show dhcpv6 server ip-in-use

【功能描述】

**show dhcpv6 server ip-in-use** 命令显示已经分配的地址。

【命令格式】

**show dhcpv6 server ip-in-use**

【视图】

任意视图

【缺省情况】

无。

【参数说明】

无。

【使用举例】

#显示租约。

```
NOS# show dhcpv6 server ip-in-use
Total dhcpv6 server ip-in-use count: 1
Hostname           :?
Duid               :00:03:00:01:08:68:8d:ab:1d:01
IPv6 address       :2001:20::2b
Expire             :23h59m37s
```

### 34.2.9 show dhcpv6 duid

【功能描述】

**show dhcpv6 duid** 命令显示本设备标识符。

【命令格式】

**show dhcpv6 duid**

【视图】

任意视图

【缺省情况】

无。

【参数说明】

无。

【使用举例】

#显示 DUID。

```
NOS# show dhcpv6 duid
DHCPv6 unique identifier: 0003000150d33b7abd01
```

## 34.3 配置举例

无。

## 34.4 常见问题

无。

# 35 DHCP Relay

## 35.1 功能简介

DHCP 中继代理是用来将一个网段的 DHCP 请求转发给其它网段的 DHCP Server，由其它网段的 DHCP Server 分配 IP 地址。DHCP 中继代理存在的原因是因为 DHCP 客户端还没有 IP 环境设定，这时由 DHCP Relay 来接管客户的 DHCP 请求然后将 DHCP 消息传递给 DHCP Server，再将 DHCP 服务器的应答消息传给客户端，客户端获得 IP 地址。

## 35.2 命令手册

### 35.2.1 dhcp relay enable server-ip

【功能描述】

**dhcp relay enable server-ip** 命令在接口开启 DHCP 中继服务。

**no dhcp relay enable** 命令在接口关闭 DHCP 中继服务。

【命令格式】

**dhcp relay enable server-ip** *A.B.C.D*

**no dhcp relay enable**

【视图】

三层接口视图（不含 loopback 接口）。

【缺省情况】

接口不开启 DHCP 中继服务。

【参数说明】

*A.B.C.D*：dhcp 服务器地址。

【使用举例】

#在接口 vlan10 上中继服务器 10.1.1.1

```
NOS# config interface vlan10
NOS(if-vlan10)# ip-address 10.100.100.1/24
NOS(if-vlan10)# dhcp relay enable server-ip 10.10.10.1
```

【注意事项】

接口不能同时作为 DHCP 中继服务器和 DHCP 客户端使用。

## 35.3 配置举例

无。

## 35.4 常见问题

无。

# 36 IPv6 DHCP Relay

## 36.1 功能简介

DHCPv6 客户端通常通过链路本地范围的组播地址与 DHCPv6 服务器通信，以获取 IPv6 地址和其他网络配置参数。服务器和客户端不在同一个链路范围内时，服务器和客户端无法直接通信，需要通过 DHCPv6 中继来转发报文。部署 DHCPv6 中继可以避免在每个链路范围内都部署 DHCPv6 服务器，既节省了成本，又便于进行集中管理。

## 36.2 命令手册

### 36.2.1 dhcpv6 relay enable

【功能描述】

**dhcpv6 relay enable** 命令在接口开启 DHCPv6 中继服务。

**no dhcpv6 relay enable** 命令在接口关闭 DHCPv6 中继服务。

【命令格式】

**dhcpv6 relay enable source-address** *X:X::X:X* **server-address** *X:X::X:X*

**no dhcpv6 relay enable**

【视图】

三层接口视图

接口不能是 loopback 口。

【缺省情况】

接口不开启 DHCPv6 中继服务

【参数说明】

- **source-address** *X:X::X:X*：填充指定源地址。
- **server-address** *X:X::X:X*：填充中继对应的服务器地址。

【使用举例】

#在接口 vlan10 上中继服务器 2001:35::10

```
NOS# config interface vlan10
NOS(if-vlan10)# ipv6-address 2001:36::10/64
NOS(if-vlan10)# dhcpv6 relay enable source-address 2001:36::10 server-address 2001:35::10
```

【注意事项】

无。

## 36.3 配置举例

无。

## 36.4 常见问题

无。

# 37 DHCP Snooping

## 37.1 功能简介

### 37.1.1 DHCP SNOOPING

DHCP Snooping 是 DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）的一种安全特性，用于保证 DHCP 客户端从合法的 DHCP 服务器获取 IP 地址，并记录 DHCP 客户端 IP 地址与 MAC 地址等参数的对应关系。DHCP Snooping 可以抵御网络中针对 DHCP 的各种攻击，为用户提供更安全的网络环境和更稳定的网络服务。

网络中如果存在私自架设的伪 DHCP 服务器，则可能导致 DHCP 客户端获取错误的 IP 地址和网络配置参数，无法正常通信。为了使 DHCP 客户端能通过合法的 DHCP 服务器获取 IP 地址，DHCP Snooping 安全机制允许将端口设置为信任端口和不信任端口：

- 信任端口正常转发接收到的 DHCP 报文。
- 不信任端口接收到 DHCP 服务器响应的 DHCP-ACK 和 DHCP-OFFER 报文后，丢弃该报文。

### 37.1.2 DHCP SNOOPING 支持option82

Option 82 称为中继代理信息选项,该选项记录了 DHCP 客户端的位置信息。

DHCP 中继或 DHCP Snooping 设备接收到 DHCP 客户端发送给 DHCP 服务器的请求报文后，在该报文中添加 Option 82，并转发给 DHCP 服务器。

管理员可以从 Option 82 中获得 DHCP 客户端的位置信息，以便定位 DHCP 客户端，实现对客户端的安全和计费等控制。支持 Option 82 的服务器还可以根据该选项的信息制定 IP 地址和其他参数的分配策略，提供更加灵活的地址分配方案。

Option 82 最多可以包含 255 个子选项。若定义了 Option 82，则至少要定义一个子选项。

目前，DHCP 中继支持两个子选项：sub-option 1（Circuit ID，电路 ID 子选项）和 sub-option 2（Remote ID，远程 ID 子选项）；

DHCP Snooping 设备支持三个子选项：sub-option 1（Circuit ID，电路 ID 子选项）、sub-option 2（Remote ID，远程 ID 子选项）和 sub-option 9（子选项 9）。

由于 Option 82 的内容没有统一规定，不同厂商通常根据需要进行填充。

设备上可以通过两种方式配置 Option 82 的内容：

- 用户自定义方式：用户手工指定 Option 82 的内容；
- 非用户自定义方式：采用默认的 normal 模式、verbose 模式填充 Option 82。

## 37.2 命令手册

### 37.2.1 config dhcp snooping

【功能描述】

**config dhcp snooping** 命令用来进入 dhcp-snooping 视图。

**no config dhcp snooping** 命令用来删除 dhcp-snooping 视图及视图下的所有配置。

【命令格式】

**config dhcp snooping**

**no config dhcp snooping**

【视图】

根视图

【缺省情况】

缺省不存在 dhcp-snooping 视图。

【参数说明】

无。

【使用举例】

#配置 dhcp snooping 并进去 dhcp-snooping 视图。

```
NOS# config dhcp snooping
NOS(dhcp-snooping)#
```

【注意事项】

无。

### 37.2.2 dhcp snooping trust

【功能描述】

**dhcp snooping trust** 命令配置接口工作在 trust 模式，正常处理来自服务器的请求。

**no dhcp snooping trust** 命令在接口恢复默认配置。

【命令格式】

**dhcp snooping trust**

**no dhcp snooping trust**

【视图】

二层以太接口视图

【缺省情况】

缺省情况下，开启 DHCP Snooping 功能后，设备的所有端口均为不信任端口。

【参数说明】

无

【使用举例】

#在接口 fe3 上开启 DHCP snooping 服务。

```
NOS# config interface fe3
NOS(if-fe3)# dhcp snooping trust
```

【注意事项】

为了使 DHCP 客户端能从合法的 DHCP 服务器获取 IP 地址，必须将与合法 DHCP 服务器相连的端口设置为信任端口，且设置的信任端口和与 DHCP 客户端相连的端口必须在同一个 VLAN 内。

如果接口是聚合口的成员口，不能配置成 trust 接口，配置跟随聚合口状态。

### 37.2.3 max-user-number

【功能描述】

**max-user-number** 命令可以在 dhcp-snooping 视图限制接口动态学习 DHCP Snooping 表项的最大数目，以防止整体学习到大量 DHCP Snooping 表项，占用过多的系统资源

**no max-user-number** 命令在 dhcp-snooping 视图恢复默认配置。

【命令格式】

**max-user-number** *USERNUM*

**no max-user-number**

【视图】

dhcp-snooping 视图

【缺省情况】

默认无限制

【参数说明】

*USERNUM*：整体动态学习 DHCP Snooping 表项的最大数目(1-1024)。

【使用举例】

#在 dhcp-snooping 视图上配置动态学习表项的最大数目为 40

```
NOS# config dhcp snooping
NOS(dhcp-snooping)# max-user-number 40
```

【注意事项】

无。

### 37.2.4 dhcp snooping max-user-number

【功能描述】

**dhcp snooping max-user-number** 命令在接口可以限制接口动态学习 DHCP Snooping 表项的最大数目，以防止接口学习到大量 DHCP Snooping 表项，占用过多的系统资源

**no dhcp snooping max-user-number** 命令在接口恢复默认配置。

【命令格式】

**dhcp snooping max-user-number** *USERNUM*

**no dhcp snooping max-user-number**

【视图】

二层以太接口视图

【缺省情况】

默认无限制

【参数说明】

*USERNUM*：接口动态学习 DHCP Snooping 表项的最大数目(1-1024)。

【使用举例】

#在接口 fe4 上配置动态学习表项的最大数目为 40

```
NOS# config interface fe4
NOS(if-fe4)# dhcp snooping max-user-num 40
```

【注意事项】

无。

### 37.2.5 show dhcp snooping table

【功能描述】

**show dhcp-snooping table** 命令显示已经分配的地址。

【命令格式】

**show dhcp-snooping table**

【视图】

任意视图

【缺省情况】

无。

【参数说明】

无。

【使用举例】

#显示租约。

```
NOS# show dhcp-snooping table
NOS # show dhcp-snooping table
Mac                 Ipaddr          Interface       Vlan    Lease
-----------------   ------------    -------------   ----    -----------------
58:b3:8f:b9:67:16    182.1.1.2         fe4            182      0d 00:02:34
58:b3:8f:b9:67:18    184.1.1.2         fe4            184      0d 00:02:33
58:b3:8f:b9:67:19    185.1.1.2         fe4            185      0d 00:02:33
```

表37-1 show dhcp server lease 命令显示详细信息描述表

| 字段 | 描述 |
|---|---|
| Interface | 客户端申请的接口 |
| MAC | 客户端MAC地址 |
| Ipaddress | 分配的IPv4地址 |
| Expire | 租约到期剩余时间 |
| vlan | 接口所属vlan |

### 37.2.6 reset dhcp snooping table

【功能描述】

**reset dhcp-snooping table** 命令清除 DHCP Snooping 表项。

【命令格式】

**reset dhcp-snooping table**

【视图】

根视图

【缺省情况】

无。

【参数说明】

无。

【使用举例】

#清除表项。

```
NOS# reset dhcp-snooping table
```

### 37.2.7 dhcp snooping option82 enable

【功能描述】

**dhcp snooping option82 enable** 命令用来进入在接口上开启 option82 功能。

**no dhcp snooping option82 enable** 命令用来恢复默认配置。

【命令格式】

**dhcp snooping option82 enable**

**no dhcp snooping option82 enable**

【视图】

二层接口视图

【缺省情况】

缺省未开启 option82 功能

【参数说明】

无。

【使用举例】

#配置 dhcp snooping 并进去 dhcp-snooping 视图，在 ge2 接口开启 option82。

```
NOS# config dhcp snooping
NOS(dhcp-snooping)#
NOS# config interface ge2
NOS(if-fe2) dhcp snooping option82 enable
```

【注意事项】

无。

### 37.2.8 dhcp snooping option82 strategy

【功能描述】

**dhcp snooping option82 strategy** 命令用来进入在接口上开启 option82 报文处理策略功能。

**no dhcp snooping option82 strategy** 命令用来恢复默认配置。

【命令格式】

**dhcp snooping option82 strategy** <**drop**|**keep**|**replace**>

**no dhcp snooping option82 strategy**

【视图】

二层接口视图

【缺省情况】

缺省 option82 功能的报文处理策略为 replace,

【参数说明】

- **drop**：如果报文中带有 Option 82，则丢弃该报文。
- **keep**：如果报文中带有 Option 82，则保持该报文中的 Option 82 不变并进行转发。
- **replace**：如果报文中带有 Option 82，则按照配置的填充内容和填充格式填充 Option 82，用该选项替换报文中原有的 Option 82，并进行转发。

【使用举例】

#配置在 ge2 接口开启 option82 策略为 drop。

```
NOS# config interface ge2
NOS(if-fe2) dhcp snooping option82 strategy drop
```

【注意事项】

本命令仅对包含 Option 82 的请求报文有效。如果开启了 DHCP SNOOPING 支持 Option 82 功能，则对于接收到的不包含 Option 82 的请求报文，DHCP SNOOPING 的处理方式始终为在请求报文中添加 Option 82，并转发给 DHCP 服务器。DHCP SNOOPING 对包含 Option 82 请求报文的处理策略为 replace 时，需要配置 Option 82 的填充模式和填充格式；处理策略为 keep 或 drop 时，不需要配置 Option 82 选项的填充模式和填充格式。

### 37.2.9 dhcp snooping option82 circuit-id

【功能描述】

**dhcp snooping option82 circuit-id** 命令用来进入在接口上开启 option82 功能填充子选项 1 circuit-id,填充模式随着配置改变。

**no dhcp snooping option82 circuit-id** 命令用来恢复默认配置。

【命令格式】

**dhcp snooping option82 circuit-id** <**string** *CIRCUITID*|**normal**|**verbose** [**node-id** <**mac**|**sysname**|**userdefined** *NODEID*>]> [**format** <**ascii**|**hex**>]

**no dhcp snooping option82 circuit-id**

【视图】

二层接口视图

【缺省情况】

缺省 circuit-id 为 normal 模式

【参数说明】

- **string** *CIRCUITID*：指定以用户配置的字符串填充 Circuit ID 子选项。*CIRCUITID* 表示用户配置的用来填充 Circuit ID 子选项的内容,为 1-100 个字符的字符串，区分大小写。
- **normal**：指定以 Normal 模式填充 Circuit ID 子选项，填充内容为 VLAN ID 和端口索引。
- **verbose**：指定以 Verbose 模式填充 Circuit ID 子选项。填充的内容为节点标识、接口信息和接口所在的 VLAN 编号。节点标识缺省以节点的 MAC 地址构成；接口信息缺省由以太网类型（取值固定为“eth”）、接口名组成。
- **node-id**：指定接入节点的标识。
- **mac**：表示以节点的 MAC 地址作为节点标识。
- **sysname**：表示以节点的设备名称作为节点标识。设备的系统名称可以通过系统视图下的 sysname 命令配置。不管配置了哪种填充格式，设备的系统名称始终采用 ASCII 码格式填充。系统名称中不能包含空格，否则 DHCP 中继添加或替换 Option 82 失败。
- **userdefined** *NODEID*：表示以指定的字符串作为节点标识，*NODEID* 为 1～100 个字符的字符串，区分大小写。不管配置了哪种填充格式，指定的字符串始终采用 ASCII 码格式填充。
- **format**：指定 Circuit ID 子选项的填充格式。
- **ascii**：指定以 ASCII 码格式填充 Circuit ID 子选项，即将数值转换为对应的 ASCII 码填充到 Circuit ID 子选项。
- **hex**：指定以十六进制数值的格式填充 Circuit ID 子选项。

【使用举例】

#配置 dhcp snooping 并进去 dhcp-snooping 视图,在 ge2 接口开启 option82 子选项 circuit-id 填充模式为 string。

```
NOS# config dhcp snooping
NOS(dhcp-snooping)#
NOS# config interface ge2
NOS(if-fe2) dhcp snooping option82 circuit-id string mengsiyi
```

【注意事项】

以不同模式填充 Circuit ID 子选项时，填充格式有所不同：

(1) 以用户配置的字符串填充 Circuit ID 子选项时，填充格式固定为 ASCII 码格式；

(2) 以 Normal 和 Verbose 模式填充 Circuit ID 子选项时，填充格式由本命令的配置决定。

(3) 如果本命令中未指定填充格式，则对于 Normal 模式，VLAN ID 和端口索引均以 hex 格式填充；对于 Verbose 模式，节点标识（MAC 地址、设备的系统名称或指定的字符串）、以太网类型、框号、槽号、子槽号、接口编号均以 ASCII 码格式填充，VLAN ID 以 hex 格式填充。

(4) 如果本命令中指定填充格式为 ascii，则所有内容均以 ASCII 码格式填充。

(5) 如果本命令中指定填充格式为 hex，则对于 Normal 模式，VLAN ID 和端口索引均以 hex 格式填充；对于 Verbose 模式，设备的节点标识、以太网类型以 ASCII 码格式填充，其余内容均以 hex 格式填充。

## 37.2.10 dhcp snooping option82 remote-id

【功能描述】

**dhcp snooping option82 remote-id** 命令用来进入在接口上开启 option82 子选项 remote-id 功能。

**no dhcp snooping option82 remote-id** 命令用来恢复默认配置。

【命令格式】

**dhcp snooping option82 remote-id** <**normal** [**format** <**ascii**|**hex**>]|**string** *REMOTEID*|**sysname**>

**no dhcp snooping option82 remote-id**

【视图】

二层接口视图

【缺省情况】

缺省未开启 option82 子选项 remote-id 功能。

【参数说明】

- **normal**：指定以 Normal 模式填充 Remote ID 子选项，填充内容为接收报文接口的 MAC 地址.
- **format**：指定 Remote ID 子选项的填充格式。如果未配置本参数，则以 hex 格式填充。
- **ascii**：指定以 ASCII 码格式填充 Remote ID 子选项，即将数值转换为对应的 ASCII 码填充到 Remote ID 子选项。
- **hex**：指定以十六进制数值的格式填充 Remote ID 子选项。
- **string** *REMOTEID*：指定以用户配置的字符串填充 Remote ID 子选项。*REMOTEID* 表示用户配置的用来填充 Remote ID 子选项的内容，为 1～100 个字符的字符串，区分大小写。
- **sysname**：指定以设备的系统名称填充 Remote ID 子选项。

【使用举例】

#配置 dhcp snooping 并进去 dhcp-snooping 视图，在 ge2 接口开启 option82 子选项 remote-id 功能。

```
NOS# config dhcp snooping
```

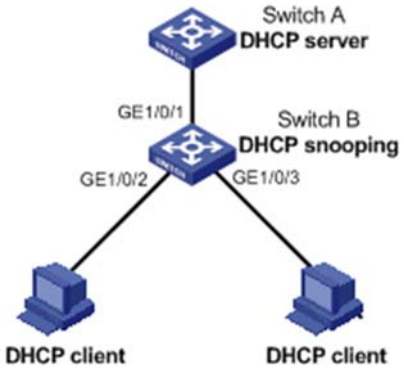
```
NOS(dhcp-snooping)#
NOS# config interface ge2
NOS(if-fe2) dhcp snooping option82 remote-id string mengsiyi
```

【注意事项】

以用户配置的字符串（string）和设备的系统名称（sysname）填充 Remote ID 子选项时，填充内容固定为 ASCII 格式；以 Normal 模式填充 Remote ID 子选项时，填充内容的格式由本命令配置的填充格式决定。

## 37.3 配置举例

图37-1 配置举例




(2) 配置全局 dhcp snooping 开启。

```
switchB# config dhcp snooping
```

(3) 在 fe3 接口上配置成 trust 接口。

```
switchB# config interface fe3
switchB(if-fe3)# dhcp snooping trust
```

(4) 验证 dhcp snooping。

```
switchB# show dhcp-snooping table
```

(5) NOS # show dhcp-snooping table

```
Mac                 Ipaddr         Interface      Vlan    Lease
-----------------   ------------   ------------   ----    ----------------
58:b3:8f:b9:67:16   182.1.1.2      fe3            182     0d 00:02:34
58:b3:8f:b9:67:18   184.1.1.2      fe3            184     0d 00:02:33
58:b3:8f:b9:67:19   185.1.1.2      fe3            185     0d 00:02:33
```

## 37.4 常见问题

无。

# 38 IPv6 DHCP Snooping

## 38.1 功能简介

### 38.1.1 dhcpv6 snooping

DHCPv6 Snooping 是 ipv6 DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）的一种安全特性，用于保证 DHCPv6 客户端从合法的 ipv6 DHCP 服务器获取 ipv6 地址，并记录 DHCPv6 客户端 ipv6 地址与 MAC 地址等参数的对应关系。DHCPv6 Snooping 可以抵御网络中针对 DHCPv6 的各种攻击，为用户提供更安全的网络环境和更稳定的网络服务。

网络中如果存在私自架设的非法 DHCPv6 服务器，则可能导致 DHCPv6 客户端获取错误的 IPv6 地址和网络配置参数，从而无法正常通信。为了使 DHCPv6 客户端能通过合法的 DHCPv6 服务器获取 IPv6 地址，DHCPv6 Snooping 安全机制允许将端口设置为信任端口和不信任端口：

- 信任端口正常转发接收到的 DHCPv6 报文。
- 不信任端口接收到 DHCPv6 服务器发送的应答报文后，丢弃该报文。

### 38.1.2 dhcpv6 snooping option

Option 18 称为接口 ID 选项（Interface ID）、Option 37 称为远程 ID 选项（Remote ID），DHCPv6 Snooping 设备接收到 DHCPv6 客户端发送给 DHCPv6 服务器的请求报文后，在该报文中添加 Option 18 或 Option 37，并转发给 DHCPv6 服务器。

## 38.2 命令手册

### 38.2.1 config dhcpv6 snooping

【功能描述】

**config dhcpv6 snooping** 命令用来进入 dhcpv6-snooping 视图。

**no config dhcpv6 snooping** 命令用来删除 dhcpv6-snooping 视图及视图下的所有配置。

【命令格式】

**config dhcpv6 snooping**

**no config dhcpv6 snooping**

【视图】

根视图

【缺省情况】

缺省不存在 dhcpv6-snooping 视图。

【参数说明】

无。

【使用举例】

#配置 dhcpv6 snooping 并进去 dhcpv6-snooping 视图。

```
NOS# config dhcpv6 snooping
NOS(dhcpv6-snooping)#
```

【注意事项】

无。

### 38.2.2 dhcpv6 snooping trust

【功能描述】

**dhcpv6 snooping trust** 命令配置接口工作在 trust 模式，正常处理来自服务器的请求。

**no dhcpv6 snooping trust** 命令在接口恢复默认配置。

【命令格式】

**dhcpv6 snooping trust**

**no dhcpv6 snooping trust**

【视图】

二层普通接口视图

【缺省情况】

缺省情况下，开启 DHCPv6 Snooping 功能后，设备的所有端口均为不信任端口。

【参数说明】

**trust**：配置接口工作在 dhcpv6 snooping 信任模式下。

【使用举例】

#在接口 fe3 上开启 DHCPv6 snooping 服务。

```
NOS# config interface fe3
NOS(if-fe3)# dhcpv6 snooping trust
```

【注意事项】

为了使 DHCPv6 客户端能从合法的 DHCPv6 服务器获取 IPv6 地址，必须将与合法 DHCPv6 服务器相连的端口设置为信任端口，且设置的信任端口和与 DHCPv6 客户端相连的端口必须在同一个 VLAN 内。

如果接口是聚合口的成员口，不能配置成 trust 接口，配置跟随聚合口状态。

### 38.2.3 dhcpv6 snooping max-user-number

【功能描述】

**dhcpv6 snooping max-user-number** 命令在接口可以限制接口动态学习 DHCPv6 Snooping 表项的最大数目，以防止接口学习到大量 DHCPv6 Snooping 表项，占用过多的系统资源

**no dhcpv6 snooping max-user-number** 命令在接口恢复默认配置。

【命令格式】

**dhcpv6 snooping max-user-number** *USERNUM*

**no dhcpv6 snooping max-user-number**

【视图】

普通二层接口视图

接口不能是 loopback 口。

【缺省情况】

默认无限制

【参数说明】

*USERNUM*：接口动态学习 DHCPv6 Snooping 表项的最大数目(1-1024)。

【使用举例】

#在接口 fe4 上配置动态学习表项的最大数目为 40

```
NOS# config interface fe4
NOS(if-fe4)# dhcpv6 snooping max-user-num 40
```

【注意事项】

无。

### 38.2.4 show dhcpv6 snooping table

【功能描述】

**show dhcpv6-snooping table** 命令显示已经分配的地址。

【命令格式】

**show dhcpv6-snooping table**

【视图】

任意视图

【缺省情况】

无。

【参数说明】

无。

【使用举例】

#显示租约。

```
NOS# show dhcpv6-snooping table

Mac               Ipaddr            Interface     Vlan    Lease
----------------    ----------------    ------------   ----    ----------------
58:b3:8f:b9:67:15   2001:181::2       fe4          181     29d 23:58:39
58:b3:8f:b9:67:16   2001:182::2       fe4          182     29d 23:59:06
58:b3:8f:b9:67:17   2001:183::2       fe4          183     29d 23:59:35
58:b3:8f:b9:67:18   2001:184::2       fe4          184     29d 23:59:48
58:b3:8f:b9:67:19   2001:185::2       fe4          185     29d 23:59:56
```

表38-1 show dhcp server lease 命令显示详细信息描述表

| 字段 | 描述 |
|---|---|
| Interface | 客户端申请的接口 |
| MAC | 客户端MAC地址 |
| Ipaddress | 分配的IPv6地址 |
| Expire | 租约到期剩余时间 |
| vlan | 接口所属vlan |

【注意事项】

无。

### 38.2.5 reset dhcp snooping table

【功能描述】

**reset dhcpv6-snooping table** 命令清除 DHCPv6 Snooping 表项。

【命令格式】

**reset dhcpv6-snooping table**

【视图】

根视图

【缺省情况】

无。

【参数说明】

无。

【使用举例】

#清除表项。

```
NOS# reset dhcpv6-snooping table
```

### 38.2.6 dhcpv6 snooping option interface-id

【功能描述】

**dhcpv6 snooping option interface-id** 命令始能 dhcpv6 snooping 支持 option18 功能。

**no dhcpv6 snooping option interface-id** 命令用来恢复默认配置。

【命令格式】

[no] **dhcpv6 snooping option interface-id** [**string** *INTERFACEID*]

【视图】

二层接口视图

【缺省情况】

缺省未开启 option18 功能。

【参数说明】

**no**:删除 dhcpv6 snooping option interface-id 命令条目。

**string** *INTERFACEID* ：配置 option18 功能为自定义内容。

【使用举例】

#在接口 fe2 上开启 dhcp snooping option18 并配置为自定义内容 mengsiyi。

```
NOS# config interface ge2
NOS(if-fe2) dhcpv6 snooping option interface-d string mengsiyi
```

【注意事项】

无。

### 38.2.7 dhcpv6 snooping option remote-id

【功能描述】

**dhcpv6 snooping option remote-id** 命令始能 dhcpv6 snooping 支持 option37 功能。

**no dhcpv6 snooping option remote-id** 命令用来恢复默认配置。

【命令格式】

[no] dhcpv6 snooping option remote-id [string *INTERFACEID*]

【视图】

二层接口视图

【缺省情况】

缺省未开启 option37 功能。

【参数说明】

no:删除 dhcpv6 snooping option remote-id 命令条目。

string *INTERFACEID*：配置 option37 功能为自定义内容。

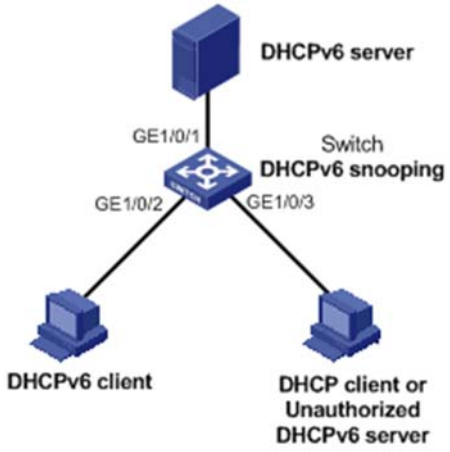
【使用举例】

#在接口 fe2 上开启 dhcp snooping option37 并配置为自定义内容 mengsiyi。

```
NOS# config interface ge2
NOS(if-fe2) dhcpv6 snooping option remote-id string mengsiyi
```

## 38.3 配置举例

图38-1 配置举例




(2) 配置全局 dhcpv6 snooping 开启

```
switchB# config dhcpv6 snooping
```

(3) 在 fe3 接口上配置成 trust 接口

```
switchB(dhcpv6-snooping)# config interface fe3
switchB(if-fe3)# dhcpv6 snooping trust
```

(4) 验证 dhcpv6 snooping。

```
switchB# show dhcpv6-snooping table
switchB# (if-fe3)# show dhcpv6-snooping table
Mac               Ipaddr            Interface     Vlan    Lease
----------------   ----------------   -----------   ----   ----------------
58:b3:8f:b9:67:15   2001:181::2       fe3          181    29d 23:58:39
58:b3:8f:b9:67:16   2001:182::2       fe3          182    29d 23:59:06
58:b3:8f:b9:67:17   2001:183::2       fe3          183    29d 23:59:35
58:b3:8f:b9:67:18   2001:184::2       fe3          184    29d 23:59:48
58:b3:8f:b9:67:19   2001:185::2       fe3          185    29d 23:59:56
```

## 38.4 常见问题

无。

# 39 路由基础

## 39.1 功能简介

在网络中路由器根据所收到的报文的目的地址选择一条合适的路径，并将报文转发到下一个路由器。路径中最后一个路由器负责将报文转发给目的主机。路由就是报文在转发过程中的路径信息，用来指导报文转发。

## 39.2 命令手册

### 39.2.1 show ip routing-table

【功能描述】

**show ip routing-table** 命令用于显示全部 IP 路由表项，显示所有协议路由。

【命令格式】

**show ip routing-table** [**protocol** <**connected**|**static**|**ospf**|**bgp**|**isis**|**rip**>|*A.B.C.D*/*A.B.C.D*/*M*|**summary**]

【视图】

任意视图

【缺省情况】

无

【参数说明】

- **static** ：指定静态路由协议。
- **ospf**：指定 OSPF 协议。
- **rip**：指定 RIP 协议。
- **isis**：指定 IS-IS 协议。
- **bgp**：指定 BGP 协议。
- **connected**：指定直连路由，一般是配置地址时生成的网段路由。
- **summary**：路由表的统计信息概要。
- A.B.C.D：指定网段。
- A.B.C.D/M：指定前缀。

【使用举例】

#显示路由表。

```
<NOS> show ip routing-table
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup

O   10.1.1.0/24 [110/10] is directly connected, vlan10, weight 1, 00:01:05
C>* 10.1.1.0/24 is directly connected, vlan10, 00:01:15
C>* 20.1.1.0/24 is directly connected, vlan20, 00:01:15
```

```
S>* 100.1.1.1/32 [1/0] via 10.1.1.1, vlan10, weight 1, 00:00:05
```

表39-1 show ip routing-table 命令显示信息描述表

| 字段 | 描述 |
| --- | --- |
| * | 下发到fib表的路由 |
| > | 最优路由 |
| via | 下一跳地址和出接口 |
| directly connected | 直连路由 |
| [110/10] | 第一个数字为协议优先级（distance）,第二个参数为路由开销（cost）协议优先级查看下表 |

表39-2 NOS 缺省管理距离

| 路由源（协议） | 管理距离（distance） |
| --- | --- |
| 直连路由 * | 0 |
| 静态路由 | 1 |
| EIGRP汇总路由 | 5 |
| 外部BGP | 20 |
| EIGRP | 90 |
| IGRP | 100 |
| OSPF | 110 |
| IS-IS | 115 |
| RIP | 120 |
| EGP | 140 |
| 外部EIGRP | 170 |
| 内部BGP | 200 |
| 未知 | 255 |

备注：数字越小优先级越高

#指定网段 100.1.1.1 显示详细路由。

```
<NOS> show ip routing-table 100.1.1.1
Routing entry for 100.1.1.1/32
  Known via "static", distance 1, metric 0, best
  Last update 00:00:33 ago
  * 10.1.1.1, via vlan10, weight 1
```

表39-3 show ip routing-table 命令显示详细信息描述表

| 字段 | 描述 |
| --- | --- |
| best | 该路由为最优路由 |
| * | 下发到fib表的路由 |

| | |
|---|---|
| via | 下一跳地址和出接口 |
| directly connected | 直连路由 |
| distance | 路由协议优先级 |
| metric | 路由开销值 |
| weight | 下一跳的权重 |

【注意事项】

无。

### 39.2.2 show ip fib

【功能描述】

**show ip fib** 命令用于显示生效的 IP 转发表项。

【命令格式】

**show ip fib** [**protocol** <**connected**|**static**|**ospf**|**bgp**|**isis**|**rip**>]

【视图】

任意视图

【缺省情况】

无

【参数说明】

- **static** ：静态路由协议。
- **ospf**：OSPF 协议。
- **rip**：RIP 协议。
- **isis**：IS-IS 协议。
- **bgp**：BGP 协议。
- **connected**：直连路由，一般是配置地址时生成的网段路由。

【使用举例】

#显示 FIB 表。

```
<NOS> show ip fib
Destination        Protocol  Nexthop           Interface
-----------------  --------  ---------------     ---------
100.1.1.0/24       static    10.1.2.1          vlan2
                             10.1.3.3           vlan3
```

表39-4 show ip fib 命令显示详细信息描述表

| 字段 | 描述 |
|---|---|
| Destination | 路由目的地址 |
| Protocol | 路由协议名称 |
| Nexthop | 下一跳地址 |
| Interface | 下一跳出接口 |

【注意事项】

无。

### 39.2.3 show ipv6 routing-table

【功能描述】

**show ipv6 routing-table** 命令用于显示全部 IPv6 路由表项，显示所有协议路由。

【命令格式】

**show ip routing-table** [**protocol** <**connected**|**static**|**ospfv3**|**bgp**|**isis**|**ripng**>| *X:X::X:X/ X:X::X:X/M*|**summary**]

【视图】

任意视图

【缺省情况】

无

【参数说明】

- **static** ：指定静态路由协议。
- **ospfv3**：指定 OSPF 协议。
- **ripng**：指定 RIP 协议。
- **isis**：指定 IS-IS 协议。
- **bgp**：指定 BGP 协议。
- **connected**：指定直连路由，一般是配置地址时生成的网段路由。
- **summary**：路由表的统计信息概要。
- X:X::X:X：指定网段。
- X:X::X:X/M：指定前缀。

【使用举例】

#显示路由表。

```
<NOS> show ipv6 routing-table
Codes: K - kernel route, C - connected, S - static, R - RIPng,
       O - OSPFv3, I - IS-IS, B - BGP, N - NHRP, T - Table,
       v - VNC, V - VNC-Direct, A - Babel, D - SHARP, F - PBR,
       f - OpenFabric,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup

Total ipv6 routing-table count: 3

C>* 2001:1::/64 is directly connected, mgt0, 19:23:34
I>* 3001:1::/64 [115/20] via fe80::a00:27ff:fedf:400, mgt0, weight 1, 00:00:21
C>* fe80::/64 is directly connected, mgt0, 19:24:23
```

表39-5 show ipv6 routing-table 命令显示信息描述表

| 字段 | 描述 |
| --- | --- |
| * | 下发到转发表的路由 |
| > | 选择的最优路由 |

| | |
|---|---|
| via | 下一跳地址和出接口 |
| directly connected | 直连路由 |
| [110/10] | 第一个数字为协议优先级（distance），第二个参数为路由开销（cost）协议优先级查看表 1.1 |

#指定网段 100.1.1.1 显示详细路由。

```
<NOS> show ipv6 routing-table 3001:1::
Routing entry for 3001:1::/64
  Known via "isis", distance 115, metric 20, best
  Last update 00:04:10 ago
  * fe80::a00:27ff:fedf:400, via mgt0, weight 1
```

表39-6 show ipv6 routing-table 命令显示详细信息描述表

| 字段 | 描述 |
|---|---|
| best | 该路由为最优路由 |
| * | 下发到转发表项的路由 |
| Known via "isis" | 生成该路由条目的协议为isis |
| via | 下一跳地址和出接口 |
| directly connected | 直连路由 |
| distance | 路由协议优先级 |
| metric | 路由开销值 |
| weight | 下一跳的权重 |

【注意事项】

无。

### 39.2.4 show ipv6 fib

【功能描述】

**show ipv6 fib** 命令用于显示生效的 IPv6 转发表项。

【命令格式】

**show ipv6 fib** [**protocol** <**connected**|**static**|**ospfv3**|**bgp**|**isis**|**ripng**>]

【视图】

任意视图

【缺省情况】

无

【参数说明】

- **static** ：静态路由协议。
- **ospfv3**：OSPF 协议。
- **ripng**：RIP 协议。

- **isis**：IS-IS 协议。
- **bgp**：BGP 协议。
- **connected**：直连路由，一般是配置地址时生成的网段路由。

【使用举例】

#显示 FIB 表。

```
<NOS> show ipv6 fib
Toal ipv6 fib count: 4
Destination : ::1/128
Nexthop     : -
Interface   : Null0
Pmtu        : -
Destination : 2001:1::/64
Nexthop     : -
Interface   : mgt0
Pmtu        : -
Destination : 3001:1::/64
Nexthop     : fe80::a00:27ff:fedf:400
Interface   : mgt0
Pmtu        : -
Destination : fe80::/64
Nexthop     : -
Interface   : mgt0
Pmtu        : -
```

表39-7 show ipv6 fib 命令显示详细信息描述表

| 字段 | 描述 |
| --- | --- |
| Destination | 路由目的地址 |
| count | 转发表中的条目总数 |
| Nexthop | 下一跳地址 |
| Interface | 下一跳出接口 |

【注意事项】

无。

### 39.2.5 config ip urpf

【功能描述】

**config ip urpf** 命令用于配置单播逆向路径检查，用来防止基于源地址欺骗的网络攻击行为。

**no config ip urpf** 命令用于删除配置单播逆向路径检查

【命令格式】

**config ip urpf** <**loose**|**strict**>

**no config ip urpf**

【视图】

根视图

【缺省情况】

无

【参数说明】

loose：指定松散模式。

strict：指定严格模式。

【使用举例】

```
NOS# config ip urpf loose
```

【注意事项】

无

### 39.2.6 config ipv6 urpf

【功能描述】

config ipv6 urpf 命令用于配置单播逆向路径检查，用来防止基于源地址欺骗的网络攻击行为。

no config ipv6 urpf 命令用于删除配置单播逆向路径检查

【命令格式】

config ipv6 urpf <loose|strict>

no config ipv6 urpf

【视图】

根视图

【缺省情况】

无

【参数说明】

loose：指定松散模式。

strict：指定严格模式。

【使用举例】

```
NOS# config ipv6 urpf loose
```

【注意事项】

无

### 39.2.7 config dlf

【功能描述】

config dlf 命令用于配置目的查找失败的报文行为。

no config dlf 命令用于删除配置单播逆向路径检查

【命令格式】

config dlf

no config dlf

【视图】

根视图

【缺省情况】

无

【参数说明】

无

【使用举例】

```
NOS# config dlf
```

【注意事项】

无

### 39.2.8 dlf drop

【功能描述】

<dlf-unicast | dlf-mcast> drop 命令用于配置目的查找失败的报文丢弃行为。

no <dlf-unicast | dlf-mcast> drop 命令用于删除该配置

【命令格式】

<dlf-unicast | dlf-mcast> drop

no <dlf-unicast | dlf-mcast> drop

【视图】

dlf 视图

【缺省情况】

无

【参数说明】

dlf-unicast：指定单播报文行为

dlf-mcast：指定组播报文行为

【使用举例】

```
NOS# config dlf
NOS(dlf)# dlf-mcast drop
```

【注意事项】

无

## 39.3 配置举例

略。

## 39.4 常见问题

无。

# 40 静态路由

## 40.1 功能简介

静态路由是一种特殊的路由，由管理员手工配置。当网络结构比较简单时，只需配置静态路由就可以使网络正常工作。

静态路由不能自动适应网络拓扑结构的变化。当网络发生故障或者拓扑发生变化后，必须由网络管理员手工修改配置。

## 40.2 命令手册

### 40.2.1 config ip route-static

【功能描述】

**config ip route-static** 命令用来创建并进入静态路由视图。

**no config ip route-static** 命令用来删除静态路由视图并删除所有静态路由。

【命令格式】

**config ip route-static**

**no config ip route-static**

【视图】

根视图

【缺省情况】

缺省不存在静态路由视图。

【参数说明】

无。

【使用举例】

# 进入静态路由视图。

```
NOS# config ip route-static
NOS(ip-route-static)#
```

【注意事项】

删除静态路由视图会删除所有配置的静态路由。

### 40.2.2 route ip

【功能描述】

**route** 命令用来配置一条静态路由。

**no route** 命令用来删除静态路由。

【命令格式】

**route** *A.B.C.D/M*<*A.B.C.D*[*L3_IF*]|**Null0**> [**distance** *(1-255)*] [**bfd** [{**multi-hop source** *A.B.C.D* |**templete** *BFDPROFILE*}]]

**no route** *A.B.C.D/M*

**no route** *A.B.C.D/M* <*A.B.C.D* [*L3_IF_NO_CHECK*]|**Null0**>

【视图】

静态路由视图

【缺省情况】

无。

【参数说明】

- *A.B.C.D/M*：静态路由的目的 IP 地址。
- *A.B.C.D*：静态路由的下一跳 IP 地址。
- *L3_IF*：静态路由的出接口名称。
- **Null0**：无接口指定。
- **distance** *(1-255)*：路由优先级，配置的值越小，优先级越高。
- **bfd**：使能 BFD 检测功能。
- **multi-hop**：多跳 BFD 会话。
- **source** *A.B.C.D*：BFD 会话源地址。
- **templete**：BFD 模板。
- *BFDPROFILE*：BFD 模板名称。
- *L3_IF_NO_CHECK*：静态路由的出接口名称。

【使用举例】

# 配置静态路由，其目的地址为 100.1.1.0/24，指定下一跳为 2.2.2.2，出接口为 vlan10，并使能 bfd。

```
NOS# config ip route-static
NOS(ip-route-static)# route 100.1.1.0/24 2.2.2.2 vlan10 bfd
```

【注意事项】

无。

### 40.2.3 config ipv6 route-static

【功能描述】

**config ipv6 route-static** 命令用来创建并进入静态路由视图。

**no config ipv6 route-static** 命令用来删除静态路由视图并删除所有静态路由。

【命令格式】

**config ipv6 route-static**

**no config ipv6 route-static**

【视图】

根视图

【缺省情况】

缺省不存在静态路由视图。

【参数说明】

无。

【使用举例】

# 进入静态路由视图。

```
NOS# config ipv6 route-static
NOS(ipv6-route-static)#
```

【注意事项】

删除静态路由视图会删除所有配置的静态路由。

### 40.2.4 route ipv6

【功能描述】

**route** 命令用来配置一条 ipv6 静态路由。

**no route** 命令用来删除 ipv6 静态路由。

【命令格式】

**route** *X:X::X:X/M X:X::X:X* [*IFNAME*] [**distance** *NUM*]

**no route** *X:X::X:X/M*

**no route** *X:X::X:X/M X:X::X:X* [**Null0**] [*IFNAME*]

【视图】

静态路由视图

【缺省情况】

无。

【参数说明】

- *X:X::X:X/M*：静态路由的目的 IPv6 地址。
- *X:X::X:X*：静态路由的下一跳 IPv6 地址。
- *IFNAME*：静态路由的出接口名称。
- **distance** *NUM*:路由优先级，配置的 *NUM*(1-255)越小，优先级越高。
- **Null0**：无接口指定。

【使用举例】

# 配置静态路由，其目的地址为 2001:36::10/64，指定下一跳为 2001:42::20，出接口为 vlan10。

```
NOS# config ipv6 route-static
NOS(ipv6-route-static)# route 2001:36::10/64 2001:42::20 vlan10
```

【注意事项】

无。

### 40.2.5 config ip mroute-static

【功能描述】

**config ip mroute-static** 命令用来创建并进入组播静态路由视图。

**no config ip mroute-static** 命令用来删除组播静态路由视图并删除所有静态路由。

【命令格式】

**config ip mroute-static**

**no config ip mroute-static**

【视图】

根视图

【缺省情况】

缺省不存在静态路由视图。

【参数说明】

无。

【使用举例】

# 进入静态路由视图。

```
NOS# config ip mroute-static
NOS(ip-mroute-static)#
```

【注意事项】

删除静态路由视图会删除所有配置的静态路由。

### 40.2.6 rpf-route-static

【功能描述】

**rpf-route-static** 命令用来配置一条组播静态路由。

**no rpf-route-static** 命令用来删除组播静态路由。

【命令格式】

**rpf-route-static** *A.B.C.D/M A.B.C.D* [*IFNAME*] [**distance** *NUM*]

**no rpf-route-static** *A.B.C.D/M A.B.C.D*

【视图】

静态组播路由视图

【缺省情况】

无。

【参数说明】

- *A.B.C.D/M*：静态路由的目的地址。
- *A.B.C.D*：静态路由的下一跳地址。
- *IFNAME*：静态路由的出接口名称。
- **distance** *NUM*:路由优先级，配置的 *NUM* 数值(1-255)越小，优先级越高。

【使用举例】

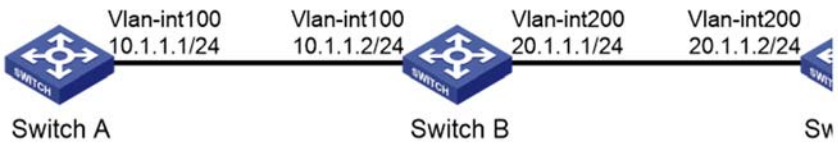
# 配置静态路由，其目的地址为 10.0.0.0/8，指定下一跳为 10.2.0.10，出接口为 vlan10。

```
NOS# config ip mroute-static
NOS(ip-mroute-static)# rpf-route-static 10.0.0.0/8 11.0.0.10 vlan10
```

【注意事项】

无。

## 40.3 配置举例




(1) 配置各接口及接口下 ip 地址略。

(2) 配静态路由，配置目的 ip，配置下一跳。

```
NOS# config ip route-static
```

```
NOS(ip-route-static)# route 20.1.1.0/24 10.1.1.2
```

(3) 配置验证

Switch A 与 Switch C 的地址互 ping。

```
NOS# ping 20.1.1.2/24
```

## 40.4 常见问题

无。

# 41 策略路由

## 41.1 功能介绍

与单纯依照 IP 报文的目的地址查找路由表进行转发不同，策略路由是一种依据用户制定的策略进行路由转发的机制。策略路由可以对于满足一定条件的报文，设置特定的出接口，指导报文的转发。策略路由的优先级要高于普通路由，即报文先按照策略路由进行转发。如果报文无法匹配所有的策略路由条件，不能按照策略路由进行转发，再按照普通路由进行转发。

## 41.2 命令手册

### 41.2.1 config policy-based-route

【功能描述】

**config policy-based-route** *RMAPNAME* **sequence** *NUMBER* 命令用于创建 PBR 并进入配置视图。

**no config policy-based-route** *RMAPNAME* **sequence** *NUMBER* 命令删除 PBR 配置。

【命令格式】

**config policy-based-route** *RMAPNAME* **sequence** *NUMBER*

【视图】

根视图

【缺省情况】

不存在配置。

【参数说明】

- RMAPNAME：指定 pbr 的名字
- NUMBER： 指定 pbr 的 sequence 号，策略路由匹配规则的 ID，数值越小优先级越高，越先被匹配。

【使用举例】

#配置 PBR。

```
NOS#  config policy-based-route asd sequence 12
NOS(pbr-asd-12)#
```

【注意事项】

无。

### 41.2.2 config ipv6 policy-based-route

【功能描述】

**config ipv6 policy-based-route** *RMAPNAME* **sequence** *NUMBER* 命令用于创建 PBR 并进入配置视图。

**no config ipv6 policy-based-route** *RMAPNAME* **sequence** *NUMBER* 命令删除 PBR 配置。

【命令格式】

**config ipv6 policy-based-route** *RMAPNAME* **sequence** *NUMBER*

【视图】

根视图

【缺省情况】

不存在配置。

【参数说明】

- RMAPNAME：指定 pbr 的名字
- NUMBER： 指定 pbr 的 sequence 号，策略路由匹配规则的 ID，数值越小优先级越高，越先被匹配。

【使用举例】

#配置 PBR。

```
NOS#  config policy-based-route asd sequence 12
NOS(pbr-asd-12)#
```

【注意事项】

无。

### 41.2.3 policy-based-route

【功能描述】

**policy-based-route** *RMAPNAME* 命令用于在接口视图应用对应名称 PBR。

**no policy-based-route** 命令删除 PBR 配置。

【命令格式】

**policy-based-route** *RMAPNAME* **sequence** *NUMBER*

**no policy-based-route**

【视图】

根视图

【缺省情况】

不存在配置。

【参数说明】

*RMAPNAME*：指定 pbr 的名字

【使用举例】

#配置 PBR。

```
NOS(if-vlan10)# policy-based-route asd
```

【注意事项】

无。

### 41.2.4 ipv6 policy-based-route

【功能描述】

**ipv6 policy-based-route** *RMAPNAME* 命令用于在接口视图应用对应名称 PBR。

**no ipv6 policy-based-route** 命令删除 PBR 配置。

【命令格式】

**ipv6 policy-based-route** *RMAPNAME* **sequence** *NUMBER*

**no ipv6 policy-based-route**

【视图】

根视图

【缺省情况】

不存在配置。

【参数说明】

*RMAPNAME*：指定 pbr 的名字

【使用举例】

#配置 PBR。

```
NOS(if-vlan10)# ipv6 policy-based-route asd
```

【注意事项】

无。

### 41.2.5 match dst-ip ip

【功能描述】

**match dst-ip** 命令用于配置匹配报文目的 IP 地址。

**no match dst-ip** 命令用于恢复默认情况。

【命令格式】

**match dst-ip** *A.B.C.D/M*

**no match dst-ip**

【视图】

策略路由配置视图

【缺省情况】

不匹配报文目的 IP 地址

【参数说明】

A.B.C.D/M：匹配报文目的 IP 地址。

【使用举例】

#配置一条策略路由 asd，匹配条件是目的 IP 地址为 10.1.1.2。

```
NOS# config policy-based-route asd sequence 12
NOS(pbr-asd-12)# match dst-ip 10.1.1.2
```

【注意事项】

无。

### 41.2.6 match dst-ip ipv6

【功能描述】

**match dst-ip** 命令用于配置匹配报文目的 IPv6 地址。

**no match dst-ip** 命令用于恢复默认情况。

【命令格式】

**match dst-ip** *X:X::X:X/M*

**no match dst-ip**

【视图】

策略路由配置视图

【缺省情况】

不匹配报文目的 IPv6 地址

【参数说明】

*X:X::X:X/M*：匹配报文目的 IPv6 地址。

【使用举例】

#配置一条策略路由 asd，匹配条件是目的 IP 地址为 123::123/128。

```
NOS# config ipv6 policy-based-route asd sequence 12
NOS(ipv6-pbr-asd-12)# match dst-ip 123::123/128
```

【注意事项】

无。

### 41.2.7 match dst-port

【功能描述】

**match dst-port** 命令用于配置匹配报文目的端口号。

**no match dst-port** 命令用于恢复默认情况。

【命令格式】

**match dst-port** *START_PORTNUM* [*END_PORTNUM*]

**no match dst-port**

【视图】

策略路由配置视图

【缺省情况】

不匹配报文目的端口号

【参数说明】

- *START_PORTNUM*:目的端口号范围的起始端口号，如果不指定 *END_PORTNUM* 表示匹配当前端口号。
- END_PORTNUM：目的端口号范围的结束端口号，必须大于等于 START_PORTNUM。

【使用举例】

#配置一条策略路由 asd，匹配条件是目的端口号是 30000。

```
NOS# config policy-based-route asd sequence 12
NOS(pbr-asd-12)#  match dst-port 30000
```

【注意事项】

只有当指定协议类型是 tcp 或者 udp 时，此配置才会起作用。

### 41.2.8 match ip-protocol

【功能描述】

**match ip-protocol** 命令用于配置匹配报文协议。

**no match ip-protocol** 命令用于恢复默认情况。

【命令格式】

**match ip-protocol** <**tcp**|**udp**|*PROTONUM*>

**no match ip-protocol**

【视图】

策略路由配置视图

【缺省情况】

不匹配报文协议

【参数说明】

- **tcp**：tcp 协议。
- **udp**：udp 协议
- (1-255)>：匹配报文协议号。

【使用举例】

#配置一条策略路由 asd，匹配条件是协议类型是 tcp。

```
NOS# config policy-based-route asd sequence 12
NOS(pbr-asd-12)# match ip-protocol tcp
```

【注意事项】

无。

### 41.2.9 match src-ip

【功能描述】

**match src-ip** 命令用于配置匹配报文源 IP 地址。

**no match src-ip** 命令用于恢复默认情况。

【命令格式】

**match src-ip** *A.B.C.D/M*

**no match src-ip**

【视图】

策略路由配置视图

【缺省情况】

不匹配报文源 IP 地址

【参数说明】

*A.B.C.D/M*：匹配报文源 IP 地址。

【使用举例】

#配置一条策略路由 asd，匹配条件是源 IP 地址为 10.1.1.2。

```
NOS# config policy-based-route asd sequence 12
NOS(pbr-asd-12)# match src-ip 10.1.1.2
```

【注意事项】

无。

### 41.2.10 match src-ip ipv6

【功能描述】

**match src-ip** 命令用于配置匹配报文源 IPv6 地址。

**no match src-ip** 命令用于恢复默认情况。

【命令格式】

**match src-ip** *X:X::X:X/M*

**no match src-ip**

【视图】

策略路由配置视图

【缺省情况】

不匹配报文源 IPv6 地址

【参数说明】

*X:X::X:X/M*：匹配报文源 IPv6 地址。

【使用举例】

#配置一条策略路由 asd，匹配条件是源 IP 地址为 123::123/128。

```
NOS# config ipv6 policy-based-route asd sequence 12
NOS(ipv6-pbr-asd-12)# match src-ip 123::123/128
```

【注意事项】

无。

### 41.2.11 match src-port

【功能描述】

**match src-port** 命令用于配置匹配报文源端口号。

**no match src-port** 命令用于恢复默认情况。

【命令格式】

**match src-port** *START_PORTNUM* [*END_PORTNUM*]

**no match src-port**

【视图】

策略路由配置视图

【缺省情况】

不匹配报文源端口号

【参数说明】

- *START_PORTNUM*:源端口号范围的起始端口号，如果不指定 *END_PORTNUM* 表示匹配当前端口号。
- END_PORTNUM：源端口号范围的结束端口号，必须大于等于 START_PORTNUM。

【使用举例】

#配置一条策略路由 asd，匹配条件是源端口号是 30000。

```
NOS# config policy-based-route asd sequence 12
NOS(pbr-asd-12)# match src-port 30000
```

【注意事项】

只有当指定协议类型是 tcp 或者 udp 时，此配置才会起作用。

### 41.2.12 set nexthop

【功能描述】

**set nexthop** 命令用于配置配置策略路由下一跳。

【命令格式】

**set nexthop** *A.B.C.D*

【视图】

策略路由配置视图

【缺省情况】

没有配置下一跳。

【参数说明】

*A.B.C.D*：配置策略路由对应下一跳。

【使用举例】

#配置一条策略路由 asd，下一跳使用 nexthop 300。

```
NOS# config policy-based-route asd sequence 12
NOS(pbr-asd-12)# set nexthop 1.2.3.4
```

【注意事项】

策略路由必须配置下一跳。

### 41.2.13 set nexthop ipv6

【功能描述】

**set nexthop** 命令用于配置配置策略路由下一跳。

【命令格式】

**set nexthop** *X:X::X:X*

【视图】

策略路由配置视图

【缺省情况】

没有配置下一跳。

【参数说明】

*X:X::X:X*：配置策略路由对应下一跳。

【使用举例】

#配置一条策略路由 asd，下一跳使用 nexthop 300。

```
NOS# config policy-based-route asd sequence 12
NOS(ipv6-pbr-asd-12)# set nexthop 123::123
```

【注意事项】

策略路由必须配置下一跳。

### 41.2.14 show fib policy-based-route nexthop

【功能描述】

**show fib policy-based-route nexthop** 命令用显示生效的 PBR 的下一跳配置。

【命令格式】

**show fib policy-based-route nexthop** *NEXTHOPID*

【视图】

任意视图

【缺省情况】

无。

【参数说明】

*NEXTHOPID*：下一跳 ID，范围 256-32765。

【使用举例】

#显示 ID 为 300 的下一跳

```
<NOS> show fib policy-based-route nexthop 300
IPv4 Address       Interface
---------------    ---------------
10.1.2.1            vlan2
10.1.3.3            vlan3
```

表41-1 show pbr nexthop 命令显示详细信息描述表

| 字段 | 描述 |
| --- | --- |
| IPv4 address | 下一跳地址 |
| Interface | 下一跳出接口 |

【注意事项】

无。

### 41.2.15 show ipv6 fib policy-based-route nexthop

【功能描述】

**show fib policy-based-route nexthop** 命令用显示生效的 PBR 的下一跳配置。

【命令格式】

**show ipv6 fib policy-based-route nexthop** *NEXTHOPID*

【视图】

任意视图

【缺省情况】

无。

【参数说明】

*NEXTHOPID*：下一跳 ID，范围 1-65535。

【使用举例】

#显示 ID 为 300 的下一跳

```
<NOS> show ipv6 fib policy-based-route nexthop 10001
IPv6 Address                            Interface
----------------------                    ---------------
123::234                                  vlan10
```

表41-2 show pbr nexthop 命令显示详细信息描述表

| 字段 | 描述 |
| --- | --- |
| IPv6 address | 下一跳地址 |
| Interface | 下一跳出接口 |

【注意事项】

无。

## 41.2.16 show policy-based-route

【功能描述】

**show policy-based-route** 命令显示策略路由匹配规则。

【命令格式】

**show policy-based-route** 〈**verbose**|*NAME*|**fib**〉

【视图】

任意视图

【缺省情况】

无。

【参数说明】

- *NAME*:pbr 对应的名称。
- **verbose**：显示详细信息。
- **fib**：显示已经下发的 pbr

【使用举例】

#显示路由策略规则

```
NOS# show policy-based-route verbose
  pbr-map asd valid: yes
    Seq: 11 rule: 310
        Installed: 1(2) Reason: Valid
        SRC Match: 123.1.1.0/24
        DST Match: 123.1.1.0/24
        nexthop 123.1.1.2
          Installed: 1(1) Tableid: 10002
NOS#  show policy-based-route fib
Priority      : 310              In-Interface   : vlan10
Src-Ip        : 123.1.1.0/24      Dst-Ip        : 123.1.1.0/24
Protocol      : -                 Dscp          : -
Src-Port      : -                 Dst-Port      : -
```

```
Nexthop-Id     : 10002
```

表41-3 show policy-based-route 命令显示详细信息描述表

| 字段 | 描述 |
| --- | --- |
| pbr-map | 策略路由名称 |
| Src-Ip | 报文源IP地址 |
| Dst-Ip | 报文目的IP地址 |
| Protocol | 报文协议号 |
| Src-Port | TCP/UDP报文源端口 |
| Dst-Port | TCP/UDP报文目的端口 |
| Nexthop | 下一跳IP |

【注意事项】

无。

### 41.2.17 show ipv6 policy-based-route

【功能描述】

**show ipv6 policy-based-route** 命令显示策略路由匹配规则。

【命令格式】

**show ipv6 policy-based-route** <**verbose**|*NAME*|**fib**>

【视图】

任意视图

【缺省情况】

无。

【参数说明】

- *NAME*:pbr 对应的名称。
- **verbose**：显示详细信息。
- **fib**：显示已经下发的 pbr。

【使用举例】

#显示路由策略规则

```
<NOS># show ipv6  policy-based-route asdf verbose
  pbr-map asdf valid: yes
    Seq: 11 rule: 310
       Installed: 1(1) Reason: Valid
       DST Match: 123::/64
       nexthop 123::234
         Installed: 1(1) Tableid: 10001
 NOS# show ipv6 policy-based-route fib

Priority      : 310              In-Interface   : vlan10
```

```
Src-Ip        : -                  Dst-Ip        : 123::/64
Protocol      : -                  Dscp          : -
Src-Port      : -                  Dst-Port      : -
Nexthop-Id    : 10001
```

表41-4 show ipv6 policy-based-route 命令显示详细信息描述表

| 字段 | 描述 |
|---|---|
| pbr-map | 策略路由名称 |
| Src-Ip | 报文源地址 |
| Dst-Ip | 报文目的地址 |
| Protocol | 报文协议号 |
| Src-Port | TCP/UDP报文源端口 |
| Dst-Port | TCP/UDP报文目的端口 |
| Nexthop | 下一跳 |

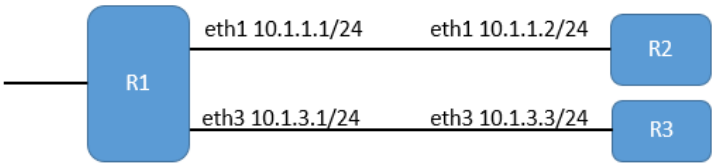
【注意事项】

无。

## 41.3 配置举例

如下图，如果 fe1 接口的开销值更小，流量到达 R1 后会从 fe1 转发至 R2。配置策略路由使源 ip 为 20.1.1.2 的报文从 fe3 接口转发至 R3。

图41-1 配置举例




(2) 配置各接口并使能 Pbr 略。

(3) 配策略路由，匹配条件是源 IP 地址，配置下一跳。

```
<R1># config policy-based-route asd sequence 12
<R1(pbr-100)># match source-ip 20.1.1.2/32
<R1(pbr-100)># set nexthop 10.1.3.3
```

(4) 配置验证

a. PBR 显示有配置的 PBR 匹配规则和下一跳，且报文转发正确。

```
<R1> show policy-based-route asd
```

## 41.4 常见问题

### 41.4.1 配置下一跳show fib policy-based-route nexthop命令没有显示

配置的下一跳地址必须可达，且出接口必须是有效出接口，否则将配置失败。

# 42 IGMP Snooping

## 42.1 功能介绍

IGMP Snooping 是 Internet Group Management Protocol Snooping（互联网组管理协议窥探）的简称，它是运行在二层设备上的组播约束机制，用于管理和控制组播组。

## 42.2 命令手册

### 42.2.1 config igmp-snooping

【功能描述】

**config igmp-snooping** 命令用来进入 igmp-snooping 视图并开启全局 igmp-snooping 功能。

**no config igmp-snooping** 命令用来关闭全局 igmp-snooping 功能和删除 igmp-snooping 视图及视图下的所有配置。

【命令格式】

**config igmp-snooping**

**no config igmp-snooping**

【视图】

根视图

【缺省情况】

缺省不存在 igmp-snooping 视图。

【参数说明】

无。

【使用举例】

#开启全局 igmp-snooping 并进入 igmp-snooping 视图。

```
NOS# config igmp-snooping
NOS(igmp-snooping)#
```

【注意事项】

无。

### 42.2.2 querier enable

【功能描述】

**querier eanble** 命令用来开启组播查询。

**no querier eanble** 命令用来关闭组播查询。

【命令格式】

**querier enable**

**no querier enable**

【视图】

igmp-snooping 视图

【缺省情况】

缺省默认不开启组播查询功能。

【参数说明】

无

【使用举例】

#开启组播查询功能。

```
NOS# config igmp-snooping
NOS(igmp-snooping)# querier eanble
```

【注意事项】

无。

### 42.2.3 robust-count

【功能描述】

IGMP 查询器的健壮系数是为了弥补可能发生的网络丢包而设置的报文重传次数，重传次数越多，IGMP 查询器就越“健壮”，但是组播组超时所需的时间也就越长。配置健壮性系数之后，下面这些参数也会随着健壮性参数的改变而改变：

- 组成员超时时间 = 健壮性系数 * 普通组查询时间 + 最大响应时间；
- 其他查询者超时时间 = 健壮性系数 * 普通查询时间 + 最大响应时间/2；
- 由此看来健壮性系数值越大 IGMP 组成员超时时间和其他查询者超时时间越长，使用者要根据网络的实际情况来设定此值。

**robust-count** 命令用来修改 igmp-snooping 的健壮性系数。

**no robust-count** 命令用来恢复 igmp-snooping 的健壮性系数的缺省情况。

【命令格式】

**robust-count** *COUNT*

**no robust-count**

【视图】

igmp-snooping 视图

【缺省情况】

缺省默认健壮性系数值为 2。

【参数说明】

*COUNT*：指定 IGMP 查询器的健壮系数，取值范围为 2～5。

【使用举例】

#修改健壮性系数为 3。

```
NOS# config igmp-snooping
NOS(igmp-snooping)# robust-count 3
```

【注意事项】

修改健壮性系数会影响组播组成员的老化时间，具体公式为：

老化时间 = robust-count × query-interval + max-response-time

### 42.2.4 lastmember-query-interval

【功能描述】

**lastmember-query-interval** 命令用来修改 igmp 发送指定组查询报文的时间间隔。

**no lastmember-query-interval** 命令用来恢复 igmp 发送指定组查询报文的时间间隔到默认值。

【命令格式】

**last-member-query-interval** *INTERVAL*

**no last-member-query-interval**

【视图】

igmp-snooping 视图

【缺省情况】

缺省默认 igmp 发送指定组查询报文的时间间隔为 1 秒。

【参数说明】

*INTERVAL*：表示 IGMP 指定组查询报文的发送间隔，取值范围为 1～20，单位为秒。

【使用举例】

#修改 igmp 指定组查询的间隔为 10 秒。

```
NOS# config igmp-snooping
NOS(igmp-snooping)# last-member-query-interval 10
```

【注意事项】

当 IGMP 查询者收到某个组播组的离开报文之后，会发送“指定组查询次数”次指定组查询报文针对该组播组在该网段上进行查询，目的是为了知道该子网内是否还有该组播组成员，上游查询器如果在 robust-count × lastmember-queryinterval 时间内，收到其他主机发送的 Report 报文，就会继续维护该组的组成员关系；如果经过 robust-count × lastmember-queryinterval 时间后，仍然没有收到任何主机发送的 Report 报文，就认为该组已经超时，不再维护该组的组成员关系。

### 42.2.5 query-interval

【功能描述】

**query-interval** 命令用来修改配置查询器发送通用查询报文的时间间隔。

**no query-interval** 命令用来恢复查询器发送通用查询报文的时间间隔的缺省情况。

【命令格式】

**query-interval** *INTERVAL*

**no query-interval**

【视图】

igmp-snooping 视图

【缺省情况】

缺省默认查询器发送通用查询报文的时间间隔为 125s。

【参数说明】

*INTERVAL*：查询器发送通用查询报文的时间间隔，取值范围为 1～65535，单位为秒。

【使用举例】

#修改查询器发送通用查询报文的时间间隔为 120 秒。

```
NOS# config igmp-snooping
```

```
NOS(igmp-snooping)# query-interval 120
```

【注意事项】

修改通用查询报文的时间间隔会影响组播组成员的老化时间，具体公式为：

老化时间 = robust-count × query-interval + max-response-time

### 42.2.6 max-response-time

【功能描述】

IGMP 查询者发送的普通组查询报文中含有最大响应时间字段，接收者将在最大响应时间间隔内发送组成员关系报告。如果接收者没有在最大响应时间间隔内发送组成员关系报告，设备就认为该子网没有该组播组的接受者，立即删除组播组信息。

**max-response-time** 命令用来修改配置下游主机回复查询器的最大响应时间。

**no max-response-time** 命令用来恢复下游主机回复查询器的最大响应时间的缺省情况。

【命令格式】

**max-response-time** *SECONDS*

**no max-response-time**

【视图】

igmp-snooping 视图

【缺省情况】

缺省默认下游主机回复查询器的最大响应时间为 10 秒。

【参数说明】

*SECONDS*：表示 IGMP 普遍组查询的最大响应时间，取值范围为 1～255，单位为秒。

【使用举例】

#修改下游主机回复查询器的最大响应时间为 30 秒。

```
NOS# config igmp-snooping
NOS(igmp-snooping)# max-response-time 30
```

【注意事项】

修改下游主机回复查询器的最大响应时间会影响组播组成员的老化时间，具体公式为：

老化时间 = robust-count × query-interval + max-response-time。

### 42.2.7 igmp-snooping enable

【功能描述】

**igmp-snooping enable** 命令用来开启指定 vlan 下的 igmp-snooping 功能。

**no igmp-snooping enable** 命令用来关闭 vlan 下的 igmp-snooping 功能。

【命令格式】

**igmp-snooping enable**

**no igmp-snooping enable**

【视图】

VLAN 视图

【缺省情况】

缺省 VLAN 不开启 igmp-snooping 功能。

【参数说明】

无。

【使用举例】

#在 vlan99 下打开 igmp-snooping 功能。

```
NOS#config vlan 99
NOS(vlan-99)# igmp-snooping enable
```

【注意事项】

只有全局打开 igmp-snooping 配置 vlan 下的配置才会生效。

vlan 删除时 vlan 下的 igmp-snooping 功能也会删除并失效

### 42.2.8 igmp-snooping bypass mrouter

【功能描述】

**igmp-snooping bypass mroute** 命令用来配置当前 vlan 内组播流量不往路由端口转发。

**no igmp-snooping enable** 命令用来恢复缺省情况。

【命令格式】

**igmp-snooping bypass mrouter**

**no igmp-snooping bypass mrouter**

【视图】

VLAN 视图

【缺省情况】

缺省 VLAN 内组播流量往路由端口转发。

【参数说明】

无。

【使用举例】

#在 vlan99 下配置组播流量不往路由端口转发功能。

```
NOS#config vlan 99
NOS(vlan-99)# igmp-snooping bypass mrouter
```

【注意事项】

无。

### 42.2.9 igmp-snooping drop-unknown

【功能描述】

**igmp-snooping drop-unknown** 命令用来开启指定 vlan 下的未知组播丢弃功能。

**no igmp-snooping drop-unknown** 命令用来关闭 vlan 下的未知组播丢弃功能。

【命令格式】

**igmp-snooping drop-unknown**

**no igmp-snooping drop-unknown**

【视图】

VLAN 视图

【缺省情况】

缺省 VLAN 不开启 igmp-snooping drop-unknown 功能，未知组播在 VLAN 内 flood。

【参数说明】

无。

【使用举例】

#在 vlan99 下打开 igmp-snooping 功能。

```
NOS#config vlan 99
NOS(vlan-99)# igmp-snooping drop-unknwon
```

【注意事项】

只有全局打开 igmp-snooping 配置 vlan 下的配置才会生效。

vlan 删除时 vlan 下的 igmp-snooping drop-unknwon 功能也会删除并失效

### 42.2.10 igmp-snooping query source-ip

【功能描述】

**query source ip** 命令用来修改 igmp 查询报文的源 ip 地址。

**no max-response-time** 命令用来恢复 igmp 查询报文的源 ip 地址的缺省情况。

【命令格式】

**igmp-snooping query source-ip** *A.B.C.D*

**no igmp-snooping query source-ip**

【视图】

vlan 视图

【缺省情况】

缺省默认 igmp 查询报文的源 ip 地址为 0.0.0.0。

【参数说明】

*A.B.C.D*: 作为 igmp 查询报文源 ip 地址的 ipv4 地址

【使用举例】

#修改 vlan 20 下网段的 igmp 查询报文源地址为 10.1.1.1。

```
NOS# config vlan 20
NOS(vlan-20)# igmp-snooping query source-ip 10.1.1.1
```

【注意事项】

无

### 42.2.11 igmp-snooping fast-leave

【功能描述】

在网络中的末梢网段只连接了一台主机频繁的进行组播组的切换动作，为了减少离开延迟可以在设备上配置组播组快速离开。

配置了快速离开后，设备收到某个组播组的离开报文，检查是否开启快速离开，如果是则设备不再向该网段内发送指定组查询报文，并且将该组播组的信息立即删除。

**igmp-snooping fast-leave** 命令用来开启指定接口的快速离开功能。

**no igmp-snooping fast-leave** 命令用来关闭指定接口的快速离开功能。

【命令格式】

**igmp-snooping fast-leave vlan** *VLANID*

**no igmp-snooping fast-leave vlan** *VLANID*

【视图】

二层接口视图

【缺省情况】

缺省默认不开启快速离开功能。

【参数说明】

*VLANID*: 指定 VLAN ID,取值范围 1-4094。

【使用举例】

#在 fe1 vlan 20 下打开 fast-leave 功能。

```
NOS# config interface fe1
NOS(if-fe1)# igmp-snooping fast-leave vlan 20
```

【注意事项】

开启该功能后该接口不会接收到符合该 vlan 的组播组的 IGMP 特定组查询报文。

### 42.2.12 igmp-snooping group deny

【功能描述】

如果不希望接口所在网段上的主机加入某些组播组，可在该接口上配置 deny 规则作为过滤器。

**group deny** 命令用来配置接口组播组过滤功能。

**no group deny** 命令用来关闭接口下的组播组过滤。

【命令格式】

**igmp-snooping group deny vlan** *VLANID A.B.C.D/M*

**no igmp-snooping group deny** [**vlan** *VLANID*] [*A.B.C.D/M*]

【视图】

二层接口视图

【缺省情况】

缺省接口不进行组播组过滤。

【参数说明】

- *VLANID*: 指定 VLAN ID,取值范围 1-4094。
- *A.B.C.D/M*: 指定过滤的组播组地址或者网段。

【使用举例】

#在接口 fe1 过滤属于 vlan 20 网段 224.1.0.0 的组播组。

```
NOS# config interface fe1
NOS(if-fe1)# igmp-snooping group deny vlan 20 224.1.1.1/16
```

【注意事项】

- 允许添加已经被原有配置网段包含的网段配置，但是当删除此配置时，因为仍有包含该网段的过滤配置生效因此接口继续过滤属于本网段的组播组。
- 多次配置都会生效不会覆盖。
- 只能配置组播地址。

### 42.2.13 igmp-snooping static-group

【功能描述】

**static group** 命令用来在接口下配置静态组播组。

**no static group** 命令用来取消接口下的静态组播组配置。

【命令格式】

**igmp-snooping static-group** A.B.C.D **vlan** *VLANID*

**no igmp-snooping static-group** [A.B.C.D [**vlan** *VLANID*]]

【视图】

二层接口视图

【缺省情况】

缺省接口不配置静态组播组。

【参数说明】

*VLANID*: 指定 VLAN ID,取值范围 1-4094。

*A.B.C.D*: 配置的静态组播组组播地址。

【使用举例】

#在接口 fe1 配置 vlan 20 组播地址 224.1.1.1 的静态组播组。

```
NOS# config interface fe1
NOS(if-fe1)# igmp-snooping static-group 224.1.1.1 vlan 20
```

【注意事项】

- 静态组播组不会在老化时间超时后自动删除。
- 只能配置组播地址。
- 多次配置不会覆盖，都会生效。

### 42.2.14 igmp-snooping static-router-port

【功能描述】

**static-router-port** 命令用来在接口下配置静态路由端口。

**no static-router-port** 命令用来取消接口下的静态路由端口。

【命令格式】

**igmp-snooping static-router-port vlan** *VLANID*

**no igmp-snooping static-router-port** [**vlan** *VLANID*]

【视图】

二层接口视图

【缺省情况】

缺省接口不配置静态路由端口。

【参数说明】

*VLANID*: 指定 VLAN ID,取值范围 1-4094。

【使用举例】

#在接口 fe1 配置 vlan 20 的静态路由端口。

```
NOS# config interface fe1
NOS(if-fe1)# igmp-snooping static-router-port vlan 20
```

【注意事项】

无。

### 42.2.15 reset igmp-snooping router-port

【功能描述】

**reset igmp-snooping router-port** 命令用来清除 igmp snooping 的 router-port 信息。

【命令格式】

**reset igmp-snooping router-port vlan** *VLANID*

【视图】

根视图

【缺省情况】

无。

【参数说明】

*VLANID*: 指定 VLAN ID,取值范围 1-4094。

【使用举例】

#清除 vlan 100 的 igmp snooping router-port 信息。

```
NOS# reset igmp-snooping router-port vlan 100
```

【注意事项】

无。

### 42.2.16 reset igmp-snooping group

【功能描述】

**reset igmp-snooping group** 命令用来清除 igmp snooping 的 group 信息。

【命令格式】

**reset igmp-snooping group vlan** *VLANID*

【视图】

根视图

【缺省情况】

无。

【参数说明】

*VLANID*: 指定 VLAN ID,取值范围 1-4094。

【使用举例】

#清除 vlan 100 的 igmp snooping group 信息。

```
NOS# reset igmp-snooping group vlan 100
```

【注意事项】

无。

### 42.2.17 show igmp-snooping

【功能描述】

show igmp-snooping 命令用来显示 igmp-snooping 当前的配置信息。

【命令格式】

**show igmp-snooping** [**vlan** *VLANID*] [**json**]

【视图】

根视图

【缺省情况】

无

【参数说明】

- *VLANID*: 指定 VLAN ID,取值范围 1-4094。
- *json*：以 json 格式输出结果。

【使用举例】

```
NOS# show igmp-snooping
Igmp-snooping       : Disabled
```

【注意事项】

无

### 42.2.18 show igmp-snooping group

【功能描述】

show igmp-snooping group 命令用来显示 igmp-snooping 目前的组播组信息。

【命令格式】

**show igmp-snooping group** [**vlan** *VLANID*] [**interface** *L2_IF*] [*A.B.C.D*] [**json**]

【视图】

根视图

【缺省情况】

无

【参数说明】

*VLANID*: 指定 VLAN ID,取值范围 1-4094。

*L2_IF* ：按照二层接口名进行过滤显示。

*A.B.C.D*: 按照组播组地址进行过滤显示。

*json*：以 json 格式输出结果。

【使用举例】

```
NOS# show igmp-snooping group
Total igmp snooping group count: 0
Interface    Vlan    group
----------    ----    --------
```

【注意事项】

无

### 42.2.19 show igmp-snooping router-port

【功能描述】

show igmp-snooping router 命令用来显示 igmp-snooping 目前的路由端口信息。

【命令格式】

**show igmp-snooping router-port** [**vlan** *VLANID*] [**json**]

【视图】

根视图

【缺省情况】

无

【参数说明】

- *VLANID*: 指定 VLAN ID,取值范围 1-4094。
- *json*：以 json 格式输出结果。

【使用举例】

```
NOS# show igmp-snooping router-port
Total igmp snooping router port count: 0
Interface    Vlan
----------   ----
```

【注意事项】

无

# 43 MLD Snooping

## 43.1 功能介绍

MLD Snooping 是 Multicast Listener Discovery Snooping（组播侦听者发现协议窥探）的简称。它是运行在二层设备上的 IPv6 组播约束机制，用于管理和控制 IPv6 组播组

## 43.2 命令手册

### 43.2.1 config mld-snooping

【功能描述】

**config mld-snooping** 命令用来进入 mld-snooping 视图并开启全局 mld-snooping 功能。

**no config mld-snooping** 命令用来关闭全局 mld-snooping 功能和删除 mld-snooping 视图及视图下的所有配置。

【命令格式】

**config mld-snooping**

**no config mld-snooping**

【视图】

根视图

【缺省情况】

缺省不存在 mld-snooping 视图。

【参数说明】

无。

【使用举例】

#开启全局 mld-snooping 并进入 mld-snooping 视图。

```
NOS# config mld-snooping
NOS(mld-snooping)#
```

【注意事项】

无。

### 43.2.2 querier enable

【功能描述】

**querier eanble** 命令用来开启组播查询。

**no querier eanble** 命令用来关闭组播查询。

【命令格式】

**querier eanble**

**no querier eanble**

【视图】

mld-snooping 视图

【缺省情况】

缺省默认不开启组播查询功能。

【参数说明】

无

【使用举例】

#开启组播查询功能。

```
NOS# config mld-snooping
NOS(mld-snooping)# querier eanble
```

【注意事项】

无

### 43.2.3 robust-count

【功能描述】

MLD 查询器的健壮系数是为了弥补可能发生的网络丢包而设置的报文重传次数，重传次数越多，MLD 查询器就越“健壮”，但是组播组超时所需的时间也就越长。配置健壮性系数之后，下面这些参数也会随着健壮性参数的改变而改变：

- 组成员超时时间 = 健壮性系数 * 普通组查询时间 + 最大响应时间；
- 其他查询者超时时间 = 健壮性系数 * 普通查询时间 + 最大响应时间/2；
- 由此看来健壮性系数值越大 MLD 组成员超时时间和其他查询者超时时间越长，使用者要根据网络的实际情况来设定此值。

**robust-count** 命令用来修改 mld-snooping 的健壮性系数。

**no robust-count** 命令用来恢复 mld-snooping 的健壮性系数的缺省情况。

【命令格式】

**robust-count** *COUNT*

**no robust-count**

【视图】

mld-snooping 视图

【缺省情况】

缺省默认健壮性系数值为 2。

【参数说明】

*COUNT*：指定 IGMP 查询器的健壮系数，取值范围为 2～5。

【使用举例】

#修改健壮性系数为 3。

```
NOS# config mld-snooping
NOS(mld-snooping)# robust-count 3
```

【注意事项】

修改健壮性系数会影响组播组成员的老化时间，具体公式为：

老化时间 = robust-count × query-interval + max-response-time

### 43.2.4 lastmember-query-interval

【功能描述】

**lastmember-query-interval** 命令用来修改 mld 发送指定组查询报文的时间间隔。

**no lastmember-query-interval** 命令用来恢复 mld 发送指定组查询报文的时间间隔到默认值。

【命令格式】

**last-member-query-interval** *INTERVAL*

**no last-member-query-interval**

【视图】

mld-snooping 视图

【缺省情况】

缺省默认 mld 组查询的最大响应时间为 1s。

【参数说明】

*INTERVAL*：表示 MLD 特定组查询报文的发送间隔，取值范围为 1～20，单位为秒。

【使用举例】

#修改 mld 指定组查询报文的间隔为 10 秒。

```
NOS# config mld-snooping
NOS(mld-snooping)# last-member-query-interval 10
```

【注意事项】

当 MLD 查询者收到某个组播组的离开报文之后，会发送“指定组查询次数”次指定组查询报文针对该组播组在该网段上进行查询，目的是为了知道该子网内是否还有该组播组成员，

上游查询器如果在 robust-count × lastmember-queryinterval 时间内，收到其他主机发送的 Report 报文，就会继续维护该组的组成员关系；如果经过 robust-count × lastmember-queryinterval 时间后，仍然没有收到任何主机发送的 Report 报文，就认为该组已经超时，不再维护该组的组成员关系。

### 43.2.5 query-interval

【功能描述】

**query-interval** 命令用来修改配置查询器发送通用查询报文的时间间隔。

**no query-interval** 命令用来恢复查询器发送通用查询报文的时间间隔的缺省情况。

【命令格式】

**query-interval** *INTERVAL*

**no query-interval**

【视图】

mld-snooping 视图

【缺省情况】

缺省默认查询器发送通用查询报文的时间间隔为 125s。

【参数说明】

*INTERVAL*：查询器发送通用查询报文的时间间隔，取值范围为 1～65535，单位为秒。

【使用举例】

#修改查询器发送通用查询报文的时间间隔为 120 秒。

```
NOS# config mld-snooping
NOS(mld-snooping)# query-interval 120
```

【注意事项】

修改通用查询报文的时间间隔会影响组播组成员的老化时间，具体公式为：

老化时间 = robust-count × query-interval + max-response-time。

### 43.2.6 max-response-time

【功能描述】

MLD 查询者发送的普通组查询报文中含有最大响应时间字段，接收者将在最大响应时间间隔内发送组成员关系报告。如果接收者没有在最大响应时间间隔内发送组成员关系报告，设备就认为该子网没有该组播组的接受者，立即删除组播组信息。

**max-response-time** 命令用来修改配置下游主机回复查询器的最大响应时间。

**no max-response-time** 命令用来恢复下游主机回复查询器的最大响应时间的缺省情况。

【命令格式】

**max-response-time** *SECONDS*

**no max-response-time**

【视图】

mld-snooping 视图

【缺省情况】

缺省默认下游主机回复查询器的最大响应时间为 10s。

【参数说明】

*SECONDS*：表示 IGMP 普遍组查询的最大响应时间，取值范围为 1～255，单位为秒。

【使用举例】

#修改下游主机回复查询器的最大响应时间为 30 秒。

```
NOS# config mld-snooping
NOS(mld-snooping)# max-response-time 30
```

【注意事项】

修改下游主机回复查询器的最大响应时间会影响组播组成员的老化时间，具体公式为：

老化时间 = robust-count × query-interval + max-response-time。

### 43.2.7 mld-snooping enable

【功能描述】

**mld-snooping enable** 命令用来开启指定 vlan 下的 mld-snooping 功能。

**no mld-snooping enable** 命令用来关闭 vlan 下的 mld-snooping 功能。

【命令格式】

**mld-snooping enable**

**no mld-snooping enable**

【视图】

VLAN 视图

【缺省情况】

缺省 VLAN 不开启 mld-snooping 功能。

【参数说明】

无。

【使用举例】

#在 vlan99 下打开 mld-snooping 功能。

```
NOS#config vlan 99
NOS(vlan-99)# mld-snooping enable
```

【注意事项】

只有全局打开 mld-snooping 配置 vlan 下的配置才会生效。

vlan 删除时 vlan 下的 mld-snooping 功能也会删除并失效

### 43.2.8 mld-snooping bypass mrouter

【功能描述】

**mld-snooping bypass mrouter** 命令用来配置当前 vlan 内组播流量不往路由端口转发。

**no mld-snooping bypass mrouter** 命令用来恢复缺省情况。

【命令格式】

**mld-snooping bypass mrouter**

**no mld-snooping bypass mrouter**

【视图】

VLAN 视图

【缺省情况】

缺省 VLAN 内组播流量往路由端口转发。

【参数说明】

无。

【使用举例】

#在 vlan99 下配置组播流量不往路由端口转发功能。

```
NOS#config vlan 99
NOS(vlan-99)# mld-snooping bypass mrouter
```

【注意事项】

无。

### 43.2.9 mld-snooping drop-unknown

【功能描述】

**mld-snooping drop-unknown** 命令用来开启指定 vlan 下的 mld-snooping drop-unknown 功能。

**no mld-snooping drop-unknown** 命令用来关闭 vlan 下的 mld-snooping drop-unknown 功能。

【命令格式】

**mld-snooping drop-unknown**

**no mld-snooping drop-unknown**

【视图】

VLAN 视图

【缺省情况】

缺省 VLAN 不开启 mld-snooping drop-unknown 功能，未知组播在 VLAN 内 flood。

【参数说明】

无。

【使用举例】

#在 vlan99 下打开 mld-snooping 功能。

```
NOS#config vlan 99
NOS(vlan-99)# mld-snooping drop-unknwon
```

【注意事项】

只有全局打开 mld-snooping 配置 vlan 下的配置才会生效。

vlan 删除时 vlan 下的 mld-snooping drop-unknwon 功能也会删除并失效

### 43.2.10 mld-snooping query source-ip

【功能描述】

**query source ip** 命令用来修改 mld 查询报文的源 ipv6 链路本地单播地址。

**no max-response-time** 命令用来恢复 mld 查询报文的源 ipv6 链路本地单播地址的缺省情况。

【命令格式】

**mld-snooping query source-ip** *X:X::X:X*

**no mld-snooping query source-ip**

【视图】

vlan 视图

【缺省情况】

缺省默认 mld 查询报文的源 ip 地址为 FE80::02FF:FFFF:FE00:0001。

【参数说明】

*X:X::X:X*: 作为 mld 查询报文源 ipv6 链路本地单播地址

【使用举例】

#修改 vlan 20 下网段的 mld 查询报文源地址为 fe80::32。

```
NOS# config vlan 20
NOS(vlan-20)# mld-snooping query source-ip fe80::32
```

【注意事项】

无。

### 43.2.11 mld-snooping fast-leave

【功能描述】

在网络中的末梢网段只连接了一台主机频繁的进行组播组的切换动作，为了减少离开延迟可以在设备上配置组播组快速离开。

配置了快速离开后，设备收到某个组播组的离开报文，检查是否开启快速离开，如果是则设备不再向该网段内发送指定组查询报文，并且将该组播组的信息立即删除。

**mld-snooping fast-leave** 命令用来开启指定接口的快速离开功能。

**no mld-snooping fast-leave** 命令用来关闭指定接口的快速离开功能。

【命令格式】

**mld-snooping fast-leave vlan** *VLANID*

**no mld-snooping fast-leave vlan** *VLANID*

【视图】

二层接口视图

【缺省情况】

缺省默认不开启快速离开功能。

【参数说明】

*VLANID*: 指定 VLAN ID,取值范围 1-4094。

【使用举例】

#在 fe1 vlan 20 下打开 fast-leave 功能。

```
NOS# config interface fe1
NOS(if-fe1)# mld-snooping fast-leave vlan 20
```

【注意事项】

开启该功能后该接口不会接收到符合该 vlan 的组播组的 MLD 特定组查询报文。

### 43.2.12 mld-snooping group deny

【功能描述】

如果不希望接口所在网段上的主机加入某些组播组，可在该接口上配置 deny 规则作为过滤器。

**group deny** 命令用来配置接口组播组过滤功能。

**no group deny** 命令用来关闭接口下的组播组过滤。

【命令格式】

**mld-snooping group deny vlan** *VLANID X:X::X:X/M*

**no mld-snooping group deny** [**vlan** *VLANID*] [*X:X::X:X/M*]

【视图】

二层接口视图

【缺省情况】

缺省接口不进行组播组过滤。

【参数说明】

- *VLANID*: 指定 VLAN ID,取值范围 1-4094。
- *X:X::X:X/M*: 指定过滤的 ipv6 组播组地址或者网段。

【使用举例】

#在接口 fe1 过滤属于 vlan 20 网段 ff02::/64 的组播组。

```
NOS# config interface fe1
NOS(if-fe1)# mld-snooping group deny vlan 20 ff02::/64
```

【注意事项】

- 允许添加已经被原有配置网段包含的网段配置，但是当删除此配置时，因为仍有包含该网段的过滤配置生效因此接口继续过滤属于本网段的组播组。

- 多次配置都会生效不会覆盖。
- 只能配置组播地址。

### 43.2.13 mld-snooping static-group

【功能描述】

**static group** 命令用来在接口下配置静态组播组。

**no static group** 命令用来取消接口下的静态组播组配置。

【命令格式】

**mld-snooping static-group** *X:X::X:X* **vlan** *VLANID*

**no mld-snooping static-group** [*X:X::X:X* [**vlan** *VLANID*]]

【视图】

二层接口视图

【缺省情况】

缺省接口不配置静态组播组。

【参数说明】

- *VLANID*: 指定 VLAN ID,取值范围 1-4094。
- *X:X::X:X*: 配置的静态 ipv6 组播组组播地址。

【使用举例】

#在接口 fe1 配置 vlan 20 组播地址 ff02:f::16 的静态组播组。

```
NOS# config interface fe1
NOS(if-fe1)# mld-snooping static-group ff02:f::16 vlan 20
```

【注意事项】

- 静态组播组不会在老化时间超时后自动删除。
- 只能配置组播地址。
- 多次配置不会覆盖，都会生效。

### 43.2.14 mld-snooping static-router-port

【功能描述】

**static-router-port** 命令用来在接口下配置静态路由端口。

**no static-router-port** 命令用来取消接口下的静态路由端口。

【命令格式】

**mld-snooping static-router-port vlan** *VLANID*

**no mld-snooping static-router-port** [**vlan** *VLANID*]

【视图】

二层接口视图

【缺省情况】

缺省接口不配置静态路由端口。

【参数说明】

*VLANID*: 指定 VLAN ID,取值范围 1-4094。

【使用举例】

#在接口 fe1 配置 vlan 20 的静态路由端口。

```
NOS# config interface fe1
NOS(if-fe1)# mld-snooping static-router-port vlan 20
```

【注意事项】

无。

### 43.2.15 reset mld-snooping router-port

【功能描述】

**reset mld-snooping router-port** 命令用来清除 mld snooping 的 router-port 信息。

【命令格式】

**reset mld-snooping router-port vlan** *VLANID*

【视图】

根视图

【缺省情况】

无。

【参数说明】

*VLANID*: 指定 VLAN ID,取值范围 1-4094。

【使用举例】

#清除 vlan 100 的 mld snooping router-port 信息。

```
NOS# reset mld-snooping router-port vlan 100
```

【注意事项】

无。

### 43.2.16 reset mld-snooping group

【功能描述】

**reset mld-snooping group** 命令用来清除 mld snooping 的 group 信息。

【命令格式】

**reset mld-snooping group vlan** *VLANID*

【视图】

根视图

【缺省情况】

无。

【参数说明】

*VLANID*: 指定 VLAN ID,取值范围 1-4094。

【使用举例】

#清除 vlan 100 的 mld snooping group 信息。

```
NOS# reset mld-snooping group vlan 100
```

【注意事项】

无。

### 43.2.17 show mld-snooping

【功能描述】

show mld-snooping 命令用来显示 mld-snooping 当前的配置信息。

【命令格式】

**show mld-snooping** [**vlan** *VLANID*] [**json**]

【视图】

根视图

【缺省情况】

无

【参数说明】

- *VLANID*: 指定 VLAN ID,取值范围 1-4094。
- *json*：以 json 格式输出结果。

【使用举例】

```
NOS# show mld-snooping group
Total mld snooping group count: 0
Interface    Vlan    group
----------    ----    --------
```

【注意事项】

无

### 43.2.18 show mld-snooping group

【功能描述】

show mld-snooping group 命令用来显示 mld-snooping 目前的组播组信息。

【命令格式】

**show mld-snooping group** [**vlan** *VLANID*] [**interface** *L2_IF*] [*X:X::X:X*] [**json**]

【视图】

根视图

【缺省情况】

无

【参数说明】

- *VLANID*: 指定 VLAN ID,取值范围 1-4094。
- *L2_IF* ：按照二层接口名进行过滤显示。
- *X:X::X:X*：按照组播组地址进行过滤显示。
- *json*：以 json 格式输出结果。

【使用举例】

```
NOS# show mld-snooping router-port
Interface    Vlan
```

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

【注意事项】

无

### 43.2.19 show mld-snooping router-port

【功能描述】

show mld-snooping router 命令用来显示 mld-snooping 目前的路由端口信息。

【命令格式】

**show mld-snooping router-port** [**vlan** *VLANID*] [**json**]

【视图】

根视图

【缺省情况】

无

【参数说明】

- *VLANID*: 指定 VLAN ID,取值范围 1-4094。
- *json*：以 json 格式输出结果。

【使用举例】

无

【注意事项】

无

# 44 组播 VLAN

## 44.1 功能简介

组播 VLAN 的全称 Multicast VLAN，用于将接收到的相同的组播数据在不同的用户 VLAN 进行复制分发。

组播 VLAN 按照配置方式可以分为基于子 VLAN 和基于端口两种实现和配置方式。

目前设备只支持基于端口的实现方式。

## 44.2 命令手册

### 44.2.1 config multicast-vlan

【功能描述】

**config multicast-vlan** 命令用来创建组播 VLAN 并进入组播 VLAN 视图。

**no config multicast-vlan** 命令删除组播 VLAN 并删除接口下该组播 VLAN 的配置。

【命令格式】

**config multicast-vlan** *VLANID*

**no config multicast-vlan** *VLANID*

【视图】

根视图

【缺省情况】

无。

【参数说明】

*VLANID*：VLAN 接口的标识号，取值范围为 1～4094。

【使用举例】

#创建组播 VLAN 10 并进入组播 VLAN 视图。

```
NOS# config multicast-vlan 10
NOS(mvlan-10)#
```

【注意事项】

创建组播 VLAN 时需要先创建该 VLAN

### 44.2.2 port multicast-vlan

【功能描述】

**port multicast-vlan** 命令用来接口下加入组播 VLAN。

**no port multicast-vlan** 命令用来接口下关闭组播 VLAN。

【命令格式】

**port multicast-vlan** *VLANID*

**no port multicast-vlan**

【视图】

二层接口视图

【缺省情况】

无。

【参数说明】

*VLANID*：VLAN 接口的标识号，取值范围为 1～4094。

【使用举例】

#将接口 ge1 加入组播 VLAN

```
NOS# config interface ge1
NOS(if-ge1)# port multicast-vlan 10
```

【注意事项】

接口加入组播 VLAN 时应该先创建组播 VLAN.

一个接口只能加入一个组播 VLAN。

### 44.2.3 show multicast-vlan

【功能描述】

**show multicast-vlan** 显示组播 VLAN 配置。

【命令格式】

**show multicast-vlan** [*VLANID*]

【参数说明】

*VLANID*：VLAN 接口的标识号，取值范围为 1～4094。

【使用举例】

#显示所有的组播 VLAN

```
NOS# show multicast-vlan
```

【注意事项】

无。

# 45 IGMP

## 45.1 功能简介

IGMP 是 Internet Group Management Protocol 的简称，又被称为互联网组管理协议，是 TCP/IP 协议族中负责 IPv4 组播成员管理的协议。IGMP 用来在接收者主机和与其直接相邻的组播路由器之间建立和维护组播组成员关系。IGMP 通过在接收者主机和组播路由器之间交互 IGMP 报文实现组成员管理功能，IGMP 报文封装在 IP 报文中。

IP 组播通信的特点是报文从一个源发出，被转发到一组特定的接收者。但在组播通信模型中，发送者不关注接收者的位置信息，只是将数据发送到约定的目的组播地址。要使组播报文最终能够到达接收者，需要某种机制使连接接收者网段的组播路由器能够了解到该网段存在哪些组播接收者，同时保证接收者可以加入相应的组播组中。IGMP 就是用来在接收者主机和与其所在网段直接相邻的组播路由器之间建立、维护组播组成员关系的协议。

## 45.2 命令手册

### 45.2.1 config igmp

【功能描述】

**config igmp** 命令用来开启 igmp 服务并进入 igmp 视图。

**no config igmp** 命令关闭 igmp 服务,并清除所有配置。

【命令格式】

**config igmp**

**no config igmp**

【视图】

根视图

【缺省情况】

igmp 服务处于关闭状态。

【参数说明】

无。

【使用举例】

#开启 igmp 服务并进入 igmp 视图

```
NOS# config igmp
NOS(igmp)#
```

【注意事项】

无

### 45.2.2 group-limit

【功能描述】

**group-limit** 命令用来配置动态创建组播组的上限。

**no group-limit** 命令用来取消动态创建组播组的上限

【命令格式】

**group-limit** *LIMIT*

**no group-limit**

【视图】

igmp 视图

【缺省情况】

**igmp** 服务处于关闭状态。

【参数说明】

*LIMIT*：可以动态创建组播组的上限值,取值范围为（10-60000)。

【使用举例】

#配置动态创建组播组的上限 200。

```
NOS# config igmp
NOS(igmp)# group-limit 200
NOS(igmp)#
```

【注意事项】

无

### 45.2.3 igmp enable

【功能描述】

**igmp enable** 命令用来开启接口下的 **igmp** 服务

**no igmp enable** 命令关闭接口下的 **igmp** 服务

【命令格式】

**igmp enable**

**no igmp enable**

【视图】

三层接口视图

【缺省情况】

**igmp** 服务处于关闭状态。

【参数说明】

无。

【使用举例】

#配置 vlan10 下面的 igmp。

```
NOS# config interface vlan10
NOS(if-vlan10)# igmp enable
```

【注意事项】

无

### 45.2.4 igmp version

【功能描述】

**igmp version** 命令用来配置接口下 igmp 的版本

**no igmp version** 命令恢复默认配置。

【命令格式】

**igmp version** *VERSION*

**no igmp version**

【视图】

三层接口视图

【缺省情况】

默认 igmp 版本是 3。

【参数说明】

*VERSION*: igmp 的版本(2-3)。

【使用举例】

#配置 vlan10 下面的 igmp 版本为 2。

```
NOS# config interface vlan10
NOS(if-vlan10)# igmp version 2
```

【注意事项】

无

### 45.2.5 igmp static

【功能描述】

**igmp static** 命令用来配置静态 igmp 组播组。

**no igmp static** 命令恢复默认配置。

【命令格式】

**igmp static** *GROUPADDR* [*SOURCEADDR*]

**no igmp static** *GROUPADDR*

【视图】

三层接口视图

【缺省情况】

无。

【参数说明】

- *GROUPADDR*: 指定组播组地址，取值范围为 224.0.1.0～239.255.255.255。
- *SOURCEADDR*: 指定组播源的地址。如果未指定本参数，表示针对所有组播源。

【使用举例】

#配置 vlan10 下面的加入组 225.2.2.2。

```
NOS# config interface vlan10
NOS(if-vlan10)# igmp static 225.2.2.2
```

【注意事项】

无

### 45.2.6 igmp query-interval

【功能描述】

**igmp query-interval** 命令用来配置接口下 igmp 的查询间隔。

**no igmp query-interval** 命令恢复默认配置。

【命令格式】

**igmp query-interval** *INTERVAL*

**no igmp query-interval**

【视图】

三层接口视图

【缺省情况】

默认 igmp 普遍组查询时间隔是 125 秒。

【参数说明】

*INTERVAL*：igmp 查询间隔时间,取值范围为(1-1800)，单位为秒。

【使用举例】

#配置 vlan10 下面的 igmp 版本为 120。

```
NOS# config interface vlan10
NOS(if-vlan10)# igmp query-interval 120
```

【注意事项】

无

### 45.2.7 igmp query-max-response-time

【功能描述】

**igmp query-max-response-time** 命令用来配置接口下 igmp 的查询最大响应时间间隔。

**no igmp query-max-response-time** 命令恢复默认配置。

【命令格式】

**igmp query-max-response-time** *SECONDS*

**no igmp query-max-response-time**

【视图】

三层接口视图

【缺省情况】

默认 igmp 最大响应时间是 10s。

【参数说明】

*SECONDS*：igmp 普遍组查询最大响应时间间隔,取值范围为(10-250)，单位为秒。

【使用举例】

#配置 vlan10 下面的 igmp 普遍组查询最大响应时间为 20。

```
NOS# config interface vlan10
NOS(if-vlan10)# igmp query-max-response-time 20
```

【注意事项】

无

### 45.2.8 igmp last-member-query-interval

【功能描述】

**igmp last-member-query-interval** 命令用来配置接口下 igmp 指定组成员查询间隔。。

**no igmp last-member-query-interval** 命令恢复默认配置。

【命令格式】

**igmp last-member-query-interval** *INTERVAL*

**no igmp last-member-query-interval**

【视图】

三层接口视图

【缺省情况】

默认 igmp 指定组成员查询间隔是 1s。

【参数说明】

*INTERVAL*：igmp 指定组成员查询间隔,取值范围为(1-255)，单位为秒。

【使用举例】

#配置 vlan10 下面的 igmp 指定组成员查询间隔为 5。

```
NOS# config interface vlan10
NOS(if-vlan10)# igmp last-member-query-interval 5
```

【注意事项】

无

### 45.2.9 igmp robust-count

【功能描述】

**igmp robust-count** 命令用来配置接口下 igmp 查询器的健壮系数。

**no igmp robust-count** 命令恢复默认配置。

【命令格式】

**igmp robust-count** *COUNT*

**no igmp robust-count**

【视图】

三层接口视图

【缺省情况】

默认 igmp 查询器的健壮系数是 2。

【参数说明】

*COUNT*：igmp 查询器的健壮系数，取值范围为(1-7)。

【使用举例】

#配置 vlan10 下面的 igmp 查询器的健壮系数为 3。

```
NOS# config interface vlan10
NOS(if-vlan10)# igmp robust-count 3
```

【注意事项】

无

### 45.2.10 reset igmp control-messages-counter

【功能描述】

**reset igmp control-messages-counter** 命令用于清除 igmp 报文统计信息。

【命令格式】

**reset igmp control-messages-counter**

【视图】

任意视图

【缺省情况】

无。

【参数说明】

无

【使用举例】

#清除组播路由统计信息。

```
NOS(pim)# reset igmp control-messages-counter
```

【注意事项】

无。

### 45.2.11 reset igmp groups

【功能描述】

**reset igmp groups** 命令用于清除 igmp 组信息。

【命令格式】

**reset igmp groups** [**interface** *IFNAME*]

【视图】

任意视图

【缺省情况】

无。

【参数说明】

IFNAME：接口名称，指定接口名称只清除指定接口的 igmp 组信息。

【使用举例】

#清除指定接口的 igmp 组信息。

```
NOS# reset igmp groups interface ge1
```

【注意事项】

无。

### 45.2.12 show igmp interface

【功能描述】

**show igmp interface** 命令用于显示 igmp 接口信息。

【命令格式】

**show igmp interface** [**detail**|*IFNAME*]

【视图】

任意视图

【缺省情况】

无。

【参数说明】

- *IFNAME*：接口名称，指定接口名称只显示指定的接口信息。
- detail：显示 igmp 接口的详细信息。

【使用举例】

#显示 igmp 接口 vlan20 的信息

```
NOS#  show igmp interface vlan20
Interface : vlan20
State     : up
Address   : 192.129.20.3
Uptime    : 00:08:36
Version   : 3
Querier
-------
Querier     : local
Start Count : 0
Query Timer : 00:00:15
Other Timer : --:--:--
Timers
------
Group Membership Interval     : 260s
Last Member Query Count       : 2
Last Member Query Time        : 2s
Older Host Present Interval    : 260s
Other Querier Present Interval : 255s
Query Interval               : 125s
Query Response Interval       : 10s
Robustness Variable          : 2
Startup Query Interval        : 31s
Flags
-----
All Multicast   : no
Broadcast       : yes
Deleted         : no
Interface Index : 44
Multicast       : yes
Multicast Loop  : 0
Promiscuous     : no
```

【注意事项】

无。

### 45.2.13 show igmp group

【功能描述】

**show igmp group** 命令用于显示 igmp 组播组的信息。

【命令格式】

**show igmp group** [*A.B.C.D*]

【视图】

任意视图

【缺省情况】

无。

【参数说明】

*A.B.C.D*: 组播组地址，只显示该组的组信息。

【使用举例】

#显示 igmp 组播组的信息

```
NOS(if-vlan30)# show igmp group
Total IGMP groups: 5
Watermark warn limit(Not Set): 0
Interface       Address        Group          Source         V  Mode Timer Fwd Uptime
vlan20          192.129.20.3   225.1.1.1       *             2 ---- 03:43   Y 00:00:48
vlan20          192.129.20.3   225.1.1.2       *             2 ---- 03:43   Y 00:00:48
vlan20          192.129.20.3   225.1.1.3       *             2 ---- 03:43   Y 00:00:48
vlan20          192.129.20.3   225.1.1.4       *             2 ---- 03:43   Y 00:00:48
vlan20          192.129.20.3   225.1.1.5       *             2 ---- 03:43   Y 00:00:48
```

【注意事项】

无。

### 45.2.14 show igmp static-group

【功能描述】

**show igmp static-group** 命令用于显示 igmp 静态组播组的信息。

【命令格式】

**show igmp static-group**

【视图】

任意视图

【缺省情况】

无。

【参数说明】

无

【使用举例】

#显示 igmp 静态组的信息

```
NOS(if-vlan30)# show igmp static-group
Interface       Address        Source         Group            Socket Uptime
```

```
vlan30          192.129.30.3    *             225.2.2.2          20 00:00:12
```

【注意事项】

无。

### 45.2.15 show igmp statistics

【功能描述】

**show igmp statistics** 命令用于显示 igmp 报文的统计信息。

【命令格式】

**show igmp statistics** [**interface** *IFNAME*]

【视图】

任意视图

【缺省情况】

无。

【参数说明】

*IFNAME*：接口名称，指定接口名称只显示指定的接口的 igmp 报文统计信息。

【使用举例】

#显示 igmp 报文统计信息信息

```
NOS#  show igmp statistics
```

【注意事项】

无。

## 45.3 配置举例

详情见 igmp snooping 模块配置举例。

## 45.4 常见问题

无。

# 46 MLD

## 46.1 功能简介

待补充。

## 46.2 命令手册

待补充。

## 46.3 配置举例

详情见 pim 模块配置举例。

## 46.4 常见问题

无。

# 47 登录管理

## 47.1 功能介绍

待补充。

## 47.2 命令手册

### 47.2.1 config console

【功能描述】

**config console** 命令用来创建并进入 console 视图。

【命令格式】

config console

【视图】

根视图

【缺省情况】

不存在 console 视图。

【参数说明】

不涉及。

【使用举例】

#创建并进入 console 视图。

```
NOS# config console
NOS(console)#
```

【注意事项】

无。

### 47.2.2 authentication enable

【功能描述】

authentication enable 命令用来打开串口登录认证。

no authentication enable 命令用来关闭串口登录认证。

【命令格式】

authentication enable [{admin-only|maintain-pwd-enable}]

no authentication enable [{admin-only|maintain-pwd-enable}]

【视图】

console 视图

【缺省情况】

串口登录认证未开启。

【参数说明】

- **admin-only**：表示仅限超管账户登录，默认无此限制。

- **maintain-pwd-enable**：表示开启维护密码，默认不开启。

【使用举例】

#打开串口登录认证。

```
NOS# config console
NOS(console)# authentication enable
```

【注意事项】

无。

### 47.2.3 config ssh server

【功能描述】

**config ssh server** 命令用来打开 SSH Server 服务。

**no config ssh server** 命令用来关闭 SSH Server 服务。

【命令格式】

config ssh server

no config ssh server

【视图】

根视图

【缺省情况】

SSH 服务处于开启状态。

【参数说明】

无。

【使用举例】

#开启 SSH server 服务。

```
NOS# config ssh server
```

【注意事项】

无。

### 47.2.4 ssh port

【功能描述】

**port** 命令用来配置 SSH 服务端口号。

**no port** 命令用来恢复缺省情况。

【命令格式】

**port** *PORT*

no port

【视图】

ssh-server 视图

【缺省情况】

端口号为 22。

【参数说明】

*PORT*：SSH 服务器端口号，取值范围(*1-65535*)，缺省为 22。

【使用举例】

```
NOS# config ssh server
NOS(ssh)# port  666
Change port will cause connection lost, continue? [Y/N] n
NOS(ssh)#
```

【注意事项】

修改前请确保端口号没有被其他业务使用。

### 47.2.5 re-generate key

【功能描述】

re-generate key 命令用来重新生成 SSH 密钥。

【命令格式】

re-generate key

【视图】

ssh-server 视图

【缺省情况】

不涉及。

【参数说明】

无。

【使用举例】

```
NOS# config ssh server
NOS(ssh)# re-generate key
```

【注意事项】

无。

### 47.2.6 config telnet server

【功能描述】

**config telnet server** 命令用来打开 telnet Server 服务。

**no config telnet server** 命令用来关闭 telnet Server 服务。

【命令格式】

config telnet server

no config telnet server

【视图】

根视图

【缺省情况】

telnet 服务处于关闭状态。

【参数说明】

无。

【使用举例】

#开启 telnet server 服务。

```
NOS# config telnet server
```

【注意事项】

无。

### 47.2.7 telnet port

【功能描述】

**port** 命令用来配置 telnet 服务端口号。

**no port** 命令用来恢复缺省情况。

【命令格式】

**port** *PORT*

no port

【视图】

telnet-server 视图

【缺省情况】

端口号为 23。

【参数说明】

*PORT*：telnet 服务器端口号，取值范围(*1-65535*)，缺省为 23。

【使用举例】

```
NOS# config telnet server
NOS(telnet)# port  666
Change port may cause connection lost, continue? [Y/N] n
NOS(telnet)#
```

【注意事项】

修改前请确保端口号没有被其他业务使用。

### 47.2.8 idle-timeout

【功能描述】

**idle-timeout** 命令用来设置闲置超时时间。

**no idle-timeout** 命令用来取消设置闲置超时时间。

【命令格式】

idle-timeout *TIME*

no idle-timeout

【视图】

telnet-server 视图

ssh-server 视图

console 视图

【缺省情况】

默认闲置 5 分钟后断开连接。

【参数说明】

*TIME*：连接闲置超时范围为(0-21600)，单位为分钟。

【使用举例】

```
NOS# config ssh server
NOS(ssh)# idle-timeout 0
NOS(ssh)# dis th
  idle-timeout 0
NOS(ssh)#
```

【注意事项】

无。

### 47.2.9 ssh client

【功能描述】

**ssh** 命令用来 ssh 登录到远端设备。

【命令格式】

**ssh** SERVER [PORT]

【视图】

根视图

【缺省情况】

不涉及。

【参数说明】

*SERVER*：要登录的 IP 地址或主机名。

*PORT*：指定登录 ssh 服务器的 TCP 端口号，范围为 1-65535，缺省为 22。

使用举例】

```
NOS# ssh 192.168.1.1
User name: admin
admin@192.168.1.1's password:
```

【注意事项】

无。

### 47.2.10 telnet client

【功能描述】

**telnet** 命令用来 telnet 登录到远端设备。

【命令格式】

**telnet** <*A.B.C.D* | **ipv6** *X:X::X:X*> [*PORT*]

【视图】

根视图

【缺省情况】

不涉及。

【参数说明】

*A.B.C.D*：要登录的目的 IPv4 地址或主机名。

*X:X::X:X*：要登录的目的 IPv6 地址或主机名。

*PORT*：指定登录 telnet 服务器的 TCP 端口号，范围为 1-65535，缺省为 23。

【使用举例】

```
NOS# telnet 192.168.1.1
Connected to 192.168.51.12

NOS login:: admin
Password:
```

【注意事项】

无。

### 47.2.11 show users

【功能描述】

**show users** 命令用来查看登录设备的用户信息。

【命令格式】

show users

【视图】

所有视图

【缺省情况】

不涉及。

【参数说明】

无。

【使用举例】

```
NOS# show users
*:current user
 ID     LINE     Login-Time      Type     Network Address
 ------------------------------------------------------------------
 0      CON      -----           CONSOLE
*10     VTY 0    0 days 0 :13:49  SSH      192.168.1.1:45216
NOS#
```

表47-1 参数说明

| 字段 | 描述 |
| --- | --- |
| * | 表示当前用户 |
| ID | 用户接口的绝对编号 |
| LINE | 用户接口的类型和相对编号 |
| Login-Time | 用户在线时间 |
| Type | 连接类型：Telnet、SSH和CONSOLE（串口） |
| Network Address | 用户IP地址和端口号 |

【注意事项】

无。

### 47.2.12 free user

【功能描述】

**free users** 命令用来断开指定的用户连接并删除该登录用户信息。

【命令格式】

**free user** <*ID* | <*A.B.C.D* | *X:X::X:X*> [**port** *PORT*]>

【视图】

根视图

【缺省情况】

不涉及。

【参数说明】

- *ID*: 每个用户独特的编号,取值范围(0-63)，其中 0 代表串口用户。
- *PORT*：指定的用户连接的端口号,取值范围(1-65535)。
- *A.B.C.D*：指定的用户连接的 IPv4 地址。
- *X:X::X:X*：指定的用户连接的 IPv6 地址。

【使用举例】

```
NOS# free user 192.168.0.99 port 61892
```

【注意事项】

无。

### 47.2.13 show ssh2 algorithm

【功能描述】

show ssh2 algorithm 命令用来查看 ssh 支持的加密算法。

【命令格式】

show ssh2 algorithm

【视图】

所有视图

【缺省情况】

不涉及。

【参数说明】

无。

【使用举例】

```
NOS# show ssh2 algorithm
-----------------------------------------------------------------
Key exchange algorithms:
   curve25519-sha256
   curve25519-sha256@libssh.org
   diffie-hellman-group14-sha256
   kexguess2@matt.ucc.asn.au
-----------------------------------------------------------------
Public key algorithms:
```

```
    ssh-ed25519
    rsa-sha2-256
-----------------------------------------------------------------
Encryption algorithms:
    chacha20-poly1305@openssh.com
    aes128-ctr
    aes256-ctr
-----------------------------------------------------------------
MAC algorithms:
    hmac-sha2-256
-----------------------------------------------------------------
```

【注意事项】

无。

### 47.2.14 show ssl algorithm

【功能描述】

show ssl algorithm 命令用来查看 tls 支持的加密算法。

【命令格式】

show ssl algorithm

【视图】

所有视图

【缺省情况】

不涉及。

【参数说明】

无。

【使用举例】

```
NOS# show ssl algorithm
TLSv1.2 ciphers:
    TLS_ECDHE_ECDSA_CHACHA20_POLY1305_SHA256
    TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
    TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
-----------------------------------------------------------------
Public key algorithms:
    ECDHE
-----------------------------------------------------------------
Encryption algorithms:
    chacha20-poly1305
    aes128
    aes256
-----------------------------------------------------------------
MAC algorithms:
    hmac-sha2-256
    hmac-sha2-384
-----------------------------------------------------------------
```

```
Certificate:
   /etc/uhttpd.crt
-----------------------------------------------------------------------
Key:
   /etc/uhttpd.key
-----------------------------------------------------------------------。\
```

【注意事项】

无。

## 47.3 配置举例

配置设备作为 SSH 服务器，端口号为 123，闲置超时时间为 1 分钟

```
NOS# config ssh server
NOS(ssh)# port 123
Change port will cause connection lost, continue? [Y/N] y
NOS(ssh)# idle-timeout 1
NOS(ssh)# dis th
  port 123
  idle-timeout 1
```

## 47.4 常见问题

无。

# 48 本地用户

## 48.1 功能简介

当选择使用本地认证方法对用户进行认证时，应在设备上创建本地用户并配置相关属性。
所谓本地用户，是指在本地设备上设置的一组用户属性的集合。该集合以用户名为用户的唯一标识。

## 48.2 命令手册

### 48.2.1 config local-user

【功能描述】

**config local-user** 命令用于创建本地用户，并进入本地用户视图。
no config local-user 命令用于删除指定的本地用户。

【命令格式】

[no] config local-user *USRNAME*

【视图】

根视图

【缺省情况】

存在缺省用户，一般为 admin。

【参数说明】

*USRNAME*：本地用户名称，只能包含大小写字母和数字，且长度不能超过 32 个字符。

【使用举例】

```
NOS# config local-user aaa
NOS(local-user-aaa)#
```

【注意事项】

- 一些特殊用户名不允许被配置，包括 daemon、ftp、network、ntp、dnsmasq、lldp、logd、ubus 和 root。
- 缺省用户不能被删除，无定制情况下为 admin 用户。
- 本地用户数量最大可以配置 256 个。

### 48.2.2 password

【功能描述】

**password** 命令用于配置本地用户的密码。
**no password** 命令用于删除本地用户的密码。

【命令格式】

password [cipher] *PASSWORD*
no password

【视图】

本地用户视图

【缺省情况】

不存在本地用户密码。

【参数说明】

- **cipher**：以密文方式设置用户密码。
- *PASSWORD*：本地用户的明文或密文密码，明文密码最大不能超过 31 个字符，密文密码最大不能超过 127 个字符。

【使用举例】

```
NOS# config local-user aaa
NOS(local-user-aaa)# password 123
NOS(local-user-aaa)# dis this
  password cipher $$/)2^UdXaS~FqNTHCl
NOS(local-user-aaa)#
```

【注意事项】

无。

### 48.2.3 user-level

【功能描述】

**user-level** 命令用于配置本地用户的权限。

**no user-level** 命令用于删除本地用户的权限配置。

【命令格式】

user-level <manage|network|guest>

no user-level

【视图】

本地用户视图

【缺省情况】

本地用户权限为 guest。

【参数说明】

- **manage**：管理用户权限，最高。
- **network**：网络用户权限。
- **guest**：来宾用户权限，最低。

【使用举例】

```
NOS# config local-user aaa
NOS(local-user-aaa)# user-level manage
NOS(local-user-aaa)# dis this
  user-level manage
NOS(local-user-aaa)#
```

【注意事项】

root 用户的权限等级不能被修改。

### 48.2.4 password-compare

【功能描述】

**password-compare** 命令用于比较明文密文密码是否一致。

【命令格式】

password-compare cipher *PASSWORD1* <cipher|plaintext> *PASSWORD2*

【视图】

根视图

【缺省情况】

不涉及。

【参数说明】

- *PASSWORD1*：需要比较的密文密码之一。
- *PASSWORD2*：另一个需要比较的密文或明文密码。

【使用举例】

```
NOS# password-compare cipher $$/+;i/lMjNuHl6/v<7~&[Ix]H=OoFvbcbxnLXziPP_ plaintext 123
Result : Match
NOS #
```

【注意事项】

无。

### 48.2.5 config password-control

【功能描述】

**config password-control** 命令用于进入 password-control 视图。

【命令格式】

config password-control

【视图】

根视图

【缺省情况】

不存在 password-control 视图。

【参数说明】

无。

【使用举例】

```
NOS# config password-control
NOS(password-control)#
```

【注意事项】

无。

### 48.2.6 policy-enable

【功能描述】

policy-enable 命令用于使能密码检查策略。

no policy-enable 命令用于取消使能密码检查策略。

【命令格式】

[no] policy-enable {composition|history|length}

【视图】

password-control 视图

【缺省情况】

默认未开启密码检查。

【参数说明】

- composition：复杂度检查。
- history：历史密码检查。
- length：密码长度检查。

【使用举例】

```
NOS# config password-control
NOS(password-control)# policy-enable composition history length
```

【注意事项】

无。

### 48.2.7 sudo

【功能描述】

**sudo** 命令用于提升到管理员权限。

【命令格式】

sudo

【视图】

根视图

【缺省情况】

不涉及。

【参数说明】

无。

【使用举例】

```
NOS# sudo
NOS# Enter Password:
NOS# Enter super user mode.
```

【注意事项】

使用 **sudo** 提权之前，必须使用 **sudo password** 配置提权密码。

### 48.2.8 sudo password

【功能描述】

**sudo password** 命令用于配置 sudo 提权使用的密码。

【命令格式】

sudo password

【视图】

根视图

【缺省情况】

缺省不存在 sudo 提权密码。

【参数说明】

无。

【使用举例】

```
NOS# sudo password
NOS# New Password:
NOS# Retype password:
```

【注意事项】

如果存在旧密码，需要先输入旧密码进行检查。

### 48.2.9 no sudo password

【功能描述】

**no sudo password** 命令用于删除配置的 sudo 提权密码。

【命令格式】

no sudo password

【视图】

根视图

【缺省情况】

缺省不存在 sudo 提权密码。

【参数说明】

无。

【使用举例】

```
NOS# no sudo password
NOS# Current Password:
```

【注意事项】

删除了配置的 sudo password 之后，无进行 **sudo** 提权操作。

## 48.3 配置举例

配置创建一个本地用户 test，明文密码为 test，用户级别为管理员权限

```
NOS# config local-user test
NOS(local-user-test)# password test
NOS(local-user-test)# user-level manage
NOS(local-user-test)# dis th
  user-level manage
  password cipher $$,*]0dyXLhw}Lzk_/p~pY@=i-HsVgN`~m~H
```

## 48.4 常见问题

无。

# 49 ISP 域管理

## 49.1 功能简介

通过在 ISP 域视图下引用预先配置的认证、授权、计费方案来实现对用户的认证、授权和计费。每个 ISP 域中都有缺省的认证、授权、计费方法，如果用户所属的 ISP 域下未应用任何认证、授权、计费方法，系统将使用缺省的认证、授权、计费方法。

NOS 当前支持配置 ISP 域，域属性暂只支持配置默认的 local 方案、radius 方案和 tacacs 方案。

## 49.2 命令手册

### 49.2.1 config domain

【功能描述】

**config domain** 命令用于创建 ISP 域，并进入 ISP 域视图。如果指定的 ISP 域已经存在，则直接进入 ISP 域视图。

no config domain 命令用于删除指定的 ISP 域。

【命令格式】

[no] config domain name *DOMAIN_NAME*

【视图】

根视图

【缺省情况】

缺省情况下仅存在系统默认 ISP 域：system。

【参数说明】

*DOMAIN_NAME*：ISP 域名称，名称长度不能超过 32 个字符。

【使用举例】

```
NOS# config domain name 123
NOS(isp-123)#
```

【注意事项】

默认域 system 不能被删除。

### 49.2.2 config default domain

【功能描述】

config default domain 命令用于配置默认生效的 ISP 域。

no config default domain 命令用于取消当前配置的默认生效的 ISP 域。

【命令格式】

config default domain *DOMAIN_NAME*

no config default domain

【视图】

根视图

【缺省情况】

缺省情况下，默认生效的 ISP 域为 system。

【参数说明】

DOMAIN_NAME：指定 ISP 域名称。

【使用举例】

```
NOS# config default domain 123
NOS#
```

【注意事项】

不能指定不存在的 ISP 域。

### 49.2.3 authentication default radius-scheme

【功能描述】

authentication default radius-scheme 命令用于配置 ISP 域生效的 radius 方案。

**no authentication default** 命令用于设置 ISP 域认证方式为默认认证方式（本地认证）。

【命令格式】

authentication default radius-scheme *RADIUS_NAME* [local]

no authentication default

【视图】

ISP 域配置视图

【缺省情况】

缺省情况下，未指定任何 radius 方案。

【参数说明】

- *RADIUS_NAME*：radius 方案名称。
- **local**：指定备用认证方式为本地认证。

【使用举例】

```
NOS(isp-123)# authentication default radius-scheme 123 local
NOS(isp-123)# dis th
  authentication default radius-scheme 123 local
```

【注意事项】

不能指定不存在的 radius 方案。

### 49.2.4 authentication default tacacs-scheme

【功能描述】

authentication default tacacs-scheme 命令用于配置 ISP 域生效的 tacacs 方案。

**no authentication default** 命令用于设置 ISP 域认证方式为默认认证方式（本地认证）。

【命令格式】

authentication default tacacs-scheme *TACACS_NAME* [radius-scheme *RADIUS_NAME* | local]

no authentication default

【视图】

ISP 域配置视图

【缺省情况】

缺省情况下，未指定任何 tacacs 方案。

【参数说明】

*TACACS_NAME*：tacacs 方案名称。

*RADIUS_NAME*：radius 方案名称。

**local**：指定备用认证方式为本地认证。

【使用举例】

```
NOS(isp-123)# authentication default tacacs-scheme 123 local
```

【注意事项】

不能指定不存在的 tacacs 方案。

### 49.2.5 authentication default local

【功能描述】

authentication default local 命令用于配置 ISP 域认证方式为本地认证

**no authentication default** 命令用于设置 ISP 域认证方式为默认认证方式（本地认证）。

【命令格式】

authentication default local

no authentication default

【视图】

ISP 域配置视图

【缺省情况】

缺省情况下，默认认证方式为本地认证。

【参数说明】

无。

【使用举例】

```
NOS(isp-123)# authentication default local
NOS(isp-123)#
```

【注意事项】

authentication default local 不显示 buildrun。

## 49.3 配置举例

配置创建一个 ISP 域，域名叫 aaa，默认主认证方式是 radius 认证，使用的 radius 方案是 rad，备用认证方案是本地认证

```
NOS# config domain name aaa
NOS(isp-aaa)# authentication default radius-scheme rad local
NOS(isp-aaa)# dis th
  authentication default radius-scheme rad local
```

## 49.4 常见问题

无。

# 50 radius

## 50.1 功能简介

RADIUS 方案中定义了设备和 RADIUS 服务器之间进行信息交互所必须的一些参数。当创建一个新的 RADIUS 方案之后，需要对属于此方案的 RADIUS 服务器的 IP 地址、UDP 端口号和报文共享密钥进行设置，这些服务器包括认证/授权和计费服务器，而每种服务器又有主服务器和从服务器的区别。每个 RADIUS 方案的属性包括：主服务器的 IP 地址、从服务器的 IP 地址、共享密钥以及 RADIUS 服务器类型等。

## 50.2 命令手册

### 50.2.1 config radius scheme

【功能描述】

**config radius scheme** 命令用于创建 radius 方案，并进入 radius 方案视图。如果指定的 radius 方案已经存在，则直接进入 radius 方案视图。

no config radius scheme 命令用于删除指定的 radius 方案。

【命令格式】

[no] config radius scheme *RADIUS_NAME*

【视图】

根视图

【缺省情况】

缺省情况下不存在 radius 方案。

【参数说明】

*RADIUS_NAME*：radius 方案名称，名称长度不能超过 32 个字符。

【使用举例】

```
NOS(isp-123)# config radius scheme 123
NOS(radius-123)#
```

【注意事项】

无。

### 50.2.2 primary authentication

【功能描述】

primary authentication 命令用于配置 radius 方案的主认证服务器。

**no primary authentication** 命令用于删除 radius 方案的主认证服务器配置。

【命令格式】

primary authentication <*A.B.C.D*|ipv6-address *X:X::X:X*> [port *PORT_NUM*] [secret *SECRET*]

no primary authentication

【视图】

radius 方案视图

【缺省情况】

未配置主认证服务器。

【参数说明】

- *A.B.C.D*：radius 主认证服务器的 ipv4 地址。
- *X:X::X:X*：radius 主认证服务器的 ipv6 地址。
- *PORT_NUM*：radius 主认证服务器的 UDP 端口号，取值范围为 1~65535，缺省值为 1812。
- *SECRET*：与 radius 主认证服务器交互的认证报文的共享密钥，长度不能超过 127 个字符。

【使用举例】

```
NOS# config radius scheme 123
NOS(radius-123)# primary authentication 10.1.1.1 port 123 secret abc
```

【注意事项】

此处配置的 UDP 端口号和共享密钥必须与服务器的配置保持一致。

### 50.2.3 secondary authentication

【功能描述】

secondary authentication 命令用于配置 radius 方案的备认证服务器。

no secondary authentication 命令用于删除 radius 方案的备认证服务器配置。

【命令格式】

secondary authentication <*A.B.C.D*|ipv6-address *X:X::X:X*> [port *PORT_NUM*] [secret *SECRET*]

no secondary authentication [<*A.B.C.D*|ipv6-address *X:X::X:X*>]

【视图】

radius 方案视图

【缺省情况】

未配置备认证服务器。

【参数说明】

- *A.B.C.D*：radius 备认证服务器的 ipv4 地址。
- *X:X::X:X*：radius 备认证服务器的 ipv6 地址。
- *PORT_NUM*：radius 备认证服务器的 UDP 端口号，取值范围为 1~65535，缺省值为 1812。
- *SECRET*：与 radius 备认证服务器交互的认证报文的共享密钥，长度不能超过 127 个字符。

【使用举例】

```
NOS# config radius scheme 123
NOS(radius-123)# secondary authentication ipv6-address 2005::1:123 port 1234
```

【注意事项】

- 每个 radius 方案中最多支持配置 4 个备认证服务器。
- **no secondary authentication** 不指定地址时会删除所有的 radius 备认证服务器。

### 50.2.4 shared-secret

【功能描述】

**shared-secret** 命令用于配置 radius 报文的共享秘钥。

no shared-secret 命令用于删除 radius 报文的共享秘钥。

【命令格式】

shared-secret *SECRET*

no shared-secret

【视图】

radius 方案视图

【缺省情况】

未配置共享秘钥。

【参数说明】

*SECRET*：共享秘钥，长度不能超过 127 个字符。

【使用举例】

```
NOS# config radius scheme 123
NOS(radius-123)# shared-secret h3c@1234
NOS(radius-123)# dis th
  primary authentication 10.1.1.1
  shared-secret h3c@1234
```

【注意事项】

设备优先采用配置 radius 认证服务器时指定的报文共享密钥。

### 50.2.5 user-name-format with-domain

【功能描述】

user-name-format with-domain 命令用配置发送给服务器的用户名携带域名。

no user-name-format with-domain 命令用于取消配置发送给服务器的用户名携带域名。

【命令格式】

[no] user-name-format with-domain

【视图】

radius 方案视图

【缺省情况】

发送给 radius 服务器的用户不携带 ISP 域名。

【参数说明】

无。

【使用举例】

```
NOS(radius-123)# config radius scheme 123
NOS(radius-123)# user-name-format with-domain
NOS(radius-123)# dis th
  primary authentication 10.1.1.1
  shared-secret h3c@1234
  user-name-format with-domain
```

【注意事项】

有些较早期的 radius 服务器不能接受携带有 ISP 域名的用户名。

### 50.2.6 nas-ip

【功能描述】

**nas-ip** 命令用配置设备发送 RADIUS 报文使用的 NAS-IP-Address 属性。

**no nas-ip** 命令用于删除配置的 NAS-IP-Address 属性。

【命令格式】

**nas-ip** *A.B.C.D*

**no nas-ip**

【视图】

RADIUS 方案视图

【缺省情况】

发送给 RADIUS 服务器的报文中不携带 NAS-IP-Address 属性。

【参数说明】

*A.B.C.D*: 指定的 NAS-IP-Address 属性值，IPv4 地址，禁止配置全 0 地址、全 1 地址、D 类地址、E 类地址和环回地址。

【使用举例】

```
NOS# config radius scheme 123
NOS(radius-123)# nas-ip 1.1.1.1
NOS(radius-123)# dis th
  nas-ip 1.1.1.1
```

【注意事项】

仅涉及 RADIUS 属性字段，不影响报文源 IP，目前仅支持 dot1x/mac 认证。

## 50.3 配置举例

配置创建一个 radius 方案为 rad，主认证服务器地址是 1.1.1.1，端口号是 123，认证密钥是 abc，备认证服务器地址是 2.2.2.2，端口号是 234，认证密钥是 bcd，全局的共享密钥是 key，发送给服务器的用户名携带域名

```
NOS# config radius scheme rad
NOS(radius-rad)# primary authentication 1.1.1.1 port 123 secret abc
NOS(radius-rad)# secondary authentication 2.2.2.2 port 234 secret bcd
NOS(radius-rad)# shared-secret key
NOS(radius-rad)# user-name-format with-domain
NOS(radius-rad)# dis th
  primary authentication 1.1.1.1 port 123 secret abc
  secondary authentication 2.2.2.2 port 234 secret bcd
  shared-secret key
  user-name-format with-domain
```

## 50.4 常见问题

无。

# 51 tacacs

## 51.1 TACACS+简介

TACACS+（Terminal Access Controller Access-Control System，终端访问控制器控制系统） 协议是思科公司（Cisco）基于 TACACS 协议进行了扩展增强的全新安全协议，不兼容之前的 TACACS 协议。

TACACS+协议的主要用于 PPP 和 VPDN（Virtual Private Dial-up Network，虚拟私有拨号网络）接入用户及终端用户的 AAA（认证、授权和计费）。本次项目实现只针对 login 用户支持 TACACS+，如 telnet、ssh 等。

TACACS+与 RADIUS 类似，都采用了客户端/服务器、请求/响应的模式，两者的主要区别：

- 传输协议：TACACS+使用 TCP 面向连接的传输，而 RADIUS 使用 UDP 尽力传输。
- 加密方式：TACACS+对整个报文进行加密，安全性更高，而 RADIUS 仅对用户的密码部分进行加密，安全性较低。
- 灵活性：TACACS+支持将认证、授权和计费这三种功能完全分开，而 RADIUS 的认证和授权过程无法分开。

## 51.2 命令手册

### 51.2.1 config tacacs scheme

【功能描述】

**config tacacs scheme** 命令用于创建 tacacs 方案，并进入 tacacs 方案视图。如果指定的 tacacs 方案已经存在，则直接进入 tacacs 方案视图。

no config tacacs scheme 命令用于删除指定的 tacacs 方案。

【命令格式】

[no] config tacacs scheme *TACACS_NAME*

【视图】

根视图

【缺省情况】

缺省情况下不存在 tacacs 方案。

【参数说明】

*TACACS_NAME*：tacacs 方案名称，名称长度不能超过 32 个字符。

【使用举例】

```
NOS(isp-123)# config tacacs scheme 123
NOS(tacacs-123)#
```

【注意事项】

无。

### 51.2.2 tacacs primary authentication

【功能描述】

primary authentication 命令用于配置 tacacs 方案的主认证服务器。

**no primary authentication** 命令用于删除 tacacs 方案的主认证服务器配置。

【命令格式】

primary authentication <*A.B.C.D*|ipv6-address *X:X::X:X*> [port *PORT_NUM*] [secret *SECRET*]

no primary authentication

【视图】

tacacs 方案视图

【缺省情况】

未配置主认证服务器。

【参数说明】

- *A.B.C.D*：tacacs 主认证服务器的 ipv4 地址。
- *X:X::X:X*：tacacs 主认证服务器的 ipv6 地址。
- *PORT_NUM*：tacacs 主认证服务器的 TCP 端口号，取值范围为 1~65535，缺省值为 49。
- *SECRET*：与 tacacs 主认证服务器交互的认证报文的共享密钥，只能包含大小写字母，数字和下划线，且长度不能超过 64 个字符。

【使用举例】

```
NOS# config tacacs scheme 123
NOS(tacacs-123)# primary authentication 10.1.1.1
NOS(tacacs-123)# dis th
  primary authentication 10.1.1.1
```

【注意事项】

此处配置的 TCP 端口号和共享密钥必须与服务器的配置保持一致。

### 51.2.3 tacacs secondary authentication

【功能描述】

secondary authentication 命令用于配置 tacacs 方案的备认证服务器。

no secondary authentication 命令用于删除 tacacs 方案的备认证服务器配置。

【命令格式】

secondary authentication <*A.B.C.D*|ipv6-address *X:X::X:X*> [port *PORT_NUM*] [secret *SECRET*]

no secondary authentication [<*A.B.C.D*|ipv6-address *X:X::X:X*>]

【视图】

tacacs 方案视图

【缺省情况】

未配置备认证服务器。

【参数说明】

- *A.B.C.D*：tacacs 备认证服务器的 ipv4 地址。
- *X:X::X:X*：tacacs 备认证服务器的 ipv6 地址。
- *PORT_NUM*：tacacs 备认证服务器的 UDP 端口号，取值范围为 1~65535，缺省值为 1812。
- *SECRET*：与 tacacs 备认证服务器交互的认证报文的共享密钥，只能包含大小写字母，数字和下划线，且长度不能超过 64 个字符。

【使用举例】

```
NOS# config tacacs scheme 123
```

```
NOS(tacacs-123)# secondary authentication ipv6-address 2005::1:123 port 1234
```

【注意事项】

- 每个 radius 方案中最多支持配置 4 个备认证服务器。
- **no secondary authentication** 不指定地址时会删除所有的 tacacs 备认证服务器。

### 51.2.4 tacacs shared-secret

【功能描述】

**shared-secret** 命令用于配置 tacacs 报文的共享秘钥。

**no shared-secret** 命令用于删除 tacacs 方案的共享秘钥。

【命令格式】

shared-secret *SECRET*

no shared-secret

【视图】

tacacs 方案视图

【缺省情况】

未配置共享秘钥。

【参数说明】

*SECRET*：共享秘钥，只能包含大小写字母，数字和下划线，且长度不能超过 64 个字符。

【使用举例】

```
NOS# config tacacs scheme 123
NOS(tacacs-123)# shared-secret Haha_1234
```

【注意事项】

设备优先采用配置 tacacs 认证服务器时指定的报文共享密钥。

### 51.2.5 tacacs user-name-format with-domain

【功能描述】

user-name-format with-domain 命令用于配置发送给服务器的用户名携带域名。

no user-name-format with-domain 命令用于取消配置发送给服务器的用户名携带域名。

【命令格式】

[no] user-name-format with-domain

【视图】

tacacs 方案视图

【缺省情况】

发送给 tacacs 服务器的用户不携带 ISP 域名。

【参数说明】

无

【使用举例】

```
NOS(tacacs-123)# config tacacs scheme 123
NOS(tacacs-123)# user-name-format with-domain
```

【注意事项】

有些 tacacs 服务器不能接受携带有 ISP 域名的用户名。

## 51.3 配置举例

配置创建一个 tacacs 方案为 tac，主认证服务器地址是 1.1.1.1，端口号是 123，认证密钥是 abc，备认证服务器地址是 2.2.2.2，端口号是 234，认证密钥是 bcd，全局的共享密钥是 key，发送给服务器的用户名携带域名

```
NOS# config tacacs scheme tac
NOS(tacacs-tac)# primary authentication 1.1.1.1 port 123 secret abc
NOS(tacacs-tac)# secondary authentication 2.2.2.2 port 234 secret bcd
NOS(tacacs-tac)# shared-secret key
NOS(tacacs-tac)# user-name-format with-domain
NOS(tacacs-tac)# dis th
  primary authentication 1.1.1.1 port 123 secret abc
  secondary authentication 2.2.2.2 port 234 secret bcd
  shared-secret key
  user-name-format with-domain
```

## 51.4 常见问题

无。

# 52 802.1x

## 52.1 802.1x简介

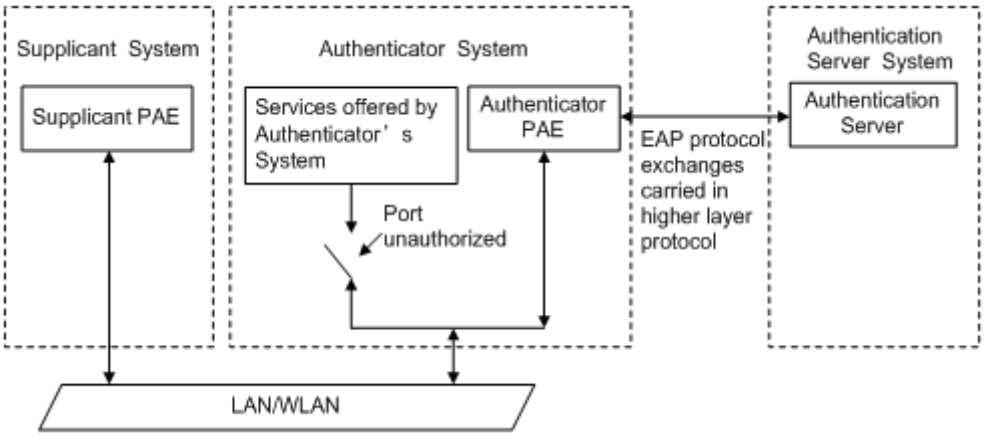
IEEE802 LAN/WAN 委员会为解决无线局域网网络安全问题，提出了 802.1x 协议。后来，802.1x 协议作为局域网端口的一个普通接入控制机制应用于以太网中，主要解决以太网内认证和安全方面的问题。

802.1x 协议是一种基于端口的网络接入控制（Port Based Network Access Control）协议。“基于端口的网络接入控制”是指在局域网接入设备的端口这一级对所接入的设备进行认证和控制。连接在端口上的用户设备如果能通过认证，就可以访问局域网中的资源；如果不能通过认证，则无法访问局域网中的资源。

### 52.1.1 802.1x的体系结构

使用 802.1x 的系统为典型的 Client/Server 体系结构，包括三个实体，如图 1-1 所示分别为：Supplicant System（客户端）、Authenticator System（设备端）以及 Authentication Server System（认证服务器）。

图52-1 802.1x 认证系统的体系结构




- 客户端是位于局域网段一端的一个实体，由该链路另一端的设备端对其进行认证。客户端一般为用户终端设备，用户通过启动客户端软件发起 802.1x 认证。客户端软件必须支持 EAPOL（Extensible Authentication Protocol over LAN，局域网上的可扩展认证协议）协议。
- 设备端是位于局域网段一端的另一个实体，用于对所连接的客户端进行认证。设备端通常为支持 802.1x 协议的网络设备（如 H3C 系列交换机），它为客户端提供接入局域网的端口，该端口可以是物理端口，也可以是逻辑端口。
- 认证服务器是为设备端提供认证服务的实体。认证服务器用于实现用户的认证、授权和计费，通常为 RADIUS 服务器。该服务器可以存储用户的相关信息，例如用户的账号、密码以及用户所属的 VLAN、优先级、用户的访问控制列表等。

三个实体涉及如下四个基本概念：PAE、受控端口、受控方向和端口受控方式。

2. PAE

PAE（Port Access Entity，端口访问实体）是认证机制中负责执行算法和协议操作的实体。

- 设备端 PAE 利用认证服务器对需要接入局域网的客户端执行认证，并根据认证结果相应地对受控端口的授权/非授权状态进行相应地控制。

- 客户端 PAE 负责响应设备端的认证请求，向设备端提交用户的认证信息。客户端 PAE 也可以主动向设备端发送认证请求和下线请求。

#### 3. 受控端口

设备端为客户端提供接入局域网的端口，这个端口被划分为两个虚端口：受控端口和非受控端口。

- 非受控端口始终处于双向连通状态，主要用来传递 EAPOL 协议帧，保证客户端始终能够发出或接受认证。
- 受控端口在授权状态下处于连通状态，用于传递业务报文；在非授权状态下处于断开状态，禁止传递任何报文。
- 受控端口和非受控端口是同一端口的两个部分；任何到达该端口的帧，在受控端口与非受控端口上均可见。

#### 4. 受控方向

在非授权状态下，受控端口可以被设置成单向受控。实行单向受控时，禁止从客户端接收帧，但允许向客户端发送帧。

缺省情况下，受控端口实行单向受控。

#### 5. 端口受控方式

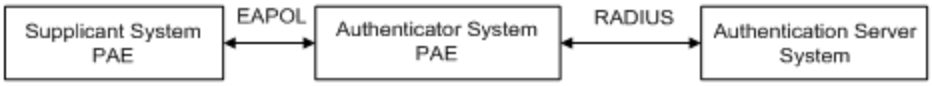
支持以下两种端口受控方式：

- 基于端口的认证： 只要该物理端口下的第一个用户认证成功后，其他接入用户无须认证就可使用网络资源，当第一个用户下线后，其他用户也会被拒绝使用网络。
- 基于 MAC 地址认证： 该物理端口下的所有接入用户都需要单独认证，当某个用户下线时，只有该用户无法使用网络，不会影响其他用户使用网络资源。

### 52.1.2 802.1x的工作机制

IEEE 802.1x 认证系统利用 EAP（Extensible Authentication Protocol，可扩展认证协议）协议，在客户端和认证服务器之间交换认证信息。

图52-2 802.1x 认证系统的工作机制



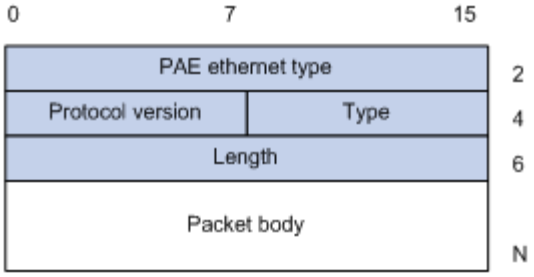

- 在客户端 PAE 与设备端 PAE 之间,EAP 协议报文使用 EAPOL 封装格式,直接承载于 LAN 环境中。
- 在设备端 PAE 与 RADIUS 服务器之间，EAP 协议报文可以使用 EAPOR（EAP over RADIUS）封装格式，承载于 RADIUS 协议中；也可以由设备端 PAE 进行终结，而在设备端 PAE 与 RADIUS 服务器之间传送 PAP 协议报文或 CHAP 协议报文。
- 当用户通过认证后，认证服务器会把用户的相关信息传递给设备端，设备端 PAE 根据 RADIUS 服务器的指示（Accept 或 Reject）决定受控端口的授权/非授权状态。

### 52.1.3 EAPOL消息的封装

#### 1. EAPOL 数据包的格式

EAPOL 是 802.1x 协议定义的一种报文封装格式,主要用于在客户端和设备端之间传送 EAP 协议报文,以允许 EAP 协议报文在 LAN 上传送。格式如图 52-3 所示。

图52-3 EAPOL 数据包格式




PAE Ethernet Type：表示协议类型，802.1x 分配的协议类型为 0x888E。

Protocol Version：表示 EAPOL 帧的发送方所支持的协议版本号。

Type：

- EAP-Packet（值为 00），认证信息帧，用于承载认证信息；
- EAPOL-Start（值为 01），认证发起帧；
- EAPOL-Logoff（值为 02），退出请求帧；
- EAPOL-Key（值为 03），密钥信息帧；
- EAPOL-Encapsulated-ASF-Alert（值为 04），用于支持 ASF（Alerting Standards Forum）的 Alerting 消息。

Length：表示数据长度，也就是“Packet Body”字段的长度。如果为 0，则表示没有后面的数据域。

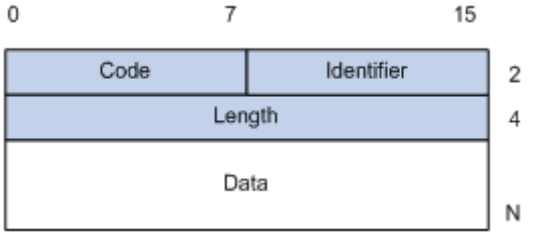
Packet Body：根据不同的 Type 有不同的格式。

其中，EAPOL-Start，EAPOL-Logoff 和 EAPOL-Key 仅在客户端和设备端之间存在；在设备端和认证服务器之间，EAP-Packet 报文重新封装承载于 RADIUS 协议上，以便穿越复杂的网络到达认证服务器；EAPOL-Encapsulated-ASF-Alert 封装与网管相关的信息，例如各种警告信息，由设备端终结。

### 2. EAP 数据包的格式

当 EAPOL 数据包的 Type 域为 EAP-Packet 时，Packet Body 为 EAP 数据包内容，如图 52-4 所示。

图52-4 EAP 数据包格式




Code：指明 EAP 包的类型，一共有 4 种：Request，Response，Success，Failure。

Identifier：辅助进行 Response 和 Request 消息的匹配。

Length：EAP 包的长度，包含 Code、Identifier、Length 和 Data 的全部内容。

Data：EAP 数据信息，内容格式由 Code 决定。

Success 和 Failure 类型的包没有 Data 域，相应的 Length 域的值为 4。

Request 和 Response 类型的 Data 域的格式如图 52-5 所示。

图52-5 Request 和 Response 类型的 Data 域的格式

Type：指出 EAP 的认证类型。其中，值为 1 时，代表 Identity，用来查询对方的身份；值为 4 时，代表 MD5-Challenge，类似于 PPP CHAP 协议，包含质询消息。

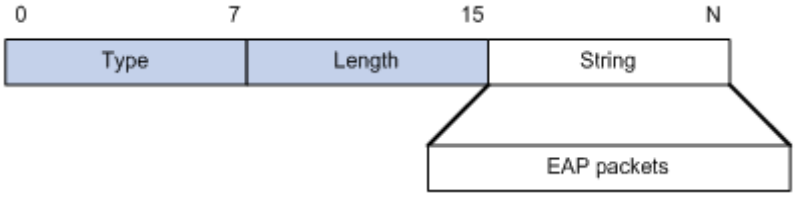
Type Data：Type Data 域的内容随不同类型的 Request 和 Response 而不同。

#### 3. EAP 属性的封装

RADIUS 为支持 EAP 认证增加了两个属性：EAP-Message（EAP 消息）和 Message-Authenticator（消息认证码）。RADIUS 协议的报文格式请参见“AAA 操作手册”中的 RADIUS 协议简介部分。

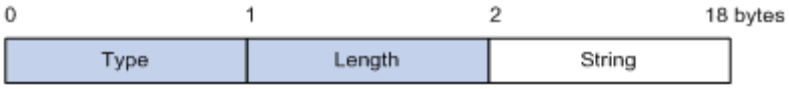
EAP-Message 属性用来封装 EAP 数据包，如图 52-6 所示，类型代码为 79，string 域最长为 253 字节，如果 EAP 数据包长度大于 253 字节，可以对其进行分片，依次封装在多个 EAP-Message 属性中。

图52-6 EAP-Message 属性封装




Message-Authenticator 可以用于在使用 CHAP、EAP 等认证方法的过程中，避免接入请求包被窃听。在含有 EAP-Message 属性的数据包中，必须同时包含 Message-Authenticator，否则该数据包会被认为无效而被丢弃。格式如图 52-7 所示。

图52-7 Message-Authenticator 属性




### 52.1.4 802.1x的认证过程

H3C S3100 系列交换机支持 EAP 终结方式和 EAP 中继方式进行认证。

#### 1. EAP 中继方式

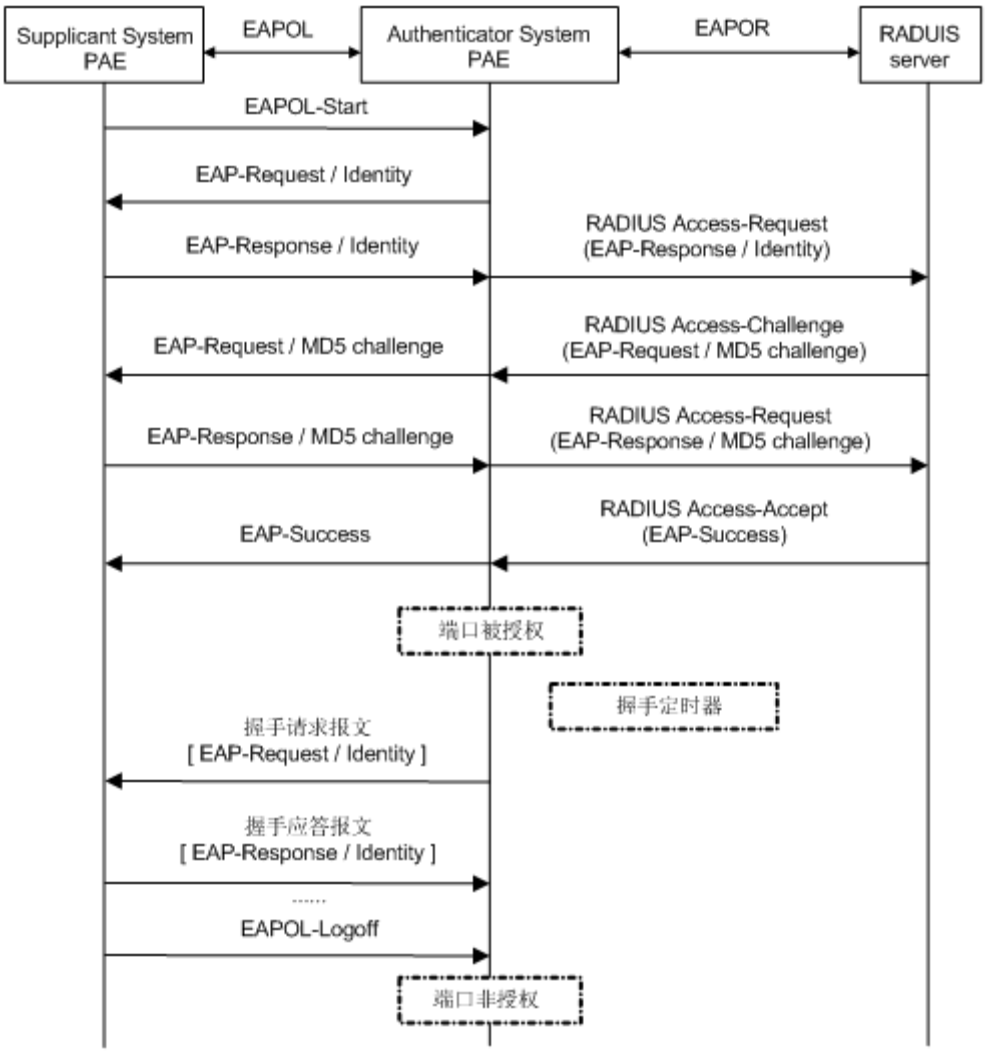
这种方式是 IEEE 802.1x 标准规定的，将 EAP 协议承载在其他高层协议中，如 EAP over RADIUS，以便扩展认证协议报文穿越复杂的网络到达认证服务器。一般来说，EAP 中继方式需要 RADIUS 服务器支持 EAP 属性：EAP-Message（值为 79）和 Message-Authenticator（值为 80）。

EAP 中继方式有四种认证方法：EAP-MD5、EAP-TLS（Transport Layer Security，传输层安全）、EAP-TTLS（Tunneled Transport Layer Security，隧道传输层安全）和 PEAP（Protected Extensible Authentication Protocol，受保护的扩展认证协议）：

- EAP-MD5：验证客户端的身份，RADIUS 服务器发送 MD5 加密字（EAP-Request/MD5 Challenge 报文）给客户端，客户端用该加密字对口令部分进行加密处理。
- EAP-TLS：客户端和 RADIUS 服务器端通过 EAP-TLS 认证方法检查彼此的安全证书，验证对方身份，保证通信目的端的正确性，防止网络数据被窃听。
- EAP-TTLS：是对 EAP-TLS 的一种扩展。在 EAP TLS 中，实现对客户端和认证服务器的双向认证。EAP-TTLS 扩展了这种实现，它使用 TLS 建立起来的安全隧道传递信息。
- PEAP：首先创建和使用 TLS 安全通道来进行完整性保护，然后进行新的 EAP 协商，从而完成对客户端的身份验证。

以下以 EAP-MD5 方式为例介绍基本业务流程，如图 52-8 所示。

图52-8 IEEE 802.1x 认证系统的 EAP 中继方式业务流程




认证过程如下：

- 当用户有上网需求时打开 802.1x 客户端，输入已经申请、登记过的用户名和口令，发起连接请求（EAPOL-Start 报文）。此时，客户端程序将发出请求认证的报文给交换机，开始启动一次认证过程。
- 交换机收到请求认证的数据帧后，将发出一个请求帧（EAP-Request/Identity 报文）要求用户的客户端程序发送输入的用户名。
- 客户端程序响应交换机发出的请求，将用户名信息通过数据帧（EAP-Response/Identity 报文）送给交换机。交换机将客户端送上来的数据帧经过封包处理后（RADIUS Access-Request 报文）送给 RADIUS 服务器进行处理。
- RADIUS 服务器收到交换机转发的用户名信息后，将该信息与数据库中的用户名表相比对，找到该用户名对应的口令信息，用随机生成的一个加密字对它进行加密处理，同时也将此加密字通过 RADIUS Access-Challenge 报文传送给交换机，由交换机传给客户端程序。
- 客户端程序收到由交换机传来的加密字（EAP-Request/MD5 Challenge 报文）后，用该加密字对口令部分进行加密处理（此种加密算法通常是不可逆的，生成 EAP-Response/MD5 Challenge 报文），并通过交换机传给 RADIUS 服务器。

- RADIUS 服务器将加密后的口令信息（RADIUS Access-Request 报文）和自己经过加密运算后的口令信息进行对比，如果相同，则认为该用户为合法用户，反馈认证通过的消息（RADIUS Access-Accept 报文和 EAP-Success 报文）。
- 交换机将端口状态改为授权状态，允许用户通过该端口访问网络。
- 客户端也可以发送 EAPoL-Logoff 报文给交换机，主动终止已认证状态，交换机将端口状态从授权状态改变成未授权状态。

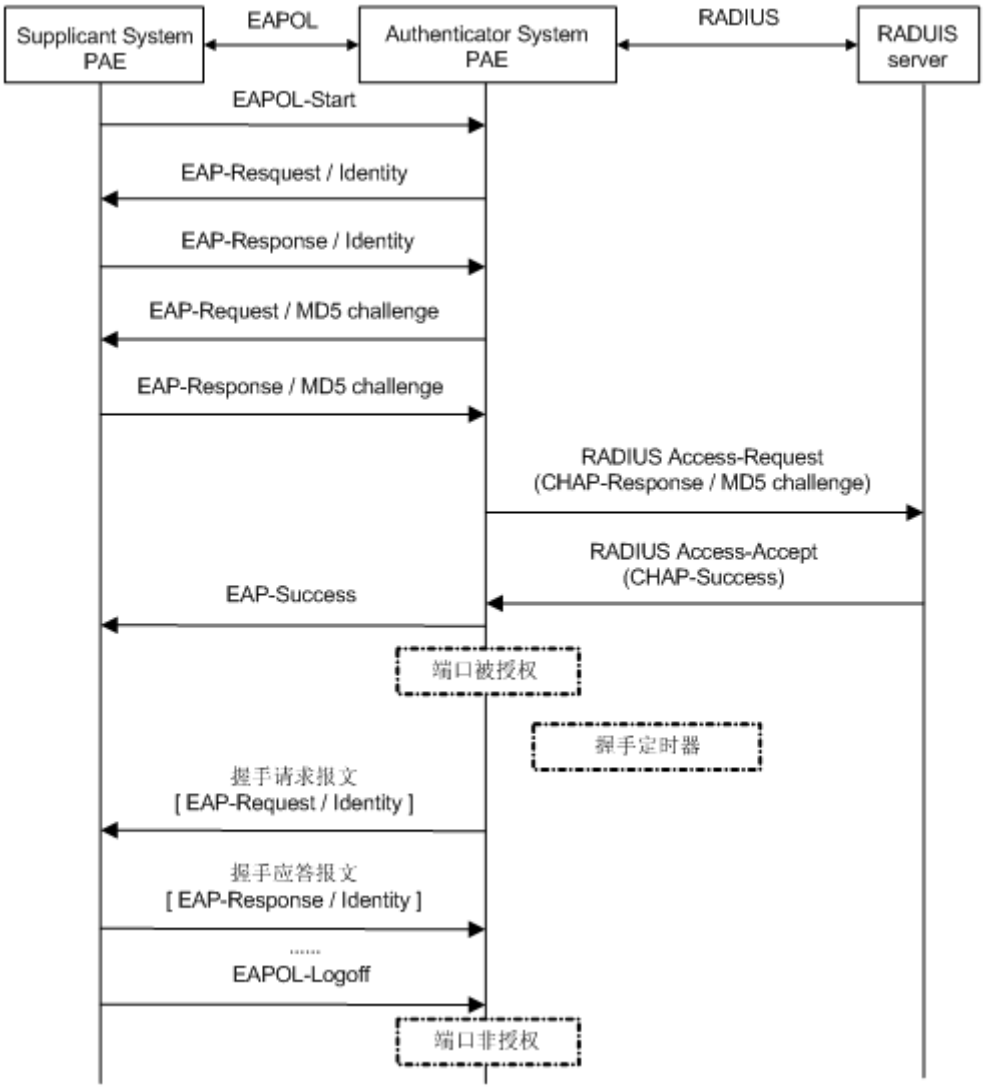
**说明**

由于 EAP 中继方式对报文的内容不做改动，如果要采用 PEAP、EAP-TLS、EAP-TTLS 或者 EAP-MD5 这四种认证方法之一，需要在客户端和 RADIUS 服务器上选择一致的认证方法，而在交换机上，只需要通过 dot1x authentication-method eap 命令启动 EAP 中继方式即可。

### 2. EAP 终结方式

这种方式将 EAP 报文在设备端终结并映射到 RADIUS 报文中，利用标准 RADIUS 协议完成认证和计费。对于 EAP 终结方式，交换机与 RADIUS 服务器之间可以采用 PAP 或者 CHAP 认证方法。以下以 CHAP 认证方法为例介绍基本业务流程，如图 52-9 所示。

图52-9 IEEE 802.1x 认证系统的 EAP 终结方式业务流程



EAP 终结方式与 EAP 中继方式的认证流程相比，不同之处在于用来对用户口令信息进行加密处理的随机加密字由交换机生成，之后交换机会把用户名、随机加密字和客户端加密后的口令信息一起送给 RADIUS 服务器，进行相关的认证处理。

### 52.1.5 802.1x支持guest vlan

802.1X Guest VLAN 功能允许用户在未认证的情况下，访问某一特定 VLAN 中的资源。这个特定的 VLAN 称之为 Guest VLAN，该 VLAN 内通常放置一些用于用户下载客户端软件或其他升级程序的服务器。

当前支持 MAC-based 方式接入：

在接入控制方式为MAC-based的端口上配置Guest VLAN后，端口上未认证的用户将被授权访问Guest VLAN 里的资源。当端口上处于 Guest VLAN 中的用户发起认证且失败时，则该用户将离开 Guest VLAN，回到加入 Guest VLAN 之前端口所在的初始 VLAN。

### 52.1.6 NOS 802.1X

NOS 当前支持 EAP 中继方式 radius 客户端，基于 MAC 的 802.1X 认证方式。

## 52.2 命令手册

### 52.2.1 config dot1x enable

【功能描述】

config dot1x enable 命令用于开启全局 802.1x。

no config dot1x enable 命令用于关闭全局 802.1x。

【命令格式】

[no] config dot1x enable

【视图】

根视图

【缺省情况】

未使能全局 802.1x。

【参数说明】

无。

【使用举例】

```
NOS# config dot1x enable
NOS#
```

【注意事项】

无。

### 52.2.2 dot1x enable

【功能描述】

**dot1x enable** 命令用于开启接口下的 802.1x。

**no dot1x enable** 命令用于关闭接口下的 802.1x。

【命令格式】

[no] dot1x enable

【视图】

二层接口视图

【缺省情况】

未使能接口下 802.1x。

【参数说明】

无。

【使用举例】

```
NOS(if-ge1)# dot1x enable
NOS(if-ge1)# dis th
 dot1x enable
```

【注意事项】

无。

### 52.2.3 dot1x mandatory-domain

【功能描述】

dot1x mandatory-domain 命令用于指定接口下的 802.1x 强制认证域。

no dot1x mandatory-domain 命令用于取消接口下的 802.1x 强制认证域。

【命令格式】

dot1x mandatory-domain *DOMAIN_NAME*

no dot1x mandatory-domain

【视图】

二层接口视图

【缺省情况】

未指定接口下的 802.1x 强制认证域。

【参数说明】

DOMAIN_NAME：ISP 域名。

【使用举例】

```
NOS(if-ge1)# dot1x mandatory-domain 123
NOS(if-ge1)# dis th
 dot1x enable
 dot1x mandatory-domain 123
```

【注意事项】

不能指定不存在的 ISP 域。

### 52.2.4 dot1x guest-vlan

【功能描述】

**dot1x guest-vlan** 命令用于指定接口下的 guest vlan。

**no dot1x guest-vlan** 命令用于取消接口下的 guest vlan。

【命令格式】

[no] dot1x guest-vlan *VLAN_ID*

【视图】

以太接口视图

【缺省情况】

未配置 dot1x 认证的 guest vlan。

【参数说明】

*VLAN_ID*：用户可以使用的 vlan id，取值范围为 1~4094。

【使用举例】

```
NOS(if-fe1)# dot1x guest-vlan 5
```

【注意事项】

需要配合 macvlan 使用。

### 52.2.5 dot1x re-authenticate

【功能描述】

**dot1x re-authenticate** 用于开启接口下对已经认证成功的用户进行重认证的功能，并配置重认证时间间隔。

no dot1x re-authenticate 用于关闭接口重认证功能。

【命令格式】

dot1x re-authenticate [timer *TIMER_VALUE*]

no dot1x re-authenticate

【视图】

二层接口视图

【缺省情况】

接口下 dot1x 重认证功能未开启。

【参数说明】

*TIMER_VALUE*：重认证时间间隔，单位为秒，取值范围为 60~3600，缺省值为 3600。

【使用举例】

```
NOS(if-ge1)# dot1x re-authenticate timer 1200
```

【注意事项】

无。

### 52.2.6 reset dot1x session

【功能描述】

**reset dot1x session** 命令用于强制当前在线的 802.1x 用户下线。

【命令格式】

reset dot1x session <all|interface *L2_IF*>

【视图】

根视图

【缺省情况】

不涉及。

【参数说明】

- **all**：所有 802.1x 会话
- *L2_IF*：二层以太网接口。

【使用举例】

```
NOS# reset dot1x session all
```

【注意事项】

无。

### 52.2.7 show dot1x connection

【功能描述】

**show dot1x connection** 命令用于显示当前 802.1x 在线用户的连接信息。

【命令格式】

show dot1x connection [interface *L2_IF* [verbose]]

【视图】

所有视图

【缺省情况】

不涉及。

【参数说明】

- *L2_IF*：二层以太网接口。
- verbose：详细信息。

【使用举例】

```
NOS(if-bagg1)# show dot1x connection
Total connections: 1   Authenticated count: 1
User Name         : scw
User MAC address   : 00:00:00:00:0a:0a
Access interface   : bagg1
Initial VLAN       : 1
Authenticated      : Yes
Reauth Enable      : No
Reauth period      : 0
Server timeout     : 30
Connected time(s)  : 20
Eap Type           : 4(MD5)
-------------------------------------
```

【注意事项】

无。

### 52.2.8 show dot1x interface

【功能描述】

show dot1x interface 命令用于显示 802.1x 接口相关信息。

【命令格式】

show dot1x interface [*L2_IF*] [json]

【视图】

所有视图

【缺省情况】

不涉及。

【参数说明】

- *L2_IF*：二层以太网接口。
- **json**：以 json 格式显示。

【使用举例】

```
NOS(if-bagg1)# show dot1x interface ge1
```

【注意事项】

无。

### 52.2.9 show dot1x radius-scheme

【功能描述】

**show dot1x radius-scheme** 命令用于显示 802.1x 的 radius 方案信息。

【命令格式】

show dot1x radius-scheme interface *L2_IF*

【视图】

所有视图

【缺省情况】

不涉及。

【参数说明】

*L2_IF*：二层以太网接口。

【使用举例】

```
NOS(if-bagg1)# show dot1x radius-scheme interface ge1
```

【注意事项】

无。

## 52.3 配置举例

配置全局使能 dot1x 认证功能，在二层接口 ge1/0/1 下使能 dot1x，配置强制认证域为 aaa，接口加入 access vlan 6

```
NOS# config dot1x enable
NOS# interface ge1/0/1
NOS(if-ge1/0/1)# dot1x enable
```

```
NOS(if-ge1/0/1)# dot1x mandatory-domain aaa
NOS(if-ge1/0/1)# vlan access 6
NOS(if-ge1/0/1)# dis th
  mac-authentication enable
  vlan access 6
  dot1x enable
  dot1x mandatory-domain aaa
```

## 52.4 常见问题

无。

# 53 MAC 认证

## 53.1 功能简介

MAC 地址认证是一种基于端口和 MAC 地址对用户的网络访问权限进行控制的认证方法，无需安装客户端软件。设备在启动了 MAC 地址认证的端口上首次检测到用户的 MAC 地址以后，启动对该用户的认证操作。认证过程中，不需要用户手动输入用户名或密码。若该用户认证成功，则允许其通过端口访问网络资源，否则该用户的 MAC 地址就被设置为静默 MAC。在静默时间内，来自此 MAC 地址的用户报文到达时，设备直接做丢弃处理，以防止非法 MAC 短时间内的重复认证。

### 53.1.1 MAC地址认证用户的账号格式

MAC 地址认证用户使用的账号格式分为以下几种：

- ①MAC 地址账号：设备使用源 MAC 地址作为用户认证时的用户名和密码。
- ②通用固定用户名:所有 MAC 地址认证用户均使用设备上指定的一个固定用户名和密码进行身份信息进行认证，由于同一个端口下可以有多个用户进行认证，因此这种情况下端口上的所有 MAC 地址认证用户均使用同一个固定用户名进行认证，服务器端仅需要配置一个用户账户即可满足所有认证用户的认证需求，适用于接入客户端比较可信的网络环境。
- ③专用固定用户名:MAC 地址认证还支持对特定 MAC 地址范围的用户单独设置用户名和密码(例如对指定 OUI 的 MAC 地址单独设置用户名和密码)，相当于对指定 MAC 地址范围的用户使用固定用户名和密码。服务器端需要根据设备配置的账号创建对应的账号。

### 53.1.2 MAC认证支持Guest vlan

MAC 地址认证 Guest vlan 功能的优先级高于 MAC 地址认证的静默 MAC 功能，即认证失败的用户可以访问指定的 guest vlan 中的资源，且该用户的 MAC 地址会被加入到两个 vlan id 中，一条原始 vlan tag 的静默 MAC，一条 guest vlan 的静态 MAC。

设备缺省开始 guest vlan 中用户的重新认证功能，并按照重新认证时间间隔对 guest vlan 中的用户定期进行重新认证。若关闭 guest vlan 中用户的重新认证功能，则加入到 guest vlan 中的用户不会重新发起认证。认证用户通过无流量下线功能进行下线。

## 53.2 命令手册

### 53.2.1 config mac-authentication

【功能描述】

**config mac-authentication** 命令用于开启全局 mac 认证并进入 mac 认证配置视图。

no config mac-authentication 命令用于关闭全局 mac 认证并退出 mac 认证视图。

【命令格式】

[no] config mac-authentication

【视图】

根视图

【缺省情况】

未使能全局 mac 认证。

【参数说明】

无。

【使用举例】

```
NOS# config mac-authentication
NOS(mac-authentication)#
```

【注意事项】

无。

### 53.2.2 domain

【功能描述】

**domain** 命令用于配置 mac 认证全局域。

**no domain** 命令用于删除 mac 认证的全局域配置。

【命令格式】

**domain** DOMAIN_NAME

no domain

【视图】

mac-authentication 视图

【缺省情况】

不存在全局域配置。

【参数说明】

DOMAIN_NAME：域名。

【使用举例】

```
NOS(mac-authentication)# domain aaa
```

【注意事项】

不能指定不存在的 domain。

### 53.2.3 fixed account

【功能描述】

**fixed-account** 命令用于配置固定用户名和密码。

**no fixed-account** 命令用于删除配置的固定用户名和密码。

【命令格式】

fixed-account user *NAME* password [cipher] *PASSWORD*

no fixed-account

【视图】

mac-authentication 视图

【缺省情况】

未配置 mac 认证固定用户名和密码。

【参数说明】

*NAME*：用于进行 mac 认证的用户名。

*PASSWORD*：用于进行 mac 认证的密码。

**cipher**：用于指定当前密码为密文。

【使用举例】

```
NOS(mac-authentication)# fixed-account user system password 123456
```

【注意事项】

无。

### 53.2.4 mac-account

【功能描述】

**mac-account** 命令用于配置指定 mac 地址范围的 mac 认证用户名和密码。

**no mac-account** 命令用于删除配置的指定 mac 地址范围的 mac 认证用户名和密码。

【命令格式】

**mac-account** *X:X:X:X:X:X* [*MASK_LEN*] **user** *NAME* **password** [**cipher**] *PASSWORD*

**no mac-account** X:X:X:X:X:X [MASK_LEN]

【视图】

mac-authentication 视图

【缺省情况】

未配置指定 mac 地址范围的 mac 认证用户名和密码。

【参数说明】

X:X:X:X:X:X：mac 地址。

*MASK_LEN*：mac 地址掩码长度，取值范围为 0~48，用于确定 mac 地址范围。

*NAME*：用于进行 mac 认证的用户名

*PASSWORD*：用于进行 mac 认证的密码

**cipher**：用户指定当前密码为密文。

【使用举例】

```
NOS(mac-authentication)# mac-account 00:09:5B:EC:EE:F2 16 user system password 123456
```

【注意事项】

可通过多次执行本命令来配置多个 MAC 地址段的用户名和密码，但不允许指定的 MAC 地址重叠。如果新配置命令的 MAC 地址范围与已有的 MAC 地址范围完全相同,则后配置的命令会覆盖已有的命令。本命令仅对单播 MAC 地址范围有效。

### 53.2.5 timer quiet

【功能描述】

**timer quiet** 命令用于设置用户认证失败以后的静默时间。

no timer quiet 命令用于恢复缺省情况。

【命令格式】

**timer quiet** TIMER_VALUE

no timer quiet

【视图】

mac-authentication 视图

【缺省情况】

静默时间为 60 秒。

【参数说明】

*TIMER_VALUE*：mac 认证失败以后的静默时间，取值范围为 10~3600，缺省值为 60，单位秒。

【使用举例】

```
NOS(mac-authentication)# timer quiet 10
```

【注意事项】

无。

### 53.2.6 timer re-authentication

【功能描述】

timer re-authentication 命令用于配置重认证定时器时长。

no timer re-authentication 命令用于恢复默认情况。

【命令格式】

timer re-authentication *TIMER_VALUE*

no timer re-authentication

【视图】

mac-authentication 视图

【缺省情况】

重认证周期为 3600 秒。

【参数说明】

*TIMER_VALUE*：mac 认证重认证周期，取值范围为 60~7200，缺省值为 3600，单位秒。

【使用举例】

```
NOS(mac-authentication)# timer re-authentication 60
```

【注意事项】

无。

### 53.2.7 offline-detect enable

【功能描述】

offline-detect enable 命令用于开启下线检测功能并设置检测间隔。

no offline-detect enable 命令用于关闭下线检测定时器。

【命令格式】

offline-detect enable [*INTERVAL*]

no offline-detect enable

【视图】

mac-authentication 视图

【缺省情况】

默认下线检测周期为 300 秒。

【参数说明】

*INTERVAL*：下线检测周期，取值范围为 60~4294967295，缺省值为 300，单位秒。

【使用举例】

```
NOS(mac-authentication)# offline-detect enable 60
```

【注意事项】

无。

### 53.2.8 mac-authentication guest-vlan re-authentication enable

【功能描述】

mac-authentication guest-vlan re-authentication enable 命令用于设置 guest vlan 认证用户的重认证时间周期。

mac-authentication guest-vlan re-authentication enable 命令用于关闭接口下的 guest vlan 认证用户的重认证功能。

【命令格式】

mac-authentication guest-vlan re-authentication enable time *TIMER_VALUE*

no mac-authentication guest-vlan re-authentication enable

【视图】

mac-authentication 视图

【缺省情况】

缺省情况下，设备对 Guest VLAN 中的用户进行重新认证的时间周期为 30 秒。

【参数说明】

*TIMER_VALUE*：可配置的重认证时间，取值范围为 1~3600，缺省值为 30，单位为秒。

【使用举例】

```
NOS(mac-authentication)# mac-authentication guest-vlan re-authentication enable time 60
```

【注意事项】

无。

### 53.2.9 mac-authentication enable

【功能描述】

mac-authentication enable 命令用于开启端口下的 mac 认证。

no mac-authentication enable 命令用于关闭端口下的 mac 认证。

【命令格式】

[no] mac-authentication enable

【视图】

二层接口视图

【缺省情况】

接口未使能端口 mac 认证。

【参数说明】

无。

【使用举例】

```
NOS(if-fe2)# mac-authentication enable
```

【注意事项】

无。

### 53.2.10 mac-authentication domain

【功能描述】

mac-authentication domain 命令用于指定端口下的 mac 认证域

no mac-authentication domain 命令用于关闭端口下的 mac 认证域

【命令格式】

mac-authentication domain *DOMAIN_NAME*

no mac-authentication domain

【视图】

二层接口视图

【缺省情况】

未配置端口下的 domain 域

【参数说明】

DOMAIN_NAME：域名

【使用举例】

```
NOS(if-fe2)# mac-authentication domain system
```

【注意事项】

- 不能指定不存在的 domain；
- 配置端口使用的认证域，如果端口有配置，以端口优先，如果端口没有配置，使用全局配置，如果全局也没有配置使用默认域。

### 53.2.11 mac-authentication guest-vlan

【功能描述】

mac-authentication guest-vlan 命令用于指定接口下的 guest vlan。

no mac-authentication guest-vlan 命令用于取消接口下的 guest vlan 配置。

【命令格式】

[no] mac-authentication guest-vlan *VLAN_ID*

【视图】

二层接口视图

【缺省情况】

未配置 guest vlan

【参数说明】

*VLAN_ID*：用户可以使用的 vlan id，取值范围为 1~4094。

【使用举例】

```
NOS(if-fe1)# mac-authentication guest-vlan 5
```

【注意事项】

需要配合 macvlan 使用。

### 53.2.12 reset mac-authentication connection

【功能描述】

reset mac-authentication connection 命令用于强制当前在线的 mac 认证用户下线。

【命令格式】

reset mac-authentication connection

【视图】

根视图

【缺省情况】

不涉及。

【参数说明】

无。

【使用举例】

```
NOS# reset mac-authentication connection
```

【注意事项】

无。

### 53.2.13 show mac-authentication user

【功能描述】

**show mac-authentication user** 命令用于显示 mac 认证的用户相关信息，包括 mac 地址、vlan、使用的认证域、接口、认证是否通过。

【命令格式】

show mac-authentication user

【视图】

所有视图

【缺省情况】

不涉及。

【参数说明】

无。

【使用举例】

```
NOS# show mac-authentication user
Totally count 0 entries.
```

【注意事项】

无。

## 53.3 配置举例

配置全局使能 mac 认证，固定用户名和密码为 test，在二层接口 ge1/0/1 下使能 mac 认证，认证域为 aaa,将接口加入 access vlan 6

```
NOS# config mac-authentication
NOS(mac-authentication)# fixed-account user test password test
NOS(mac-authentication)# quit
NOS# interface ge1/0/1
NOS(if-ge1/0/1)# mac-authentication enable
NOS(if-ge1/0/1)# mac-authentication domain  aaa
NOS(if-ge1/0/1)# vlan access 6
NOS(if-ge1/0/1)# dis th
  mac-authentication enable
  mac-authentication domain aaa
  vlan access 6
NOS(if-ge1/0/1)#
```

## 53.4 常见问题

无。

# 54 审计日志

## 54.1 功能简介

审计日志是记录系统操作和活动的日志，包括用户登录、操作行为、系统事件等信息。其主要作用是监控系统状态、发现异常行为、追溯问题源头以及评估系统的安全性。

## 54.2 命令手册

### 54.2.1 config audit log

【功能描述】

**config audit log** 命令用于创建进入 audit-log 视图，并打开日志审计功能。

**no config audit log** 命令用于删除退出 audit-log 视图，并关闭日志审计功能。

【命令格式】

[no] config audit log

【视图】

根视图

【缺省情况】

未开启日志审计功能。

【参数说明】

无。

【使用举例】

```
NOS# config audit log
NOS(audit-log)#
```

【注意事项】

无。

### 54.2.2 audithost host

【功能描述】

**audithost host** 命令用于配置审计日志发送的远程主机信息。

no audithost 用于取消配置。

【命令格式】

audithost host *HOST* [port *PORTNUM*]

no audithost

【视图】

audit-log 视图

【缺省情况】

未配置远程主机，日志缓存在本机。

【参数说明】

- *HOST*：远程主机的名称或地址。
- *PORTNUM*：远程主机的端口号，取值范围为 1~65535，默认为 514。

【使用举例】

```
NOS# config audit log
NOS(audit-log)# audithost host 192.168.1.1
```

【注意事项】

无。

### 54.2.3 log file-size

【功能描述】

**log file-size** 命令用于配置本地缓存的审计日志文件大小。

no log file-size 命令用于恢复默认文件大小配置。

【命令格式】

log file-size *QUOTA*

no log file-size

【视图】

audit-log 视图

【缺省情况】

默认最大 1MB。

【参数说明】

*QUOTA*：审计日志文件的大小，取值范围 1~10，单位 MB。

【使用举例】

```
NOS# config audit log
NOS(audit-log)# log file-size 2
```

【注意事项】

无。

### 54.2.4 log over-action

【功能描述】

**log over-action** 命令用于配置审计日志文件写满后的超限动作。

no log over-action 命令用于恢复默认超限动作。

【命令格式】

log over-action <append|drop>

no log over-action

【视图】

audit-log 视图

【缺省情况】

缺省超出文件大小，丢弃该条日志，不缓存。

【参数说明】

**append**：追加动作，即丢弃最旧的 log，余出空间，在尾部写入新 log。

**drop**：丢弃动作，即不写入审计日志文件。

【使用举例】

```
NOS# config audit log
NOS(audit-log)# log over-action append
```

【注意事项】

无。

### 54.2.5 show audit log

【功能描述】

show audit log 命令用于查看审计日志。

【命令格式】

show audit log

【视图】

所有视图

【缺省情况】

不涉及。

【参数说明】

无。

【使用举例】

```
NOS# show audit log
```

【注意事项】

无。

## 54.3 配置举例

配置打开日志审计功能，远程日志主机地址为 192.168.1.1，日志文件最大 2MB，超过限制追加写入，覆盖最旧的记录

```
NOS# config audit log
NOS(audit-log)# audithost host 192.168.1.1
NOS(audit-log)# log file-size 2
NOS(audit-log)# log over-action append
```

## 54.4 常见问题

无。

# 55 Portal 认证

## 55.1 功能简介

在传统的组网环境中，用户只要能接入局域网设备，就可以访问网络中的设备或资源，为加强网络资源的安全控制和运营管理，很多情况下需要对用户的访问进行控制。例如，在小区或公司的网络接入点，提供接入服务的供应商希望只允许付费的合法用户接入。另外，一些企业会提供一些内部关键资源给外部用户访问，希望经过有效认证的用户才可以访问这些资源。

未认证用户上网时，设备强制用户登录到特定站点，用户可以免费访问其中的服务。当用户需要使用互联网中的其它信息时，必须在门户网站进行认证，只有认证通过后才可以使用互联网资源。

## 55.2 命令手册

### 55.2.1 config portal

【功能描述】

**config portal** 命令用于开启全局 portal 认证，并进入 Portal 认证视图。

**no config portal** 命令用于关闭全局 portal 认证。

【命令格式】

[no] **config portal**

【视图】

根视图

【缺省情况】

未使能全局 Portal 认证。

【参数说明】

无。

【使用举例】

```
NOS# config portal
NOS(portal)#
```

【注意事项】

无。

### 55.2.2 server

【功能描述】

**server** 命令用于配置 Portal 认证服务器。

**no server** 命令用于删除 Portal 认证服务器。

【命令格式】

**server** *SERVER_NAME* <**ip** *A.B.C.D*|**ipv6** *X:X::X:X*> [**port** *PORT_NUM*] [**secret** *SECRET*]

**no server** *SERVER_NAME*

【视图】

Portal 认证视图

【缺省情况】

未配置 Portal 认证服务器。

【参数说明】

- *SERVER_NAME*: Portal 认证服务器的名称，为 1～31 个字符的字符串。
- *A.B.C.D*: Portal 认证服务器的 IPv4 地址。
- *X:X::X:X*: Portal 认证服务器的 IPv6 地址。
- *PORT_NUM*: 缺省情况下，接入设备主动向 Portal 认证服务器发送 Portal 报文时使用的 UDP 端口号为 50100，取值范围 1-65535。
- secret: 与 Portal 认证服务器通信时使用的共享密钥。设备与 Portal 认证服务器交互的 Portal 报文中会携带一个在该共享密钥参与下生成的验证字，该验证字用于接受方校验收到的 Portal 报文的正确性。
- *SECRET*: 共享密钥字符串，长度为 1～254 个字符。

【使用举例】

```
NOS# config portal
NOS(portal)# server svr_hz ip 1.1.1.1 secret Lee
NOS(portal)#
```

【注意事项】

Portal 认证服务器通过 Portal 协议与 NOS 交互，完成用户认证功能。NOS 只接受配置了的 Portal 认证服务器的 Portal 认证请求。

### 55.2.3 web-server

【功能描述】

**web-server** 命令用于配置 Portal 重定向 web 服务器，并进入 web-server 视图。

**no web-server** 命令用于删除 Portal 重定向 web 服务器。

【命令格式】

[no] **web-server** *SERVER_NAME*

【视图】

Portal 认证视图

【缺省情况】

未配置 Portal 重定向 web 服务器。

【参数说明】

*SERVER_*NAME: Portal Web 服务器的名称，为 1～31 个字符的字符串，区分大小写。

【使用举例】

```
NOS# config portal
NOS(portal)# portal web-server svr_hz
NOS(portal-web-server-svr_hz)#
```

【注意事项】

无。

### 55.2.4 url

【功能描述】

**url** 命令用于配置 Portal 重定向 url。

**no url** 命令用于删除 Portal 重定向 url。

【命令格式】

**url** *URLVAL*

**no url**

【视图】

web-server 视图

【缺省情况】

未配置 Portal 重定向 url。

【参数说明】

**url** *URLVAL*: Portal 重定向 Web 服务器的 URL，为 1～255 个字符的字符串，区分大小写。

【使用举例】

```
NOS# config portal
NOS(portal)# portal web-server svr_hz
NOS(portal-web-server-svr_hz)# url http://www.svr_hz.com/portal
```

【注意事项】

用户认证前的 web 请求会重定各到此 URL。

### 55.2.5 url-parameter

【功能描述】

**url-parameter** 命令用于配置 Portal 重定向 url 中需要带的自定义参数。

**no url-parameter** 命令用于删除 Portal 重定向 url 中需要带的自定义参数。

【命令格式】

**url-parameter** *NAME* <**user-url**|**user-address**|**user-mac**|**value** *VALUE*>

**no url-parameter** *NAME*

【视图】

web-server 视图

【缺省情况】

未配置 Portal 重定向 url 中需要带的自定义参数。

【参数说明】

- *NAME*：URL 参数名，为 1～31 个字符的字符串，不能包括“=”字符，区分大小写。URL 参数名对应的参数内容由 **value** *VALUE* 指定。
- **user-url**：用户初始访问的 Web 页面的 URL。
- **source-address**：用户的 IP 地址。
- **source-mac**：用户的 MAC 地址。
- **value** *VALUE*: 参数内容，为 1～255 个字符的字符串，区分大小写。

【使用举例】

```
NOS# config portal
```

```
NOS(portal)# portal web-server svr_hz
NOS(portal/websvr-svr_hz)# url-parameter ac-ip value 1.1.1.1
NOS(portal/websvr-svr_hz)# url-parameter umac user-mac
```

【注意事项】

可以通过多次执行本命令配置多条参数信息。

对于同一个参数名 param-name 后的参数设置，最后配置的生效。

### 55.2.6 portal enable

【功能描述】

**portal enable** 命令用于开启接口下的 portal 认证。

**no portal enable** 命令用于关闭接口下的 portal 认证。

【命令格式】

[no] **portal enable**

【视图】

三层接口视图

【缺省情况】

接口下未开启 Portal 认证。

【参数说明】

无。

【使用举例】

```
NOS# vlan 10
NOS(vlan-10)# config interface vlan 10
NOS(if-vlan10)# portal enable
NOS(if-vlan10)#
```

【注意事项】

无。

### 55.2.7 portal domain

【功能描述】

**portal domain** 命令用于配置接口下 portal 认证域。

**no portal domain** 命令用于取消接口下 portal 认证域。

【命令格式】

**portal domain** *DOMAIN_NAME*

**no portal domain**

【视图】

三层接口视图

【缺省情况】

接口下未配置 portal 认证域。

【参数说明】

*DOMAIN_NAME*：被引用的 ISP 认证域名，为 1～31 个字符的字符串，区分大小写，且必须已经存在。

【使用举例】

```
NOS# vlan 10
NOS(vlan-10)# config interface vlan 10
NOS(if-vlan10)# portal domain do1
NOS(if-vlan10)#
```

【注意事项】

无。

### 55.2.8 portal web-server

【功能描述】

**portal web-server** 命令用于配置接口下 portal 重定向 web 服务器。

**no portal web-server** 命令用于取消接口下 portal 重定向 web 服务器配置。

【命令格式】

**portal web-server** *SERVER_NAME*

**no portal web-server**

【视图】

三层接口视图

【缺省情况】

接口下未配置 portal 重定向 web 服务器。

【参数说明】

*SERVER_NAM*：被引用的 Portal Web 服务器的名称，为 1～31 个字符的字符串，区分大小写，且必须已经存在。

【使用举例】

```
NOS# vlan 10
NOS(vlan-10)# config interface vlan 10
NOS(if-vlan10)# portal web-server wbs1
NOS(if-vlan10)#
```

【注意事项】

无。

### 55.2.9 portal mac-authentication enable

【功能描述】

**portal mac-authentication enable** 命令用于配置接口下 portal mac 认证。

**no portal mac-authentication enable** 命令用于取消接口下 portal mac 认证配置。

【命令格式】

[no] **portal mac-authentication enable**

【视图】

三层接口视图

【缺省情况】

接口下未开启 portal mac 认证。

【参数说明】

无。

【使用举例】

```
NOS# vlan 10
NOS(vlan-10)# config interface vlan 10
NOS(if-vlan10)# portal mac-authentication enable
NOS(if-vlan10)#
```

【注意事项】

portal mac 认证是指用户进行 portal 认证成功后，在一定时间内断开网络重新连接，能够直接通过 portal mac 认证接入，无需输入用户名密码重新进行 portal 认证。

### 55.2.10 free-rule

【功能描述】

**free-rule** 命令用于配置 portal 免认证规则。

免认证规则的匹配项包括 IP 地址、TCP/UDP 端口号、所连接设备的接口，符合免认证规则的用户报文才不会触发 Portal 认证，可直接访问网络资源。

**no free-rule** 命令用于删除 portal 免认证规则。

【命令格式】

**free-rule** *RULEID* {**destination ip** <*A.B.C.D/M*|*A.B.C.D MASKLEN*> [**dst-tcp-port** *DSTTCPPORTVAL*|**dst-udp-port** *DSTUDPPORTVAL*] | **source ip** <*A.B.C.D/M*|*A.B.C.D MASKLEN* > [**src-tcp-port** *SRCTCPPORTVAL*|**src-udp-port** *SRCUDPPORTVAL*]} [**interface** *L3_IF*]

**no free-rule** <*RULEID*|**all**>

【视图】

Portal 认证视图

【缺省情况】

未配置免认证规则。

【参数说明】

- *RULEID*: 免认证规则编号。取值范围为 0～2047。
- **destination**: 指定目的信息。
- **source**: 指定源信息。
- **ip**: 指定免认证规则的 IPv4 地址。
- *A.B.C.D/M*|*A.B.C.D MASKLEN*: 免认证规则的 IPv4 地址和掩码长度，其中，*MASKLEN*为子网掩码长度，取值范围为 1～32。
- **dst-tcp-port** *DSTTCPPORTVAL*: 免认证规则的目的 TCP 端口号，取值范围为 1～65535。
- **dst-udp-port** *DSTUDPPORTVAL*: 免认证规则的目的 UDP 端口号，取值范围为 1～65535。
- **src-tcp-port** *SRCTCPPORTVAL*: 免认证规则的源 TCP 端口号，取值范围为 1～65535。
- **src-udp-port** *SRCUDPPORTVAL*: 免认证规则的源 UDP 端口号，取值范围为 1～65535。
- **interface** *L3_IF*: 指定免认证规则生效的三层接口。
- **all**: 指定所有免认证规则。

【使用举例】

```
NOS# config portal
NOS(portal)# free-rule 10 destination ip 1.1.1.1 24 dst-tcp-port 80 interface vlan1
```

```
NOS(portal)#
```

【注意事项】

无。

### 55.2.11 max-user

【功能描述】

**max-user** 命令用于配置允许 Portal 最大用户数。

**no max-user** 命令用于删除允许 Portal 最大用户数配置。

【命令格式】

**max-user** *MAXUSERVAL*

**no max-user**

【视图】

Portal 认证视图

【缺省情况】

缺省值为 100。

【参数说明】

*MAXUSERVAL*：系统中允许同时在线的最大 Portal 用户数，取值范围为 1～MAX。其中，MAX 最大取值范围根据各产品定制确定。

【使用举例】

```
NOS# config portal
NOS(portal)# max-user 50
NOS(portal)#
```

【注意事项】

无。

### 55.2.12 reset portal user

【功能描述】

**reset portal user** 命令用于强制用户下线。

【命令格式】

**reset portal user** <**ip** *A.B.C.D*|**ipv6** *X:X::X:X* |**all**|**interface** *L3_IF*|**mac** *X:X:X:X:X:X*>

【视图】

根视图

【缺省情况】

不涉及。

【参数说明】

- **ip** *A.B.C.D*：指定 IPv4 地址。
- **ipv6** *X:X::X:X*：指定 IPv6 地址。
- **all**：指定所有用户连接。
- **interface** *L3_IF*：指定所有三层接口。
- **mac** *X:X:X:X:X:X*：指定 mac 地址。

【使用举例】

```
NOS# config portal
NOS(portal)# reset portal user ip 1.1.1.1
NOS(portal)#
```

【注意事项】

执行命令强制在线用户下线需要一定的时间，在此期间，请勿进行 Portal 相关配置操作。否则会导致在线用户删除操作不能正常完成。

### 55.2.13 show portal interface

【功能描述】

**show portal interface** 命令用于显示指定接口的 Portal 认证配置和运行信息。

【命令格式】

**show portal interface** *L3_IF* [**json**]

【视图】

任意视图

【缺省情况】

不涉及。

【参数说明】

- interface L3_IF：指定三层接口。
- json：以 json 格式打印。

【使用举例】

```
NOS# show portal interface vlan 10
 Portal information of interface vlan10
 Portal status: Enabled
Portal web server: wbs-hz
 Authentication domain: domain1
User info: Idle time: 660s, user numbers:1
```

【注意事项】

无。

### 55.2.14 show portal user

【功能描述】

**show portal user** 命令用于显示 portal 用户的信息。

【命令格式】

**show portal user** <**ip** *A.B.C.D*|**ipv6** *X:X::X:X* |**all**|**interface** *L3_IF*> [**verbose**] [**json**]

【视图】

任意视图

【缺省情况】

不涉及。

【参数说明】

- **ip** *A.B.C.D*：指定 IPv4 地址。
- **ipv6** *X:X::X:X*：指定 IPv6 地址。
- **all**：指定所有用户连接。
- **interface** *L3_IF*：指定所有三层接口。
- **verbose**：显示详细信息。
- **json**：以 json 格式打印。

【使用举例】

```
NOS# show portal user all
Total portal users: 1
MAC             IP          State    Username  Interface
000d-88f8-0eab    2.2.2.2      Online    abc      vlan100

NOS# show portal user ip  1.2.1.6  verbose
------------------------------------------------------
Basic:
  Current IP address: 1.2.1.6
  Original IP address: 1.2.1.6
  Username: test
  Session ID: 176396416900000001
  Access interface: vlan1
  MAC address: 02-00-4C-4F-4F-50
  Domain: dm1
  Status: online
  Portal server: N/A
AAA:
  Realtime accounting interval: N/A, retry times: N/A
  Idle cut: 0
  Session duration: 0, remaining: 0
  Login time: 2025-11-24 14:07:51
  DHCP IP pool: N/A
ACL&QoS:
  ACL number: N/A
  User profile: N/A
Flow statistic:
  Uplink packets/bytes: 0/0
  Downlink packets/bytes: 0/0
```

【注意事项】

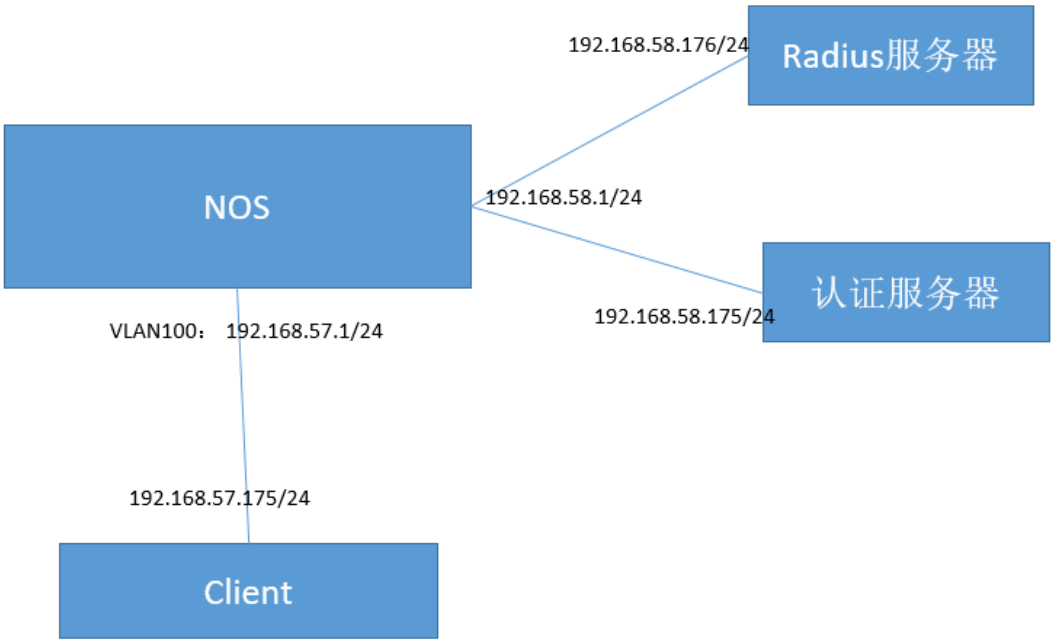
无。

## 55.3 配置举例

配置 Client 通过 NOS 进行 Portal 认证。

准备配置（略）：如下图配置相关 IP，并配置路由使 Client 与 Raidus 服务器、认证服务器间能互通。

图55-1 组网图




```
NOS# config radius scheme ra1
NOS(radius-ra1)# primary authentication 192.168.58.176 secret abc
NOS(radius-ra1)# config domain name dm1

NOS(isp-dm1)# authentication default radius-scheme ra1
NOS(isp-dm1)# config portal

NOS(portal)# server svr1 ip 192.168.58.175 port 50100 secret Lee
NOS(portal)# web-server wbs1
NOS(portal/websvr-wbs1)# url http://192.168.58.175:8080/OpenPortal/
NOS(portal/websvr-wbs1)# url-parameter uaddress user-address
NOS(portal/websvr-wbs1)# url-parameter umac user-mac
NOS(portal/websvr-wbs1)# url-parameter ac-ip value 192.168.58.1
NOS(portal/websvr-wbs1)#  config interface vlan 100

NOS(if-vlan100)# ipv4-address 192.168.58.1/24
NOS(if-vlan100)# portal enable
NOS(if-vlan100)# portal domain dm1
NOS(if-vlan100)# portal web-server wbs1
```

用户上线后查看相关信息：

```
NOS# show portal  interface vlan100
Portal information of interface vlan100
Portal status: Enabled
Portal web server: wbs1
Authentication domain: dm1
```

```
User info: Idle time: 660s, user numbers:1

NOS# show portal  user all
Total portal users: 1
MAC             IPADDR        State    Username          Interface
00-E0-4C-42-0E-56  192.168.57.175  online   user1             vlan100
```

## 55.4 常见问题

无。

# 56 端口安全

## 56.1 功能简介

### 56.1.1 端口隔离

为了实现报文之间的二层隔离，可以将不同的端口加入不同的 VLAN，但会浪费有限的 VLAN 资源。采用端口隔离特性，可以实现同一 VLAN 内端口之间的隔离。用户只需要将端口加入到隔离组中，就可以实现隔离组内端口之间二层数据的隔离。端口隔离功能为用户提供了更安全、更灵活的组网方案。

目前：

本设备支持八个隔离组，由系统自动创建隔离组 1～8，用户不可删除该隔离组或创建其它的隔离组。

隔离组内可以加入的端口数量没有限制。

相同隔离组内的端口二层隔离，隔离组之间的端口不相互隔离。

端口隔离特性与端口所属的 VLAN 无关。隔离组内端口和隔离组外属于同一 VLAN 内的端口二层流量双向互通。

## 56.2 命令手册

### 56.2.1 port-isolate enable group

【功能描述】

**port-isolate enable group** 用于将二层端口加入隔离组。

**no port-isolate enable** 由于将二层端口剥离隔离组。

【命令格式】

**port-isolate enable group** *GROUP*

**no port-isolate enable**

【视图】

二层接口视图

【缺省情况】

默认创建了 8 个隔离组。

【参数说明】

*GROUP*:指定要加入的隔离组,取值范围为(1～8)。

【使用举例】

- 将端口 ge2 加入隔离组 4

```
NOS# config interface fe2
NOS(if-ge2)# port-isolate enable group 4
NOS(if-ge2)# show this
port-isolate enable group 4
```

- 将聚合口 bagg4 加入隔离组 2

```
NOS# config bridge-aggregation 4
NOS(if-bagg4)# member interface fe2
NOS(if-bagg4)# port-isolate enable group 2
NOS(if-bagg4)# show this
port-isolate enable group 2
```

【注意事项】

- 将聚合口配置到隔离组，聚合口的所有成员端口也同步加入到隔离组。
- 将聚合口剥离出隔离组，成员端口也剥离隔离隔离组。
- 将聚合组配置到隔离组，将某个成员端口从聚合口剥离，该成员端口仍属于隔离组，需要到端口下单独剥离。

### 56.2.2 show port-isolate

【功能描述】

**show port-isolate** 命令用于显示端口隔离信息。

【命令格式】

**show port-isolate** [**json**]

【视图】

所有视图

【缺省情况】

无

【参数说明】

**json**：以 json 格式显示。

【使用举例】

```
# 显示端口隔离信息组
NOS# show port-isolate
 Ifname            Group
 ------------       ----
 ge1               1
 ge2               ----
 ge3               ----
 ge4               2
 ge5               ----
 ge6               ----
 ge7               ----
```

```
ge8                 ----
ge9                 ----
```

【注意事项】

无

## 56.3 配置举例

将二层端口 ge1/0/1 加入隔离组 4

```
NOS# config interface ge1/0/1
NOS(if-ge1/0/1)# port-isolate enable group 4
NOS(if-ge1/0/1)# show this
port-isolate enable group 4
```

## 56.4 常见问题

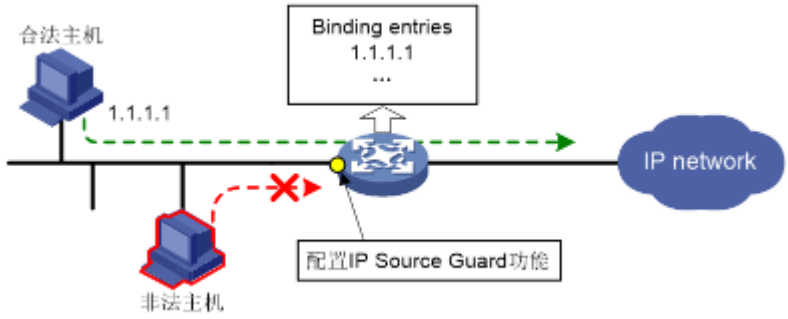
无。

# 57 IP Source Guard

## 57.1 功能简介

IP Source Guard 功能用于对接口收到的报文进行过滤控制，通常配置在接入用户侧的接口上，以防止非法用户报文通过，从而限制了对网络资源的非法使用（比如非法主机仿冒合法用户 IP 接入网络），提高了接口的安全性。

图57-1 IP Source Guard




如上图所示，配置了 IP Source Guard 功能的接口接收到用户报文后，根据 IP Source Guard 绑定表项匹配报文，如果报文的信息与某绑定表项匹配，则转发该报文；若匹配失败，则丢弃该报文。IP Source Guard 可以根据报文的源 IP 地址、源 MAC 地址和 VLAN 标签对报文进行过滤。报文的这些特征项可单独或组合起来与接口进行绑定，形成 IP Source Guard 绑定。

IP Source Guard 的绑定功能是针对接口的，一个接口配置了绑定功能后，仅对该接口接收的报文进行限制，其它接口不受影响。

IP Source Guard 绑定可以通过静态配置和动态获取两种方式生成。

- 静态配置：支持全局静态绑定和接口静态绑定两种，接口静态绑定支持普通口、聚合口、VLAN 接口。
- 动态获取：支持通过 DHCP Snooping、DHCP Relay 等方式获取。

动态获取的匹配方式支持三种：

ip：仅匹配 IP 地址；mac：仅匹配 MAC 地址；ip-mac：需要同时匹配 IP 地址和 MAC 地址。

## 57.2 命令手册

### 57.2.1 config ip-source-guard

【功能描述】

**config ip-source-guard** 命令用于创建并进入 ip-source-guard 全局视图。

【命令格式】

**config ip-source-guard**

【视图】

根视图

【缺省情况】

不存在 IP Source Guard 全局视图

【参数说明】

无

【使用举例】

```
NOS# config ip-source-guard
NOS(ipsg)#
```

【注意事项】

无

### 57.2.2 ip-source-guard static

【功能描述】

**ip-source-guard static** 命令用于配置一条 IP Source Guard 静态绑定。

**no ip-source-guard static** 命令用于删除一条 IP Source Guard 静态绑定。

【命令格式】

[**no**] **ip-source-guard static** {<**ipv4** *A.B.C.D* | **ipv6** *X:X::X:X* > [**mac** *X:X:X:X:X:X*]} [**vlan** *VLAN_ID*]

**no ip-source-guard static all**

【视图】

二层以太网接口视图、聚合接口视图、VLAN 接口视图、全局视图（config ip-source-guard）

【缺省情况】

不存在 IP Source Guard 静态绑定。

【参数说明】

*A.B.C.D*：IPv4 地址。

*X:X::X:X*：IPv6 地址。

*X:X:X:X:X:X*：MAC 地址。

*VLAN_ID*：最外层 VLAN ID，取值范围为 1~4094。

**all**：删除该视图下的所有 IP Source Guard 静态绑定配置。

【使用举例】

```
NOS# config interface ge17
NOS(if-ge17)# ip-source-guard static ipv4 30.1.1.1
```

【注意事项】

- 在二层以太网接口视图、聚合接口视图、VLAN 接口视图下，必须配置 ip source guard 使能之后，配置 IP Source Guard 静态绑定才有效果；配置全局 IP Source Guard 静态绑定，仅针对配置 ip source guard 使能的接口才有效果。
- 配置 ip source guard 使能的动态匹配方式，对 IP Source Guard 静态绑定不起作用；
- VLAN 接口视图、全局视图下，无[**vlan** (1-4094)]配置。

### 57.2.3 ip-source-guard static macv6

【功能描述】

**ip-source-guard static macv6** 命令用于配置一条 IP Source Guard 静态绑定 mac 地址。

**no ip-source-guard static macv6** 命令用于删除一条 IP Source Guard 静态绑定 mac 地址。

【命令格式】

[no] **ip-source-guard static macv6** *X:X:X:X:X:X* [**vlan** *VLAN_ID*]

【视图】

二层以太网接口视图、聚合接口视图、VLAN 接口视图、全局视图（config ip-source-guard）

【缺省情况】

不存在 IP Source Guard 静态绑定 mac 地址。

【参数说明】

- *X:X:X:X:X:X*：IPV6 报文的 MAC 地址。
- *VLAN_ID*：最外层 VLAN ID，取值范围为 1~4094。

【使用举例】

```
NOS# config interface ge17
NOS(if-ge17)# ip-source-guard static macv6 00:00:00:00:00:01
```

【注意事项】

同 **ip-source-guard static** 命令。

### 57.2.4 ip-source-guard enable

【功能描述】

**ip-source-guard enable** 命令用于配置接口的 IP Source Guard 使能，以及设置动态获取的匹配方式。

**no ip-source-guard enable** 命令用于取消接口的 IP Source Guard 使能。

【命令格式】

**ip-source-guard enable** <**ip**|**ip-mac**|**mac**>

**no ip-source-guard enable**

【视图】

二层以太网接口视图、聚合接口视图、VLAN 接口视图

【缺省情况】

IP Source Guard 未使能。

【参数说明】

- **mac**：对于动态获取的匹配方式，仅匹配 MAC 地址。
- **ip**：对于动态获取的匹配方式，仅匹配 IP 地址。
- **ip-mac**：对于动态获取的匹配方式，需要同时匹配 IP 地址和 MAC 地址。

【使用举例】

```
NOS# config interface ge17
NOS(if-ge17)# ip-source-guard enable mac
```

【注意事项】

- 配置了 ip source guard 使能，配置 IP Source Guard 静态绑定才有效果。
- 配置 ip source guard 使能的动态匹配方式，对 IP Source Guard 静态绑定不起作用。

### 57.2.5 show ip-source-guard

【功能描述】

**show ip-source-guard** 命令用于显示 IP Source Guard 的静态及动态绑定。

【命令格式】

**show ip-source-guard** <**interface** *ALL_IF*|**global**>

【视图】

所有视图

【缺省情况】

无

【参数说明】

- *ALL_IF*：二层以太网接口、聚合接口、VLAN 接口的 IP Source Guard 的静态及动态绑定。
- **global**：全局 IP Source Guard 的静态绑定。

【使用举例】

# 显示 IP Source Guard 的静态及动态绑定

```
NOS# show ip-source-guard interface bagg13
 T -- Type
 S -- Static
 N -- Dhcp snooping
 R -- Dhcp relay
 No. IP address                MAC address           Interface    Vlan T
---- ---------------------------------- ---------------- -------- ---- -
   1 2030::4                                            bagg13       13    S
   2 2030::6                                            bagg13            S
   3 2030::8                   00:00:01:00:00:03        bagg13            S
   4 2030::10                  00:00:01:00:00:03       bagg13       13    S
   5                           00:00:01:00:00:03        bagg13       13    S
   6                           00:00:01:00:00:03        bagg13            S
```

【注意事项】

无

## 57.3 配置举例

(1) 在接口 ge1/0/1 下使能 ipsg，配置静态规则仅允许源 ip 为 1.1.1.1 的流量通过

```
NOS# config interface ge1/0/1
NOS(if-ge1/0/1)# ip-source-guard enable ip
NOS(if-ge1/0/1)# ip-source-guard static ipv4 1.1.1.1
NOS(if-ge1/0/1)# dis th
  ip-source-guard enable ip
  ip-source-guard static ipv4 1.1.1.1
NOS(if-ge1/0/1)#
```

(2) 在全局 ipsg 视图下配置静态规则仅允许源 ip 为 1.1.1.1 的流量通过，在接口 ge1/0/2 下使能 ipsg 使之生效

```
NOS# config ip-source-guard
NOS(ipsg)# ip-source-guard static ipv4 1.1.1.1
```

```
NOS(ipsg)# quit
NOS# interface ge1/0/2
NOS(if-ge1/0/2)# ip-source-guard enable ip
```

## 57.4 常见问题

无。

# 58 ARP 防攻击

## 58.1 功能简介

### 58.1.1 ARP探测

ARP 探测（ARP Detection）功能主要应用于接入设备上，通过检测并丢弃非法用户的 ARP 报文来防止仿冒用户、仿冒网关的攻击。

### 58.1.2 ARP源抑制

TBD

### 58.1.3 ARP限速

限速是对流经设备接口的报文速度做限制，流量超出阈值的部分直接被丢弃，低于阈值的部分则进入或离开设备。

## 58.2 命令手册

### 58.2.1 config arp-detection

【功能描述】

**config arp-detection** 命令用于创建并进入 arp-detection 视图。

**no config arp-detection** 命令用于删除 arp-detection 视图。

【命令格式】

**config arp-detection**

**no config arp-detection**

【视图】

根视图。

【缺省情况】

缺省不存在 arp-detection 视图。

【参数说明】

无。

【使用举例】

#创建并进入 arp-detection 视图。

```
NOS# config arp-detection
NOS(arp-detection)#
```

【注意事项】

无。

### 58.2.2 arp detection enable

【功能描述】

**arp detection enable** 命令用来开启 ARP Detection 功能，即对 ARP 报文进行用户合法性检查。

**no arp detection enable** 命令用来关闭 ARP Detection 功能。

【命令格式】

**arp detection enable**

**no arp detection enable**

【视图】

VLAN 视图。

【缺省情况】

ARP Detection 功能处于关闭状态，即不进行用户合法性和报文合法性检查。

【参数说明】

无。

【使用举例】

#在 vlan10 上开启 ARP Detection 功能。

```
NOS(vlan-10)# arp detection enable
```

【注意事项】

无。

### 58.2.3 arp detection trust

【功能描述】

**arp detection trust** 命令配置接口为 ARP 信任接口。

**no arp detection trust** 命令用来恢复缺省情况。

【命令格式】

**arp detection trust**

**no arp detection trust**

【视图】

二层接口视图。

【缺省情况】

未开启 ARP Detection trust 功能。

【参数说明】

无。

【使用举例】

#配置接口 ge1 为 ARP 信任接口。

```
NOS(if-ge1)# arp detection trust
```

【注意事项】

无。

### 58.2.4 validate

【功能描述】

**validate** 命令用来开启对 ARP 报文进行报文合法性检查。

**no validate** 命令用来关闭 ARP 报文合法性检查功能。

【命令格式】

**validate** {**dst-mac**|**ip**|**src-mac**}

**no validate** [{**dst-mac**|**ip**|**src-mac**}]

【视图】

arp-detection 视图。

【缺省情况】

validate 功能处于关闭状态，即不进行报文合法性检查。

【参数说明】

- dst-mac：检查 ARP 报文目的 MAC 是否合法，即检查 ARP 应答报文中的目的 MAC 地址是否为全 0 或者全 1，是否和以太网报文头中的目的 MAC 地址一致，全 0、全 1、不一致的报文需要被丢弃。
- ip：会检查 ARP 报文中的源 IP 和目的 IP 地址，全 1、或者组播 IP 地址都是不合法的，需要丢弃。对于 ARP 应答报文，源 IP 和目的 IP 地址都进行检查；对于 ARP 请求报文，只检查源 IP 地址。
- src-mac：会检查 ARP 报文中的源 MAC 地址和以太网报文头中的源 MAC 地址是否一致，一致则认为有效，否则丢弃报文。

【使用举例】

#在 arp-detection 视图下开启对 ARP 报文目的 MAC 和源 MAC 的合法性检查。

```
NOS(arp-detection)# validate dst-mac src-mac
```

【注意事项】

开启 validate 功能前，需先开启 arp detection enable。

### 58.2.5 config arp-source-suppression

【功能描述】

**config arp-source-suppression** 命令用于创建并进入 arp-src-suppression 视图。

**no config arp-source-suppression** 命令用于删除 arp-src-suppression 视图。

【命令格式】

**config arp-source-suppression**

**no config arp-source-suppression**

【视图】

根视图。

【缺省情况】

不存在 arp-src-suppression 视图。

【参数说明】

无。

【使用举例】

#创建并进入 arp 源抑制视图。

```
NOS# config arp-source-suppression
NOS(arp-src-suppression)# dis th
NOS(arp-src-suppression)#
```

【注意事项】

无。

### 58.2.6 source-suppression limit

【功能描述】

**source-suppression limit** 命令用来开启 arp 源抑制功能。

**no source-suppression limit** 命令用来关闭 arp 源抑制功能。

【命令格式】

**source-suppression limit** *VALUE*

**no source-suppression limit**

【视图】

arp-src-suppression 视图。

【缺省情况】

未开启 arp 源抑制功能。

【参数说明】

*VALUE*：ARP 源抑制的阈值，即设备在 5 秒间隔内可以处理的源 IP 相同，但目的 IP 地址不能解析的 IP 报文的最大数目，取值范围为 2-1024。

【使用举例】

#配置 arp 源抑制的阈值为 2。

```
NOS(arp-src-suppression)# source-suppression  limit 2
NOS(arp-src-suppression)# dis th
  source-suppression limit 2
NOS(arp-src-suppression)#
```

【注意事项】

无。

### 58.2.7 rate-limit

【功能描述】

**rate-limit** 命令用来开启 ARP 限速功能。

**no rate-limit** 命令用来关闭 ARP 限速功能。

【命令格式】

**rate-limit** *PPSNUM*

**no rate-limit**

【视图】

arp 视图。

【缺省情况】

未开启 ARP 限速功能。

【参数说明】

*PPSNUM*：速率限制值(1-500)，单位为 pps。

【使用举例】

```
NOS(arp)# rate-limit 200
```

【注意事项】

无。

### 58.2.8 rate-limit log enable

【功能描述】

**rate-limit log enable** 命令用来开启 ARP 限速日志。

**no rate-limit log enable** 命令用来关闭 ARP 限速日志。

【命令格式】

**rate-limit log enable**

**no rate-limit log enable**

【视图】

arp 视图。

【缺省情况】

未开启开启 ARP 限速日志。

【参数说明】

无。

【使用举例】

```
NOS(arp)# rate-limit log enable
```

【注意事项】

无。

## 58.3 配置举例

(1) 在 VLAN 开启 ARP Detection 功能，即进行用户合法性检查，将不需要进行用户合法性检查的接口 ge1/0/1 配置为 ARP 信任接口，对于 ARP 非信任接口，配置对目的 MAC 地址检查模式

```
NOS# config vlan  6
NOS(vlan-6)# arp detection enable
NOS(vlan-6)# dis th
  arp detection
NOS(vlan-6)# interface ge1/0/1
NOS(if-ge1/0/1)# arp detection trust
NOS(if-ge1/0/1)# dis th
  vlan access 6
  arp detection trust
NOS(if-ge1/0/1)# quit
NOS# config arp-detection
```

```
NOS(arp-detection)# validate dst-mac
NOS(arp-detection)# dis th
  validate dst-mac
NOS(arp-detection)#
```

(2) 配置开启 ARP 源抑制功能，阈值为 10

```
NOS# config arp-source-suppression
NOS(arp-src-suppression)# source-suppression limit 10
NOS(arp-src-suppression)# dis th
  source-suppression limit 10
NOS(arp-src-suppression)#
```

(3) 配置开启 ARP 报文限速功能，限制 500pps,开启 ARP 报文限速日志功能

```
NOS# config arp
NOS(arp)# rate-limit 500
NOS(arp)# rate-limit log enable
NOS(arp)# dis th
  rate-limit 500
  rate-limit log enable
```

## 58.4 常见问题

无。

# 59 DDoS

## 59.1 功能简介

DDoS 攻击又称为分布式拒绝服务（Distributed Denial of Service）攻击是一种常见的网络攻击手段，它通过控制大量计算机、物联网终端或网络僵尸（Zombie）来向目标网站发送大量请求，从而耗尽其服务器资源，导致正常用户无法访问服务的攻击方式。

为了防范 DDoS 攻击，需要按报文的来源信息进行分类统计，对突然收到的大量报文进行监控，并发布告警通知管理员对此类报文增加限制。

网络上可能会出现大量攻击报文攻击设备的 CPU，如果使能攻击溯源功能，通过分析上送 CPU 的报文是否会对 CPU 造成攻击，设备能够追溯到攻击源并以日志或告警的方式通知网络管理员，以便网络管理员采取措施对攻击源进行防御部署。

## 59.2 命令手册

### 59.2.1 config ddos

【功能描述】

**config ddos** 命令用于进入 DDoS 视图。

**no config ddos** 命令用于删除 DDoS 视图。

【命令格式】

[**no**] **config ddos**

【视图】

根视图。

【缺省情况】

默认不开启。

【参数说明】

无。

【使用举例】

```
NOS# config ddos
NOS(ddos)#
```

【注意事项】

创建视图后，视图下 **defense** *相关配置命令即自动创建默认值，**show ddos config** 即可查询相关默认配置。

- defense disable
- defense trace-type source-ip
- defense protocol all
- defense threshold 10
- defense sample 10

### 59.2.2 defense enable

【功能描述】

**defense enable** 命令用来使能攻击溯源功能。

**no defense enable** 命令用来去使能攻击溯源功能。

【命令格式】

**defense enable**

**no defense enable**

【视图】

DDoS 视图。

【缺省情况】

默认不使能。

【参数说明】

无。

【使用举例】

```
NOS# config ddos
NOS(ddos)# defense enable
NOS(ddos)# dis this
  defense enable
NOS(ddos)#
```

【注意事项】

无。

### 59.2.3 defense protocol

【功能描述】

**defense protocol** 命令用来配置攻击溯源防范的报文类型。

**no defense protocol** 命令用来删除攻击溯源防范的报文类型。

【命令格式】

**defense protocol <all|{arp|dhcp|tcp|udp|icmp|igmp|mld|nd|ttl-expired}>**

**no defense protocol**

【视图】

DDoS 视图。

【缺省情况】

默认 all(所有支持攻击溯源防范的报文类型)。

【参数说明】

**arp**：ARP 报文。

**dhcp**：DHCP 报文。

**tcp**：TCP 报文。

**udp**：udp 报文。

**icmp**：ICMP 报文。

**igmp**：IGMP 报文。

**mld**：MLD 报文。

**nd**：ND 报文。

**ttl-expired**：Icmp Time Exceeded 差错报文。

【使用举例】

```
NOS# config ddos
NOS(ddos)# defense protocol arp tcp udp dhcp
NOS(ddos)# dis this
  defense protocol arp tcp udp dhcp
NOS(ddos)#
```

【注意事项】

- defense enable 情况下配置此命令，因策略变动原记录报文信息将清空，重新收集。
- 使用 defense enable 命令使能攻击溯源功能后，即使未使用 defense protocol 命令进行配置，设备也将对默认的溯源防范的报文类型进行溯源。

### 59.2.4 defense sample

【功能描述】

**defense sample** 命令用来配置攻击溯源的采样比。

**no defense sample** 命令用来恢复默认攻击溯源的采样比。

【命令格式】

**defense sample** *SAMPLE*

**no defense sample**

【视图】

DDoS 视图。

【缺省情况】

默认攻击溯源的采样比为 50。

【参数说明】

*SAMPLE*：指定攻击溯源溯源的采样比。整数形式，取值范围是 1～100。

【使用举例】

```
NOS# config ddos
NOS(ddos)# defense sample 60
NOS(ddos)# dis this
  defense sample 60
NOS(ddos)#
```

【注意事项】

- defense enable 情况下配置此命令，因策略变动原记录报文信息将清空，重新收集。
- 使用 defense enable 命令使能攻击溯源功能后，即使未使用 defense sample 命令进行配置，设备也将使用缺省的攻击溯源的采样比对攻击源采样。

### 59.2.5 defense threshold

【功能描述】

**defense threshold** 命令用来配置攻击溯源检查阈值。

**no defense threshold** 命令用来恢复默认攻击溯源检查阈值。

【命令格式】

**defense threshold** *THRESHOLD*

**no defense threshold**

【视图】

DDoS 视图。

【缺省情况】

默认攻击溯源检查阈值为 10。

【参数说明】

*THRESHOLD*：指定攻击溯源检查阈值。整数形式，取值范围是 1～100，单位是 pps。

【使用举例】

```
NOS# config ddos
NOS(ddos)# defense threshold 90
NOS(ddos)# dis this
  defense threshold 90
NOS(ddos)#
```

【注意事项】

- defense enable 情况下配置此命令，因策略变动原记录报文信息将清空，重新收集。
- 使用 defense enable 命令使能攻击溯源功能后，即使未使用 defense threshold 命令进行配置，设备也将使用缺省的攻击溯源检查阈值对攻击源进行溯源。

### 59.2.6 defense trace-type

【功能描述】

**defense trace-type** 命令用于配置攻击溯源的溯源模式。

**no defense trace-type** 命令用于恢复攻击溯源的默认溯源模式。

【命令格式】

**defense trace-type <source-ip|source-mac|source-portvlan>**

**no defense trace-type**

【视图】

DDoS 视图。

【缺省情况】

默认攻击溯源为 **source-ip**。

【参数说明】

- **source-ip**：指定攻击溯源的方式为基于源 IP 地址，设备根据源 IP 地址进行分类统计，识别攻击源。
- **source-mac**：指定攻击溯源的方式为基于源 MAC 地址，设备根据源 MAC 地址进行分类统计，识别攻击源。
- **source-portvlan**：指定攻击溯源的方式为基于源接口 VLAN，设备根据基于源接口 VLAN 进行分类统计，识别攻击源。

【使用举例】

```
NOS# config ddos
NOS(ddos)# defense trace-type source-mac source-portvlan
NOS(ddos)# dis this
```

```
  defense trace-type source-mac source-portvlan
NOS(ddos)#
```

【注意事项】

1、**defense enable** 情况下配置此命令，因策略变动原记录报文信息将清空，重新收集。

2、使用 **defense enable** 命令使能攻击溯源功能后，即使未使用 **defense trace-type** 命令进行配置，设备也将使用缺省的攻击溯源模式对攻击源进行溯源。

### 59.2.7 show ddos config

【功能描述】

**show ddos config** 命令用来查看 DDoS 攻击配置信息。

【命令格式】

**show ddos config**

【视图】

所有视图。

【缺省情况】

不涉及。

【参数说明】

无。

【使用举例】

```
NOS# show ddos config
DDOS global status: Enabled
  Defense status    : enable
  Defense trace-type: source-ip source-mac source-portvlan
  Defense protocol  : all
  Defense threshold : 10
  Defense sample    : 10
```

【注意事项】

在创建 DDoS 视图后查看配置会有配置显示，没有创建则无数据返回。

### 59.2.8 show ddos statistic

【功能描述】

**show ddos statistic** 命令用来查看攻击源统计计数信息。

【命令格式】

**show ddos statistic <all|{arp|dhcp|tcp|udp|icmp|igmp|mld|nd|ttl-expired}>**

【视图】

所有视图。

【缺省情况】

不涉及。

【参数说明】

- **arp**：ARP 报文。
- **dhcp**：DHCP 报文。

- **tcp**：TCP 报文。
- **udp**：udp 报文。
- **icmp**：ICMP 报文。
- **igmp**：IGMP 报文。
- **mld**：MLD 报文。
- **nd**：ND 报文。
- **ttl-expired**：Icmp Time Exceeded 差错报文。

【使用举例】

```
NOS# show ddos statistics udp igmp
Defense trace-type: source-ip source-mac source-portvlan
Defense protocol:udp
-------------------------------------------------------------
|Ipv4 address     |VlanId   |Mac             |PPs        |
-------------------------------------------------------------
|192.85.1.2       |1       |00:10:94:00:00:02 |62.00      |
-------------------------------------------------------------
Defense protocol:igmp
-------------------------------------------------------------
|Ipv4 address     |VlanId   |Mac             |PPs        |
-------------------------------------------------------------
|192.85.1.2       |1       |00:10:94:00:00:02 |124.00     |
-------------------------------------------------------------
```

【注意事项】

在 **defense enable** 后，可查攻击源统计计数信息，没有则无攻击报文。

## 59.3 配置举例

(1) 进入 DDoS 视图
(2) 使能攻击溯源功能
(3) 配置攻击溯源防范的报文类型为所有类型
(4) 配置攻击溯源的采样比为 50
(5) 配置攻击溯源检查阈值为 20
(6) 配置攻击溯源的溯源模式为源 ip 地址

```
NOS# config ddos
NOS(ddos)# defense enable
NOS(ddos)# defense protocol all
NOS(ddos)# defense sample 50
NOS(ddos)# defense threshold 20
NOS(ddos)# defense trace-type source-ip
```

#查看 DDoS 攻击配置信息

```
NOS# show ddos config
DDOS global status: Enabled
  Defense status    : Enabled
  Defense trace-type: source-ip
  Defense protocol  : all
  Defense threshold : 20
```

```
Defense sample    : 50
```

## 59.4 常见问题

无。

# 60 白名单

## 60.1 功能简介

TBD

## 60.2 命令手册

### 60.2.1 apply acl

【功能描述】

**apply acl** 命令用来配置 telnet/ssh/web 服务应用 acl 规则。

**no apply acl** 命令用来恢复缺省情况。

【命令格式】

**apply acl** <*BASIC_ACL* | *ADVANCED_ACL*>

**no apply acl**

【视图】

ssh server 视图/telnet sever 视图/web server 视图。

【缺省情况】

未使用 acl 限制 telnet/ssh/web 客户端。

【参数说明】

- *BASIC_ACL*：表示 ipv4 基本 acl，取值范围 2000-2999。
- *ADVANCED_ACL*：表示 ipv4 高级 acl，取值范围 3000-3999。

【使用举例】

```
NOS# config ssh server
NOS(ssh)# apply acl 2000
NOS(ssh)# dis th
  apply acl 2000
NOS(ssh)# config web server
NOS(web)# apply acl 3000
NOS(web)# dis th
  apply acl 3000
NOS(web)# config telnet server
NOS(telnet)# apply acl 2001
NOS(telnet)# dis th
  apply acl 2001
NOS(telnet)#
```

【注意事项】

对 telnet/web/ssh 客户端的访问控制通过应用 acl 来实现，如下：

- 当应用的 acl 不存在或者是复用的 acl 为空的时候，允许所有 telnet/web/ssh 客户端访问设备。
- 当应用的 acl 存在时，匹配 acl 中 permit 规则的 telnet/web/ssh 客户端可以访问设备，其他客户端不可以访问设备。

- 如果多次使用该命令配置 telnet/web/ssh 服务与 acl 关联，则按照 acl 规则中最小的 rule 生效。

### 60.2.2 apply acl ipv6

【功能描述】

**apply acl ipv6** 命令用来配置 telnet/ssh/web 服务应用 ipv6 acl 规则。

**no apply acl ipv6** 命令用来恢复缺省情况。

【命令格式】

**apply acl ipv6** <*BASIC_ACL* | *ADVANCED_ACL*>

**no apply acl ipv6**

【视图】

ssh server 视图/telnet sever 视图/web server 视图。

【缺省情况】

未使用 ipv6 acl 限制 telnet/ssh/web 客户端。

【参数说明】

- *BASIC_ACL*：表示 ipv6 基本 acl，取值范围 5000-5999。
- *ADVANCED_ACL*：表示 ipv6 高级 acl，取值范围 6000-6999。

【使用举例】

```
NOS# config ssh server
NOS(ssh)# apply acl ipv6 5000
NOS(ssh)# dis th
  apply acl ipv6 5000
NOS(ssh)# config web server
NOS(web)# apply acl ipv6 6000
NOS(web)# dis th
  apply acl ipv6 6000
NOS(web)# config telnet server
NOS(telnet)# apply acl ipv6 6999
NOS(telnet)# dis th
  apply acl ipv6 6999
NOS(telnet)#
```

【注意事项】

同 **apply acl** 命令。

## 60.3 配置举例

配置使用 acl 2000 和 5000 来限制 ssh 客户端流量

```
NOS# config ssh server
NOS(ssh)# apply acl 2000
NOS(ssh)# apply acl ipv6 5000
NOS(ssh)# dis th
  apply acl 2000
  apply acl ipv6 5000
```

## 60.4 常见问题

无。

# 61 带内管理

## 61.1 功能简介

带内管理（In-Band Management）是一种通过业务网络通道对设备进行监控和管理的方式。通过设备自身的业务接口（如以太网端口）进行管理，管理流量与业务流量共享同一网络路径。管理数据（如配置命令、监控信息）与业务数据（如用户数据）共用相同的网络资源，通常利用现有的 TCP/IP 协议栈进行通信。

## 61.2 命令手册

### 61.2.1 in-band management disable

【功能描述】

**in-band management disable** 命令用来使设备只允许通过管理口登录。

**no in-band management disable** 命令用来恢复默认。

【命令格式】

**in-band management disable**

**no in-band management disable**

【视图】

ssh-server 视图

telnet-server 视图

web-server 视图

ftp-server 视图

snmp 视图

【缺省情况】

管理口和业务口都可以登录。

【参数说明】

不涉及。

【使用举例】

```
NOS# config ssh server
NOS(ssh)# in-band management disable
```

【注意事项】

无。

## 61.3 配置举例

配置 ssh 客户端仅可以通过管理口登录设备

```
NOS# config ssh server
NOS(ssh)# in-band management disable
NOS(ssh)# dis th
 in-band management disable
```

## 61.4 常见问题

无。

# 62 CPU 防攻击

## 62.1 功能简介

TBD

## 62.2 命令手册

### 62.2.1 config control-plane

【功能描述】

**config control-plane** 命令用于创建并进入 control-plane 视图。

**no config control-plane** 命令用于删除 control-plane 视图。

【命令格式】

**config control-plane**

**no config control-plane**

【视图】

根视图。

【缺省情况】

缺省不存在 control-plane 视图。

【参数说明】

无。

【使用举例】

#创建并进入 control-plane 视图。

```
NOS# config control-plane
NOS(control-plane)#
```

【注意事项】

无。

### 62.2.2 qos policy inbound

【功能描述】

**qos policy** 命令用于在入方向上应用 QoS 策略。

**no qos policy inbound** 命令用于取消在入方向上应用 QoS 策略。

【命令格式】

**qos policy name** *NAME* **inbound**

**no qos policy inbound**

【视图】

control-plane 视图。

【缺省情况】

缺省不存在 control-plane 视图。

【参数说明】

*NAME*：QoS 策略名称。

【使用举例】

```
NOS(control-plane)# qos policy  name  AA inbound
NOS(control-plane)# dis th
   qos policy name AA inbound
NOS(control-plane)# no qos  policy  inbound
NOS(control-plane)# dis th
NOS(control-plane)#
```

【注意事项】

无。

### 62.2.3 show qos policy control-plane

【功能描述】

**show qos policy control-plane** 命令用来查看控制平面上 QoS 策略信息。

【命令格式】

**show qos policy control-plane**

【视图】

所有视图。

【缺省情况】

不涉及。

【参数说明】

无。

【使用举例】

```
NOS# show qos  policy control-plane
        Class          Action      limit(pps)      hit
 ---------------- ---------------- ------------- ----------
```

【注意事项】

无。

## 62.3 配置举例

在 QoS 控制平台上配置在入方向上应用 QoS 策略 test

```
NOS# config control-plane
NOS(control-plane)# qos policy name  test inbound
NOS(control-plane)# dis th
   qos policy name test inbound
```

## 62.4 常见问题

无。

# 63 ACL

## 63.1 功能简介

### 63.1.1 特性简介

ACL（Access Control List，访问控制列表）是一系列用于识别报文流的规则的集合。这里的规则是指描述报文匹配条件的判断语句，匹配条件可以是报文的源地址、目的地址、端口号等。设备依据 ACL 规则识别出特定的报文，并根据预先设定的策略对其进行处理，最常见的应用就是使用 ACL 进行报文过滤。此外，ACL 还可应用于诸如路由、安全、QoS 等业务中识别报文，对这些报文的具体处理方式根据应用 ACL 的业务模块来决定。

### 63.1.2 ACL的编号与分类

用户在创建 ACL 时必须为其指定编号，不同的编号对应不同类型的 ACL，根据规则制订依据的不同，可以将 ACL 分为如下表所示的几种类型。

表63-1 ACL 类型

| 编号范围 | ACL 类型 | 适用的 IP 版本 | 规则制订依据 |
|---|---|---|---|
| 2000-2999 | 基本ACL | IPv4 | 报文的源IPv4地址 |
| 3000-3999 | 高级ACL | IPv4 | 报文的源IPv4地址、目的IPv4地址、Dscp优先级、IPv4承载的协议类型等三、四层信息 |
| 4000-4999 | 二层ACL | IPv4、IPv6 | 报文的源MAC地址、目的MAC地址、VLAN、CoS优先级、数据链路层协议类型等二层信息 |
| 5000-5999 | 基本ACL | IPv6 | 报文的源IPv6地址 |
| 6000-6999 | 高级ACL | IPv6 | 报文的源IPv6地址、目的IPv6地址、Dscp优先级、IPv6承载的协议类型及特性等三、四层信息 |
| 7000-7999 | 自定义ACL | IPv4、IPv6 | 根据报文头、偏移位置、字符串掩码和用户自定义字符串来进行报文信息匹配 |

### 63.1.3 ACL中规则的编号与步长

ACL 中的每条规则都有自己的编号，这个编号在该 ACL 中是唯一的。在创建规则时，可以手工为其指定一个编号，如未手工指定编号，则由系统为其自动分配一个编号。由于规则的编号可能影响规则匹配的顺序，因此当由系统自动分配编号时，为了方便后续在已有规则之前插入新的规则，系统通常会在相邻编号之间留下一定的空间，这个空间的大小（即相邻编号之间的差值）就称为 ACL 的步长。例如：当步长为 5 时，系统会将编号 0、5、10、15、……依次分配给新创建的规则。

系统为 ACL 规则自动分配编的值：首次为 0，非首次为现有最大编号加步长的值。例如：原有编号为 0、5、9、10 和 12 的五条规则，步长为 5，此时如果创建一条规则且不指定编号，那么系统将自动为其分配编号 17。

步长可以进行修改和选择是否更新。如果修改了步长及编号起始值，并且选择更新，ACL 内原有全部规则的编号都将自动从规则编号的起始值开始按步长重新排列。譬如，某 ACL 内原有编号为 0、5、9、10 和 15 的五条规则，当修改步长为 9，编号的起始值为 16 之后，这些规则的编号将依次变为 16、25、34、43 和 52。

### 63.1.4 ACL的匹配顺序

当一个 ACL 中包含多条规则时，报文会按照一定的顺序与这些规则进行匹配，一旦匹配上某条规则便结束匹配过程。

ACL 支持配置为全局 ACL，也支持配置在端口上，端口 ACL 优先级高于全局 ACL。

对于不同类型的 ACL，优先级由高到低依次为：IPv4 ACL、IPv6 ACL、二层 ACL。

在同一条 ACL 中，规则的编号越小，优先级越高。

### 63.1.5 ACL规则中的掩码

ACL 规则中的掩码，是将掩码转换成二进制后，“1”表示“匹配”，“0”表示“不关心”；也有的掩码采用前缀表示，前面的前缀长度个 bit 表示“匹配”，后面的不关心。

例 1：IPv4 地址的掩码：采用点分十进制表示，转换为二进制后，“1”表示“匹配”，“0”表示“不关心”，掩码中的“0”或“1”可以是不连续的。

例 2：IPv6 地址的掩码，采用前缀表示，前缀越长，范围越小。

例 3： MAC 地址的掩码，与 MAC 地址表示方式相同，使用十六进制，转换为二进制后，“1”表示“匹配”，“0”表示“不关心”，掩码中的“0”或“1”可以是不连续的。

## 63.2 命令手册

### 63.2.1 config acl basic-ipv4

【功能描述】

**config acl** *ACLID* 命令用于进入指定编号的基本 IPv4 ACL 视图。

**no config acl** *ACLID* 命令用于删除指定编号的基本 IPv4 ACL 视图及视图下的所有配置。

**no config acl basic-ipv4** 命令用于删除编号范围在(2000-2999)间所有基本 IPv4 ACL 视图及视图下的所有配置。

【命令格式】

**config acl** *ACLID*

**no config acl** *ACLID*

**no config acl basic-ipv4**

【视图】

根视图

【缺省情况】

不存在基本 IPv4 ACL。

【参数说明】

*ACLID*：基本 IPv4 ACL 的编号，范围(2000-2999)。

【使用举例】

# 进入编号为 2000 的基本 IPv4 ACL 视图

```
NOS# config acl 2000
```

```
NOS(acl-2000)#
```

【注意事项】

无。

### 63.2.2 config acl basic-ipv6

【功能描述】

**config acl** *ACLID* 命令用于进入指定编号的基本 IPv6 ACL 视图。

**no config acl** *ACLID* 命令用于删除指定编号的基本 IPv6 ACL 视图及视图下的所有配置。

**no config acl basic-ipv6** 命令用于删除编号范围在(5000-5999)间所有基本 IPv6 ACL 视图及视图下的所有配置。

【命令格式】

**config acl** *ACLID*

**no config acl** *ACLID*

**no config acl basic-ipv6**

【视图】

根视图

【缺省情况】

不存在基本 IPv6 ACL。

【参数说明】

*ACLID*: 基本 IPv6 ACL 的编号,范围(5000-5999)。

【使用举例】

```
# 进入编号为 5000 的基本 IPv6 ACL 视图
NOS# config acl 5000
NOS(acl-5000)#
```

【注意事项】

无。

### 63.2.3 config acl advanced-ipv4

【功能描述】

**config acl** *ACLID* 命令用于进入指定编号的高级 IPv4 ACL 视图。

**no config acl** *ACLID* 命令用于删除指定编号的高级 IPv4 ACL 视图及视图下的所有配置。

**no config acl advanced-ipv4** 命令用于删除编号范围在(3000-3999)间所有高级 IPv4 ACL 视图及视图下的所有配置。

【命令格式】

**config acl** *ACLID*

**no config acl** *ACLID*

**no config acl advanced-ipv4**

【视图】

根视图

【缺省情况】

不存在高级 IPv4 ACL。

【参数说明】

*ACLID*：高级 IPv4 ACL 的编号，范围(3000-3999)。

【使用举例】

# 进入编号为 3000 的基本 IPv4 ACL 视图

```
NOS# config acl 3000
NOS(acl-3000)#
```

【注意事项】

无。

### 63.2.4 config acl advanced-ipv6

【功能描述】

**config acl** *ACLID* 命令用于进入指定编号的高级 IPv6 ACL 视图。

**no config acl** *ACLID* 命令用于删除指定编号的高级 IPv6 ACL 视图及视图下的所有配置。

**no config acl advanced-ipv6** 命令用于删除编号范围在(6000-6999)间所有高级 IPv6 ACL 视图及视图下的所有配置。

【命令格式】

**config acl** *ACLID*

**no config acl** *ACLID*

**no config acl advanced-ipv6**

【视图】

根视图

【缺省情况】

不存在高级 IPv6 ACL。

【参数说明】

*ACLID*：高级 IPv6 ACL 的编号，范围(6000-6999)。

【使用举例】

# 进入编号为 6000 的基本 IPv6 ACL 视图

```
NOS# config acl 6000
NOS(acl-6000)#
```

【注意事项】

无。

### 63.2.5 config acl mac

【功能描述】

**config acl** *ACLID* 命令用于进入指定编号的二层 ACL 视图。

**no config acl** *ACLID* 命令用于删除指定编号的二层 ACL 视图及视图下的所有配置。

**no config acl mac** 命令用于删除编号范围在(4000-4999)间所有二层 ACL 视图及视图下的所有配置。

【命令格式】

**config acl** *ACLID*

**no config acl** *ACLID*

**no config acl mac**

【视图】

根视图

【缺省情况】

不存在二层 ACL。

【参数说明】

*ACLID*：二层 ACL 的编号，范围(4000-4999)。

【使用举例】

```
# 进入编号为 4000 的二层 ACL 视图
NOS# config acl 4000
NOS(acl-4000)#
```

【注意事项】

无。

### 63.2.6 config acl user-defined

【功能描述】

**config acl** *ACLID* 命令用于进入指定编号的自定义 ACL 视图。

**no config acl** *ACLID* 命令用于删除指定编号的自定义 ACL 视图及视图下的所有配置。

**no config acl user-defined** 命令用于删除编号范围在(7000-7999)间所有自定义 ACL 视图及视图下的所有配置。

【命令格式】

**config acl** *ACLID*

**no config acl** *ACLID*

**no config acl user-defined**

【视图】

根视图

【缺省情况】

不存在自定义 ACL。

【参数说明】

*ACLID*：自定义 ACL 的编号，范围(7000-7999)。

【使用举例】

```
# 进入编号为 7000 的自定义 ACL 视图
NOS# config acl 7000
NOS(acl-7000)#
```

【注意事项】

无。

### 63.2.7 rule basic ipv4

【功能描述】

**rule basic ipv4** 命令用于在指定编号的基本 IPv4 ACL 视图下配置规则。

**no rule** *RULEID* 命令用于在指定编号的基本 IPv4/基本 IPv6/高级 IPv4/高级 IPv6/二层/自定义 ACL 视图下，删除指定规则编号的规则。

【命令格式】

**rule** [*RULEID*] <**deny**|**permit**> **source** [*A.B.C.D* [*A.B.C.D*]] [**time-range** *NAME*]

**no rule** *RULEID*

【视图】

基本 IPv4 ACL 视图

【缺省情况】

不存在基本 IPv4 的规则。

【参数说明】

- *RULEID*：规则编号，范围(0-2047)。如果未输入规则编号，则规则编号取值，首次为 0，非首次为现有最大编号加上步长的值。如果输入规则编号，且该规则的配置存在，则覆盖原配置。
- **deny**：符合条件的报文拒绝通过。
- **permit**：符合条件的报文允许通过。
- **source** [*A.B.C.D* [*A.B.C.D*]]：源 IPv4 地址及掩码，掩码缺省值为 255.255.255.255；如果未输入 IPv4 地址，表示匹配所有 IPv4 报文。
- **time-range** *NAME*：生效时间范围对应的名字。

【使用举例】

# 创建一条基本 IPv4 规则

```
NOS# config acl 2001
NOS(acl-2001)# rule deny source 192.168.1.0 255.255.255.0
```

【注意事项】

无。

### 63.2.8 rule basic ipv6

【功能描述】

**rule basic ipv6** 命令用于在指定编号的基本 IPv6 ACL 视图下配置规则。

**no rule** *RULEID* 命令用于在指定编号的基本 IPv4/基本 IPv6/高级 IPv4/高级 IPv6/二层/自定义 ACL 视图下，删除指定规则编号的规则。

【命令格式】

**rule** [*RULEID*] <**deny**|**permit**> **source** [*X:X::X:X* [*IPSAMASK*]] [**time-range** *NAME*]

**no rule** *RULEID*

【视图】

基本 IPv6 ACL 视图

【缺省情况】

不存在基本 IPv6 的规则。

【参数说明】

- *RULEID*：规则编号，范围(0-2047)。如果未输入规则编号，则规则编号取值，首次为 0，非首次为现有最大编号加上步长的值。如果输入规则编号，且该规则的配置存在，则覆盖原配置。
- **deny**：符合条件的报文拒绝通过。
- **permit**：符合条件的报文允许通过。
- **source** [*X:X::X:X* [*IPSAMASK*]]：源 IPv6 地址及掩码，掩码缺省值为 128，范围(0-128)；如果未输入 IPv6 地址，表示匹配所有 IPv6 报文。
- **time-range** *NAME*：生效时间范围对应的名字。

【使用举例】

# 创建一条基本 IPv6 规则

```
NOS# config acl 5001
NOS(acl-5001)# rule 24 deny source 2020::8 126
```

【注意事项】

无。

### 63.2.9 rule advanced ipv4

【功能描述】

**rule advanced ipv4** 命令用于在指定编号的高级 IPv4 ACL 视图下配置 IPv4 规则。

**no rule** *RULEID* 命令用于在指定编号的基本 IPv4/基本 IPv6/高级 IPv4/高级 IPv6/二层/自定义 ACL 视图下，删除指定规则编号的规则。

【命令格式】

**rule** [*RULEID*] <**deny**|**permit**> **ipv4** [{**destination** *A.B.C.D* [*A.B.C.D*] | **source** *A.B.C.D* [*A.B.C.D*] | **protocol** *PROTO* | **dscp** *DSCPPRI* | **fragment**}] [**time-range** *NAME*]

**no rule** *RULEID*

【视图】

高级 IPv4 ACL 视图

【缺省情况】

不存在高级 IPv4 的规则。

【参数说明】

- *RULEID*：规则编号，范围(0-2047)。如果未输入规则编号，则规则编号取值，首次为 0，非首次为现有最大编号加上步长的值。如果输入规则编号，且该规则的配置存在，则覆盖原配置。
- **deny**：符合条件的报文拒绝通过。
- **permit**：符合条件的报文允许通过。
- **ipv4**：如果输入的命令以 ipv4 结尾，表示匹配所有 IPv4 报文。
- **destination** [*A.B.C.D* [*A.B.C.D*]]：目的 IPv4 地址及掩码，掩码缺省值为 255.255.255.255。
- **source** [*A.B.C.D* [*A.B.C.D*]]：源 IPv4 地址及掩码，掩码缺省值为 255.255.255.255。
- **protocol** *PROTO*：IPv4 承载的协议类型，范围(0-255)。
- **dscp** *DSCPPRI*：DSCP 优先级，范围(0-63)。
- **fragment**：IPv4 分片报文，包含首片及后续分片。不包含非分片报文。
- **time-range** *NAME*：生效时间范围对应的名字。

【使用举例】

# 创建一条高级 IPv4 规则

```
NOS# config acl 3001
NOS(acl-3001)# rule 100 deny ipv4 destination 23.1.1.2 source 12.1.1.2 dscp 0 fragment
```

【注意事项】

无。

### 63.2.10 rule advanced ipv6

【功能描述】

**rule advanced ipv6** 命令用于在指定编号的高级 IPv6 ACL 视图下配置 IPv6 规则。

**no rule** *RULEID* 命令用于在指定编号的基本 IPv4/基本 IPv6/高级 IPv4/高级 IPv6/二层/自定义 ACL 视图下，删除指定规则编号的规则。

【命令格式】

**rule** [*RULEID*] <**deny**|**permit**> **ipv6** [{**destination** *X:X::X:X* [*IPDAMASK*] | **source** *X:X::X:X* [*IPSAMASK*] | **protocol** *PROTO* | **dscp** *DSCPPRI* | **fragment**}] [**time-range** *NAME*]

**no rule** *RULEID*

【视图】

高级 IPv6 ACL 视图

【缺省情况】

不存在高级 IPv6 的规则。

【参数说明】

- *RULEID*：规则编号，范围(0-2047)。如果未输入规则编号，则规则编号取值，首次为 0，非首次为现有最大编号加上步长的值。如果输入规则编号，且该规则的配置存在，则覆盖原配置。
- **deny**：符合条件的报文拒绝通过。
- **permit**：符合条件的报文允许通过。
- **Ipv6**：如果输入的命令以 ipv6 结尾，表示匹配所有 IPv6 报文。
- **destination** [*X:X::X:X* [*IPDAMASK*]]：目的 IPv6 地址及掩码，掩码缺省值为 128，范围(0-128)。
- **source** [*X:X::X:X* [*IPSAMASK*]]：源 IPv6 地址及掩码，掩码缺省值为 128，范围(0-128)。
- **protocol** *PROTO*：IPv6 承载的协议类型，范围(0-255)。
- **dscp** *DSCPPRI*：DSCP 优先级，范围(0-63)。
- **fragment**：IPv6 分片报文，包含首片及后续分片。不包含非分片报文。
- **time-range** *NAME*：生效时间范围对应的名字。

【使用举例】

# 创建一条高级 IPv6 规则

```
NOS# config acl 6001
NOS(acl-6001)# rule 123 deny ipv6 destination 2023::2 source 2012::2 protocol 89
```

【注意事项】

无。

### 63.2.11 rule advanced ipv4 tcp

【功能描述】

**rule advanced ipv4 tcp** 命令用于在指定编号的高级 IPv4 ACL 视图下配置 TCP 规则。

**no rule** *RULEID* 命令用于在指定编号的基本 IPv4/基本 IPv6/高级 IPv4/高级 IPv6/二层/自定义 ACL 视图下，删除指定规则编号的规则。

【命令格式】

**rule** [*RULEID*] <**deny**|**permit**> **tcp** [{**destination** *A.B.C.D* [*A.B.C.D*] | **source** *A.B.C.D* [*A.B.C.D*] | **dstport** <*DSTPORTVAL DSTPORTVAL* | eq *KNOWNL4PORT* > | **srcport** <*SRCPORTVAL SRCPORTVAL* | **eq** *KNOWNL4PORT*> | **dscp** *DSCPPRI* | **tcpflag** {**fin** *FINVAL* | **syn** *SYNVAL* | **rst** *RSTVAL* | **psh** *PSHVAL* | **ack** *ACKVAL* | **urg** *URGVAL*} | **fragment**}] [**time-range** *NAME*]

**no rule** *RULEID*

【视图】

高级 IPv4 ACL 视图

【缺省情况】

不存在高级 IPv4 的规则。

【参数说明】

*RULEID*：规则编号，范围(0-2047)。如果未输入规则编号，则规则编号取值，首次为 0，非首次为现有最大编号加上步长的值。如果输入规则编号，且该规则的配置存在，则覆盖原配置。

**deny**：符合条件的报文拒绝通过。

**permit**：符合条件的报文允许通过。

**tcp**：如果输入的命令以 tcp 结尾，表示匹配所有 IPv4 TCP 报文。

**Destination** *A.B.C.D* [*A.B.C.D*]：目的 IPv4 地址及掩码，掩码缺省值为 255.255.255.255。

**source** *A.B.C.D* [*A.B.C.D*]：源 IPv4 地址及掩码，掩码缺省值为 255.255.255.255。

**dstport** *DSTPORTVAL DSTPORTVAL*：TCP 承载的目的端口号范围，包含两端值，每端取值范围(0-65535)。

**srcport** *SRCPORTVAL SRCPORTVAL*：TCP 承载的源端口号范围，包含两端值，每端取值范围(0-65535)。

*KNOWNL4PORT*：知名端口号。

*DSCPPRI*：DSCP 优先级范围(0-63)。

**tcpflag** {**fin** *FINVAL* | **syn** *SYNVAL* | **rst** *RSTVAL* | **psh** *PSHVAL* | **ack** *ACKVAL* | **urg** *URGVAL*}：TCP 报文标识，与 TCP 报文中的 ACK、FIN、PSH、RST、SYN 和 URG 六种标识相对应。取值为 0 或 1，不输入的标识则不关心。

**fragment**：分片报文，包含首片及后续分片。不包含非分片报文。

**time-range** *NAME*：生效时间范围对应的名字。

【使用举例】

# 创建一条高级 IPv4 TCP 规则

```
NOS# config acl 3001
NOS(acl-3001)# rule 105 deny tcp destination 34.1.1.3 source 23.1.1.3 dstport 2000 2000 srcport 1000 1000 tcpflag syn 0 rst 1
```

【注意事项】

部分产品，源/目的端口号的 ACL 规则有数量限制。

### 63.2.12 rule advanced ipv6 tcp

【功能描述】

**rule advanced ipv6 tcp** 命令用于在指定编号的高级 IPv6 ACL 视图下配置 TCP 规则。

**no rule** *RULEID* 命令用于在指定编号的基本 IPv4/基本 IPv6/高级 IPv4/高级 IPv6/二层/自定义 ACL 视图下，删除指定规则编号的规则。

【命令格式】

**rule** [*RULEID*] <**deny**|**permit**> **tcp** [{**destination** *X:X::X:X* [*IPDAMASK*] | **source** *X:X::X:X* [*IPSAMASK*] | **dstport** <*DSTPORTVAL DSTPORTVAL* | **eq** *KNOWNL4PORT* > | **srcport** <*SRCPORTVAL SRCPORTVAL* | **eq** *KNOWNL4PORT*> | **dscp** *DSCPPRI* | **tcpflag** {**fin** *FINVAL* | **syn** *SYNVAL* | **rst** *RSTVAL* | **psh** *PSHVAL* | **ack** *ACKVAL* | **urg** *URGVAL*} | **fragment**}] [**time-range** *NAME*]

**no rule** *RULEID*

【视图】

高级 IPv6 ACL 视图

【缺省情况】

不存在高级 IPv6 的规则。

【参数说明】

- *RULEID*：规则编号，范围(0-2047)。如果未输入规则编号，则规则编号取值，首次为 0，非首次为现有最大编号加上步长的值。如果输入规则编号，且该规则的配置存在，则覆盖原配置。
- **deny**：符合条件的报文拒绝通过。
- **permit**：符合条件的报文允许通过。
- **tcp**：如果输入的命令以 tcp 结尾，表示匹配所有 IPv6 TCP 报文。
- **destination** [*X:X::X:X* [*IPDAMASK*]]：目的 IPv6 地址及掩码，掩码缺省值为 128，范围(0-128)。
- **source** [*X:X::X:X* [*IPSAMASK*]]：源 IPv6 地址及掩码，掩码缺省值为 128，范围(0-128)。
- **dstport** *DSTPORTVAL DSTPORTVAL* ：TCP 承载的目的端口号范围，包含两端值,每端取值范围(0-65535)。
- **srcport** *SRCPORTVAL SRCPORTVAL*：TCP 承载的源端口号范围，包含两端值,每端取值范围(0-65535)。
- *KNOWNL4PORT*：知名端口号。
- *DSCPPRI*：DSCP 优先级范围(0-63)。
- **tcpflag** [**fin** *FINVAL*] [**syn** *SYNVAL*] [**rst** *RSTVAL*] [**psh** *PSHVAL*] [**ack** *ACKVAL*] [**urg** *URGVAL*]：TCP 报文标识，与 TCP 报文中的 ACK、FIN、PSH、RST、SYN 和 URG 六种标识相对应。取值为 0 或 1，不输入的标识则不关心。
- **fragment**：分片报文，包含首片及后续分片。不包含非分片报文。
- **time-range** *NAME*：生效时间范围对应的名字。

【使用举例】

# 创建一条高级 IPv6 TCP 规则

```
NOS# config acl 6002
NOS(acl-6002)# rule 128 deny tcp destination 2034:: 126 source 2023::3 srcport 0 65535
```

【注意事项】

部分产品，源/目的端口号的 ACL 规则有数量限制。

### 63.2.13 rule advanced ipv4 udp

【功能描述】

**rule advanced ipv4 udp** 命令用于在指定编号的高级 IPv4 ACL 视图下配置 UDP 规则。

**no rule** *RULEID* 命令用于在指定编号的基本 IPv4/基本 IPv6/高级 IPv4/高级 IPv6/二层/自定义 ACL 视图下，删除指定规则编号的规则。

【命令格式】

**rule** [*RULEID*] <**deny**|**permit**> **udp** [{**destination** *A.B.C.D* [*A.B.C.D*] | **source** *A.B.C.D* [*A.B.C.D*] | **dstport** <*DSTPORTVAL DSTPORTVAL* | **eq** *KNOWNL4PORT* > | **srcport** <*SRCPORTVAL SRCPORTVAL* | **eq** *KNOWNL4PORT* > | **dscp** *DSCPPRI* | **fragment**}] [**time-range** *NAME*]

**no rule** *RULEID*

【视图】

高级 IPv4 ACL 视图

【缺省情况】

不存在高级 IPv4 的规则。

【参数说明】

- *RULEID*：规则编号，范围(0-2047)。如果未输入规则编号，则规则编号取值，首次为 0，非首次为现有最大编号加上步长的值。如果输入规则编号，且该规则的配置存在，则覆盖原配置。
- **deny**：符合条件的报文拒绝通过。
- **permit**：符合条件的报文允许通过。
- **udp**：如果输入的命令以 udp 结尾，表示匹配所有 IPv4 UDP 报文。
- **destination** [*A.B.C.D* [*A.B.C.D*]]：目的 IPv4 地址及掩码，掩码缺省值为 255.255.255.255。
- **source** [*A.B.C.D* [*A.B.C.D*]]：源 IPv4 地址及掩码，掩码缺省值为 255.255.255.255。
- **dstport** *DSTPORTVAL DSTPORTVAL*：TCP 承载的目的端口号范围，包含两端值,每端取值范围(0-65535)。
- **srcport** *SRCPORTVAL SRCPORTVAL*：TCP 承载的源端口号范围，包含两端值,每端取值范围(0-65535)。
- *KNOWNL4PORT*：知名端口号。
- *DSCPPRI*：DSCP 优先级范围(0-63)。
- **fragment**：分片报文，包含首片及后续分片。不包含非分片报文。
- **time-range** *NAME*：生效时间范围对应的名字。

【使用举例】

# 创建一条高级 IPv4 UDP 规则

```
NOS# config acl 3001
NOS(acl-3001)# rule 110 deny udp destination 45.1.1.4 source 34.1.1.4 dstport 10000 20000
```

【注意事项】

部分产品，源/目的端口号的 ACL 规则有数量限制。

### 63.2.14 rule advanced ipv6 udp

【功能描述】

**rule advanced ipv6 udp** 命令用于在指定编号的高级 IPv6 ACL 视图下配置 UDP 规则。

**no rule** *RULEID* 命令用于在指定编号的基本 IPv4/基本 IPv6/高级 IPv4/高级 IPv6/二层/自定义 ACL 视图下，删除指定规则编号的规则。

【命令格式】

**rule** [*RULEID*] <**deny**|**permit**> **udp** [{**destination** *X:X::X:X* [*IPDAMASK*] | **source** *X:X::X:X* [*IPSAMASK*] | **dstport** <*DSTPORTVAL DSTPORTVAL* | **eq** *KNOWNL4PORT*> | **srcport** <*SRCPORTVAL SRCPORTVAL* | **eq** *KNOWNL4PORT*> | **dscp** *DSCPPRI* | **fragment**}] [**time-range** *NAME*]

**no rule** *RULEID*

【视图】

高级 IPv6 ACL 视图

【缺省情况】

不存在高级 IPv6 的规则。

【参数说明】

- *RULEID*：规则编号，范围(0-2047)。如果未输入规则编号，则规则编号取值，首次为 0，非首次为现有最大编号加上步长的值。如果输入规则编号，且该规则的配置存在，则覆盖原配置。
- **deny**：符合条件的报文拒绝通过。
- **permit**：符合条件的报文允许通过。
- **udp**：如果输入的命令以 udp 结尾，表示匹配所有 IPv6 UDP 报文。
- **destination** [*X:X::X:X* [*IPDAMASK*]]：目的 IPv6 地址及掩码，掩码缺省值为 128，范围(0-128)。
- **source** [*X:X::X:X* [*IPSAMASK*]]：源 IPv6 地址及掩码，掩码缺省值为 128，范围(0-128)。
- **dstport** *DSTPORTVAL DSTPORTVAL* ：TCP 承载的目的端口号范围，包含两端值,每端取值范围(0-65535)。
- **srcport** *SRCPORTVAL SRCPORTVAL*：TCP 承载的源端口号范围，包含两端值,每端取值范围(0-65535)。
- *KNOWNL4PORT*：知名端口号。
- *DSCPPRI*：DSCP 优先级范围(0-63)。
- **fragment**：分片报文，包含首片及后续分片。不包含非分片报文。
- **time-range** *NAME*：生效时间范围对应的名字。

【使用举例】

# 创建一条高级 IPv6 UDP 规则

```
NOS# config acl 6003
NOS(acl-6003)# rule permit udp destination 2040::2 fragment
```

【注意事项】

部分产品，源/目的端口号的 ACL 规则有数量限制。

### 63.2.15 rule mac

【功能描述】

**rule mac** 命令用于在指定编号二层 ACL 视图下配置规则。

**no rule** *RULEID* 命令用于在指定编号的基本 IPv4/基本 IPv6/高级 IPv4/高级 IPv6/二层/自定义 ACL 视图下，删除指定规则编号的规则。

【命令格式】

**rule** [*RULEID*] <**deny**|**permit**> **mac** [{**destination** *X:X:X:X:X:X* [*X:X:X:X:X:X*] | **source** *X:X:X:X:X:X* [*X:X:X:X:X:X*] | **ethtype** *ETHTYPE* | **vlan** *VLANID* | **cos** *COSVAL*}] [**time-range** *NAME*]

**no rule** *RULEID*

【视图】

二层 ACL 视图

【缺省情况】

不存在二层的规则。

【参数说明】

- *RULEID*：规则编号，范围(0-2047)。如果未输入规则编号，则规则编号取值，首次为 0，非首次为现有最大编号加上步长的值。如果输入规则编号，且该规则的配置存在，则覆盖原配置。
- **deny**：符合条件的报文拒绝通过。
- **permit**：符合条件的报文允许通过。
- **mac**：如果输入的命令以 mac 结尾，表示匹配所有二层报文。
- **destination** *X:X:X:X:X:X* [*X:X:X:X:X:X*]：目的 MAC 地址及掩码，掩码缺省值为 FF:FF:FF:FF:FF:FF。
- **source** *X:X:X:X:X:X* [*X:X:X:X:X:X*]：源 MAC 地址及掩码，掩码缺省值为 FF:FF:FF:FF:FF:FF。
- **ethtype** *ETHTYPE*：数据链路层协议类型。
- *VLANID*：最外层 VLAN ID,范围(0-4095)。
- *COSVAL*：最外层 CoS 优先级范围(0-7)。
- **time-range** *NAME*：生效时间范围对应的名字。

【使用举例】

# 创建一条高级 IPv4 UDP 规则

```
NOS# config acl 4999
NOS(acl-4999)# rule deny mac destination 78:b6:01:00:00:00 fe:ff:ff:00:00:00 ethtype 88b7
vlan 1
```

【注意事项】

部分产品，二层 ACL 规则对 IPv6 报文不生效。可以通过配置 QoS 策略来规避此问题。

### 63.2.16 rule user-defined

【功能描述】

**rule** User-Defined 命令用于在指定编号自定义 ACL 视图下配置规则。

**no rule** *RULEID* 命令用于在指定编号的基本 IPv4/基本 IPv6/高级 IPv4/高级 IPv6/二层/自定义 ACL 视图下，删除指定规则编号的规则。

【命令格式】

**rule** [*RULEID*] <**deny**|**permit**> **l2-head** *RULE MASK OFFSET* [**time-range** *NAME*]

**no rule** *RULEID*

【视图】

自定义 ACL 视图

【缺省情况】

不存在自定义 ACL 规则。

【参数说明】

- *RULEID*：规则编号，范围(0-2047)。如果未输入规则编号，则规则编号取值，首次为 0，非首次为现有最大编号加上步长的值。如果输入规则编号，且该规则的配置存在，则覆盖原配置。
- *RULE*： 用户需要匹配的数据，必须以 0x 开头的十六进制且长度为 2 的倍数
- *MASK*： 用户需要匹配的数据的掩码，必须以 0x 开头的十六进制且长度为 2 的倍数
- *OFFSET*：从 12 层头部匹配的偏移位置,范围(0-112)。
- **time-range** *NAME*：生效时间范围对应的名字。

【使用举例】

# 创建一条匹配目的 mac 为 00:11:94:00:00:02 的规则

```
NOS# config acl 7000
NOS(acl-7000)# rule deny l2-head 0x001194000002 0xffffffffffff 0
```

【注意事项】

OFFSET 必须是 4 的倍数。

RULE,MASK,必须是以 0x 开头的 16 进制的字符串，最大长度为 16 个字节，并且长度为 2 的倍数。

### 63.2.17 rule step

【功能描述】

**rule step** 命令用于在基本 IPv4/基本 IPv6/高级 IPv4/高级 IPv6/二层/自定义 ACL 视图下，配置规则编号的步长。

**no rule step** 命令用于在指定编号的基本 IPv4/基本 IPv6/高级 IPv4/高级 IPv6/二层/自定义 ACL 视图下，恢复规则编号的缺省步长，为 5。

【命令格式】

**step** *STEPLENGTH* [**update** [**start** *RULEID*]]

**no step**

【视图】

基本 IPv4/基本 IPv6/高级 IPv4/高级 IPv6/二层/自定义 ACL 视图

【缺省情况】

不存在规则编号的步长配置，规则编号的步长缺省值为 5，起始规则编号的缺省值为 0。

【参数说明】

*STEPLENGTH* ：规则编号的步长，范围(1-20)。

**update**：对于本 ACL 已存在的所有规则，更新规则编号。无此关键字，表示不更新。

*RULEID*：起始规则编号，范围(0-100)。

【使用举例】

# 更新 ACL 的规则编号的步长

```
NOS# config acl 4999
NOS(acl-4999)# step 8 update start 96
```

【注意事项】

无。

### 63.2.18 copy acl

【功能描述】

**copy acl** 命令用于复制并生成一个新的 ACL。

【命令格式】

**copy acl** SRC*ACLID* to DST*ACLID*

【视图】

根视图

【缺省情况】

无。

【参数说明】

**copy acl** SRC*ACLID* to DST*ACLID*：前者为源 ACL 编号，后者为目的 ACL 编号。

【使用举例】

```
# 复制并生成一个新的 ACL
NOS# copy acl 2000 to 2001
```

【注意事项】

- 源 ACL 与目的 ACL 的类型必须相同。
- 源 ACL 必须已存在。
- 目的 ACL 必须不存在。

### 63.2.19 config acl global

【功能描述】

**config acl global** 命令用于进入全局 ACL 视图。在全局 ACL 视图下应用的 ACL，对于任何端口都生效。

【命令格式】

**config acl global**

【视图】

根视图

【缺省情况】

无全局 ACL 配置。

【参数说明】

无。

【使用举例】

```
# 进入全局 ACL 视图
NOS# config acl global
NOS(acl-global)#
```

【注意事项】

无。

### 63.2.20 acl apply

【功能描述】

**acl apply** 命令用于应用 ACL。

在端口对应的二层以太网接口视图下应用的 ACL，仅对该端口生效。

在全局 ACL 视图下应用的 ACL，对任何端口都生效。

在 VLAN 视图下应用的 ACL，对 VLAN 所有成员口都生效。

【命令格式】

**acl** *ACLID* <**inbound**|**outbound**>

**no acl** *ACLID* <**inbound**|**outbound**>

【视图】

二层以太网接口视图，或全局 ACL 视图，或 VLAN 视图

【缺省情况】

无 ACL 应用。

【参数说明】

*ACLID*：应用的 ACL 编号，范围(2000-7999)。

**inbound**：对收到的报文应用 ACL。

**outbound**：对发出的报文应用 ACL。

【使用举例】

# 应用 ACL

```
NOS# config interface fe1
NOS(if-fe1)# acl 3999 inbound
```

【注意事项】

- ACL 的应用类型有 IPv4/IPv6/二层/自定义这四种。
- 每个端口，每个方向，每种应用类型，只能应用一个 ACL。
- 全局 ACL，每个方向，每种应用类型，只能应用一个 ACL。
- 端口 ACL，优先级高于全局 ACL。
- 对于不同的 ACL 应用类型，优先级由高到低依次为：IPv4、IPv6、二层、自定义。
- 仅 IPv4 基础/高级 ACL 可在 VLAN 视图下下发。

### 63.2.21 acl show basic ipv4

【功能描述】

显示基本 IPV4 ACL 的配置情况。

【命令格式】

**show acl ipv4 basic** [*ACLID*] [**json**]

【视图】

全局视图

【缺省情况】

无。

【参数说明】

- *ACLID* ：基本 IPv4 ACL 的编号，范围(2000-2999)。

- **json**：以 json 格式显示。

【使用举例】

```
NOS# show acl ipv4 basic
acl_2000:
        rule 0  permit source 1.1.1.1
```

【注意事项】

无。

### 63.2.22 acl show basic ipv6

【功能描述】

显示基本 IPV6 ACL 的配置情况。

【命令格式】

**show acl ipv6 basic** [*ACLID*] [**json**]

【视图】

全局视图

【缺省情况】

无。

【参数说明】

- *ACLID*: 基本 IPv6 ACL 的编号，范围(5000-5999)。
- **json**：以 json 格式显示。

【使用举例】

```
NOS# show  acl ipv6 basic
acl_5000:
        rule 0  permit source 1:1::1:1
```

【注意事项】

无。

### 63.2.23 acl show advanced ipv4

【功能描述】

显示高级 IPV4 ACL 的配置情况。

【命令格式】

**show acl ipv4 advance** [*ACLID*] [**json**]

【视图】

全局视图

【缺省情况】

无。

【参数说明】

*ACLID*: 高级 IPv4 ACL 的编号，范围(3000-3999)。

**json**：以 json 格式显示。

【使用举例】

```
NOS# show  acl ipv4 advance
acl_3000:
        rule 0  permit ipv4 destination 1.1.1.2
```

【注意事项】

无。

### 63.2.24 acl show advanced ipv6

【功能描述】

显示高级 IPV6 ACL 的配置情况。

【命令格式】

**show acl ipv6 advanced** [*ACLID*] [**json**]

【视图】

全局视图

【缺省情况】

无。

【参数说明】

*ACLID*: 高级 IPv6 ACL 的编号，范围(6000-6999)。

**json**：以 json 格式显示。

【使用举例】

```
NOS# show  acl ipv6 advance
acl_6000:
        rule 0  permit ipv6 destination 1:1::1:2
```

【注意事项】

无。

### 63.2.25 show acl mac

【功能描述】

显示 MAC ACL 的配置情况。

【命令格式】

**show acl mac** [*ACLID*] [**json**]

【视图】

全局视图

【缺省情况】

无。

【参数说明】

*ACLID*: MAC ACL 的编号，范围(4000-4999)。

**json**：以 json 格式显示。

【使用举例】

```
NOS# show  acl mac
```

```
acl_4000:
        rule 0  permit mac vlan 100
```

【注意事项】

无。

### 63.2.26 show acl user-defined

【功能描述】

显示自定义 ACL 的配置情况。

【命令格式】

**show acl user-defined** [*ACLID*] [**json**]

【视图】

全局视图

【缺省情况】

无。

【参数说明】

- *ACLID*：自定义 ACL 的编号，范围(7000-7999)。
- **json**：以 json 格式显示。

【使用举例】

```
NOS# show  acl user-defined
acl_7000:
        rule 0  permit l2-head 0x12 0x0f 12
```

【注意事项】

无。

### 63.2.27 show acl counters

【功能描述】

**show acl counters** 命令用于显示应用于端口或全局命中 ACL 的报文统计。

【命令格式】

**show acl counters** <**interface** *L2_ETH_IF*|*AGGREGATIONINTF*|**global**> <**inbound**|**outbound**> [**clear**]

【视图】

任意视图

【缺省情况】

无。

【参数说明】

- **interface** *L2_ETH_IF*：应用于端口的 ACL 规则。
- *AGGREGATIONINTF*：应用于聚合口的 ACL 规则。
- **global**：应用于全局的 ACL 规则。
- **inbound**：统计收到的 ACL 命中报文。
- **outbound**：统计发出的 ACL 命中报文。

- clear：清零报文统计。

【使用举例】

# 显示 ACL 的报文统计

```
Nos(ac1-global)# show acl counters global outbound
IPV4 ACL 2000
rule 0 deny source 1.1.1.2 (0 matches)
rule l deny source 1.1.1.1 (0 matches)
IPV6 ACL 6000
rule 0 deny ipv6 source 2025::1(0 matches)
MAC ACL 4000
rule o deny mac source 00:00:00:00:00:11(0 matches)
rule l deny mac van 777(0 matches)
```

【注意事项】

无。

## 63.3 配置举例

某公司内的各部门之间通过设备实现互连，通过配置，允许总裁办、财务部，访问财务数据库服务器，禁止其它部门访问该服务器。

```
NOS# config acl 3000
NOS(acl-3000)# rule permit ipv4 destination 192.168.0.100 source 192.168.1.0 255.255.255.0
NOS(acl-3000)# rule permit ipv4 destination 192.168.0.100 source 192.168.2.0 255.255.255.0
NOS(acl-3000)# rule deny ipv4 destination 192.168.0.100
NOS(acl-3000)# quit
NOS# config interface fe1
NOS(if-fe1)# acl 3999 outbound
```

## 63.4 常见问题

无。

# 64 QoS 策略

## 64.1 功能简介

### 64.1.1 QoS简介

QoS（Quality of Service）即服务质量。对于网络业务，影响服务质量的因素包括传输的带宽、传送的时延、数据的丢包率等。在网络中可以通过保证传输的带宽、降低传送的时延、降低数据的丢包率以及时延抖动等措施来提高服务质量。网络资源总是有限的，在保证某类业务的服务质量的同时，可能就是在损害其它业务的服务质量。因此，网络管理者需要根据各种业务的特点来对网络资源进行合理的规划和分配，从而使网络资源得到高效利用。

### 64.1.2 QoS策略简介

QoS 策略由如下部分组成：

- 流分类：定义对报文进行识别的规则。
- 流行为：为符合流分类的报文，指定流量控制或资源分配的动作。
- 流策略：将指定的流分类和指定的流行为绑定，形成完整的策略。
- 应用流策略：将流策略应用到端口，或应用为全局流策略。

## 64.2 命令手册

### 64.2.1 config qos policy

【功能描述】

**config qos policy** 命令用于进入 QoS 策略视图。

【命令格式】

**config qos policy**

**no config qos policy**

【视图】

根视图

【缺省情况】

不存在 QoS 策略。

【参数说明】

无。

【使用举例】

```
# 进入 QoS 策略视图
NOS# config qos policy
NOS(qos-policy)#
# 删除 QoS 策略视图下的所有配置,包括已绑定的配置
NOS# no config qos policy
```

【注意事项】

无。

### 64.2.2 class name

【功能描述】

**class** *NAME* 命令用于进入指定名称的流分类视图。

**no class** *NAME* 命令用于删除指定名称的流分类视图及视图下的所有配置。

【命令格式】

**class** *NAME* [**mode** <**or**|**and**>]

**no class** *NAME*

【视图】

QoS 策略视图

【缺省情况】

不存在流分类。

【参数说明】

- **class** *NAME*：流分类的名称，不超过 15 个字符，合法字符的范围：A-Z，a-z，_，0-9。
- **mode**：在流分类视图下配置的各规则之间的逻辑关系，缺省情况为“或”类型流分类。
- **or**：“或”类型流分类。
- **and**：“与”类型流分类。

【使用举例】

```
# 进入指定名称的“或”类型流分类视图
NOS(qos-policy)# class a1 mode or
NOS(qos-policy/class-or-a1)# quit
# 进入指定名称的“与”类型流分类视图
NOS(qos-policy)# class a2 mode and
NOS(qos-policy/class-and-a2)#
```

【注意事项】

无。

### 64.2.3 match acl (class mode or view)

【功能描述】

**match acl** 命令，用于使用 ACL 实现“或”类型流分类的功能。

在“或”类型流分类视图下，可以配置多个 ACL，每个 ACL 中可以配置多个规则。流分类的计算结果为：所有 ACL 下的规则相“或”。

ACL 中配置规则的方法请参考《ACL 用户手册》。

【命令格式】

**match acl** *ACLID*

**no match acl** *ACLID*

【视图】

“或”类型流分类视图。

【缺省情况】

不存在“或”类型流分类。

【参数说明】

**acl** *ACLID*：ACL 编号(2000-6999)。

【使用举例】

# 创建一个流分类，匹配所有的 OSPF 报文、ISIS 报文、ARP 报文。

```
NOS# config acl 3501
NOS(acl-3501)# rule permit ipv4 protocol 89
NOS(acl-3501)# quit
NOS# config acl 6501
NOS(acl-6501)# rule permit ipv6 protocol 89
NOS(acl-6501)# quit
NOS# config acl 4501
NOS(acl-4501)# rule permit mac destination 01:80:c2:00:00:14 ff:ff:ff:ff:ff:fe
NOS(acl-4501)# rule permit mac destination 09:00:2b:00:00:05
NOS(acl-4501)# quit
NOS# config acl 4502
NOS(acl-4502)# rule permit mac ethtype 0806
NOS(acl-4502)# quit
NOS# config qos policy
NOS(qos-policy)# class fwd1 mode or
NOS(qos-policy/class-or-fwd1)# match acl 3501
NOS(qos-policy/class-or-fwd1)# match acl 6501
NOS(qos-policy/class-or-fwd1)# match acl 4501
NOS(qos-policy/class-or-fwd1)# match acl 4502
```

【注意事项】

无。

### 64.2.4 match acl (class mode and view)

【功能描述】

**match acl** 命令，用于使用 ACL 实现“与”类型流分类的功能。

在“与”类型流分类视图下，只能配置一个 ACL，这个 ACL 中可以配置多个规则。

流分类的计算结果为：这一个 ACL 中的各个规则，和本“与”类型流分类下其他非 ACL 配置，分别相“与”。

例如：ACL 3601 中配置了 2 条规则，分别为：匹配 IGMP 报文、匹配 PIMv4 报文；在“与”类型流分类视图下，配置了 match acl 3601，还配置了 match mac vlan 1。流分类的计算结果为：共 2 条规则：一条为匹配 VLAN 1 的 IGMP 报文；另一条为匹配 VLAN 1 的 PIMv4 报文。这 2 条规则是逻辑“或”的关系。

ACL 中配置规则的方法请参考《ACL 用户手册》。“与”类型流分类下其他非 ACL 配置，参考本文后续章节。

【命令格式】

**match acl** *ACLID*

**no match acl**

【视图】

“与”类型流分类视图

【缺省情况】

不存在“与”类型流分类。

【参数说明】

**acl** *ACLID*：ACL 编号(2000-6999)。

【使用举例】

# 创建一个流分类，匹配 VLAN 1 的报文 IGMP 报文，和 VLAN 1 的 PIMv4 报文。

```
NOS# config acl 3601
NOS(acl-3601)# rule permit ipv4 protocol 2
NOS(acl-3601)# rule permit ipv4 protocol 103
NOS(acl-3601)# quit
NOS# config qos policy
NOS(qos-policy)# class fwd2 mode and
NOS(qos-policy/class-and-fwd2)# match acl 3601
NOS(qos-policy/class-and-fwd2)# match mac vlan 1
```

【注意事项】

无。

### 64.2.5 match mac (class mode and view)

【功能描述】

**match mac** 命令，用于配合 ACL 实现“与”类型流分类的功能。match mac 命令可以匹配报文的二层特征，match acl 命令可以匹配报文的三层特征及四层特征，二者组合，可以实现匹配报文的二三四层特征。在“与”类型流分类视图下，只能配置一条 match acl 命令。

【命令格式】

**match mac** {**destination** X:X:X:X:X:X [X:X:X:X:X:X] | **source** X:X:X:X:X:X [X:X:X:X:X:X] | [**vlan** *VID*] | **cos** *COSVAL*}

**no match mac**

【视图】

“与”类型流分类视图

【缺省情况】

不存在“与”类型流分类。

【参数说明】

- **destination** X:X:X:X:X:X [X:X:X:X:X:X]：目的 MAC 地址及掩码，掩码缺省值为 FF:FF:FF:FF:FF:FF。
- **source** X:X:X:X:X:X [X:X:X:X:X:X]：源 MAC 地址及掩码，掩码缺省值为 FF:FF:FF:FF:FF:FF。
- **ethtype** *ETHTYPE*：数据链路层协议类型。
- **vlan** *VID*：最外层 VLAN ID(1-4094)。
- **cos** *COSVAL*：最外层 CoS 优先级(0-7)。

【使用举例】

# 创建一个流分类，匹配目的 MAC 为 33:33:00:00:00:05 的 OSPFv3 报文。

```
NOS# config acl 6501
NOS(acl-6501)# rule permit ipv6 protocol 89
```

```
NOS(acl-6501)# quit
NOS# config qos policy
NOS(qos-policy)# class fwd3 mode and
NOS(qos-policy/class-and-fwd3)# match acl 6501
NOS(qos-policy/class-and-fwd3)# match mac destination 33:33:00:00:00:05
```

【注意事项】

在一个“与”类型流分类视图下，仅配置 match mac 命令，未配置 match acl 命令，则流分类的计算结果为空。原因为“与”类型流分类的计算结果为：ACL 中的各个规则，与 match mac 设置的规则分别相“与”，如果 ACL 中规则为空，那么流分类的计算结果也为空。

### 64.2.6 Action-set name

【功能描述】

**action-set** *NAME* 命令用于进入指定名称的流行为视图。

**no action-set** *NAME* 命令用于删除指定名称的流行为视图及视图下的所有配置。

【命令格式】

**action-set** *NAME*

**no action-set** *NAME*

【视图】

QoS 策略视图

【缺省情况】

不存在流行为。

【参数说明】

**action-set** *NAME*：流行为的名称，不超过 15 个字符，合法字符的范围：A-Z, a-z, _, 0-9。

【使用举例】

```
# 进入指定名称的流行为视图
NOS(qos-policy)# action-set b1
NOS(qos-policy/action-set-b1)#
```

【注意事项】

无。

### 64.2.7 action permit

【功能描述】

**action permit** 命令，用于实现符合条件的报文允许通过的流行为。

【命令格式】

**action permit**

**no action permit**

【视图】

流行为视图

【缺省情况】

不存在流行为。

【参数说明】

**permit**：符合条件的报文允许通过。

【使用举例】

```
# 创建一个流行为，动作是 permit。
NOS(qos-policy)# action-set b2
NOS(qos-policy/action-set-b2)# action permit
```

【注意事项】

action permit、action deny、action mirror、action redirect，这四种流行为是互斥关系。

### 64.2.8 action deny

【功能描述】

**action deny** 命令，用于实现符合条件的报文拒绝通过的流行为。

【命令格式】

**action deny**

**no action deny**

【视图】

流行为视图

【缺省情况】

不存在流行为。

【参数说明】

**deny**：符合条件的报文拒绝通过。

【使用举例】

```
# 创建一个流行为，动作是 deny。
NOS(qos-policy)# action-set b3
NOS(qos-policy/action-set-b3)# action deny
```

【注意事项】

action permit、action deny、action mirror、action redirect，这四种流行为是互斥关系。

### 64.2.9 action mirror

【功能描述】

**action mirror** 命令，用于实现镜像符合条件的报文的流行为。

【命令格式】

**action mirror** <**interface** *PHY_IF* | **cpu**>

**no action mirror**

【视图】

流行为视图

【缺省情况】

不存在流行为。

【参数说明】

**mirror**：镜像符合条件的报文。

**interface** *PHY_IF*：镜像符合条件的报文至端口。

**cpu**：镜像符合条件的报文至 CPU。

【使用举例】

# 创建一个流行为，动作是镜像。

```
NOS(qos-policy)# action-set b4
NOS(qos-policy/action-set-b4)# action mirror interface ge19
```

【注意事项】

action permit、action deny、action mirror、action redirect，这四种流行为是互斥关系。

部分产品，镜像到端口的数量有限制。

### 64.2.10 action redirect

【功能描述】

**action redirect** 命令，用于实现重定向符合条件的报文的流行为。

【命令格式】

**action redirect** <**interface** *PHY_IF* | **cpu**>

**no action redirect**

【视图】

流行为视图

【缺省情况】

不存在流行为。

【参数说明】

- **redirect**：重定向符合条件的报文。
- **interface** *PHY_IF*：重定向符合条件的报文至端口。
- **cpu**：重定向符合条件的报文至 CPU。

【使用举例】

# 创建一个流行为，动作是重定向。

```
NOS(qos-policy)# action-set b5
NOS(qos-policy/action-set-b5)# action redirect interface ge8
```

【注意事项】

action permit、action deny、action mirror、action redirect，这四种流行为是互斥关系。

部分产品，只能重定向收到的报文，不能重定向发出的报文。

### 64.2.11 action remark

【功能描述】

**action remark** 命令，用于实现重标记符合条件的报文的流行为。

【命令格式】

**action remark** {**dscp** *DSCPVAL* | **vlan** *VID* |**cos** *COSVAL*}

**no action remark**

【视图】

流行为视图

【缺省情况】

不存在流行为。

【参数说明】

- **remark**：重标记符合条件的报文。
- **dscp** *DSCPVAL*：DSCP 优先级，范围(0-63)。
- **vlan** *VID*：最外层 VLAN ID，范围(1-4094)。
- **cos** *COSVAL*：最外层 CoS 优先级，范围(0-7)。

【使用举例】

# 创建一个流行为，动作是重标记。

```
NOS(qos-policy)# action-set b6
NOS(qos-policy/action-set-b6)# action remark vlan 4094 cos 2
```

【注意事项】

部分产品，只能重标记收到的报文，不能重标记发出的报文。

### 64.2.12 action car

【功能描述】

**action car** 命令，用于实现流量监管的流行为。

支持两种流量监管技术：

- RFC2697 单速双桶三色模型，参数为 cir [cbs [ebs]]。
- RFC2698 双速双桶三色模型，参数为 cir [cbs] pir [pbs]。

请参阅后文的限速与整形章节。

【命令格式】

**action car cir** *CIRVAL* [**cbs** *CBSVAL* [**ebs** *EBSVAL*]] [**pir** *PIRVAL* [**pbs** *PBSVAL*]]

**no action car**

【视图】

流行为视图

【缺省情况】

不存在流行为。

【参数说明】

- **car**：对符合条件的报文进行流量监管（Committed access rate）。
- **cir** *CIRVAL*：承诺信息速率，单位为 kbps，设置的值会模 10 取整，范围(10-10000000)。
- **cbs** *CBSVAL*：承诺突发尺寸，单位为 kbyte。若不输入，取值为 cir/16，范围(2-32768)。
- **ebs** *EBSVAL*：超出突发尺寸，单位为 kbyte。若不输入，取值为 cir/16，范围(2-32768)。
- **pir** *PIRVAL*：峰值信息速率，单位为 kbps，设置的值会模 10 取整，范围(10-10000000)。
- **pbs** *PBSVAL*：峰值突发尺寸，单位为 kbyte。若不输入，取值为 pir/16，范围(2-32768)。

【使用举例】

# 创建一个流行为，动作是流量监管。

```
NOS(qos-policy)# action-set b7
NOS(qos-policy/action-set-b7)# action car cir 100 pir 200
```

【注意事项】

- 部分产品，只能对收到的报文进行流量监管，不能对发出的报文进行流量监管。

- 参数范围随产品不同。

### 64.2.13 action rate-limit

【功能描述】

action rate-limit 命令，用于实现包限速的流行为。

【命令格式】

action rate-limit cir *CIRVAL*

no action rate-limit

【视图】

流行为视图

【缺省情况】

不存在流行为。

【参数说明】

- rate-limit：对符合条件的报文进行包限速。
- cir *CIRVAL*：承诺信息速率，单位为 pps，范围(1-10000)。

【使用举例】

```
# 创建一个流行为，动作是包限速。
NOS(qos-policy)# action-set b7
NOS(qos-policy/action-set-b7)# action rate-limit cir  200
```

【注意事项】

部分产只能对收到的报文进行包限速，不能对发出的报文进行包限速。

### 64.2.14 action set-queue

【功能描述】

action set-queue 命令，用于实现流量出方向队列控制的流行为。

【命令格式】

action  set-queue *QUEUEID*

no action set-queue

【视图】

流行为视图

【缺省情况】

不存在流行为。

【参数说明】

set-queue：对符合条件的报文进行出方向队列控制。

*QUEUEID*：出方向队列，范围(0-7)。

【使用举例】

```
# 创建一个流行为，动作是控制出方向队列。
NOS(qos-policy)# action-set b7
NOS(qos-policy/action-set-b7)# action set-queue 4
```

【注意事项】

无。

### 64.2.15 policy name

【功能描述】

**policy** *NAME* 命令用于进入指定名称的流策略视图。

**no policy** *NAME* 命令用于删除指定名称的流策略视图及视图下的所有配置。

【命令格式】

**policy** *NAME*

**no policy** *NAME*

【视图】

QoS 策略视图

【缺省情况】

不存在流策略。

【参数说明】

**policy** *NAME*：流策略的名称，不超过 15 个字符，合法字符的范围：A-Z，a-z，_，0-9。

【使用举例】

```
# 进入指定名称的流策略视图
NOS(qos-policy)# policy c1
NOS(qos-policy/policy-c1)#
```

【注意事项】

无。

### 64.2.16 sequence

【功能描述】

**sequence** 命令，用于将指定的流分类和指定的流行为绑定，形成完整的策略。

【命令格式】

**sequence** *SEQUENCEID* **class** *CLASSNAME* **action-set** *ACTIONNAME*

**no sequence** *SEQUENCEID*

【视图】

流策略视图

【缺省情况】

不存在流策略。

【参数说明】

- **sequence** *SEQUENCEID*：流策略的编号。编号越小，优先级越高，范围(0-127)。
- **class** *CLASSNAME*：流分类的名称。
- **action-set** *ACTIONNAME*：流行为的名称。

【使用举例】

```
# 创建一个流策略，绑定指定的流分类和指定的流行为。
NOS(qos-policy)# policy c1
```

```
NOS(qos-policy/policy-c1)# sequence 14 class a1 action-set b1
NOS(qos-policy/policy-c1)# sequence 18 class a2 action-set b2
```

【注意事项】

绑定流分类和流行为，并最终生效时，会忽略 ACL 中各规则的 permit 或 deny 行为。

### 64.2.17 config qos global-policy

【功能描述】

**config qos global-policy** 命令用于进入 QoS 策略全局应用视图。在 QoS 策略全局应用视图下应用的流策略，对于任何端口都生效。

【命令格式】

**config qos global-policy**

【视图】

根视图

【缺省情况】

无全局 QoS 策略。

【参数说明】

无。

【使用举例】

```
# 进入 QoS 策略全局应用视图
NOS# config qos global-policy
NOS(qos-policy-global)#
```

【注意事项】

无。

### 64.2.18 qos policy name

【功能描述】

**qos policy name** 命令用于应用 QoS 策略。

在端口对应的二层以太网接口视图下应用 QoS 策略，仅对该端口生效。

在全局 QoS 策略视图下应用 QoS 策略，对任何端口都生效。

【命令格式】

**qos policy name** *NAME* <**inbound**|**outbound**>

**no qos policy** <**inbound**|**outbound**>

【视图】

二层以太网接口视图，或全局 QoS 策略视图

【缺省情况】

无 QoS 策略应用。

【参数说明】

- **policy name** *NAME*：流策略的名称。
- **inbound**：对收到的报文应用 QoS 策略。
- **outbound**：对发出的报文应用 QoS 策略。

【使用举例】

```
# 应用 ACL
NOS# config interface fe1
NOS(if-fe1)# qos policy name c1 inbound
```

【注意事项】

- 每个端口，每个方向，只能应用一个 QoS 策略。
- 全局 QoS 策略，每个方向，只能应用一个 QoS 策略。
- 端口的 QoS 策略，优先级高于 QoS 策略。

### 64.2.19 qos policy acl

【功能描述】

**qos policy acl** 命令用于采用简易的方式，应用 QoS 策略。

在端口对应的二层以太网接口视图下应用 QoS 策略，仅对该端口生效。

在全局 QoS 策略视图下应用 QoS 策略，对任何端口都生效。

【命令格式】

**qos policy acl** *ACLID* <**inbound**|**outbound**> **action** <**permit** | **deny** | <**mirror** | **redirect**> <**interface** *PHY_IF* | **cpu**> | [**remark** {**dscp** *DSCPVAL*] | **vlan** *VID* | **cos** *COSVAL*} | **car cir** *CIRVAL* [**cbs** *CBSVAL* [**ebs** *EBSVAL*]] [**pir** *PIRVAL* [**pbs** *PBSVAL*]]>

**no qos policy** <**inbound**|**outbound**>

【视图】

二层以太网接口视图，或全局 QoS 策略视图

【缺省情况】

无 QoS 策略应用。

【参数说明】

- **acl** *ACLID*：ACL 编号，范围(2000-6999)。
- **inbound**：对收到的报文应用 QoS 策略。
- **outbound**：对发出的报文应用 QoS 策略。
- **permit**：符合条件的报文允许通过。
- **deny**：符合条件的报文拒绝通过。
- **mirror**：镜像符合条件的报文。
- **redirect**：重定向符合条件的报文。
- **interface** PHY_IF：镜像或重定向符合条件的报文至端口。
- **cpu**：镜像或重定向符合条件的报文至 CPU。
- **remark**：重标记符合条件的报文。
- **dscp** *DSCPVAL*：DSCP 优先级，范围(0-63)。
- **vlan** *VID*：最外层 VLAN ID，范围(1-4094)。
- **cos** *COSVAL*：最外层 CoS 优先级，范围(0-7)。
- **car**：对符合条件的报文进行流量监管（Committed access rate）。
- **cir** *CIRVAL*：承诺信息速率，单位为 kbps，设置的值会模 10 取整，范围(10-10000000)。
- **cbs** *CBSVAL*：承诺突发尺寸，单位为 kbyte。若不输入，取值为 cir/16，范围(2-32768)。
- **ebs** *EBSVAL*：超出突发尺寸，单位为 kbyte。若不输入，取值为 cir/16，范围(2-32768)。
- **pir** *PIRVAL*：峰值信息速率，单位为 kbps，设置的值会模 10 取整，范围(10-10000000)。

- **pbs** *PBSVAL*：峰值突发尺寸，单位为 kbyte。若不输入，取值为 pir/16，范围(2-32768)。

【使用举例】

# 将端口 1 收到的 ISIS 报文镜像到端口 2

```
NOS# config acl 4501
NOS(acl-4501)# rule permit mac destination 01:80:c2:00:00:14 ff:ff:ff:ff:ff:fe
NOS(acl-4501)# rule permit mac destination 09:00:2b:00:00:05
NOS# config interface fe1
NOS(if-fe1)# qos policy acl 4501 inbound action mirror interface fe2
```

【注意事项】

- 每个端口，每个方向，只能应用一个 QoS 策略。
- 全局 QoS 策略，每个方向，只能应用一个 QoS 策略。
- 端口的 QoS 策略，优先级高于 QoS 策略。
- qos policy acl 与 qos policy name 命令互斥，只能二选一。
- 部分产品，重定向、重标记、流量监管等流行为，仅能对收到的报文应用，不能对发出的报文应用。
- 流量监管动作参数范围随产品不同。

### 64.2.20 show qos policy counters

【功能描述】

**show qos policy counters** 命令用于显示应用于端口或全局的 QoS 策略的报文统计。

【命令格式】

**show qos policy counters** <**interface** *PHY_IF*|**global**> <**inbound**|**outbound**> [**clear**]

【视图】

任意视图

【缺省情况】

无。

【参数说明】

**interface** *PHY_IF*：应用于端口的 QoS 策略。

**global**：应用于全局的 QoS 策略。

**inbound**：统计收到的 QoS 策略报文。

**outbound**：统计发出的 QoS 策略报文。

**clear**：清零报文统计。

【使用举例】

# 显示 QoS 策略的报文统计

```
CTC# show acl qos counters interface ge17 inbound
 Acl   Rule             Packets               Bytes
 ----  ----  --------------------  --------------------
 3998     5                 625             750000
 3998    10                 625             750000
 3998    15                 625             750000
 3998    20                 625             750000
 3999     0                 625             750000
 3999     5                 625             750000
```

```
3999    15                625             750000
3999    20                625             750000
3997     5                625             750000
3997    10                625             750000
3997    15                625             750000
3997    20                625             750000
```

【注意事项】

无。

### 64.2.21 show qos policy car

【功能描述】

**show qos policy car** 命令用于显示应用于端口或全局的流量监管的报文统计。

【命令格式】

**show qos policy car** <**interface** *PHY_IF*|**global**> <**inbound**|**outbound**> [**clear**]

【视图】

任意视图

【缺省情况】

无。

【参数说明】

- **interface** *PHY_IF*：应用于端口的 QoS 策略。
- **global**：应用于全局的 QoS 策略。
- **inbound**：统计收到的流量监管报文。
- **outbound**：统计发出的流量监管报文。
- **clear**：清零流量监管报文统计。

【使用举例】

```
# 显示流量监管的报文统计
CTC# show acl qos car interface ge17 inbound
 Acl   Rule     Mode  Cir(kbps) Cbs(kB) Ebs(kB) Pir(kbps) Pbs(kB)
 ----  ----  -------  --------  ------  ------  --------  ------
 3998     5  RFC2698       100      22       0       300      34
 3998    10  RFC2698       100      22       0       300      34
 3998    15  RFC2698       100      22       0       300      34
 3998    20  RFC2698       100      22       0       300      34
 3999     0  RFC2698       100      22       0       300      34
 3999     5  RFC2698       100      22       0       300      34
 3999    15  RFC2698       100      22       0       300      34
 3999    20  RFC2698       100      22       0       300      34
 3997     5  RFC2698       100      22       0       300      34
 3997    10  RFC2698       100      22       0       300      34
 3997    15  RFC2698       100      22       0       300      34
 3997    20  RFC2698       100      22       0       300      34
 Acl   Rule      Confirm Packets       Exceed Packets      Violate Packets
 ----  ----  --------------------  --------------------  --------------------
 3998     5                 107                   209                   309
```

```
3998    10              107             209             309
3998    15              107             209             309
3998    20              107             209             309
3999     0              107             209             309
3999     5              107             209             309
3999    15              107             209             309
3999    20              107             209             309
3997     5              107             209             309
3997    10              107             209             309
3997    15              107             209             309
3997    20              107             209             309
```

| Acl | Rule | Confirm Bytes | Exceed Bytes | Violate Bytes |
|---|---|---|---|---|
| 3998 | 5 | 128400 | 250800 | 370800 |
| 3998 | 10 | 128400 | 250800 | 370800 |
| 3998 | 15 | 128400 | 250800 | 370800 |
| 3998 | 20 | 128400 | 250800 | 370800 |
| 3999 | 0 | 128400 | 250800 | 370800 |
| 3999 | 5 | 128400 | 250800 | 370800 |
| 3999 | 15 | 128400 | 250800 | 370800 |
| 3999 | 20 | 128400 | 250800 | 370800 |
| 3997 | 5 | 128400 | 250800 | 370800 |
| 3997 | 10 | 128400 | 250800 | 370800 |
| 3997 | 15 | 128400 | 250800 | 370800 |
| 3997 | 20 | 128400 | 250800 | 370800 |

【注意事项】

无。

## 64.3 配置举例

将目的 MAC 为 33:33:00:00:00:05 和 33:33:00:00:00:06 的 OSPFv3 报文，由端口 1 镜像到端口 2。

```
#ACL
NOS# config acl 6501
NOS(acl-6501)# rule permit ipv6 protocol 89
NOS(acl-6501)# quit
#流分类
NOS# config qos policy
NOS(qos-policy)# class fwd1 mode and
NOS(qos-policy/class-and-fwd1)# match acl 6501
NOS(qos-policy/class-and-fwd1)# match mac destination 33:33:00:00:00:05
NOS(qos-policy/class-and-fwd1)# quit
NOS(qos-policy)# class fwd2 mode and
NOS(qos-policy/class-and-fwd2)# match acl 6501
NOS(qos-policy/class-and-fwd2)# match mac destination 33:33:00:00:00:06
NOS(qos-policy/class-and-fwd1)# quit
#流行为
NOS(qos-policy)# action-set act
NOS(qos-policy/action-set-act)# action mirror interface fe2
```

```
NOS(qos-policy/action-set-act)# quit
#流策略
NOS(qos-policy)# policy ospf_mirror
NOS(qos-policy/policy-ospf_mirror)# sequence 5 class fwd1 action-set act
NOS(qos-policy/policy-ospf_mirror)# sequence 6 class fwd2 action-set act
NOS(qos-policy/policy-ospf_mirror)# quit
NOS(qos-policy)# quit
#应用
NOS# config interface fe1
NOS(if-fe1)# qos policy name ospf_mirror inbound
NOS(if-fe1)# qos policy name ospf_mirror outbound
```

## 64.4 常见问题

无。

# 65 优先级映射

## 65.1 功能简介

### 65.1.1 优先级映射简介

优先级映射可以将报文携带的优先级字段映射成指定优先级字段值，设备根据映射后的优先级字段，为报文提供有差别的 QoS 服务，从而为全面有效的控制报文的转发调度等级提供依据。

报文优先级（又称外部优先级）：报文自身携带的优先级信息。常见的报文优先级有 CoS(802.1p)优先级、DSCP 优先级等，这些优先级都有公认的标准和协议。

设备内部优先级（又称本地优先级）：对进入设备内部的数据报文给予一个内部优先级标记值，根据该值可在设备内部进行资源分配，比如选择队列等。

优先级映射是在设备内部，把报文携带的报文优先级与设备内部优先级做映射转换，从而使进入设备的报文在设备内部根据设备内部优先级提供有差别的 QoS 服务。

### 65.1.2 优先级信任模式

优先级信任模式，配置在端口上，用于对端口收到的报文，选择一个优先级映射表，来完成报文优先级与设备内部优先级的映射转换。如果未选择任何优先级映射表，设备会将收到报文的端口的一个固定优先级的值，作为报文的设备内部优先级。

## 65.2 命令手册

### 65.2.1 config qos map cos

【功能描述】

**config qos map cos** 命令用于进入 CoS 优先级映射表视图。

**no config qos map cos** 命令用于删除 CoS 优先级映射表，使用缺省的映射表数值。

【命令格式】

**config qos map cos**

**no config qos map cos**

【视图】

根视图

【缺省情况】

CoS 优先级与设备内部优先级的缺省映射表：

cos->local_priority

0->0 1->1 2->2 3->3 4->4 5->5 6->6 7->7

【参数说明】

无。

【使用举例】

# 进入 CoS 优先级映射表视图

```
NOS# config qos map cos
NOS(qos-map-cos)#
```

【注意事项】

无。

### 65.2.2 cos lp

【功能描述】

**cos lp** 命令，用于设置报文的 CoS 优先级与设备内部优先级的映射关系。

【命令格式】

**cos** *COSVAL* **lp** *LPVAL*

**no cos** *COSVAL*

【视图】

CoS 优先级映射表视图

【缺省情况】

未配置 CoS 优先级的索引，按照以下缺省值进行映射：

```
cos->local_priority
  0->0   1->1   2->2   3->3   4->4   5->5   6->6   7->7
```

【参数说明】

**cos** *COSVAL*：报文最外层 CoS 优先级，范围(0-7)。

**lp** *LPVAL*：设备内部优先级，范围(0-7)。

【使用举例】

```
# 设置 CoS 优先级映射。
NOS# config qos map cos
NOS(qos-map-cos)# cos 0 lp 2
```

【注意事项】

无。

### 65.2.3 config qos map dscp

【功能描述】

**config qos map dscp** 命令用于进入 DSCP 优先级映射表视图。

**no config qos map dscp** 命令用于删除 DSCP 优先级映射表，使用缺省的映射表数值。

【命令格式】

**config qos map dscp**

**no config qos map dscp**

【视图】

根视图

【缺省情况】

DSCP 优先级与设备内部优先级的缺省映射表：

```
dscp->local_priority
  0->0   1->0   2->0   3->0   4->0   5->0   6->0   7->0
  8->1   9->1  10->1  11->1  12->1  13->1  14->1  15->1
 16->2  17->2  18->2  19->2  20->2  21->2  22->2  23->2
```

24->3 25->3 26->3 27->3 28->3 29->3 30->3 31->3
32->4 33->4 34->4 35->4 36->4 37->4 38->4 39->4
40->5 41->5 42->5 43->5 44->5 45->5 46->5 47->5
48->6 49->6 50->6 51->6 52->6 53->6 54->6 55->6
56->7 57->7 58->7 59->7 60->7 61->7 62->7 63->7

【参数说明】

无。

【使用举例】

# 进入 DSCP 优先级映射表视图

```
NOS# config qos map dscp
NOS(qos-map-dscp)#
```

【注意事项】

无。

### 65.2.4 dscp lp

【功能描述】

**dscp lp** 命令，用于设置报文的 DSCP 优先级与设备内部优先级的映射关系。

【命令格式】

**dscp** *DSCPVAL* **lp** *LPVAL*

**no dscp** *DSCPVAL*

【视图】

DSCP 优先级映射表视图

【缺省情况】

未配置 DSCP 优先级的索引，按照以下缺省值进行映射：

dscp->local_priority
0->0 1->0 2->0 3->0 4->0 5->0 6->0 7->0
8->1 9->1 10->1 11->1 12->1 13->1 14->1 15->1
16->2 17->2 18->2 19->2 20->2 21->2 22->2 23->2
24->3 25->3 26->3 27->3 28->3 29->3 30->3 31->3
32->4 33->4 34->4 35->4 36->4 37->4 38->4 39->4
40->5 41->5 42->5 43->5 44->5 45->5 46->5 47->5
48->6 49->6 50->6 51->6 52->6 53->6 54->6 55->6
56->7 57->7 58->7 59->7 60->7 61->7 62->7 63->7

【参数说明】

**dscp** *DSCPVAL*：报文 DSCP 优先级，范围(0-63)。

**lp** *LPVAL*：设备内部优先级，范围(0-7)。

【使用举例】

# 设置 DSCP 优先级映射。

```
NOS# config qos map dscp
NOS(qos-map-dscp)# dscp 7 lp 1
```

【注意事项】

无。

### 65.2.5 qos port-priority

【功能描述】

**qos port-priority** 命令，用于设置端口的一个固定优先级的值。

【命令格式】

**qos port-priority** *PORTPRI*

**no qos port-priority**

【视图】

端口对应的二层以太网接口视图。

【缺省情况】

端口的一个固定优先级的值，缺省为 0。

【参数说明】

**port priority** *PORTPRI*：端口的一个固定优先级的值，范围(0-7)。

【使用举例】

# 设置端口的一个固定优先级的值。

```
NOS# config interface fe1
NOS(if-fe1)# qos port-priority 2
```

【注意事项】

无。

### 65.2.6 qos trust (interface view)

【功能描述】

**qos trust** 命令用于设置端口的优先级信任模式。

**no qos trust** 命令用于将端口的优先级信任模式恢复缺省值：信任 CoS 优先级映射表。

【命令格式】

**qos trust** <**port**|**cos**|**dscp**>

**no qos trust**

【视图】

端口对应的二层以太网接口视图

【缺省情况】

信任 CoS 优先级映射表。

【参数说明】

- **port**：信任端口的一个固定优先级的值。
- **cos**：信任 CoS 优先级映射表。
- **dscp**：信任 DSCP 优先级映射表。

【使用举例】

# 设置端口的优先级信任模式

```
NOS# config interface fe1
```

```
NOS(if-fe1)# qos trust dscp
```

【注意事项】

无。

### 65.2.7 qos trust dscp(vlan view)

【功能描述】

**qos trust dscp** 命令用于设置 VLAN 接口收到的 IP 三层转发报文信任 DSCP 优先级映射表。

即设置以后，此 VLAN 接口收到的 IP 三层转发报文，优先选择信任 DSCP 优先级映射表。此 VLAN 接口收到的非 IP 报文及未进行三层转发的 IP 报文，依然按照端口的优先级信任模式进行选择。

**no qos trust dscp** 命令用于取消 VLAN 接口收到的 IP 报文信任 DSCP 优先级映射表。此时所有报文，按照端口的优先级信任模式进行选择。

【命令格式】

**qos trust dscp**

**no qos trust dscp**

【视图】

VLAN 接口视图

【缺省情况】

未设置 VLAN 接口收到的 IP 三层转发报文信任 DSCP 优先级映射表。

缺省按照端口的优先级信任模式进行选择。

【参数说明】

**dscp**：信任 DSCP 优先级映射表。

【使用举例】

# 设置 VLAN 接口收到的 IP 三层转发报文信任 DSCP 优先级映射表。

```
NOS# config vlan-interface 1
NOS(if-vlan1)# qos trust dscp
```

【注意事项】

无。

### 65.2.8 show qos map

【功能描述】

**show qos map** 命令用于显示优先级映射表信息。

【命令格式】

**show qos map**

【视图】

任意视图

【缺省情况】

无。

【参数说明】

无。

【使用举例】

```
# 显示优先级映射表信息
NOS# show qos map
 cos->local_priority
  0->0  1->1  2->2  3->3  4->4  5->5  6->6  7->7
 dscp->local_priority
  0->0  1->0  2->0  3->0  4->0  5->0  6->0  7->0
  8->1  9->1 10->1 11->1 12->1 13->1 14->1 15->1
 16->2 17->2 18->2 19->2 20->2 21->2 22->2 23->2
 24->3 25->3 26->3 27->3 28->3 29->3 30->3 31->3
 32->4 33->4 34->4 35->4 36->4 37->4 38->4 39->4
 40->5 41->5 42->5 43->5 44->5 45->5 46->5 47->5
 48->6 49->6 50->6 51->6 52->6 53->6 54->6 55->6
 56->7 57->7 58->7 59->7 60->7 61->7 62->7 63->7
```

【注意事项】

无。

## 65.3 配置举例

修改 CoS 优先级映射表为：

```
cos->local_priority
  0->2  1->0  2->1  3->3  4->4  5->5  6->6  7->7
NOS# config qos map cos
NOS(qos-map-cos)# cos 0 lp 2
NOS(qos-map-cos)# cos 1 lp 0
NOS(qos-map-cos)# cos 2 lp 1
```

## 65.4 常见问题

无。

# 66 队列调度

## 66.1 功能简介

### 66.1.1 队列技术简介

队列技术是一种基于队列的拥塞管理机制。报文通过优先级映射，得到设备内部优先级的值；在设备内部，不同的设备内部优先级，对应不同的队列；队列技术是在因资源紧张而产生报文拥塞的情况下，通过队列调度，保证高优先级业务所在队列所需要的服务，牺牲低优先级业务所在队列的报文。

### 66.1.2 队列调度

在每个端口的出方向，有 8 个队列，分为 8 类，依次为 7、6、5、4、3、2、1、0 队列，它们的优先级依次降低。

队列的调度方式有以下几种：

- SP 调度

SP（Strict Priority）调度，严格按照优先级从高到低的次序，优先发送高优先级队列中的报文，当较高优先级队列为空时，再发送较低优先级队列中的报文。

优点：确保关键业务永远被优先转发。

缺点：拥塞发生时，当较高优先级队列持续不为空时，较低优先级队列中的报文将一直得不到服务。

- WRR 调度

WRR（Weighted round robin）调度，是在队列之间进行轮流调度，保证每个队列都得到一定的服务。WRR 调度可以为每个队列配置一个权值（依次为 w7、w6、w5、w4、w3、w2、w1、w0），权值表示获取资源的比重。如一个 100Mbps 的端口，配置它的 WRR 队列的权值为 50、50、30、30、10、10、10、10（依次对应 w7、w6、w5、w4、w3、w2、w1、w0），这样可以保证最低优先级队列至少获得 5Mbps 的带宽，解决了采用 SP 调度时低优先级队列中的报文可能长时间得不到服务的问题。

优点：解决了采用 SP 调度时低优先级队列中的报文可能长时间得不到服务的问题。

缺点：关键业务不一定能及时得到服务。

如果将 WRR 调度与 SP 调度二者结合起来，则可以发挥两种调度的优势。此时 WRR 调度将 8 个队列分成若干组，组内进行 WRR 调度，组间进行 SP 调度。

- WFQ 调度

WFQ（Weighted Fair）调度，是将 WRR 调度进行改进，可以为每个队列增加配置一个最小保证带宽，从而保证当端口带宽不够而拥塞时，低优先级队列能够获得最小队列带宽。

如果将 WFQ 调度与 SP 调度二者结合起来，则可以发挥两种调度的优势。此时 WRR 调度将 8 个队列分成若干组，组内进行 WRR 调度，组间进行 SP 调度。

## 66.2 命令手册

### 66.2.1 qos schedule

【功能描述】

**qos schedule** 命令用于设置端口出方向的队列调度方式和队列的权值。

**no qos schedule** 命令用于将设置端口出方向的队列调度方式恢复缺省值：SP 调度。

【命令格式】

**qos schedule sp**

**qos schedule** <**wrr**|**wfq**|**wdrr**> *q0 q1 q2 q3 q4 q5 q6 q7*

**no qos schedule**

【视图】

端口对应的二层以太网接口视图。

【缺省情况】

缺省使用 SP 调度。

【参数说明】

q0-q7:队列 0-队列 7 的权值。

【使用举例】

```
# 设置端口使用 WRR 调度
NOS# config interface fe1
NOS(if-fe1)# qos schedule wrr 1 1 2 2 4 4 0 0
```

【注意事项】

- **qos schedule wdrr** 命令暂时只提供给部分使用，且只支持以下两种配置方式：
  - [6-7]队列 SP+[0-5]队列 WRR。
  - [4-7]队列 SP+[0-3]队列 WRR。
- 当配置 wdrr 队列时，主要用于设置端口出方向的队列调度方式为部分队列 SP+部分队列 WRR，权重值为 0 的队列代表 sp 队列。

### 66.2.2 qos bandwidth

【功能描述】

**qos bandwidth** 命令用于设置 WFQ 队列的最小保证带宽。

**no qos bandwidth** 命令用于取消 WFQ 队列的最小保证带宽。

【命令格式】

**qos bandwidth queue** *QUEUEID VALUE*

**no qos bandwidth** <**queue** *QUEUEID* |**all**>

【视图】

端口对应的二层以太网接口视图

【缺省情况】

未设置最小保证带宽

【参数说明】

- **queue** *QUEUEID*：队列号.范围(0-7)。
- *VALUE*：最小保证带宽，单位为 kbps，范围(0-10000000)。

【使用举例】

```
# 设置端口使用 WFQ 调度，队列 2 的最小保证带宽为 1Mbps。
NOS# config interface fe1
NOS(if-fe1)# qos schedule wfq 1 1 2 2 4 4 8 8
NOS(if-fe1)# qos bandwidth queue 2 1000
```

【注意事项】

本命令仅支持在 WFQ 调度方式时设置。

## 66.3 配置举例

设置端口 4 的队列调度：

(1) 8 个队列的最小保证带宽从队列 0 到队列 7 依次为 0、10M、10M、10M、15M、15M、10M、10M。

```
NOS# config interface fe4
NOS(if-fe4)# qos schedule wfq 1 1 2 2 4 4 8 8
NOS(if-fe4)# qos schedule bandwidth queue 1 10000
NOS(if-fe4)# qos schedule bandwidth queue 2 10000
NOS(if-fe4)# qos schedule bandwidth queue 3 10000
NOS(if-fe4)# qos schedule bandwidth queue 4 15000
NOS(if-fe4)# qos schedule bandwidth queue 5 15000
NOS(if-fe4)# qos schedule bandwidth queue 6 10000
NOS(if-fe4)# qos schedule bandwidth queue 7 10000
```

## 66.4 常见问题

无。

# 67 限速与整形

## 67.1 功能简介

### 67.1.1 令牌桶技术

如果不限制用户发送的流量，那么大量用户不断突发的数据只会使网络更拥挤。为了使有限的网络资源能够更好地发挥效用，更好地为更多的用户服务，必须对用户的流量加以限制。流量监管、流量整形和限速可以实现流量的速率限制功能，而要实现此功能就必须对通过设备的流量进行度量。一般采用令牌桶（Token Bucket）对流量进行度量。

令牌桶可以看作是一个存放一定数量令牌的容器。系统按设定的速度向桶中放置令牌，当桶中令牌满时，多出的令牌溢出，桶中令牌不再增加。

用令牌桶评估流量：在用令牌桶评估流量规格时，是以令牌桶中的令牌数量是否足够满足报文的转发为依据的。如果桶中存在足够的令牌可以用来转发报文，称流量遵守或符合这个规格，否则称为不符合或超标。

评估流量时令牌桶的参数包括：

- 信息速率：向桶中放置令牌的速率。
- 突发尺寸：令牌桶的容量，即每次突发所允许的最大的流量尺寸。

每到达一个报文就进行一次评估。每次评估，如果桶中有足够的令牌可供使用，则说明流量控制在允许的范围内，此时要从桶中取走满足报文的转发的令牌；否则说明已经耗费太多令牌，流量超标了。

复杂评估

为了评估更复杂的情况，实施更灵活的调控策略，可以使用两个令牌桶（分别称为 C 桶和 E 桶）对流量进行评估。主要有如下三种算法。

- 单速率单桶双色算法
  - 承诺信息速率 CIR：表示向 C 桶中投放令牌的速率，即 C 桶允许传输或转发报文的平均速率；
  - 承诺突发尺寸 CBS：表示 C 桶的容量，即 C 桶瞬间能够通过的承诺突发流量。
- 每次评估时，依据下面的情况，可以分别实施不同的流控策略：
  - 如果 C 桶有足够的令牌，报文被标记为绿色报文；
  - 如果 C 桶令牌不足，报文被标记为红色报文。
- 单速率双桶三色算法（RFC2697）
  - 承诺信息速率 CIR：表示向 C 桶中投放令牌的速率，即 C 桶允许传输或转发报文的平均速率；
  - 承诺突发尺寸 CBS：表示 C 桶的容量，即 C 桶瞬间能够通过的承诺突发流量；
  - 超出突发尺寸 EBS：表示 E 桶的容量的增量，即 E 桶瞬间能够通过的超出突发流量，取值不为 0。E 桶的容量等于 CBS 与 EBS 的和。
- 每次评估时，依据下面的情况，可以分别实施不同的流控策略：
  - 如果 C 桶有足够的令牌，报文被标记为绿色报文；
  - 如果 C 桶令牌不足，但 E 桶有足够的令牌，报文被标记为黄色报文；
  - 如果 C 桶和 E 桶都没有足够的令牌，报文被标记为红色报文。
- 双速率双桶三色算法（RFC2698）
  - 承诺信息速率 CIR：表示向 C 桶中投放令牌的速率，即 C 桶允许传输或转发报文的平均速率；

- 承诺突发尺寸 CBS：表示 C 桶的容量，即 C 桶瞬间能够通过的承诺突发流量；
- 峰值信息速率 PIR：表示向 E 桶中投放令牌的速率，即 E 桶允许传输或转发报文的最大速率；
- 峰值突发尺寸 PBS：表示 E 桶的容量，即 E 桶瞬间能够通过的超出突发流量。

- 每次评估时，依据下面的情况，可以分别实施不同的流控策略：
  - 如果 C 桶有足够的令牌，报文被标记为绿色报文；
  - 如果 C 桶令牌不足，但 E 桶有足够的令牌，报文被标记为黄色报文；
  - 如果 C 桶和 E 桶都没有足够的令牌，报文被标记为红色报文。

### 67.1.2 流量监管

流量监管是对流量进行控制，通过监督进入网络的流量速率，对超出部分的流量进行“惩罚”，使进入的流量被限制在一个合理的范围之内，以保护网络资源。

流量通过流分类配置来确定，流量监管动作通过流行为进行配置，流量监管功能通过流策略应用于端口上来完成。流量监管的配置请参考 QoS 策略的相关章节。

流量监管可以采用单速率双桶三色算法（RFC2697）或双速率双桶三色算法（RFC2698）。

### 67.1.3 流量整形

流量整形是一种主动调整流量输出速率的措施。流量整形对需要丢弃的报文进行缓存，将它们放入队列内。当令牌桶有足够的令牌时，再均匀的向外发送这些被缓存的报文。流量整形可能会增加延迟。流量整形仅作用于端口的出方向。

### 67.1.4 限速

限速是对流经设备接口的报文速度做限制，流量超出阈值的部分直接被丢弃，低于阈值的部分则进入或离开设备。

## 67.2 命令手册

### 67.2.1 qos shape

【功能描述】

**qos shape** 命令用于配置端口出方向队列整形。

**no qos shape** 命令用于取消端口出方向队列整形配置。

【命令格式】

**qos shape queue** *QUEUEID* **cir** *CIRVAL* [**cbs** *CBSVAL*]

**no qos shape** <**queue** *QUEUEID* |**all**>

【视图】

端口对应的二层以太网接口视图

【缺省情况】

端口未配置整形。

【参数说明】

- **queue** *QUEUEID*：队列号，范围(0-7)。
- **all**：本端口的所有 8 个队列。

- **cir** *CIRVAL*：承诺信息速率，单位为 kbps，设置的值会模 10 取整，范围(10-10000000)。
- **cbs** *CBSVAL*：承诺突发尺寸，单位为 kbyte。若不输入，取值为 cir/16，范围(2-32768)。

【使用举例】

# 端口 5 的队列 0，设置承诺信息速率为 10M。

```
NOS# config interface ge5
NOS(if-ge5)# qos shape queue 0 cir 10000
```

【注意事项】

参数范围随产品不同。

### 67.2.2 rate-limit

【功能描述】

**rate-limit** 命令用于配置端口限速。

**no qos rate-limit** 命令用于取消端口限速配置。

【命令格式】

**qos rate-limit cir** <**inbound**|**outbound**> *CIRVAL* [**cbs** *CBSVAL*]

**no qos rate-limit** <**inbound**|**outbound**>

【视图】

端口对应的二层以太网接口视图。

【缺省情况】

端口未配置限速。

【参数说明】

- **cir** *CIRVAL*：承诺信息速率，单位为 kbps，设置的值会模 10 取整，范围(10-10000000)。
- **cbs** *CBSVAL*：承诺突发尺寸，单位为 kbyte。若不输入，取值为 cir/16，范围(2-32768)。

【使用举例】

# 端口 6 的收报文速率和发报文速率，均设置限速为 10M。

```
NOS# config interface ge6
NOS(if-ge6)# rate-limit cir inbound 10000
NOS(if-ge6)# rate-limit cir outbound 10000
```

【注意事项】

参数范围随产品不同。

### 67.2.3 show qos rate-limit

【功能描述】

**show qos rate-limit** 命令用于显示各个端口限速信息。

【命令格式】

**show qos rate-limit** [**json**]

【视图】

任意视图

【缺省情况】

无。

【参数说明】

json：以 json 格式显示。

【使用举例】

# 显示端口限速信息

```
NOS# show qo rate-limit
Interface          In-Cir     In-Cbs     Out-Cir    Out-Cbs
-------------------------------------------------------------------
ge1               100         0          100        0
ge2               0           0           200        0
```

【注意事项】

无。

## 67.3 配置举例

设置端口 6 的队列整形：从队列 1 到队列 7 依次为：10M、20M、30M、40M、50M、60M、80M、100M。

```
NOS# config interface ge6
NOS(if-ge6)# qos shape queue 0 cir 10000
NOS(if-ge6)# qos shape queue 1 cir 20000
NOS(if-ge6)# qos shape queue 2 cir 30000
NOS(if-ge6)# qos shape queue 3 cir 40000
NOS(if-ge6)# qos shape queue 4 cir 50000
NOS(if-ge6)# qos shape queue 5 cir 60000
NOS(if-ge6)# qos shape queue 6 cir 80000
NOS(if-ge6)# qos shape queue 7 cir 100000
```

## 67.4 常见问题

无。

# 68 拥塞避免

## 68.1 功能简介

拥塞避免是一种流量控制机制，它通过监视网络资源（如队列或内存缓冲区）的使用情况，在拥塞产生或有加剧的趋势时主动丢弃报文，通过调整网络的流量来避免网络过载。

传统的丢包策略采用尾部丢弃（Tail-Drop）的方法。当队列的长度达到最大值后，所有新到来的报文都将被丢弃。

这种丢弃策略会引发某些问题，例如，TCP 全局同步现象：当队列同时丢弃多个 TCP 连接的报文时，将造成多个 TCP 连接同时进入拥塞避免和慢启动状态以降低并调整流量，而后又会在某个时间同时出现流量高峰。如此反复，使网络流量忽大忽小，网络不停震荡。

为了解决上述问题而引入了 WRED（Weighted Random Early Detection）技术：“提早”并“随机”地丢弃一些低级别的数据报文。这种不同时丢包行为可以使多个 TCP 连接不会同时降低发送速度，从而避免 TCP 全局同步现象的发生，使 TCP 流量都趋于平缓稳定。

WRED 技术为每个队列都设定上限和下限，对队列中的报文进行如下处理：

- 当队列的长度小于下限时，不丢弃报文。
- 当队列的长度超过上限时，丢弃所有到来的报文。
- 当队列的长度在上限和下限之间时，开始随机丢弃到来的报文。队列越长，丢弃概率越高，但有一个最大丢弃概率。

在进行 WRED 配置时，需要事先确定如下参数：

- 队列上限和下限：当队列平均长度小于下限时，不丢弃报文。当队列平均长度在上限和下限之间时，设备随机丢弃报文，队列越长，丢弃概率越高。当队列平均长度超过上限时，丢弃所有到来的报文。
- 丢弃优先级：在进行报文丢弃时，可分别对绿色报文、黄色报文、红色报文分别配置。
- 计算平均队列长度的指数：指数越大，计算平均队列长度时对队列的实时变化越不敏感。计算队列平均长度的公式为：平均队列长度=（以前的平均队列长度×（1-1/$2^n$））＋（当前队列长度×（1/$2^n$））。其中 n 表示指数。
- 丢弃概率：配置接口应用 WRED 表时，使用百分数的形式表示丢弃报文的概率，取值越大，报文被丢弃的机率越大。

## 68.2 命令手册

### 68.2.1 config qos wred

【功能描述】

**config qos wred** 命令用于进入 WRED 表视图。

**no config qos wred** 命令用于删除一个 WRED 表的所有配置。

【命令格式】

**config qos wred**

**no config qos wred**

【视图】

根视图

【缺省情况】

未配置 WRED 表。

【参数说明】

无。

【使用举例】

```
# 进入配置 WRED 表的视图
NOS# config qos wred
NOS(qos-wred)#
```

【注意事项】

无。

### 68.2.2 queue wred

【功能描述】

**queue** wred 命令用于设置 WRED 表的内容。

【命令格式】

**queue** *QUEUEID* <**red**|**yellow**|**green**> **min** *MINVAL* **max** *MAXVAL* **pro** *PRO*

**no queue** *QUEUEID* <**red**|**yellow**|**green**>

【视图】

WRED 表视图。

【缺省情况】

未配置 WRED 表。

【参数说明】

**queue** ：队列号，范围(0-7)。

**red**：红色报文。

**yellow**：黄色报文。

**green**：绿色报文。

**min** *MINVAL*：队列长度下限，范围(0-2047)。

**max** *MAXVAL*：队列长度上限，范围(0-2047)。

**pro** *PRO*：最大丢弃概率，范围(0-100)。

【使用举例】

```
# 设置 WRED 表的队列 1，绿色、黄色、红色报文的丢弃概率分别为 25%、50%、75%。
NOS# config qos wred
NOS(qos-wred)# queue 1 green min 128 max 512 pro 25
NOS(qos-wred)# queue 1 yellow min 128 max 512 pro 50
NOS(qos-wred)# queue 1 red min 128 max 512 pro 75
```

【注意事项】

无。

### 68.2.3 qos wred

【功能描述】

**qos wred** 命令用于将 WRED 表应用到端口。每个端口只能应用一张 WRED 表。

**no qos wred** 命令用于取消端口的 WRED 表应用。

【命令格式】

qos wred

no qos wred

【视图】

端口对应的二层以太网接口视图

【缺省情况】

端口未应用 WRED 表。

【参数说明】

无。

【使用举例】

# 将 WRED 表应用到端口 3。

```
NOS# config interface fe3
NOS(if-fe3)# qos wred
```

【注意事项】

无。

## 68.3 配置举例

端口 3 应用 WRED 策略，当发生报文拥塞时，采用如下丢弃方式：

- 队列 0-2，绿色、黄色、红色报文的丢弃概率分别为 25%、50%、75%；
- 队列 3-5，绿色、黄色、红色报文的丢弃概率分别为 5%、10%、25%；
- 队列 6-7，绿色、黄色、红色报文的丢弃概率分别为 1%、5%、10%。

```
NOS# config qos wred
NOS(qos-wred)# queue 0 green min 128 max 512 pro 25
NOS(qos-wred)# queue 0 yellow min 128 max 512 pro 50
NOS(qos-wred)# queue 0 red min 128 max 512 pro 75
NOS(qos-wred)# queue 1 green min 128 max 512 pro 25
NOS(qos-wred)# queue 1 yellow min 128 max 512 pro 50
NOS(qos-wred)# queue 1 red min 128 max 512 pro 75
NOS(qos-wred)# queue 2 green min 128 max 512 pro 25
NOS(qos-wred)# queue 2 yellow min 128 max 512 pro 50
NOS(qos-wred)# queue 2 red min 128 max 512 pro 75
NOS(qos-wred)# queue 3 green min 256 max 768 pro 5
NOS(qos-wred)# queue 3 yellow min 256 max 768 pro 10
NOS(qos-wred)# queue 3 red min 256 max 768 pro 25
NOS(qos-wred)# queue 4 green min 256 max 768 pro 5
NOS(qos-wred)# queue 4 yellow min 256 max 768 pro 10
NOS(qos-wred)# queue 4 red min 256 max 768 pro 25
NOS(qos-wred)# queue 5 green min 256 max 768 pro 5
NOS(qos-wred)# queue 5 yellow min 256 max 768 pro 10
NOS(qos-wred)# queue 5 red min 256 max 768 pro 25
NOS(qos-wred)# queue 6 green min 384 max 1024 pro 1
NOS(qos-wred)# queue 6 yellow min 384 max 1024 pro 5
NOS(qos-wred)# queue 6 red min 384 max 1024 pro 10
NOS(qos-wred)# queue 7 green min 384 max 1024 pro 1
```

```
NOS(qos-wred)# queue 7 yellow min 384 max 1024 pro 5
NOS(qos-wred)# queue 7 red min 384 max 1024 pro 10
NOS(qos-wred)# quit
NOS# config interface fe3
NOS(if-fe3)# qos wred
```

## 68.4 常见问题

无。

# 69 链路聚合

## 69.1 功能介绍

### 69.1.1 什么是链路聚合

以太网链路聚合 Eth-Trunk 简称链路聚合，通过将多个物理接口捆绑为一个逻辑接口，可以在不进行硬件升级的条件下，达到增加链路带宽的目的。

链路聚合技术主要有以下三个优势：

1. 增加带宽

链路聚合接口的最大带宽可以达到各成员接口带宽之和。

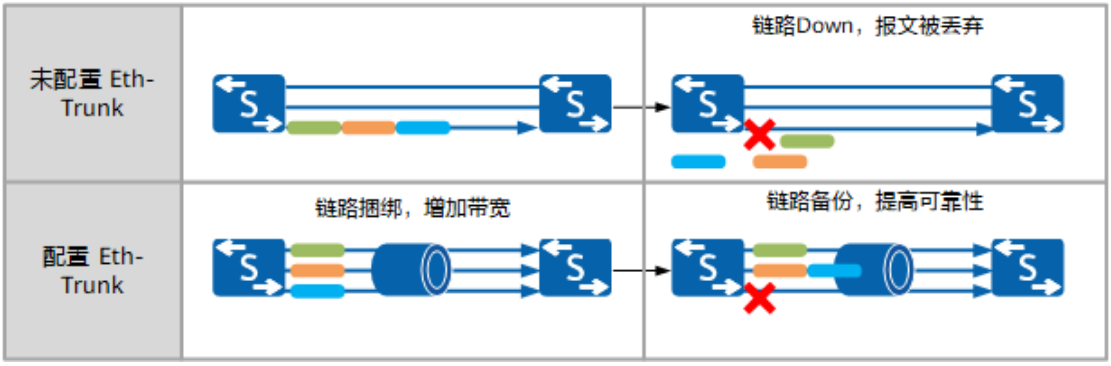
2. 提高可靠性

当某条活动链路出现故障时，流量可以切换到其他可用的成员链路上，从而提高链路聚合接口的可靠性。

3. 负载分担

在一个链路聚合组内，可以实现在各成员活动链路上的负载分担。

图69-1 负载分担




链路聚合组的成员接口存在活动接口和非活动接口两种。转发数据的接口称为活动接口，不转发数据的接口称为非活动接口。

根据是否启用链路聚合控制协议 LACP（Link Aggregation Control Protocol），链路聚合分为手工模式和 LACP 模式。

- 手工模式链路聚合（也称静态聚合）
  - 手工模式下，Eth-Trunk 的建立、成员接口的加入由手工配置，没有链路聚合控制协议 LACP 的参与。该模式下所有活动链路都参与数据的转发，平均分担流量。如果某条活动链路故障，链路聚合组自动在剩余的活动链路中平均分担流量。
  - 当需要在两个直连设备之间提供一个较大的链路带宽，而其中一端或两端设备都不支持 LACP 协议时，可以配置手工模式链路聚合。
- LACP 模式（也称动态聚合）：LACP 模式通过成员端口之间交互 LACP 动态灵活确定成员端口的选中状态。

### 69.1.2 静态聚合

NOS 支持静态聚合，每个聚合接口最多支持 8 个成员口负载分担。负载分担方式为根据报文二层特性：即 src-dst-mac，哈希散列为：XOR。

### 69.1.3 动态聚合

NOS 支持动态聚合，动态聚合模式采用 LACP 实现，该协议的工作机制如下。

LACP 协议遵循 IEEE802.3ad 标准,用于动态建立链路聚合。运行该协议的设备通过交换 LACPDU(Link Aggregation Control Protocol Data Unit，链路聚合控制协议数据单元）来共享聚合配置信息。在动态聚合组中，各成员端口具备收发 LACPDU 的能力。本地设备通过发送 LACPDU 向对端传递自身信息。对端设备收到 LACPDU 后，会将这些信息与其他成员端口接收到的信息进行比对，从而确定哪些端口应处于活动状态。通过这种方式，通信双方能够就端口的激活状态达成一致。

## 69.2 命令手册

### 69.2.1 config bridge-aggregation

【功能描述】

**config bridge-aggregation** 命令用于创建聚合视图。

**no config bridge-aggregation** 命令删除聚合视图。

【命令格式】

[no] **config bridge-aggregation**

【视图】

根视图。

【缺省情况】

缺省未创建聚合视图

【参数说明】

无。

【使用举例】

```
NOS# config  interface bridge-aggregation
NOS(config-bagg)#
```

【注意事项】

无。

### 69.2.2 load-balance mode

【功能描述】

**load-balance mode** 命令用于设置负载分担方式。

**no load-balance mode** 命令取消负载分担。

【命令格式】

**load-balance mode** <{ipsa|ipda}|{macsa|macda}|{sport|dport}|ingress-port>

**no load-balance mode**

【视图】

聚合视图

【缺省情况】

缺省根据报文类型进行负载分担。

【参数说明】

- **ipsa**：按照源 ip 进行负载分担。
- **ipda**：按照目的 ip 进行负载分担
- **macsa**：按照源 mac 进行负载分担。
- **macda**：按照目的 mac 进行负载分担。
- **sport**：按照源端口进行负载分担。
- **dport**：按照源目的进行负载分担。
- **ingress-port**：按照入端口进行负载分担。

【使用举例】

```
NOS# config  interface bridge-aggregation
NOS(config-bagg)# load-balance mode dport
```

【注意事项】

无。

### 69.2.3 config interface bridge-aggregation

【功能描述】

**config interface bridge-aggregation** 命令用于创建一个聚合组。

**no config interface bridge-aggregation** 命令删除一个聚合组。

【命令格式】

**[no] config interface bridge-aggregation** *(1-maxNum)*

【视图】

根视图

【缺省情况】

缺省未配置聚合组

【参数说明】

**bridge-aggregation** *(1-maxNum)*：聚合接口号，*maxNum* 为最大聚合接口号，产品不同，规格不一样。

【使用举例】

```
NOS# config  interface bridge-aggregation 1
NOS(if-bagg1)#
```

【注意事项】

该命令仅创建一个未包含成员口的聚合接口。

### 69.2.4 member interface

【功能描述】

**member interface** 命令用于将支持聚合的接口加入聚合组。

**no member interface** 命令用于将指定接口移出聚合组。

**no member all** 用于移除聚合组下的所有成员接口。

【命令格式】

**member interface** *L2_ETH_IF...*

**no member** <**interface** *L2_ETH_IF* | **all**>

【视图】

聚合接口视图

【缺省情况】

不涉及

【参数说明】

- **interface** *L2_ETH_IF*：指定成员口，可选二层接口号。
- **all**：移除聚合组下的所有成员接口。

【使用举例】

创建聚合组 bagg10 并将 fe1 加入该聚合组。

```
NOS# config bridge-aggregation 10
NOS(if-bagg10)# member interface fe1
NOS(if-bagg10)# show this
member interface fe1
```

【注意事项】

无。

### 69.2.5 description

【功能描述】

**description** 用于配置聚合口描述信息。

**no description** 用于取消配置描述信息。

【命令格式】

**description** *DESC*

**no description**

【视图】

聚合接口视图。

【缺省情况】

无描述信息。

【参数说明】

*DESC*：接口描述信息，1～255 个字符描述。

【使用举例】

```
NOS# config bridge-aggregation 10
NOS(if-bagg10)# description uplink-agg
NOS(if-bagg10)# show this
description uplink-agg
```

【注意事项】

无。

### 69.2.6 mode

【功能描述】

**mode dynamic** 用于配置聚合口为动态聚合。

**mode static** 用于配置聚合口为静态聚合。

【命令格式】

**mode <static|dynamic>**

【视图】

聚合接口视图。

【缺省情况】

缺省情况端口为静态聚合模式。

【参数说明】

无。

【使用举例】

将聚合组 bagg10 设置为动态聚合模式

```
NOS# config bridge-aggregation 10
NOS(if-bagg10)# mode dynamic
NOS(if-bagg10)# show this
  mode dynamic
```

【注意事项】

- 动态模式下聚合口的成员口不能是半双工模式，否则无法动态协商。
- 修改聚合模式会导致聚合接口震荡。

### 69.2.7 lacp period short

【功能描述】

**lacp period short** 用于配置聚合组短周期超时。

**no lacp period short** 用于取消配置聚合组短周期超时。

【命令格式】

**[no] lacp period short**

【视图】

聚合接口视图。

【缺省情况】

缺省情况聚合组为长周期超过。

【参数说明】

无。

【使用举例】

```
NOS# config bridge-aggregation 10
NOS(if-bagg10)# lacp period short
```

【注意事项】

动态模式下聚合口的才能配置超时周期。

### 69.2.8 lacp enable

【功能描述】

**lacp enable** 用于配置端口使能 lacp 协议。

**no lacp enable** 用于配置端口去使能 lacp 协议。

【命令格式】

[no] lacp enable

【视图】

二层物理接口视图。

【缺省情况】

加入了动态聚合组的接口缺省使能 lacp 协议。

【参数说明】

无。

【使用举例】

```
NOS# interface ge1
NOS(if-ge1)# lacp enable
```

【注意事项】

- 只有加入了动态聚合组的接口才允许配置 lacp 使能状态。
- 接口去使能 lacp，则该接口不再收/发 LACPDU，导致对端无法接收本端的 LACP 信息。

### 69.2.9 show link-aggregation

【功能描述】

**show link-aggregation** 命令用于显示指定聚合接口自身和成员的状态。

【命令格式】

**show link-aggregation** [*(1-maxNum)*] [**json**]

【视图】

任意视图

【缺省情况】

不涉及。

【参数说明】

- *(1-maxNum)*：聚合接口号，产品不同，规格不一样。
- **json**：以 json 格式输出。

【使用举例】

```
NOS(if-bagg110)# show link-aggregation 110
 Link-Aggregation 110 state information is:
 KER Hash arithmetic: balance-XOR
 KER Xmit policy: layer 2 (MAC only)
 SDK Hash arithmetic: According to src-dst-mac(xor)
 Max Bandwitch-affected-linknumber:3
 Operate status:Up        Number of Up port:3
 ---------------------------------------------
```

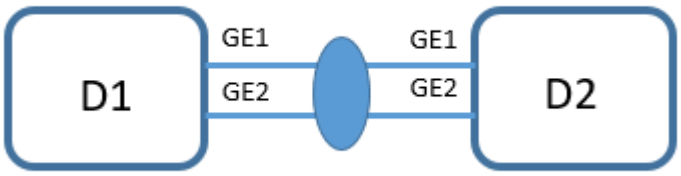
```
PortName          Status    Select
fe1               Up         Y
fe2               Up         Y
fe3               Up         Y
```

【注意事项】

无。

## 69.3 配置举例

### 69.3.1 静态聚合




Device 1 与 Device 2 通过各自的二层以太网接口 GE1～GE2 相互连接。

在 Device 1 和 Device 2 上分别配置二层静态链路聚合组，实现设备间通过聚合组互通。

(1) Device 1 配置

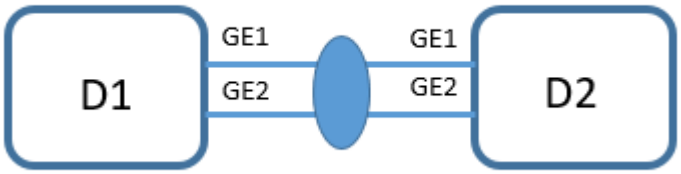
```
NOS# config interface bridge-aggregation 1
NOS(if-bagg1)# member interface ge1 ge2

NOS(if-bagg1)# show  link-aggregation
 Link-Aggregation 1 state information is:
 KER Hash arithmetic: balance-XOR
 KER Xmit policy: layer 2 (MAC only)
 KER Lacp fast: 0
 SDK Hash arithmetic: According to src-dst-mac(xor)
 Max Bandwitch-affected-linknumber:2
 Operate status:Up        Number of Up port:2
 ---------------------------------------------
 PortName          Status    Select
 ge1           Up       Y
 ge2           Up       Y
```

(2) Device 2 配置

```
NOS# config interface bridge-aggregation 1
NOS(if-bagg1)# member interface ge1 ge2

NOS(if-bagg1)# show  link-aggregation
 Link-Aggregation 1 state information is:
 KER Hash arithmetic: balance-XOR
 KER Xmit policy: layer 2 (MAC only)
 KER Lacp fast: 0
```

```
SDK Hash arithmetic: According to src-dst-mac(xor)
Max Bandwitch-affected-linknumber:2
Operate status:Up        Number of Up port:2
-----------------------------------------------
PortName          Status    Select
ge1           Up       Y
ge2           Up       Y
```

### 69.3.2 动态聚合




Device 1 与 Device 2 通过各自的二层以太网接口 GE1～GE2 相互连接。

在 Device 1 和 Device 2 上分别配置二层动态链路聚合组，实现设备间通过聚合组互通。

(1) Device 1 配置

```
NOS# config interface bridge-aggregation 1
NOS(if-bagg1)# mode dynamic
NOS(if-bagg1)# member interface ge1 ge2

NOS(if-bagg1)# show  link-aggregation
 Link-Aggregation 1 state information is:
 KER Hash arithmetic: balance-802.3ad
 KER Xmit policy: layer 2 (MAC only)
 KER Lacp fast: 0
 SDK Hash arithmetic: According to src-dst-mac(xor)
 Max Bandwitch-affected-linknumber:2
 Operate status:Up        Number of Up port:2
 -----------------------------------------------
 PortName          Status    Select
 ge1           Up       Y
 ge2           Up       Y
```

(2) Device 2 配置

```
NOS# config interface bridge-aggregation 1
NOS(if-bagg1)# mode dynamic
NOS(if-bagg1)# member interface ge1 ge2

NOS(if-bagg1)# show  link-aggregation
 Link-Aggregation 1 state information is:
 KER Hash arithmetic: balance-802.3ad
 KER Xmit policy: layer 2 (MAC only)
```

```
KER Lacp fast: 0
SDK Hash arithmetic: According to src-dst-mac(xor)
Max Bandwitch-affected-linknumber:2
Operate status:Up        Number of Up port:2
-----------------------------------------------
PortName          Status    Select
ge1           Up       Y
ge2           Up       Y
```

## 69.4 常见问题

无。

# 70 STP

## 70.1 特性简介

以下内容简介主要为 MSTP。

多生成树协议 MSTP（Multiple Spanning Tree Protocol）是 IEEE。

802.1s 中定义的生成树协议，通过生成多个生成树，来解决以太网环路问题。

### 70.1.1 MSTP的功能

在以太网中部署 MSTP 协议后可实现如下功能：

- 形成多棵无环路的树，解决广播风暴并实现冗余备份。
- 多棵生成树在 VLAN 间实现负载均衡，不同 VLAN 的流量按照不同的路径转发。

### 70.1.2 MSTP原理描述

STP/RSTP 的缺陷：

RSTP 在 STP 基础上进行了改进，实现了网络拓扑快速收敛。但 RSTP 和 STP 还存在同一个缺陷：由于局域网内所有的 VLAN 共享一棵生成树，因此无法在 VLAN 间实现数据流量的负载均衡，链路被阻塞后将不承载任何流量，还有可能造成部分 VLAN 的报文无法转发。

### 70.1.3 MSTP对STP和RSTP的改进

为了弥补 STP 和 RSTP 的缺陷，IEEE 于 2002 年发布的 802.1S 标准定义了 MSTP。MSTP 兼容 STP 和 RSTP，既可以快速收敛，又提供了数据转发的多个冗余路径，在数据转发过程中实现 VLAN 数据的负载均衡。

MSTP 把一个交换网络划分成多个域，每个域内形成多棵生成树，生成树之间彼此独立。每棵生成树叫做一个多生成树实例 MSTI（Multiple Spanning Tree Instance），每个域叫做一个 MST 域（MST Region：Multiple Spanning Tree Region）。

所谓生成树实例就是多个 VLAN 的一个集合。通过将多个 VLAN 捆绑到一个实例，可以节省通信开销和资源占用率。MSTP 各个实例拓扑的计算相互独立，在这些实例上可以实现负载均衡。可以把多个相同拓扑结构的 VLAN 映射到一个实例里，这些 VLAN 在端口上的转发状态取决于端口在对应 MSTP 实例的状态。

### 70.1.4 MSTP基本概念

#### 1. MST 域（MST Region）

- 都启动了 MSTP。
- 具有相同的域名。
- 具有相同的 VLAN 到生成树实例映射配置。
- 具有相同的 MSTP 修订级别配置。
- 一个局域网可以存在多个 MST 域，各 MST 域之间在物理上直接或间接相连。用户可以通过 MSTP 配置命令把多台交换设备划分在同一个 MST 域内。

#### 2. VLAN 映射表：

VLAN 映射表是 MST 域的属性，它描述了 VLAN 和 MSTI 之间的映射关系。

### 3. CST

公共生成树 CST（Common Spanning Tree）是连接交换网络内所有 MST 域的一棵生成树。
如果把每个 MST 域看作是一个节点，CST 就是这些节点通过 STP 或 RSTP 协议计算生成的一棵生成树。

### 4. IST

内部生成树 IST（Internal Spanning Tree）是各 MST 域内的一棵生成树。
IST 是一个特殊的 MSTI，MSTI 的 ID 为 0，通常称为 MSTI0。
IST 是 CIST 在 MST 域中的一个片段。

### 5. SST

运行 STP 或 RSTP 的交换设备只能属于一个生成树。
MST 域中只有一个交换设备，这个交换设备构成单生成树。

### 6. CIST

公共和内部生成树 CIST（Common and Internal Spanning Tree）是通过 STP 或 RSTP 协议计算生成的，连接一个交换网络内所有交换设备的单生成树。

### 7. 域根

域根（Regional Root）分为 IST 域根和 MSTI 域根。
一个 MST 域内可以生成多棵生成树，每棵生成树都称为一个 MSTI。MSTI 域根是每个多生成树实例的树根。

### 8. 总根/根桥

总根是 CIST（Common and Internal Spanning Tree）的根桥。

### 9. 主桥（Master Bridge）

也就是 IST Master，它是域内距离总根最近的交换设备。

### 10. 端口角色

根端口、指定端口、Alternate 端口、Backup 端口和边缘端口的作用同 RSTP 协议中定义。
除边缘端口外，其他端口角色都参与 MSTP 的计算过程。
同一端口在不同的生成树实例中可以担任不同的角色。

表70-1 说明

| 端口角色 | 说明 |
| --- | --- |
| 根端口 | 在非根桥上，离根桥最近的端口是本交换设备的根端口。根交换设备没有根端口。根端口负责向树根方向转发数据 |
| 指定端口 | 对一台交换设备而言，它的指定端口是向下游交换设备转发BPDU报文的端口 |
| Alternate端口 | 从配置BPDU报文发送角度来看，Alternate端口就是由于学习到其它网桥发送的配置BPDU报文而阻塞的端口。 从用户流量角度来看，Alternate端口提供了从指定桥到根的另一条可切换路径，作为根端口的备份端口 |
| Backup端口 | 从配置BPDU报文发送角度来看，Backup端口就是由于学习到自己发送的配置BPDU报文而阻塞的端口。 从用户流量角度来看，Backup端口作为指定端口的备份，提供了另外一条从根节点到叶节点的备份通路 |
| Master端口 | • Master 端口是 MST 域和总根相连的所有路径中最短路径上的端口，它是交换设备上连接 MST 域到总根的端口<br>• Master 端口是域中的报文去往总根的必经之路<br>• Master 端口是特殊域边缘端口，Master 端口在 CIST 上的角色是 Root Port，在其它各实例上的角色都是 Master 端口 |

| 端口角色 | 说明 |
| --- | --- |
| 域边缘端口 | 域边缘端口是指位于MST域的边缘并连接其它MST域或SST的端口 |
| 边缘端口 | 如果指定端口位于整个域的边缘，不再与任何交换设备连接，这种端口叫做边缘端口<br>边缘端口一般与用户终端设备直接连接<br>端口使能MSTP功能后，会默认启用边缘端口自动探测功能，当端口在（2×Hello Timer + 1）秒的时间内收不到BPDU报文，自动将端口设置为边缘端口，否则设置为非边缘端口 |

### 11. 端口状态

MSTP 定义的端口状态与 RSTP 协议中定义相同。

**注意**

根端口、Master 端口、指定端口和域边缘端口支持 Forwarding、Learning 和 Discarding 状态，Alternate 端口和 Backup 端口仅支持 Discarding 状态。

### 12. MSTP 报文

MSTP 使用多生成树桥协议数据单元 MST BPDU（Multiple Spanning Tree Bridge Protocol Data Unit）作为生成树计算的依据。MST BPDU 报文用来计算生成树的拓扑、维护网络拓扑以及传达拓扑变化记录。

STP 中定义的配置 BPDU、RSTP 中定义的 RST BPDU、MSTP 中定义的 MST BPDU 及 TCN BPDU 差异对比如下：

四种 BPDU 差异比较：

表70-2 说明

| 版本 | 类型 | 名称 |
| --- | --- | --- |
| 0 | 0x00 | 配置BPDU |
| 0 | 0x80 | TCN BPDU |
| 2 | 0x02 | RST BPDU |
| 3 | 0x02 | MST BPDU |

### 13. MSTP 帧格式：

具体格式参照如下对象文件

STP_RSTP_MSTP 帧格式.mhtml

### 14. MSTP 报文字段解释

表70-3 说明

| 字段 | 说明 |
| --- | --- |
| Protocol Identifier | 协议标识符 |

| 字段 | 说明 |
| --- | --- |
| Protocol Version Identifier | 协议版本标识符，STP为0，RSTP为2，MSTP为3 |
| BPDU Type | BPDU类型，MSTP为0x02。0x00：STP的Configuration BPDU0x80：STP的TCN BPDU（Topology Change Notification BPDU）0x02：RST BPDU（Rapid Spanning-Tree BPDU）或者MST BPDU（Multiple Spanning-Tree BPDU） |
| CIST Flags | CIST标志字段 |
| CIST Root Identifier | CIST的总根交换机ID |
| CIST External Path Cost | CIST外部路径开销指从本交换机所属的MST域到CIST根交换机的累计路径开销。CIST外部路径开销根据链路带宽计算 |
| CIST Regional Root Identifier | CIST的域根交换机ID，即IST Master的ID。 如果总根在这个域内，那么域根交换机ID就是总根交换机ID |
| CIST Port Identifier | 本端口在IST中的指定端口ID |
| Message Age | BPDU报文的生存期 |
| Max Age | BPDU报文的最大生存期，超时则认为到根交换机的链路故障 |
| Hello Time | Hello定时器，缺省为2秒 |
| Forward Delay | Forward Delay定时器，缺省为15秒 |
| Version 1 Length | Version1 BPDU的长度，值固定为0 |
| Version 3 Length | Version3 BPDU的长度 |
| MST Configuration Identifier | MST配置标识，表示MST域的标签信息，包含4个字段：Configuration Identifier Format Selector：固定为0。Configuration Name：“域名”，32字节长字符串。Revision Level：2字节非负整数。Configuration Digest：利用HMAC-MD5算法将域中VLAN和实例的映射关系加密成16字节的摘要。只有MST Configuration Identifier中的四个字段完全相同的，并且互联的交换机，才属于同一个域 |
| CIST Internal Root Path Cost | CIST内部路径开销指从本端口到IST Master交换机的累计路径开销。CIST内部路径开销根据链路带宽计算 |
| CIST Bridge Identifier | CIST的指定交换机ID |
| CIST Remaining Hops | BPDU报文在CIST中的剩余跳数 |
| MSTI Configuration Messages (may be absent) | MSTI配置信息。每个MSTI的配置信息占16 bytes，如果有n个MSTI就占用n×16bytes。单个MSTI Configuration Messages的字段说明如下：MSTI Flags：MSTI标志。MSTI Regional Root Identifier：MSTI域根交换机ID。MSTI Internal Root Path Cost：MSTI内部路径开销指从本端口到MSTI域根交换机的累计路径开销。MSTI内部路径开销根据链路带宽计算。MSTI Bridge Priority：本交换机在MSTI中的指定交换机的优先级。MSTI Port Priority：本交换机在MSTI中的指定端口的优先级。MSTI Remaining Hops：BPDU报文在MSTI中的剩余跳数 |

### 15. 优先级向量

MSTI 和 CIST 都是根据优先级向量来计算的，这些优先级向量信息都包含在 MST BPDU 中。各交换设备互相交换 MST BPDU 来生成 MSTI 和 CIST。

优先级向量简介

参与 CIST 计算的优先级向量为：

{根交换设备 ID，外部路径开销，域根 ID，内部路径开销，指定交换设备 ID，指定端口 ID，接收端口 ID}

参与 MSTI 计算的优先级向量为：

{域根 ID，内部路径开销，指定交换设备 ID，指定端口 ID，接收端口 ID}

**括号中的向量的优先级从左到右依次递减。**

表70-4 向量说明

| 向量名 | 说明 |
| --- | --- |
| 根交换设备ID | 根交换设备ID用于选择CIST中的根交换设备。根交换设备ID = Priority(16bits) + MAC(48bits)。其中Priority为MSTI0的优先级 |
| 外部路径开销（ERPC） | 从CIST的域根到达总根的路径开销。MST域内所有交换设备上保存的外部路径开销相同。若CIST根交换设备在域中，则域内所有交换设备上保存的外部路径开销为0 |
| 域根ID | 域根ID用于选择MSTI中的域根。域根ID = Priority(16bits) + MAC(48bits)。其中Priority为MSTI0的优先级 |
| 内部路径开销（IRPC） | 本桥到达域根的路径开销。域边缘端口保存的内部路径开销大于非域边缘端口保存的内部路径开销 |
| 指定交换设备ID | CIST或MSTI实例的指定交换设备是本桥通往域根的最邻近的上游桥。如果本桥就是总根或域根，则指定交换设备为自己 |
| 指定端口ID | 指定交换设备上同本设备上根端口相连的端口。Port ID = Priority(4位) + 端口号（12位）。端口优先级必须是16的整数倍 |
| 接收端口ID | 接收到BPDU报文的端口。Port ID = Priority(4位) + 端口号（12位）。端口优先级必须是16的整数倍 |

**比较原则**

同一向量比较，值最小的向量具有最高优先级。

优先级向量比较原则如下。

- 首先，比较根交换设备 ID。
- 如果根交换设备 ID 相同，再比较外部路径开销。
- 如果外部路径开销相同，再比较域根 ID。
- 如果域根 ID 仍然相同，再比较内部路径开销。
- 如果内部路径仍然相同，再比较指定交换设备 ID。
- 如果指定交换设备 ID 仍然相同，再比较指定端口 ID。
- 如果指定端口 ID 还相同，再比较接收端口 ID。
- 如果端口接收到的 BPDU 内包含的配置消息优于端口上保存的配置消息，则端口上原来保存的配置消息被新收到的配置消息替代。端口同时更新交换设备保存的全局配置消息。反之，新收到的 BPDU 被丢弃。

16. CIST 中端口角色的选举：

- 比价 CIST 的总根 ID，越小越优。
- 比较 CIST 到达总根的 ERPC，越小越优。
- 比较 CIST 域根的 BID，越小越优。
- 比较 CIST 到达域根的 IPRC，越小越优。
- 比较 CIST 中 BPDU 报文发送者的 BID，越小越优。
- 比较 CIST 中 BPDU 报文发送者的 PID，越小越优。

- 比较 CIST 中 BPDU 报文接收者的 PID，越小越优。

17. CIST 的计算：

经过比较配置消息后，在整个网络中选择一个优先级最高的交换设备作为 CIST 的树根。在每个 MST 域内 MSTP 通过计算生成 IST；同时 MSTP 将每个 MST 域作为单台交换设备对待，通过计算在 MST 域间生成 CST。CST 和 IST 构成了整个交换设备网络的 CIST

18. MSTI 的计算

在 MST 域内，MSTP 根据 VLAN 和生成树实例的映射关系，针对不同的 VLAN 生成不同的生成树实例。每棵生成树独立进行计算，计算过程与 STP 计算生成树的过程类似。

19. MSTI 的特点

- 每个 MSTI 独立计算自己的生成树，互不干扰。
- 每个 MSTI 的生成树计算方法与 STP 基本相同。
- 每个 MSTI 的生成树可以有不同的根，不同的拓扑。
- 每个 MSTI 在自己的生成树内发送 BPDU。
- 每个 MSTI 的拓扑通过命令配置决定。
- 每个端口在不同 MSTI 上的生成树参数可以不同。
- 每个端口在不同 MSTI 上的角色、状态可以不同。
- 在 MST 域内，沿着其对应的 MSTI 转发。
- 在 MST 域间，沿着 CST 转发。

20. MSTP 对拓扑变化的处理：

MSTP 拓扑变化处理与 RSTP 拓扑变化处理过程类似。

- 在 RSTP 中检测拓扑是否发生变化只有一个标准：一个非边缘端口迁移到 Forwarding 状态。
- 为本交换设备的所有非边缘指定端口启动一个 TC While Timer，该计时器值是 Hello Time 的两倍。
- 在这个时间内，清空所有端口上学习到的 MAC 地址。
- 同时，由非边缘端口向外发送 RST BPDU，其中 TC 置位。一旦 TC While Timer 超时，则停止发送 RST BPDU。
- 其他交换设备接收到 RST BPDU 后，清空所有端口学习到 MAC 地址，除了收到 RST BPDU 的端口。然后也为自己所有的非边缘指定端口和根端口启动 TC While Timer，重复上述过程。

如此，网络中就会产生 RST BPDU 的泛洪。

## 70.2 命令手册

### 70.2.1 config stp

【功能描述】

**config stp** 用于进入 STP 视图。

**no config stp** 用于删除 STP 视图。

【命令格式】

**no config stp**

**config stp**

【视图】

根视图

【缺省情况】

未进入 STP 视图

【参数说明】

无

【使用举例】

配置进入 STP 视图

```
NOS# config stp
NOS(stp)#
```

【注意事项】

无。

### 70.2.2 global enable （STP视图）

【功能描述】

**no global enable** 用于关闭生成树协议。

**global enable** 用于开启生成树协议。

【命令格式】

**no global enable**

**global enable**

【视图】

STP 视图

【缺省情况】

未开启全局生成树协议。

【参数说明】

无

【使用举例】

配置开启/关闭 STP 协议。

```
NOS# config stp
NOS(stp)# global enable
NOS(stp)# no global enable
```

【注意事项】

在使能端口之前请先开启全局生成树协议，默认情况下，全局生成树启用后，所有端口均加入拓扑，可以关闭指定端口的 STP 使能。

### 70.2.3 timer max-age

【功能描述】

**timer max-age** 用于设置 STP 实例的 max-age 定时器的值。

**no timer max-age** 用于恢复 max-age 定时器缺省配置。

【命令格式】

**timer max-age** *VALUE*

**no timer max-age**

【视图】

stp 视图

【缺省情况】

缺省 max-age 值为 20s。

【参数说明】

*VALUE*：取值范围(6～40)。

【使用举例】

配置 max-age 值。

```
NOS# config stp
NOS(stp)# timer max-age 10
```

【注意事项】

Max Age 用于确定 BPDU 是否超时。

为保证网络拓扑的快速收敛，需要配置合适的时间参数。Forward Delay，Max Age，Hello Time 三个时间参数之间应满足以下关系，

否则会引起网络的频繁震荡：

•2×（Forward Delay－1 秒）≥Max Age

•Max Age≥2×（Hello Time＋1 秒）

### 70.2.4 timer hello

【功能描述】

**timer hello** 用于设置 STP 实例的 hello 定时器的值。

**no timer hello** 用于恢复 hello 定时器的缺省配置。

【命令格式】

**timer hello** *VALUE*

**no timer hello**

【视图】

stp 视图

【缺省情况】

缺省 hello 值为 2s。

【参数说明】

*VALUE:* 取值范围(1～10)。

【使用举例】

配置 hello 值 e 值。

```
NOS# config stp
NOS(stp)# timer hello 8
```

【注意事项】

Hello Time 用于检测链路是否存在故障。生成树协议每隔 Hello Time 时间会发送 BPDU，以确认链路是否存在故障。如果设备在 Hello Time 时间内没有收到 BPDU，则会由于消息超时而重新计算生成树。

为保证网络拓扑的快速收敛，需要配置合适的时间参数。Forward Delay，Max Age，Hello Time 三个时间参数之间应满足以下关系，

否则会引起网络的频繁震荡：

•2×（Forward Delay－1 秒）≥Max Age

•Max Age≥2×（Hello Time＋1 秒）

### 70.2.5 timer forward-delay

【功能描述】

**timer forward-delay** 用于设置 STP 实例的 forward-delay 定时器的值。

**no timer forward-delay** 用于恢复 forward-delay 定时器缺省配置。

【命令格式】

**timer forward-delay** *VALUE*

**no timer forward-delay**

【视图】

stp 视图

【缺省情况】

缺省值为 15s。

【参数说明】

*VALUE*：取值范围(4～30)。

【使用举例】

```
NOS# config stp
NOS(stp)# timer forward-delay 8
```

【注意事项】

Forward Delay 用于确定状态迁移的延迟时间。为了防止产生临时环路，生成树协议在端口由 Discarding 状态向 Forwarding 状态迁移的过程中设置了 Learning 状态作为过渡，并规定状态迁移需要等待 Forward Delay 时间，以保持与远端的设备状态切换同步。

为保证网络拓扑的快速收敛，需要配置合适的时间参数。Forward Delay，Max Age，Hello Time 三个时间参数之间应满足以下关系，

否则会引起网络的频繁震荡：

•2×（Forward Delay－1 秒）≥Max Age

•Max Age≥2×（Hello Time＋1 秒）

### 70.2.6 max-hops

【功能描述】

**max-hops** 命令用来配置 MST 域的最大跳数，该跳数用来限制 MST 域的规模。

**no max-hops** 命令用来恢复 max-hops 缺省情况。

【命令格式】

**max-hops** *VALUE*

**no max-hops**

【视图】

stp 视图

【缺省情况】

MST 域的最大跳数为 20 跳。

【参数说明】

*VALUE*：取值范围(1～40)。

【使用举例】

```
NOS# config stp
NOS(stp)# max-hops 8
```

【注意事项】

stp max-hops 命令用来配置 MST 域的最大跳数，该跳数用来限制 MST 域的规模。

### 70.2.7 instance priority

【功能描述】

**instance priority** 命令用来配置 STP 实例的优先级。

**no instance priority** 命令用来恢复 STP 实例的缺省优先级。

【命令格式】

**no instance** *INSTANCE-ID* **priority**

**instance** *INSTANCE-ID* **priority** *VALUE*

【视图】

stp 视图

【缺省情况】

stp 实例的优先级为 8 * 4094 = 32768。

【参数说明】

- INSTANCE-ID：msti 实例 ID，取值范围(0～31)。
- VALUE：优先级，取值范围(0～15)，步长为 4096，即实际优先级为配置值（0～15） *4094。

【使用举例】

```
NOS# config stp
NOS(stp)# instance 1 priority 8
```

【注意事项】

用于设定指定 STP 实例的优先级。

### 70.2.8 mode

【功能描述】

**no mode** 用来恢复 STP 默认模式。

**mode** 用来配置 STP 运行模式。

【命令格式】

**mode** <**mstp**|**rstp**|**stp**>

**no mode**

【视图】

stp 视图

【缺省情况】

默认模式为 mstp 模式。

【参数说明】

- mstp：配置生成树的工作模式为 MSTP 模式。
- rstp：配置生成树的工作模式为 RSTP 模式。
- stp：配置生成树的工作模式为 STP 模式。

【使用举例】

```
NOS# config stp
NOS(stp)# mode mstp
```

【注意事项】

MSTP 兼容 RSTP 和 STP。

RSTP 兼容 STP。

### 70.2.9 tc-protection

【功能描述】

**no tc-protection** 用来关闭 STP TC-BPDU 攻击保护功能。

**tc-protection** 用来开启 STP TC-BPDU 攻击保护功能。

【命令格式】

**no tc-protection**

**tc-protection**

【视图】

stp 视图

【缺省情况】

缺省情况下，防 TC-BPDU 攻击保护功能处于开启状态。

【参数说明】

无

【使用举例】

```
NOS# config stp
NOS(stp)# tc-protection
```

【注意事项】

建议不要关闭防 TC-BPDU 攻击保护功能。

### 70.2.10 tc-protection threshold

【功能描述】

**no tc-protection threshold** 用来恢复默认值。

**tc-protection threshold** 用来设置在单位时间内收到 TC-BPDU 后立即刷新转发地址表项的最高次数。

【命令格式】

**no tc-protection threshold**

**tc-protection threshold** *NUMBER*

【视图】

stp 视图

【缺省情况】

缺省情况下，在单位时间（固定为十秒）内，设备收到 TC-BPDU 后立即刷新转发地址表项的最高次数为 6。

【参数说明】

*NUMBER*：在单位时间（固定为十秒）内，设备收到 TC-BPDU 后立即刷新转发地址表项的最高次数。

【使用举例】

配置 tc-protection 阈值为 10。

```
NOS# config stp
NOS(stp)# tc-protection threshold 10
```

【注意事项】

无。

### 70.2.11 region-configuration

【功能描述】

**region-configuration** 用于进入 stp region 视图。

**no region-configuration** 用于删除 stp region 视图。

【命令格式】

**no region-configuration**

**region-configuration**

【视图】

stp 视图

【缺省情况】

未进入 stp region 视图

【参数说明】

无

【使用举例】

配置进入/退出 region 视图。

```
NOS# config stp
NOS(stp)# region-configuration
NOS(stp/region)#
NOS(stp)# no region-configuration
```

【注意事项】

无。

### 70.2.12 region-name （STP域视图）

【功能描述】

**region-name** 用于配置 STP 域名。

**no region-name** 用于恢复 STP 默认域名。

【命令格式】

**region-name** *NAME*

【视图】

stp/region 视图

【缺省情况】

NAME：缺省为设备的 MAC 地址。

【参数说明】

NAME：域名，字符串。

【使用举例】

配置域名为 abc

```
NOS# config stp
NOS(stp)# region-configuration
NOS(stp/region)# region-name abc
```

【注意事项】

- MSTP 模式下，修改域配置会重新计算网络拓扑。
- 相关显示信息请参照命令 show stp region。

### 70.2.13 revision-level

【功能描述】

**revision-level** 用于配置 STP 修订等级。

**no revision-level** 用户恢复默认 STP 修订等级。

【命令格式】

**revision-level** *VALUE*

【视图】

stp/region 视图

【缺省情况】

VALUE 缺省值 0。

【参数说明】

*VALUE*：修订等级，范围 0～65535。

【使用举例】

配置域修订级别为 1

```
NOS# config stp
rscu(stp)# region-configuration
rscu(stp/region)# revision-level 1
```

【注意事项】

- MSTP 模式下，修改域配置会重新计算网络拓扑。
- 相关显示信息请参照命令 show stp region。

### 70.2.14 instance vlan

【功能描述】

**instance vlan** 用于配置 STP 实例与 VLAN 的映射或绑定关系。

**no instance vlan** 用于删除 STP 实例与 VLAN 的映射或绑定关系。

【命令格式】

**no instance** *INSTANCE-ID* **vlan** [*VLAN_LIST*]

**instance** *INSTANCE-ID* **vlan** *VLAN_LIST*

【视图】

stp/region 视图

【缺省情况】

所有 vlan 映射到实例 0。

【参数说明】

- INSTANCE-ID：msti 实例 ID，取值范围(1～31)。
- VLAN_LIST：vlan ID，范围 0～4094，VLAN_LIST 支持单个 vlan 输入（如：1），多个 vlan 输入（如：1 3 5 7；多个 VLAN 之间空格分隔）或 vlan 范围（如：1 3 5 10-20 30 50；vlan 列表之间空格分隔）。

【使用举例】

配置域中 vlan 2 3 6 9-15 映射到实例 2 中

```
NOS# config stp
NOS(stp)# region-configuration
NOS(stp/region)# instance 2 vlan 2 3 6 9-15
```

【注意事项】

无

### 70.2.15 stp instance priority（接口视图）

【功能描述】

**no stp instance priroty** 用来恢复 STP 实例端口的缺省优先级。

**stp instance priroty** 用来配置 STP 实例端口的优先级。

【命令格式】

**no stp instance** *INSTANCE-ID* **priority**

**stp instance** *INSTANCE-ID* **priority** *VALUE*

【视图】

接口视图

【缺省情况】

stp 实例端口的优先级为 8 * 4094 = 32768。

【参数说明】

- INSTANCE-ID：取值范围 0～31。
- VALUE：取值范围 0～15，步长为 4096，即实际优先级为配置值（0～15） * 4094。

【使用举例】

配置 ge1 在实例 1 端口优先级为 0

```
NOS# config interface ge1
NOS(if-ge1)# stp instance  1 priority  0
```

【注意事项】

端口优先级改变会触发端口角色改变，或触发拓扑变化。

### 70.2.16 stp external-cost

【功能描述】

**no stp external-cost** 命令用于删除配置。

**stp external-cost** 命令用于配置 CIST 实例的端口路径开销。

【命令格式】

**no stp external-cost**

**stp external-cost** *VALUE*

【视图】

接口视图

【缺省情况】

未配置

【参数说明】

*VALUE*：取值范围(1～200000000)，STP 实例端口的路径消耗值。

【使用举例】

```
NOS# int ge1
NOS(if-ge1)# stp external-cost 8
```

【注意事项】

仅对 CIST 生效。

### 70.2.17 stp internal-cost

【功能描述】

**no stp instance internal-cost** 命令用于删除配置。

**stp instance internal-cost** 命令用于配置 MSTI 实例的端口内部路径开销。

【命令格式】

**no stp instance** *INSTANCE-ID* **internal-cost**

**stp instance** *INSTANCE-ID* **internal-cost** *VALUE*

【视图】

接口视图

【缺省情况】

未配置

【参数说明】

- INSTANCE-ID：msti 实例 ID，取值范围(0～31)。
- VALUE：取值范围(1～200000000)：STP 实例端口的路径消耗值。

【使用举例】

配置 ge1 外部路径开销为 2

```
NOS# config interface ge1
NOS(if-ge1)# stp external-cost 2
```

【注意事项】

无。

### 70.2.18 stp admin-edge

【功能描述】

no stp admin-edge 命令用来恢复缺省情况。

stp admin-edge 命令用来配置端口为边缘端口。

【命令格式】

no stp admin-edge

stp admin-edge

【视图】

接口视图

【缺省情况】

端口为非边缘端口

【参数说明】

无

【使用举例】

配置 ge1 为边缘端口

```
NOS# config interface ge1
NOS(if-ge1)# stp admin-edge
```

【注意事项】

仅对 CIST 生效

### 70.2.19 stp role-restriction

【功能描述】

stp role-restriction 命令用来开启端口角色限制功能。

no stp role-restriction 命令用来关闭端口角色限制功能。

【命令格式】

no stp role-restriction

stp role-restriction

【视图】

接口视图

【缺省情况】

端口角色限制功能处于关闭状态。

【参数说明】

无

【使用举例】

在 ge1 配置角色限制

```
NOS# config interface ge1
NOS(if-ge1)# stp role-restriction
```

【注意事项】

当开启了某端口的端口角色限制功能之后，该端口将不能被计算为根端口,而是成为替换端口。

另外，开启该功能后可能影响生成树拓扑的连通性，请慎重配置。

### 70.2.20 stp tcn-restriction

【功能描述】

**stp tcn-restriction** 命令用来开启 TC-BPDU 传播限制功能。

**no stp tcn-restriction** 命令用来关闭防 TC-BPDU 传播限制功能。

【命令格式】

**no stp tcn-restriction**

**stp tcn-restriction**

【视图】

接口视图

【缺省情况】

TC-BPDU 传播限制功能处于关闭状态。

【参数说明】

无

【使用举例】

在 ge1 配置 tcn 限制

```
NOS# config interface ge1
NOS(if-ge1)# stp tcn-restriction
```

【注意事项】

无

### 70.2.21 stp mcheck

【功能描述】

stp mcheck 命令用来在端口上执行 mcheck 操作。

【命令格式】

**stp mcheck**

【视图】

接口视图

【缺省情况】

不涉及

【参数说明】

无

【使用举例】

在 ge1 执行 mcheck

```
NOS# config interface ge1
NOS(if-ge1)# stp mcheck
```

【注意事项】

在运行 MSTP、RSTP 或 PVST 的设备上，若某端口连接着运行 STP 协议的设备，该端口收到 STP 报文后会自动迁移到 STP 模式。同时满足以下情况，该端口将无法自动迁移回原有模式：

- 当对端运行 STP 协议的设备关机或撤走。
- 该端口无法感知变化。
- 此时需要通过执行 mCheck 操作将其手工迁移回原有模式。只有当生成树的工作模式为 MSTP 模式、RSTP 模式时执行本命令才有效。

### 70.2.22 stp bpdu-protection

【功能描述】

**no stp bpdu-protection** 命令用来关闭端口的 BPDU 保护功能。

**stp bpdu-protection** 命令用来开启端口的 BPDU 保护功能。

【命令格式】

**no stp bpdu-protection**

**stp bpdu-protection**

【视图】

接口视图

【缺省情况】

BPDU 保护功能处于关闭状态。

【参数说明】

无。

【使用举例】

在 ge1 配置 bpdu 保护

```
NOS# config interface ge1
NOS(if-ge1)# stp bpdu-protection
```

【注意事项】

端口触发 bpdu 保护，通过下发 shutdwon 命令，down 端口。

### 70.2.23 stp enable

【功能描述】

**stp enable** 用于开启端口使能 stp。

**no stp enable** 用于关闭端口使能 stp。

【命令格式】

**no stp enable**

**stp enable**

【视图】

接口视图

【缺省情况】

默认情况下所有端口都使能 stp。

【参数说明】

无

【使用举例】

在 ge1 口去使能 stp 协议。

```
NOS# config interface ge1
NOS(if-ge1)# no stp enable
```

【注意事项】

无

### 70.2.24 stp p2p-detect

【功能描述】

**stp p2p-detect** 用于开启端口使能/去使能 stp 点对对链路检测。

**no stp p2p-detect** 用于关闭端口使能/去使能 stp 点对对链路检测。

【命令格式】

**no stp p2p-detect**

**stp p2p-detect** <**enable** | **disable**>

【视图】

接口视图

【缺省情况】

缺省情况下，端口的链路类型为 auto，即由系统自动检测与本端口相连的链路是否为点对点链路。

【参数说明】

**enable**：配置与本端口相连的链路为点对点链路。

**disable**：配置与本端口相连的链路非点对点链路。

【使用举例】

在 ge1 口配置链路类型为点对点链路

```
NOS# config interface ge1
NOS(if-ge1)# stp p2p-detect enable
```

【注意事项】

无。

### 70.2.25 stp loop-protection

【功能描述】

**no stp loop-protection** 命令用来关闭端口的环路保护功能。

**stp loop-protection** 命令用来开启端口的环路保护功能。

【命令格式】

**no stp loop-protection**

**stp loop-protection**

【视图】

接口视图

【缺省情况】

端口的环路保护功能处于关闭状态。

【参数说明】

无

【使用举例】

在 ge1 配置 loop 保护

```
NOS# config interface ge1
NOS(if-ge1)# stp loop-protection
```

【注意事项】

- 请在设备的根端口和替换端口上配置该命令。
- 请不要在与用户终端相连的端口上开启环路保护功能，否则该端口会因收不到 BPDU 而导致其所有 MSTI 将一直处于 Discarding 状态。
- 在同一个端口上，不允许同时配置边缘端口和环路保护功能，或者同时配置根保护功能和环路保护功能。

### 70.2.26 stp root-protection

【功能描述】

**no stp root-protection** 命令用来关闭端口的根保护功能。

**stp root-protection** 命令用来开启端口的根保护功能。

【命令格式】

**no stp root-protection**

**stp root-protection**

【视图】

接口视图

【缺省情况】

缺省情况下，端口上的根保护功能处于关闭状态。

【参数说明】

无

【使用举例】

在 ge1 配置 root 保护

```
NOS# config interface ge1
NOS(if-ge1)# stp root-protection
```

【注意事项】

请在设备的指定端口上进行配置。

在同一个端口上，不允许同时配置根保护功能和环路保护功能。

### 70.2.27 show stp

【功能描述】

**show stp brief** 命令显示所有实例所有接口简要信息。

**show stp cist** 用于查看 cist 实例下的详细信息。

**show stp cist global-info** 用于显示 STP 全局运行信息

**show stp instance** 用于查看指定实例的相关信息。

**show stp instance topology** 用于查看指定实例 topology 信息。

**show stp instance list** 命令用于查看已创建的 msti 实例。

**show stp instance vlan** 用于查看 mstp 实例域 vlan 的映射关系。

**show stp port-vlan** 用于查看 stp 协议端口 vlan 信息。

**show stp region** 用于查看 mstp 域配置信息。

【命令格式】

**show stp brief** [**instance** *INSTANCE-ID* ] [**json**]

**show stp cist** [**brief**] [**interface** *SWITCH_IF*] [**json**]

**show stp cist global-info** [**json**]

**show stp instance** *INSTANCE-ID* [**interface** *SWITCH_IF*] [**json**]

**show stp instance** *INSTANCE-ID* **topology** [**json**]

**show stp instance list** [**json**]

**show stp instance vlan** [**json**]

**show stp port-vlan** [**interface** *SWITCH_IF*]

**show stp region** [**json**]

【视图】

任意视图

【缺省情况】

不涉及

【参数说明】

- INSTANCE-ID：取值范围 0～31。
- SWITCH_IF：接口名字。
- **json**：以 json 格式输出。

【使用举例】

显示生成树中实例 0 的所有接口实例状态

```
NOS# show stp brief instance  0
-------[Global Info][Mode MSTP]-------
MSTID   Port             Role    State   Protection
----    ---------------   ----    ----    --------
0      bagg1             ROOT    FORW    N
0      ge1               DESI    FORW    N
0      ge2               DESI    FORW    N
NOS#
```

显示 cist 简要信息

```
NOS# show stp cist brief
Port             Role    State   Desg.bridge/port
---------------   ----    ----    -------------------
bagg1            ROOT    FORW    32768.000/50D3-3BCB-2201
ge1              DESI    FORW    32768.000/50D3-3BCB-2201
ge2              DESI    FORW    32768.000/50D3-3BCB-2201
```

显示 cist 全局信息

```
NOS# show stp cist global-info
-------[CIST Global Info][Mode MSTP]-------
  bridge id        : 32768.50D3-3BCB-2201
  designated root   : 0.50D3-3B94-3401
  regional root     : 32768.50D3-3BCB-2201
  root port        : bagg1 (#53)
```

```
  bridge timers    : Hello 2s, MaxAge 20s, FwdDelay 15s, AgeTime 300s
  max hops         : 20
  remaining hops   : 20
  config tc-guard  : yes
  config tc-threshold       : 6
  time since topology change : 910
  topology change count     : 1
  topology change          : no
  topology change port      : None
  last topology change port  : bagg1
```

显示聚合口 1 在 cist 中的信息

```
NOS# show stp cist  interface bagg1
Port              Role    State   Desg.bridge/port
----------------    ----    ----    --------------------
--------------Port bagg1 [Forwarding]--------------
  Enabled            : yes
  Speed              : 20
  Duplex             : Full
  Mac Addr           : 50:d3:3b:cb:22:01
  Role              : Root
  Port ID            : 0x8035
  External Port Cost   : 1000000
  Admin External Cost  : 0
  Internal Port Cost   : 1000000
  Admin Internal Cost  : 0
  Designated Root     : 0.000/50D3-3B94-3401
  Dsgn External Cost   : 1000000
  Dsgn Regional Root   : 32768.000/50D3-3BCB-2201
  Dsgn Internal cost   : 0
  Designated Bridge    : 32768.000/50D3-3BCB-2201
  Designated Port     : 0x8035
  Port Edged         : config: no, active: no
  Root Guard         : config: no
  Loop Guard         : config: no
  Topology Change Ack  : no
  Point-to-Point      : config: auto, active: yes
  Role Restricted     : no
  Tcn Restricted      : no
  Port Hello Time     : 2
  Port Protected      : no
  BPDU Filtered       : 0
  BPDU Sent          : 8
          STP: 0, RSTP: 0, MSTP: 8, TCN: 2
  BPDU Received       : 367
          STP: 0, RSTP: 0, MSTP: 367, TCN: 2
NOS#
```

显示聚合口 1 在特定实例上的信息

```
NOS# show stp instance  0 interface bagg1
```

```
------------Port bagg1 MSTI 0-------------
  role             : Root
  port id          : 0x8035
  state            : Forwarding
  disputed         : no
  active root-guard  : no
  active loop-guard  : no
  internal port cost : 1000000
  admin internal cost: 0
  dsgn regional root : 0.000/50D3-3B94-3401
  dsgn internal cost : 0
  designated bridge  : 0.000/50D3-3B94-3401
  designated port    : 0x8035
```

显示实例拓扑变化信息

```
NOS# show stp instance  0 topology
---------[MSTI 0 Global info]-------
  bridge id         : 32768.000/50D3-3BCB-2201
  regional root     : 32768.000/50D3-3BCB-2201
  root port         : bagg1 (#53)
  internal path cost : 0
  time since topology change : 593s
  topology change count     : 1
  topology change          : no
  topology change port      : None
  last topology change port  : bagg1
```

显示生成树上所有实例

```
NOS# show stp instance list
bridge0 list of known MSTIs:
 0 1
```

显示实例 vlan 映射信息

```
NOS# show stp instance  vlan
STP VID-to-MSTID allocation table:
  MSTID 0: 1-9,11-19,21-4094
  MSTID 1: 10,20
```

显示 stp 端口 vlan 信息信息

```
NOS# show stp port-vlan interface  ge1
Port       VLAN List
ge1        +------------
           | 10 20 30 40
```

显示设备域信息

```
NOS# show stp region
bridge0 MST Configuration Identifier:
  Format Selector:     0
  Configuration Name:   aaa
  Revision Level:      0
  Configuration Digest: 9BBDA9C70D91F633E1E145FBCBF8D321
```

【注意事项】

无。

## 70.3 配置举例

### 1. 组网需求

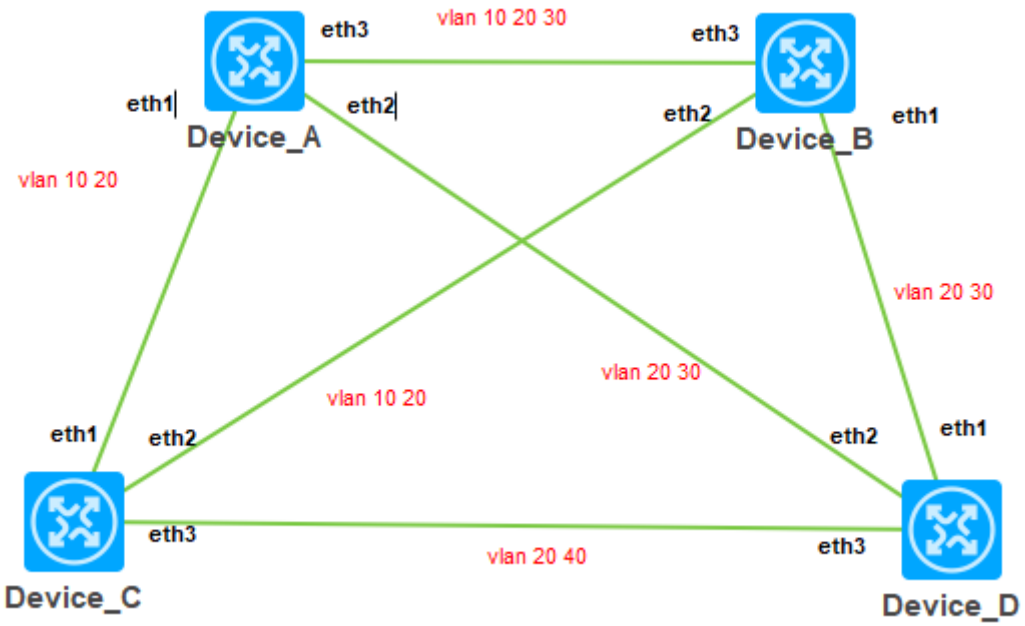
网络中所有设备都属于同一个 MST 域。Device A 和 Device B 为汇聚层设备，Device C 和 Device D 为接入层设备。

通过配置 MSTP，使不同 VLAN 的报文按照不同的 MSTI 转发：VLAN 10 的报文沿 MSTI 1 转发，VLAN 30 沿 MSTI 3 转发，VLAN 40 沿 MSTI 4 转发，VLAN 20 沿 MSTI 0 转发。

由于 VLAN 10 和 VLAN 30 在汇聚层设备终结、VLAN 40 在接入层设备终结，因此配置 MSTI 1 和 MSTI 3 的根桥分别为 Device A 和 Device B，MSTI 4 的根桥为 Device C。

### 2. 组网图

图70-1 组网图




### 3. 配置步骤

(1) 配置 VLAN 和端口

请照上图所示，在 Device A ,B,C,D 上分别创建 vlan 并配置接口 vlan 信息，配置过程略。

(2) 配置 STP Device A

#配置 MSTI 域的域名为 123，修订级别为 0，将 vlan 10 30 40 分别映射到 MSTI 1,3,4 上。并配置 MSTI 1 在此设备的优先级为 0（默认为 32768，此配置作用是使 Device A 作为 MSTI 1 的根桥）。

```
NOS# config stp
NOS(stp)# region-configuration
NOS(stp/region)#revision-level 0
NOS(stp/region)#region-name 123
NOS(stp/region)#instance 1 vlan 10
NOS(stp/region)#instance 1 priority 0
NOS(stp/region)#instance 3 vlan 30
```

```
NOS(stp/region)#instance 4 vlan 40
```
#使能 STP 全局生效。
```
NOS(stp)# global enable
```
(3) 配置 Device B

#配置 MSTI 域的域名为 123，修订级别为 0，将 vlan 10 30 40 分别映射到 MSTI 1,3,4 上，并配置 Device B 作为 MSTI 3 的根桥（设置优先级为 0）。
```
NOS# config stp
NOS(stp)# region-configuration
NOS(stp/region)#revision-level 0
NOS(stp/region)#region-name 123
NOS(stp/region)#instance 1 vlan 10
NOS(stp/region)#instance 3 priority 0
NOS(stp/region)#instance 3 vlan 30
NOS(stp/region)#instance 4 vlan 40
```
#使能 STP 全局生效。
```
NOS(stp)# global enable
```
(4) 配置 Device C

#配置 MSTI 域的域名为 123，修订级别为 0，将 vlan 10 30 40 分别映射到 MSTI 1,3,4 上，并配置 Device B 作为 MSTI 4 的根桥（设置优先级为 0）。
```
NOS# config stp
NOS(stp)# region-configuration
NOS(stp/region)#revision-level 0
NOS(stp/region)#region-name 123
NOS(stp/region)#instance 1 vlan 10
NOS(stp/region)#instance 4 priority 0
NOS(stp/region)#instance 3 vlan 30
NOS(stp/region)#instance 4 vlan 40
```
#使能 STP 全局生效。
```
NOS(stp)# global enable
```
(5) 配置 Device C

#配置 MSTI 域的域名为 123，修订级别为 0，将 vlan 10 30 40 分别映射到 MSTI 1,3,4 上。
```
NOS# config stp
NOS(stp)# region-configuration
NOS(stp/region)#revision-level 0
NOS(stp/region)#region-name 123
NOS(stp/region)#instance 1 vlan 10
NOS(stp/region)#instance 3 vlan 30
NOS(stp/region)#instance 4 vlan 40
```
#使能 STP 全局生效。
```
NOS(stp)# global enable
```
### 4. 验证配置

在本次配置中，Device A 的根桥 ID 最小，因此该设备在 MSTI0 中被选举为根桥。
```
NOS# show stp cist brief
Port             Role    State   Desg.bridge/port
----------------   ----    ----    --------------------
eth1             DESI    FORW    32768.000/0868-8DA1-CD02
eth2             DESI    FORW    32768.000/0868-8DA1-CD02
```

```
eth3              DESI    FORW    32768.000/0868-8DA1-CD02
eth4              DESI    FORW    32768.000/0868-8DA1-CD02
```

当网络拓扑稳定后，通过使用 display stp brief 命令可以查看各设备上生成树的简要信息。例如：

#查看 Device A 上生成树的简要信息。

```
NOS# show stp brief
MSTID   Port              Role    State   Protection
----    ----------------    ----    ----    --------
0       eth1              DESI    FORW       N
1       eth1              DESI    FORW       N
0       eth2              DESI    FORW       N
3       eth2              DESI    FORW       N
0       eth3              DESI    FORW       N
1       eth3              DESI    FORW       N
3       eth3              ROOT    FORW       N
0       eth4              DESI    FORW       N
```

因配置 Device A 作为 MSTI 1 的根桥，因此，可以查看到，此时 MSTI 1 生效的 Device A， B，C 的端口状态分别为

Device A

```
NOS# show stp brief instance 1
MSTID   Port              Role    State   Protection
----    ----------------    ----    ----    --------
1       eth1              DESI    FORW       N
1       eth3              DESI    FORW       N
```

Device B

```
NOS# show stp brief instance 1
MSTID   Port              Role    State   Protection
----    ----------------    ----    ----    --------
1       eth2              DESI    FORW       N
1       eth3              ROOT    FORW       N
```

Device C

```
NOS# show stp brief instance 1
MSTID   Port              Role    State   Protection
----    ----------------    ----    ----    --------
1       eth1              ROOT    FORW       N
1       eth2              ALTE    DISC       N
```

可以看出，Device A 作为根桥，Device C 的 eth2 被阻塞。

#查看 Device B 上生成树的简要信息。

```
NOS# show stp brief
MSTID   Port              Role    State   Protection
----    ----------------    ----    ----    --------
0       eth1              DESI    FORW       N
3       eth1              DESI    FORW       N
0       eth2              DESI    FORW       N
1       eth2              DESI    FORW       N
0       eth3              ROOT    FORW       N
1       eth3              ROOT    FORW       N
3       eth3              DESI    FORW       N
0       eth4              DESI    FORW       N
```

#查看 Device C 上生成树的简要信息。

```
NOS# show stp brief
MSTID   Port              Role    State   Protection
----    ----------------    ----    ----    --------
0       eth1              ROOT    FORW       N
1       eth1              ROOT    FORW       N
0       eth2              ALTE    DISC       N
1       eth2              ALTE    DISC       N
0       eth3              DESI    FORW       N
4       eth3              DESI    FORW       N
0       eth4              DESI    FORW       N
```

#查看 Device D 上生成树的简要信息。

```
NOS# show stp brief
MSTID   Port              Role    State   Protection
----    ----------------    ----    ----    --------
0       eth1              ALTE    DISC       N
3       eth1              ROOT    FORW       N
0       eth2              ROOT    FORW       N
3       eth2              ALTE    DISC       N
0       eth3              ALTE    DISC       N
4       eth3              ROOT    FORW       N
0       eth4              DESI    FORW       N
```

**端口角色说明**

- 根端口（Root Port）：在非根桥上负责向根桥方向转发数据的端口就称为根端口，根桥上没有根端口。
- 指定端口（Designated Port）：负责向下游网段或设备转发数据的端口就称为指定端口。
- 替换端口（Alternate Port）：是根端口和主端口的备份端口。当根端口或主端口被阻塞后，替换端口将成为新的根端口或主端口。
- 备份端口（Backup Port）：是指定端口的备份端口。当指定端口失效后，备份端口将转换为新的指定端口。当开启了生成树协议的同一台设备上的两个端口互相连接而形成环路时，设备会将其中一个端口阻塞，该端口就是备份端口。
- 边缘端口（Edge Port）：不与其他设备或网段连接的端口就称为边缘端口，边缘端口一般与用户终端设备直接相连。
- 主端口（Master Port）：是将 MST 域连接到总根的端口（主端口不一定在域根上），位于整个域到总根的最短路径上。主端口是 MST 域中的报文去往总根的必经之路。主端口在 IST/CIST 上的角色是根端口，而在其他 MSTI 上的角色则是主端口。
- 域边界端口（Boundary Port）：是位于 MST 域的边缘、并连接其他 MST 域或 MST 域与运行 STP/RSTP 的区域的端口。主端口同时也是域边界端口。在进行 MSTP 计算时，域边界端口在 MSTI 上的角色与 CIST 的角色一致，但主端口除外——主端口在 CIST 上的角色为根端口，在其他 MSTI 上的角色才是主端口。

**端口状态**

不同状态对流量的转发如下表所示。

表70-5 说明

| 状态 | 描述 |
| --- | --- |
| Forwarding | 该状态下的端口可以接收和发送BPDU，也转发用户流量 |

| | |
|---|---|
| Learning | 是一种过渡状态，该状态下的端口可以接收和发送BPDU，但不转发用户流量 |
| Discarding | 该状态下的端口可以接收和发送BPDU，但不转发用户流量 |

## 70.4 常见问题

无。

# 71 ERPS

## 71.1 特性简介

### 71.1.1 功能介绍

ERPS（Ethernet Ring Protection Switching），即以太网多环保护技术，是 ITU-T 定义的一种二层破环协议标准，标准号为 ITU-T G.8032/Y1344，因此又称为 G.8032。它定义了 RAPS(Ring Auto Protection Switching)协议报文和保护倒换机制。

可以有效防止广播风暴的产生，实现流量的快速迁移。收敛速度可以满足电信级的要求，提高网络的可靠性。

### 71.1.2 基本概念

#### 1. ERPS 环

ERPS 环,就是由一组配置了相同的控制 VLAN 且互连的二层交换设备构成,是 ERPS 协议的基本单位。

ERPS 环分为主环和子环。缺省情况下，ERPS 环都是主环。主环是封闭的环，子环是非封闭的环，需要通过命令进行配置。

子环仅在 ERPSv2 版本支持配置。

#### 2. 节点

加入 ERPS 环的二层交换设备称之为节点。每个节点不能多于两个端口加入同一个 ERPS 环。

#### 3. 端口角色

ERPS 协议中规定的端口角色主要有 RPL owner 端口、RPL neighbour 端口和普通端口三种类型。其中 RPL neighbour 端口类型只有 ERPSv2 版本支持。

- **RPL owner 端口：**一个 ERPS 环只有一个 RPL owner 端口，由用户配置决定，通过阻塞 RPL owner 端口转发用户流量来防止 ERPS 环中产生环路。当 RPL owner 端口所在设备收到故障报文得知 ERPS 环上其他节点或链路故障时，会自动放开 RPL owner 端口，此端口恢复流量的接收和发送，保证流量不会中断。RPL owner 端口所在的链路即为环保护链路 RPL（Ring Protection Link）。
- **RPL neighbour 端口：**RPL neighbour 端口指的是与 RPL owner 端口直接相连的端口。正常情况下，RPL owner 端口和 RPL neighbour 端口都会被阻塞，以防止环路产生。当 ERPS 环出现故障时，RPL owner 端口和 RPL neighbour 端口都会被放开。
- **普通端口：**在 ERPS 环中，除 RPL owner 端口和 RPL neighbour 端口以外的端口都是普通端口。普通端口负责监测自己直连的 ERPS 协议的链路状态，并把链路状态的变化消息及时通知其他端口

#### 4. 端口状态

在 ERPS 环中，启动 ERPS 协议的端口状态分为两种：

- **Forwarding：**在 Forwarding 状态下，端口既转发用户流量又接收/发送 ERPS 协议报文。
- **Discarding：**在 Discarding 状态下，端口仅能发送和接收 ERPS 协议报文。

#### 5. 控制 vlan

在 ERPS 环中，控制 VLAN 用来传递 ERPS 协议报文。每个 ERPS 环必须配置控制 VLAN。当端口加入已经配置控制 VLAN 的 ERPS 环后，端口将自动加入控制 VLAN。不同 ERPS 环不能使用相同 ID 的控制 VLAN。对于 NOS，控制 vlan 必须是未通过命令行创建过的 vlan。

### 6. 数据 vlan

与控制 vlan 相对，数据 vlan 用来传递数据报文。

### 7. ERPS 实例

ERPS 组网中一个环可以支持多个实例，每个实例都是一个逻辑环。每个实例中有自己的协议通道和数据通道，以及 Owner 节点；每个实例作为一个独立的协议实体，维护各自的状态和数据。

### 8. ERPS 运行状态

**Init 状态：**环配置不完整时处于 Init 状态。

**Idle 状态：**环初始化过后进入到稳定状态，当 Owner 节点进入 Idle 状态后，其它节点随之进入 Idle 状态。其中，Owner 节点和 Neighbor 节点的 RPL 端口为阻塞状态，即 RPL 不通；Owner 节点定时发送(NR, RB)报文。

**Protection 状态：**当环网某段链路出现故障，环路经过保护倒换，最终稳定到的状态。Owner 节点和 Neighbor 节点的 RPL 端口放开，即 RPL 放开，保证整个环网仍然是通的。当链路中某个节点进入 Protection 状态后，其它节点随之进入 Protection 状态。

**MS 状态：**MS 状态下可以手动倒换流量转发路径。当对链路中某个节点进行 MS 操作后，其它节点随之进入 MS 状态。

**FS 状态：**FS 状态下可以强制倒换流量转发路径。当对链路中某个节点进行 FS 操作后，其它节点随之进入 FS 状态。

**Pending 状态：**Pending 状态是一个不稳定的状态，是各状态在进行跳转时的一个过渡状态。

### 9. ERSP 定时器描述

ERPS 协议中使用的定时器主要有 Guard Timer 定时器、WTR(Wait+to Restore)Timer 定时器、Holdoff Timer 定时器和 WTB（Wait to Block） Timer 定时器。其中 WTB Timer 定时器只有 ERPSv2 版本支持，v1 版本不支持。

**Guard Timer 定时器 ：**链路故障或节点故障所涉及到的设备在故障恢复或执行清除操作后，向其他设备发送 NR RAPS 报文，并同时启动 Guard Timer 定时器，在该定时器超时前不处理 NR RAPS 报文，目的是防止收到过期的 NR RAPS 报文。如果定时器超时后还能收到其他端口发送的 NR RAPS 报文，则本端口的转发状态变为 Forwarding 状态。

**WTR Timer 定时器：**RPL owner 端口由于其他设备或链路故障而被放开后，当故障恢复时，有的端口可能还未由 Down 状态变为 Up 状态。为了防止立即阻塞 RPL owner 端口而引起网络震荡，当 RPL owner 端口收到某端口的 NR RAPS 报文后，会启动 WTR Timer 定时器。如果在定时器未超时前收到其他端口的 SF RAPS 报文，则关闭 WTR Timer 定时器。如果在 WTR Timer 定时器超时前始终没有收到其他端口的 SF RAPS 报文，则当 WTR Timer 定时器超时后，阻塞 RPL owner 端口，发送 NRRB RAPS 报文。其他端口在收到该报文后，再将自己端口的转发状态设置为 Forwarding 状态。

**Holdoff Timer 定时器：**对于运行 ERPS 的二层网络，保护倒换的顺序可能会有不同的要求，例如：多层业务的应用中，服务器出现故障后，用户可能会希望能有一段时间恢复服务器的故障，而客户端感知不到，即不会立即进行保护倒换。可设置合适的 Holdoff Timer 定时器，当发生故障时，故障并不会立即上报 ERPS，而只有当 Holdoff Timer 定时器超时后，如果故障仍未能恢复才会上报。

**WTB Timer 定时器：**当清除端口的手工切换状态（强制切换或手工切换）时，RPL owner 端口启用 WTB Timer 定时器，因为 ERPS 环内可能存在多个手工切换阻塞节点，只有当定时器超时后，清除操作才起作用，这样可以防止立即阻塞 RPL owner 端口而引起阻塞点震荡。 WTB Timer 定时器不支持配置，NOS 将该定时器的缺省值设定为 5s。

### 10. 回切/非回切模式

当 ERPS 链路恢复正常后，可以通过设置 ERPS 的回切/非回切模式来决定是否重新阻塞 RPL owner 端口。在回切模式下，如果故障链路恢复，等待 WTR 时间后，会重新阻塞 RPL owner 端口。阻塞链路会重新切回到 RPL 上。在非回切模式下，如果故障链路恢复，不启动 WTR Timer 定时器，而且阻塞链路还保持在原来的故障链路上，不会重新切回到 RPL 上。缺省情况下，ERPS 环处于回切模式。ERPSv1 版本只支持回切模式，ERPSv2 版本两种模式都支持。

#### 11. 阻塞点切换模式

ERPS 支持通过人为的配置来干预端口的阻塞，包括强制切换（Force Switch）和手工切换（Manual Switch）两种倒换方式。

**强制切换：**配置了强制切换的端口会马上被阻塞，不管环上其他链路是否存在故障等情况

**手工切换：**如果环的状态为 Idle 或 Pending 时，配置手工切换的端口就会阻塞，否则不阻塞。

除了强制切换和手工切换，ERPS 还支持清除操作，该功能主要用于如下三种情况：清除本地配置的手工切换和强制切换功能。当 ERPS 环处于回切模式时，在 WTB Timer 定时器或 WTR Timer 定时器超时之前，手工触发回切动作。当 ERPS 环处于非回切模式时，手工触发回切动作。

## 71.2 命令手册

### 71.2.1 config erps

【功能描述】

**config erps** 命令用来开启 erps 功能进入 erps 视图。

**no config erps** 命令关闭 erps 功能,并清除所有配置。

【命令格式】

**config erps**

**no config erps**

【视图】

根视图

【缺省情况】

erps 功能处于关闭状态。

【参数说明】

无

【使用举例】

启动 erps 功能，进入 erps 视图

```
NOS# config erps
NOS(erps)#
```

【注意事项】

无

### 71.2.2 ring

【功能描述】

**ring** 命令用来进入环视图进行 erps 环配置。

**no ring** 命令退出 ring 视图并且删除该 erps 环下配置。

【命令格式】

**ring** *RING-ID*

**no ring** *RING-ID*

【视图】

erps 视图

【缺省情况】

不存在 erps 环配置

【参数说明】

*RING-ID*：erps 环对应的环 id,取值范围 1-8。

【使用举例】

创建 ring id 为 1 的环

```
NOS# config erps
NOS(erps)# ring 1
NOS(erps/ring-1)#
```

【注意事项】

无

### 71.2.3 ring port

【功能描述】

**ring port** 命令用来在当前环配置端口为端口节点。

**no ring port** 命令取消当前环的端口节点配置。

【命令格式】

**<port0|port1> interface** *SWITCH_IF*

**no <port0|port1>**

【视图】

erps/ring 视图

【缺省情况】

erps 环无端口节点配置。

【参数说明】

- **port0**：配置环的第一个端口节点。
- **port1**：配置环的第二个端口节点。
- *SWITCH_IF*：二层接口名。

【使用举例】

在 ring id 为 1 的环将接口 ge17 配置为第一个端口节点

```
NOS# config erps
NOS(erps)# ring 1
NOS(erps/ring-1)#port0 interface ge17
```

【注意事项】

配置的接口 vlan-mode 必须是 trunk 模式。

配置的接口下必须无其他二层协议运行（例如 stp）。

若环下已经有实例使能则不能再进行端口节点的配置。

若已经配置端口节点则不能替换，只能反向配置后重新进行配置。

### 71.2.4 ring-type

【功能描述】

**ring-type sub-ring** 命令用来将当前 erps 环配置为子环。

**no ring-type sub-ring** 命令用来将当前 erps 环配置为主环。

【命令格式】

**ring-type sub-ring**

**no ring-type sub-ring**

【视图】

erps/ring 视图

【缺省情况】

erps 环为主环。

【参数说明】

无

【使用举例】

将 ring id 为 1 的环配置为子环

```
NOS# config erps
NOS(erps)# ring 1
NOS(erps/ring-1)#ring-type sub-ring
```

【注意事项】

环下已经有实例的情况下不允许将环的模式进行切换。

### 71.2.5 instance

【功能描述】

**instance** 命令用在当前环下配置实例并进入实例视图。

**no instance** 命令用来删除当前环下指定实例配置。

【命令格式】

**instance** *INSTANCE-ID*

**no instance** *INSTANCE-ID*

【视图】

erps/ring 视图

【缺省情况】

缺省状态环无实例配置

【参数说明】

*INSTANCE-ID*:实例 id,取值 1-4。

【使用举例】

为 ring id 为 1 的环配置为实例 id 为 1 的实例

```
NOS# config erps
NOS(erps)# ring 1
NOS(erps/ring-1)#instance 1
NOS(erps/ring-1/instance-1)#
```

【注意事项】

实例若已经使能则不能通过反向配置进行删除。

### 71.2.6 instance enable

【功能描述】

**instance enable** 命令用来使实例开始使能 erps 协议。

**no instance enable** 命令用来使实例取消使能 erps 协议。

【命令格式】

**instance enable**

**no instance enable**

【视图】

erps/ring/instance 视图

【缺省情况】

缺省情况实例下未使能 erps 协议。

【参数说明】

无

【使用举例】

在 ring id 为 1，实例 id 为 1 的实例上使能 erps 协议。

```
NOS# config erps
NOS(erps)# ring 1
NOS(erps/ring-1)#instance 1
NOS(erps/ring-1/instance-1)# instance enable
```

【注意事项】

无

### 71.2.7 control-vlan

【功能描述】

**control vlan** 命令用来为本实例配置控制 vlan。

**no control vlan** 命令用来删除当前实例配置的控制 vlan。

【命令格式】

**control-vlan** *VLAN-ID*

**no control-vlan**

【视图】

erps/ring/instance 视图

【缺省情况】

缺省情况实例无控制 vlan 配置。

【参数说明】

*VLAN-ID:* vlan id,取值 1-4094。

【使用举例】

为 ring id 为 1 的环下的实例 id 为 1 的实例配置 vlan id 为 123 的控制 vlan

```
NOS# config erps
NOS(erps)# ring 1
NOS(erps/ring-1)#instance 1
```

```
NOS(erps/ring-1/instance-1)#control-vlan 123
```

【注意事项】

- 实例若已经使能则不能进行 control-vlan 的配置操作。
- 已经配置为其他实例的控制 vlan 的 vlan 不能在本实例上重复进行配置。
- 已经创建过的 vlan 不能作为控制 vlan。
- 配置在 stp 非默认实例的 vlan 不能作为控制 vlan。

### 71.2.8 protected-vlan

【功能描述】

**protected-vlan** 命令用来为本实例配置保护 vlan。

**no protected-vlan** 命令用来删除当前实例配置的保护 vlan。

【命令格式】

**protected-vlan instance** *INSTANCE_LIST*

**no protected-vlan instance** *INSTANCE_LIST*

【视图】

erps/ring/instance 视图

【缺省情况】

缺省情况实例无保护 vlan 配置。

【参数说明】

*INSTANCE_LIST*: stp 下配置的 vlan 映射关系实例。

【使用举例】

将 stp instance 1 下绑定的 vlan 作为 ring id 为 1，实例 id 为 1 的实例的保护 vlan。

```
NOS# config erps
NOS(erps)# ring 1
NOS(erps/ring-1)#instance 1
NOS(erps/ring-1/instance-1)# protected-vlan instance 1
```

【注意事项】

若 stp instance 绑定的 vlan 数量变化则 erps instance 也会响应变化修改保护 vlan 的范围。

已经配置为其他实例的保护 vlan 的 stp instance 不能在本实例上重复进行配置。

未创建的 stp instance 不能作为保护 vlan。

### 71.2.9 node-role

【功能描述】

**node-role** 命令用来修改本实例的端口角色。

**no node-role** 命令用来恢复本实例的端口角色的缺省配置。

【命令格式】

**node-role** <owner|neighbor> **rpl** <port0|port1>

**no node-role**

【视图】

erps/ring/instance 视图

【缺省情况】

缺省情况实例下本节点所有端口角色都为 normal。

【参数说明】

- **owner**：端口角色修改为 RPL owner 端口。
- **neighbor**：端口角色修改为 RPL neighbour 端口。
- **port0**：指定 port0 作为 RPL 端口。
- **port1**：指定 port1 作为 RPL 端口。

【使用举例】

将 ring id 为 1，实例 id 为 1 的实例的第一个端口配置为 RPL owner 端口。

```
NOS# config erps
NOS(erps)# ring 1
NOS(erps/ring-1)#instance 1
NOS(erps/ring-1/instance-1)# node-role neighbor rpl port0
```

【注意事项】

实例已经使能的情况下不能修改端口角色。

### 71.2.10 switch

【功能描述】

**switch** 命令用来修改本实例下的指定端口的倒换模式。

**switch clear** 命令用来清除本实例下指定端口的倒换模式配置。

【命令格式】

**switch** <**force**|**manual**> <**port0**|**port1**>

**switch clear**

【视图】

erps/ring/instance 视图

【缺省情况】

缺省情况实例下本节点所有端口角色都未配置倒换模式。

【参数说明】

- **force**：配置 ERPS 环为强制倒换模式。
- **manual**：配置 ERPS 环为手动倒换模式。
- **port0**：本节点的第一个端口。
- **port1**：本节点的第二个端口。

【使用举例】

将 ring id 为 1，实例 id 为 1 的实例的第一个端口配置为强制倒换模式。

```
NOS# config erps
NOS(erps)# ring 1
NOS(erps/ring-1)#instance 1
NOS(erps/ring-1/instance-1)# switch force port0
```

【注意事项】

无

### 71.2.11 revertive

【功能描述】

**non-revertive** 命令用来配置本实例为非回切模式。

**no non-revertive** 命令用来配置本实例为回切模式。

【命令格式】

**non-revertive**

**no non-revertive**

【视图】

erps/ring/instance 视图

【缺省情况】

缺省情况实例为回切模式。

【参数说明】

无

【使用举例】

将 ring id 为 1，实例 id 为 1 的实例配置为非回切模式。

```
NOS# config erps
NOS(erps)# ring 1
NOS(erps/ring-1)#instance 1
NOS(erps/ring-1/instance-1)# non-revertive
```

【注意事项】

无

### 71.2.12 tc-notify

【功能描述】

**tc-notify** 命令用来配置本实例拓扑变化时通知其他实例。

**no tc-notify** 命令用来取消配置本实例拓扑变化时通知其他实例。

【命令格式】

**tc-notify ring-id** *RING-ID* **instance-id** *INSTANCE-ID*

**no tc-notify ring-id** *RING-ID* **instance-id** *INSTANCE-ID*

【视图】

erps/ring/instance 视图

【缺省情况】

缺省情况实例拓扑变化时不通知任何其他实例。

【参数说明】

*RING-ID*：需要通知的其他实例所属的环 id,取值范围 1-8。

*INSTANCE-ID*：需要通知的其他实例所属的实例 id，取值范围 1-4。

【使用举例】

为 ring id 为 1，实例 id 为 1 的实例配置拓扑变化时通知 ring id 为 1，实例 id 为 2 的实例

```
NOS# config erps
NOS(erps)# ring 1
```

```
NOS(erps/ring-1)#instance 1
NOS(erps/ring-1/instance-1)# tc-notify ring-id 1 instance-id 2
```

【注意事项】

需要通知的其他实例必须已创建。

一个实例在拓扑变化时最多只能通知 16 个其他实例。

不能配置通知本实例。

### 71.2.13 timer guard

【功能描述】

**timer guard** 命令用来配置 guard timer 定时器的超时时间。

**no timer guard** 命令用来配置恢复 guard timer 定时器的缺省配置。

【命令格式】

**timer guard** *GUARD-TIMER*

**no timer guard**

【视图】

erps/ring/instance 视图

【缺省情况】

Guard Timer 定时器的缺省配置超时时间为 500ms。

【参数说明】

*GUARD-TIMER*：guard timer 定时器的超时时间范围为 10-2000ms。

【使用举例】

为 ring id 为 1，实例 id 为 1 的实例的 guard 定时器超时时间配置为 100ms。

```
NOS# config erps
NOS(erps)# ring 1
NOS(erps/ring-1)#instance 1
NOS(erps/ring-1/instance-1)# timer guard 100
```

【注意事项】

无

### 71.2.14 timer wtr

【功能描述】

**timer wtr** 命令用来配置 wtr timer 定时器的超时时间。

**no timer wtr** 命令用来配置恢复 wtr timer 定时器的缺省配置。

【命令格式】

**timer wtr** *WTR-TIMER*

**no timer wtr**

【视图】

erps/ring/instance 视图

【缺省情况】

wtr timer 定时器的缺省配置超时时间为 5min。

【参数说明】

*WTR-TIMER*：wtr timer 定时器的超时时间范围为 1-12min。

【使用举例】

为 ring id 为 1，实例 id 为 1 的实例的 wtr 定时器超时时间配置为 10min

```
NOS# config erps
NOS(erps)# ring 1
NOS(erps/ring-1)#instance 1
NOS(erps/ring-1/instance-1)# timer wtr 10
```

【注意事项】

无

### 71.2.15 timer hold-off

【功能描述】

**timer hold-off** 命令用来配置 hold-off timer 定时器的超时时间。

**no timer hold-off** 命令用来配置恢复 hold-off timer 定时器的缺省配置。

【命令格式】

**timer hold-off** *HOLDOFF-TIMER*

**no timer hold-off**

【视图】

erps/ring/instance 视图

【缺省情况】

hold-off timer 定时器的缺省配置超时时间为 0ms。

【参数说明】

*HOLDOFF-TIMER*：hold-off timer 定时器的超时时间范围为 0-10000ms。

【使用举例】

为 ring id 为 1，实例 id 为 1 的实例的 hold-off 定时器超时时间配置为 10ms

```
NOS# config erps
NOS(erps)# ring 1
NOS(erps/ring-1)#instance 1
NOS(erps/ring-1/instance-1)# timer hold-off 10
```

【注意事项】

无

### 71.2.16 show erps

【功能描述】

**show stp brief** 命令用于查看 erps 相关配置的信息。

【命令格式】

**show erps** [**ring** *RING-ID* **instance** *INSTANCE-ID*] [**json**]

【视图】

任意视图

【缺省情况】

不涉及

【参数说明】

- *RING-ID*：环 ID， 取值范围(1-8)
- *INSTANCE-ID*：ERPS 实例 ID， 取值范围(1-4)。
- **json**：以 json 格式输出。

【使用举例】

若不指定环 id 和实例 id 则显示所有 erps 实例的端口角色状态以及该节点的状态：

```
NOS(erps/ring-1/instance-1)# show erps
Flags: B - Blocked  R - Rpl Port  D -- Down
      S - Force Switch or Manual Switch
Ring  Instance  NodeRole  State      Port0           Port1
--------------------------------------------------------------------------
1     1         Normal    Pending    ge15(B)         ge16
```

若指定环 id 和实例 id 则显示该实例的详细信息：

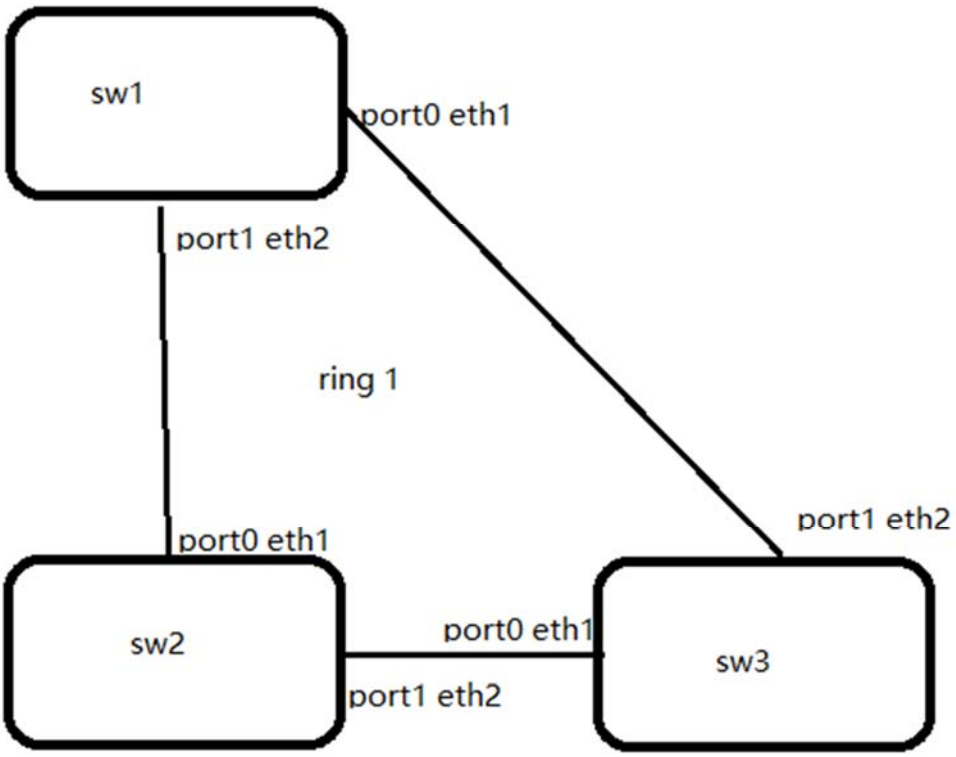
```
NOS(erps/ring-1/instance-1)# show erps ring 1 instance 1
Ring ID                    : 1
Instance ID                : 1
Control Vlan               : 999
Port0                      : ge15
Port1                      : ge16
Protected Instance         : 0
Protected Vlan             : 1-998,1000-4094
State                      : Pending
Node Role                  : Normal
Sub Ring                   : No
Revertive Mode             : Revertive
Wtr Timer                  : 5 min
Guard Timer                : 500 ms
Hold-off Timer             : 0 ms
--------------------------------------------------------------------------
Port               Port Role       Status
--------------------------------------------------------------------------
ge15               Normal          Block
ge16               Normal          Forwarding
```

【注意事项】

无。

## 71.3 配置举例

图71-1 配置举例




按照如上图的 ring1 所示进行配置，将 sw2 的 eth2 接口作为 rpl owner 端口：

SW1 上配置：

```
SW/1#:config interface eth1
sw/1(if-eth1)#:no stp enable
sw/1(if-eth1)#:vlan-mode trunk
sw/1# config stp
sw/1(stp)# region-configuration
sw/1(stp/region)# instance 1 vlan  123 234
SW/1(erps)#  ring 2
SW/1(erps/ring-1)# port0 interface eth1
SW/1(erps/ring-1)# port1 interface eth2
SW/1(erps/ring-1)# instance 1
SW/1(erps/ring-1/instance-1)# control-vlan 4090
SW/1(erps/ring-1/instance-1)#node-role neighbor rpl port1
SW/1(erps/ring-1/instance-1)# protected-vlan instance 1
SW/1(erps/ring-1/instance-1)#instance enable
```

SW2 上配置

```
SW/2#:config interface eth1
sw/2(if-eth1)#:no stp enable
sw/2(if-eth1)#:vlan-mode trunk
```

```
sw/2# config stp
sw/2(stp)# region-configuration
sw/2(stp/region)# instance 1 vlan  123 234
SW/2(erps)#  ring 2
SW/2(erps/ring-1)# port0 interface eth1
SW/2(erps/ring-1)# port1 interface eth2
SW/2(erps/ring-1)# instance 1
SW/2(erps/ring-1/instance-1)# control-vlan 4090
SW/2(erps/ring-1/instance-1)#node-role owner rpl port1
SW/2(erps/ring-1/instance-1)# protected-vlan instance 1
SW/2(erps/ring-1/instance-1)#instance enable
```

SW3 上配置

```
SW/3#:config interface eth1
sw/3(if-eth1)#:no stp enable
sw/3(if-eth1)#:vlan-mode trunk
sw/3# config stp
sw/3 (stp)# region-configuration
sw/3 (stp/region)# instance 1 vlan  123 234
SW/3(erps)#  ring 2
SW/3(erps/ring-1)# port0 interface eth1
SW/3(erps/ring-1)# port1 interface eth2
SW/3(erps/ring-1)# instance 1
SW/3(erps/ring-1/instance-1)# control-vlan 4090
SW/3(erps/ring-1/instance-1)# protected-vlan instance 1
SW/3(erps/ring-1/instance-1)#instance enable
```

此时对于 sw1 和 sw3，show erps 指定环 id 1，实例 id 1 得到的结果一致，以 sw3 举例：

```
SW/3# show erps ring 1 instance 1
Ring ID                    : 1
Instance ID                : 1
Control Vlan               : 4090
Port0                      : eth1
Port1                      : eth2
Protected Instance         : 1
Protected Vlan             : 123,234
State                      : Idle
Node Role                  : Normal
Sub Ring                   : No
Revertive Mode             : Revertive
Wtr Timer                  : 5 min
Guard Timer                : 500 ms
Hold-off Timer             : 0 ms
---------------------------------------------------------------------
Port               Port Role       Status
---------------------------------------------------------------------
eth1               Normal        Forwarding
eth2               Normal        Forwarding
```

对于 sw2，show erps 指定环 id 1，实例 id 1 得到的结果为：

```
SW/2# show erps ring 1 instance 1
Ring ID                    : 1
Instance ID                : 1
```

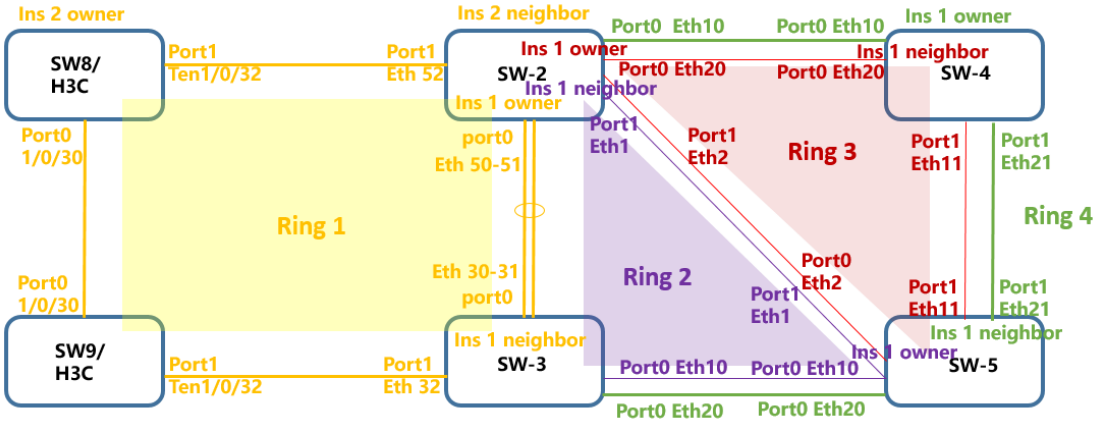
```
Control Vlan               : 4090
Port0                     : eth1
Port1                     : eth2
Protected Instance          : 1
Protected Vlan             : 123,234
State                     : Owner
Node Role                  : Normal
Sub Ring                   : No
Revertive Mode             : Revertive
Wtr Timer                 : 5 min
Guard Timer                : 500 ms
Hold-off Timer             : 0 ms
--------------------------------------------------------------------------
Port               Port Role       Status
--------------------------------------------------------------------------
eth1                   Rpl            Block
eth2               Normal         Forwarding
```

## 71.4 说明

ERPS 协议本身不支持主环和子环相切配置，例如以下组网。如果配置 Ring1 为主环，Ring3 为子环，在 Ring3 的管理 Vlan 内，协议报文广播风暴。此时应该把 Ring3 也配置成主环。

ERPS 不支持两个节点之间存在多条物理链路成环。如下图，Ring1 为主环，Ring2 和 Ring4 为子环，即使在不考虑 Ring3 的情况下，即在 SW3 的 eth10，eth20；SW5 的 eth10，eth20 之间形成数据报文环路。因此，不要在同一个节点之间配置多个环。

图71-2 物理链路



# 72 环路检测

## 72.1 功能介绍

### 72.1.1 功能简介

loopback detect 是用于发现二层网络中的环路并在发现是时及时通知用户检查配置并将出问题端口状态进行取消使能，避免对整个网络造成严重影响的检测技术。

### 72.1.2 原理描述

当使能了环路检测功能后，系统开始以一定的时间间隔发送环路检测报文，该间隔越长耗费的系统性能越少，该间隔越短环路检测的灵敏度越高。用户可以通过本配置调整发送环路检测报文的时间间隔，以在系统性能和环路检测的灵敏度之间进行平衡。之后会开始检查该报文是否返回本设备，进而判断该接口、设备下挂网络或设备，或者设备双接口间是否存在环路。在发现环路后，环路检测能向网管发送告警和记录日志，并能根据用户事先的配置对接口进行关闭处理，从而使接口处于受控状态，减小环路对本设备乃至整个网络的影响。

## 72.2 命令手册

### 72.2.1 config loopback-detect

【功能描述】

**config loopback-detect** 用于进入 loopdd 视图。

**no config loopback-detect** 用于删除 loopdd 视图。

【命令格式】

**no config loopback-detect**

**config loopback-detect enable**

【视图】

根视图

【缺省情况】

未进入 loopdd 视图。

【参数说明】

不涉及。

【使用举例】

配置进入 loopdd 视图。

```
NOS# config loopback-detect enable
NOS(loopdd)#
```

【注意事项】

无。

### 72.2.2 detect-interval

【功能描述】

**detect-interval** 命令用于设置定期发送环路检测报文的时间间隔。

**no detect-interval** 命令用于恢复发送环路检测报文的时间间隔为默认值。

【命令格式】

**detect-interval** *VALUE*

**no detect-interval**

【视图】

loopdd 视图

【缺省情况】

缺省为系统默认值 30s。

【参数说明】

*VALUE*：环路检测报文的时间间隔 3～300：（单位：秒）。

【使用举例】

将环路检测报文的时间间隔改为 50 秒：

```
NOS# config loop-detect enable
NOS(loopdd)# detect-interval 50
```

【注意事项】

无。

### 72.2.3 shutdown-interval

【功能描述】

**shutdown-interval** 命令用于设置 shutdown 接口的时间间隔。

**no shutdown-interval** 命令用于恢复 shutdown 接口时间间隔为默认值。

【命令格式】

**shutdown-interval** *VALUE*

**no shutdown-interval**

【视图】

loopdd 视图

【缺省情况】

缺省为系统默认值 30s。

【参数说明】

*VALUE*: 环路检测报文的时间间隔 10～3600：（单位：秒）。

【使用举例】

将环路检测 shutdown 接口时间间隔改为 50 秒。

```
NOS# config loop-detect enable
NOS(loopdd)# shutdown-interval 50
```

【注意事项】

无。

### 72.2.4 loopback-detect enable

【功能描述】

**loopback-detect enable** 命令用于开启该接口下指定 VLAN 的环路检测功能。

**no loopback-detect enable** 命令关闭该接口下指定 VLAN 的环路检测功能。

【命令格式】

**no loopback-detect enable vlan** [*VLAN_LIST...*]

**loopback-detect enable vlan** *VLAN_LIST...*

【视图】

二层接口视图

【缺省情况】

接口未开启环路检测。

【参数说明】

*VLAN_LIST*：vlan ID，范围 0～4094，VLAN_LIST 支持单个 vlan 输入（如：1），多个 vlan 输入（如：1 3 5 7；多个 VLAN 之间空格分隔）或 vlan 范围（如：1 3 5 10-20 30 50；vlan 列表之间空格分隔）。

【使用举例】

聚合口 bagg10 vlan 10 开启环路检测：

```
NOS# config interface bagg10
NOS(if-bagg10)# loopback-detect enable vlan 10
```

【注意事项】

目前最多支持 16 个 VLAN 配置。

### 72.2.5 show loopback-detect

【功能描述】

**show loopback-detect** 命令用于查看使能环路检测的接口的 VLAN，报文收发，接口状态基本信息。

【命令格式】

**show loopback-detect interface** [*SWITCH_IF*] [**json**]

【视图】

所有视图

【缺省情况】

显示所有使能环路检测的接口

【参数说明】

*SWITCH_IF*：指定接口名。

**json**：以 json 格式输出。

【使用举例】

```
NOS# show loopback-detect interface ge1
 Interface   : ge1
 MAC         : 50:d3:3b:b0:c9:02
 Port No     : 1
 State       : UP
```

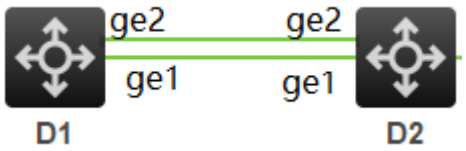
```
 Packet Tx  : 3
 Packet Rx  : 0
 Looped     : No
 VLAN    Tx            Rx            Looped
 ----    --------       --------       ------
 10      3             1             Y
-----------------------------------------------
```

【注意事项】

无

## 72.3 配置举例

图72-1 配置举例




按照如上图所示组网，在 D1 上做如下配置：

```
NOS# config vlan 10
NOS(vlan-10)#
NOS# config loopback-detect enable
NOS(loopdd)# config interface ge1
NOS(if-ge1)# loopback-detect enable vlan 10
NOS(if-ge1)# config interface ge2
NOS(if-ge2)# loopback-detect enable vlan 10
```

在 D2 上做如下配置

```
NOS# config vlan 10
NOS(vlan-10)#
NOS# config loopback-detect enable
NOS(loopdd)# config interface ge1
NOS(if-ge1)# loopback-detect enable vlan 10
NOS(if-ge1)# config interface ge2
NOS(if-ge2)# loopback-detect enable vlan 10
```

查看环上接口状态：

```
NOS# show loopback-detect interface ge1
 Interface   : ge1
 MAC        : 50:d3:3b:b0:c9:02
 Port No     : 1
 State      : UP
 Packet Tx   : 3
 Packet Rx   : 0
 Looped     : No
 VLAN    Tx            Rx            Looped
 ----    --------       --------       ------
 10      3             1             Y
```

---

## 72.4 常见问题

无。

# 73 Smart link

## 73.1 特性简介

Smart link 是针对双上行组网的解决方案，目的是实现高效可靠的主备链路的冗余备份和故障快速切换。

## 73.2 相关概念

### 73.2.1 运行机制

双上行的两个端口组成一个 Smart link 组，配置为主端口和副端口，主端口链路故障，立即切换为副端口转发数据。

保护 VLAN Smart link 组允许转发的 VLAN,以 MST 实例的形式进行映射。

### 73.2.2 控制VLAN

FLUSH 报文转发的 VLAN。

### 73.2.3 FLUSH报文

说明：不配置 flush 报文，Smart Link 主端口故障链路也会立即切换到从端口，但是由于上行交换机学习的 MAC 地址仍然对应原接口，此时需要等到 mac 地址表刷新业务才能恢复故障。通过 flush 报文可以立即刷新正确的 MAC 地址记录

技术背景

链路发生故障切换时,上行交换机学习的 MAC 地址仍然对应原接口,需要通过流量来刷新正确的 MAC 地址记录。

解决方案

收到 Flush 报文的交换机，会在接收报文的端口重新学习 MAC 地址记录。

### 73.2.4 Smart link角色抢占模式

默认主端口故障恢复后，会发生角色抢占，即主链路故障恢复后业务切换回到主链路。可通过配置为非回切模式，即主链路故障恢复后业务仍然走备链路，除非备链路故障再次切换到主链路。

## 73.3 命令手册

### 73.3.1 config smart-link

【功能描述】

**config smart-link** 命令用来开启 smart-link 功能进入 smart-link 视图。

**no config smart-link** 命令关闭 smart-link 功能,并清除所有配置。

【命令格式】

config smart-link

no config smart-link

【视图】

根视图

【缺省情况】

smart-link 功能处于关闭状态。

【参数说明】

无。

【使用举例】

#启动 smart-link 功能，进入 smart-link 视图

```
NOS# config smart-link
NOS(smart-link)#
```

【注意事项】

无。

### 73.3.2 group

【功能描述】

**group** 命令用来创建一个灵活链路组。

**no group** 命令删除一个灵活链路组。

【命令格式】

group *GROUP*

no group *GROUP*

【视图】

smart-link 视图

【缺省情况】

缺省未创建灵活链路组。

【参数说明】

*GROUP*：灵活链路组 id，取值范围(1-32)。

【使用举例】

#进入 smart-link 视图,创建灵活链路组 id 为 2 的灵活链路组

```
NOS# config smart-link
NOS(smart-link)# group 2
NOS(smlk/group-2)#
```

【注意事项】

无。

### 73.3.3 protected-vlan

【功能描述】

**protected-vlan** 命令用来为本灵活链路组配置保护 vlan。

**no protected-vlan** 命令用来删除当前灵活链路组配置的保护 vlan。

【命令格式】

protected-vlan instance *INSTANCE_ID*

no protected-vlan instance *INSTANCE_ID*

【视图】

smart-link/group 视图

【缺省情况】

缺省情况灵活链路组无保护 vlan 配置

【参数说明】

*INSTANCE_ID*：stp 下配置的 vlan 映射关系实例。

【使用举例】

#将 stp instance 1 下绑定的 vlan 作为灵活链路组 id 为 1 的保护 vlan

```
NOS# config smart-link
NOS(smart-link)# group 1
NOS(smart-link /group-1)# protected-vlan instance 1
```

【注意事项】

若 stp instance 绑定的 vlan 数量变化，则 smart-link instance 也会响应变化修改保护 vlan 的范围。

### 73.3.4 control-vlan

【功能描述】

**control vlan** 命令用来为本灵活链路组配置控制 vlan。

**no control vlan** 命令用来删除本灵活链路组配置的控制 vlan。

【命令格式】

control-vlan *VLANID*

no control-vlan

【视图】

smart-link/group 视图

【缺省情况】

缺省情况灵活链路组无控制 vlan 配置。

【参数说明】

*VLANID*：配置灵活链路组配置控制的 vlan id，id 范围为(1-4094)。

【使用举例】

#为 group id 为 1 的灵活链路组配置 vlan id 为 123 的控制 vlan

```
NOS# config smart-link
NOS(smart-link)# group 1
NOS(smart-link /group-1)# control-vlan 123
```

【注意事项】

控制 vlan 必须已创建。

配置控制 vlan 之前必须已经配置保护 vlan。

控制 vlan 必须属于对应灵活链路组配置的保护 vlan 映射 MST 实例中的 vlan。

### 73.3.5 group port

【功能描述】

**group port** 命令用来为本灵活链路组配置指定角色的端口。

**no group port** 命令用来删除本灵活链路组的指定角色端口。

【命令格式】

<master|slave> interface *SWITCH_IF*

no <master|slave> interface

【视图】

smart-link/group 视图

【缺省情况】

缺省情况灵活链路组无主端口和备从端口配置。

【参数说明】

- master：主端口。
- slave：从端口。
- *SWITCH_IF*：指定接口号，可选二层接口号。

【使用举例】

#为 group id 为 1 的灵活链路组配置端口 ge1 为主端口

```
NOS# config smart-link
NOS(smart-link)# group 1
NOS(smart-link /group-1)# master interface fe1
```

【注意事项】

指定接口必须为二层端口，可以是聚合口，但是不能是聚合口成员端口。

只有完成主端口和从端口的配置以后灵活链路组才会开启端口下进行保护 vlan 的链路备份功能。

加入灵活链路组的接口不能使能 mvrp 功能。

### 73.3.6 revertive

【功能描述】

**non-revertive** 命令用来配置本灵活链路组为非回切模式。

no non-revertive 命令用来配置本灵活链路组为回切模式。

【命令格式】

non-revertive

no non-revertive

【视图】

smart-link/group 视图

【缺省情况】

缺省情况灵活链路组为回切模式。

【参数说明】

无。

【使用举例】

#将 group id 为 1 的灵活链路组配置为非回切模式

```
NOS# config smart-link
NOS(smart-link)# group 1
NOS(smart-link /group-1)# non-revertive
```

【注意事项】

无。

### 73.3.7 timer wtr

【功能描述】

**timer wtr** 命令用来配置 wtr timer 定时器的超时时间。

**no timer wtr** 命令用来配置恢复 wtr timer 定时器的缺省配置。

【命令格式】

timer wtr *TIME*

no timer wtr

【视图】

smart-link/group 视图

【缺省情况】

wtr timer 定时器的缺省配置超时时间为 0ms。

【参数说明】

*TIME*：wtr timer 定时器的超时时间范围为 0-10000ms。

【使用举例】

#为 group id 为 1 的灵活链路组的 wtr 定时器超时时间配置为 2s

```
NOS# config smart-link
NOS(smart-link)# group 1
NOS(smart-link /group-1)# timer wtr 2000
```

【注意事项】

无

### 73.3.8 timer hold-off

【功能描述】

**timer hold-off** 命令用来配置 hold-off timer 定时器的超时时间。

**no timer hold-off** 命令用来配置恢复 hold-off timer 定时器的缺省配置。

【命令格式】

timer hold-off *TIME*

no timer hold-off

【视图】

smart-link/group 视图

【缺省情况】

hold-off timer 定时器的缺省配置超时时间为 0ms。

【参数说明】

*TIME* ：hold-off timer 定时器的超时时间范围为 0-10000ms。

【使用举例】

#为 group id 为 1 的灵活链路组的 hold-off 定时器超时时间配置为 20ms

```
NOS# config smart-link
NOS(smart-link)# group 1
NOS(smart-link /group-1)# timer hold-off 20
```

【注意事项】

无。

### 73.3.9 flush enable

【功能描述】

**flush enable** 命令用来配置端口开启接收指定 vlan 的 flush 报文。

**no flush enable** 命令用来配置端口不接收指定 vlan 的 flush 报文。

【命令格式】

smart-link flush enable control-vlan *VLAN_LIST...*

no smart-link flush enable control-vlan *VLAN_LIST...*

【视图】

二层端口视图

【缺省情况】

缺省情况接口不接受任何 vlan 的 flush 报文。

【参数说明】

*VLAN_LIST...*：vlan ID，范围 0-4094，VLAN_LIST 支持单个 vlan 输入（如：1），多个 vlan 输入（如：1 3 5 7；多个 VLAN 之间空格分隔）或 vlan 范围（如：1 3 5 10-20 30 50；vlan 列表之间空格分隔）。

【使用举例】

#配置端口 ge1 接收 vlan 100 的 flush 报文

```
NOS# config interface ge1
NOS(if-ge1)# smart-link  flush enable control-vlan 100
```

【注意事项】

无。

### 73.3.10 show smart-link

【功能描述】

show smart-link group 用于查看灵活链路组配置情况。

**show smart-link flush** 用于查看接收 flush 报文总数和最后接收的 flush 报文参数。

【命令格式】

show smart-link group [*GROUP*]

show smart-link flush

【缺省情况】

不涉及。

【参数说明】

*GROUP*:指定要显示的灵活链路组 id,若不指定则显示当前配置的全部灵活链路组。取值范围为 1-32。

【使用举例】

#显示 group 2 下的全部配置

```
SW/14# show smart-link group 2
smart-link group 2 infomation:
preemption mode : enable
preemption delay: 0
Control VLAN    : 1002
Protect instance: 2
interface Role          state     Flush-count        Last-Send-time
bagg20    master        active     3488               09:09:12  2023-12-26
ge17      slave         blocking  3491               09:09:07  2023-12-26
```

#显示设备 sw14 接收 flush 报文情况

```
SW/14# show smart-link flush
Recv flush pkt count     :  2895
Last recv interface      :  bagg10
Last recv pkt time       :  09:00:43  2023-12-26
Last recv Control Vlan   :  1000
Last recv pkt device id  :  08:68:8d:ab:49:01
```

# 74 Monitor Link

## 74.1 功能介绍

### 74.1.1 功能简介

Monitor Link 是一种端口联动方案，主要用于配合二层拓扑协议的组网应用。它通过监控设备的上行端口，根据其 up/down 状态的变化来触发下行端口 up/down 状态的变化，从而触发下游设备上的拓扑协议进行链路的切换。

### 74.1.2 基本概念

#### 1. Monitor Link 组

Monitor Link 组也叫监控链路组，每个组由上行端口和下行端口共同组成。一个 Monitor Link 组可以有多个上行端口或下行端口，但一个端口只能属于一个 Monitor Link 组。

#### 2. 上行、下行端口

上行端口和下行端口是 Monitor Link 组中的两个端口角色：

- 上行端口又称为 Uplink 端口，是 Monitor Link 组中被监控的端口，Monitor Link 组的状态与之保持联动。当 Monitor Link 组中没有上行端口或所有上行端口都 down 时，Monitor Link 组就处于 down 状态；而只要有一个上行端口 up，Monitor Link 组就处于 up 状态。
- 下行端口又称为 Downlink 端口，是 Monitor Link 组中的监控端口，其状态与 Monitor Link 组的状态保持联动。当 Monitor Link 组的 up/down 状态发生改变时，下行端口的状态就会发生相应的改变，从而与 Monitor Link 组的状态保持一致。

## 74.2 命令手册

### 74.2.1 config monitor-link group

【功能描述】

**config monitor-link group** 命令用于创建 monitorlink 组并进入对应视图。

**no config monitor-link group** 命令用于删除对应 monitorlink 组并删除对应视图。

【命令格式】

[no] **config monitor-link group** *GROUP*

【视图】

根视图

【缺省情况】

无

【参数说明】

*GROUP*：monitorlink 组 id,范围为（1-16）。

【使用举例】

#创建 monitorlink 组 1，并进入对应视图

```
NOS# config monitor-link group 1
NOS(monitorlink-group-1)#
```

【注意事项】

无

### 74.2.2 <uplink|downlink> interface

【功能描述】

**<uplink|downlink> interface** 命令用配置 monitorlink 组的成员端口。

**no interface** 命令用于删除 monitorlink 组的成员端口。

【命令格式】

**<uplink|downlink> interface** *L2_GRP*

**no interface** *L2_GRP*

【视图】

monitorlink 组视图

【缺省情况】

monitorlink 组无成员端口。

【参数说明】

- **uplink**：配置上行接口 。
- **downlink**：配置下行接口。
- *L2_GRP*：monitorlink 组的成员接口名称。

【使用举例】

#为 monitorlink 组 1 配置上行接口 ge5。

```
NOS(monitorlink-group-1)# uplink interface ge5
NOS(monitorlink-group-1)# show this
  uplink interface ge5
NOS(monitorlink-group-1)#
```

【注意事项】

monitorlink 组的成员端口只支持二层以太网端口和二层聚合口。

聚合口的成员端口无法配置为 monitorlink 组的成员端口。

将 monitorlink 组的成员端口加入聚合口时，该成员端口会退出对应的 monitorlink 组。

### 74.2.3 show monitor-link group

【功能描述】

**show monitor-link group** 命令用于查看 monitorlink 组信息。

【命令格式】

**show monitor-link group** [*GROUP*]

【视图】

任意视图

【缺省情况】

无

【参数说明】

*GROUP*：monitorlink 组 id,取值范围为（1-16）。

【使用举例】

#查看 monitorlink 组 1 的信息。

```
NOS(monitorlink-group-1)# show monitor-link group 1

Monitor link group 1
  Group status   : up
  Last up time   : 01:01:08 2023/09/26
  Last down time : 00:52:33 2023/09/26
  Member    Role       Status
  ------------------------------------
  fe1       uplink     up
  fe2       downlink    up
```

【注意事项】

无。

# 75 BFD

## 75.1 功能简介

BFD（Bidirectional Forwarding Detection，双向转发检测）是一个通用的、标准化的、介质无关和协议无关的快速故障检测机制，用于检测转发路径的连通状况，保证设备之间能够快速检测到通信故障，以便能够及时采取措施，保证业务持续运行。BFD 可以为各种上层协议（如路由协议）快速检测两台设备间双向转发路径的故障。上层协议通常采用 Hello 报文机制检测故障，所需时间为秒级，而 BFD 可以提供毫秒级检测。

控制报文封装在 UDP 报文中传送，对于单跳检测其 UDP 目的端口号为 3784，对于多跳检测其 UDP 目的端口号为 4784。链路两端的设备通过控制报文中携带的参数（会话标识符、期望的收发报文最小时间间隔、本端 BFD 会话状态等）协商建立 BFD 会话。

在建立控制报文方式的 BFD 会话时，用户可以根据网络状况和性能需求，调整设备接收控制报文的时间间隔、发送控制报文的时间间隔以及检测时间倍数,两端协议通过发送相应的协商报文后采用新的参数，不影响会话的当前状态。

**时间协商原理：**

假如 Router A 的 Desired Min Tx Interval 为 100 毫秒，Required Min Rx Interval 为 300 毫秒，Detect Mult 为 5；Router B 的 Desired Min Tx Interval 为 150 毫秒，Required Min Rx Interval 为 400 毫秒，Detect Mult 为 10。那么会有以下结果：

- Router A 的实际发送时间为 Router A 发送控制报文的最小时间间隔和 Router B 接收控制报文的最小时间间隔之间的较大值＝Max（100，400）＝400 毫秒。
- Router B 的实际发送时间为 Router B 发送控制报文的最小时间间隔和 Router A 接收控制报文的最小时间间隔之间的较大值＝Max（150，300）＝300 毫秒。
- Router A 的实际检测时间为 Router B 的检测时间倍数和 Router B 的实际发送时间的乘积＝10×300＝3000 毫秒。
- Router B 的实际检测时间为 Router A 的检测时间倍数和 Router A 的实际发送时间的乘积＝5×400＝2000 毫秒。

## 75.2 命令手册

### 75.2.1 config bfd

【功能描述】

**config bfd** 命令用来进入 bfd 视图。

**no config bfd** 命令用来删除 bfd 视图及视图下的所有配置。

【命令格式】

**config bfd**

**no config bfd**

【视图】

根视图

【缺省情况】

不存在 bfd 视图。

【参数说明】

无。

【使用举例】

#配置 bfd 并进去 bfd 视图。

```
NOS# config bfd
NOS(bfd)#
```

【注意事项】

无。

### 75.2.2 templete

【功能描述】

**templete word** 命令用于建立一个 bfd 配置模板，该模板可以被 bfd 会话引用，用来改变会话时间参数

**no templete word** 命令用来删除相应的模板。

【命令格式】

**templete** WORD

**no templete** WORD

【视图】

bfd 视图

【缺省情况】

不存在 bfd 模板

【参数说明】

WORD：所配置的 bfd 模板名称。

【使用举例】

#进入 **bfd** 视图配置模板 **msy**。

```
NOS# config bfd
NOS(bfd)# templete msy
```

【注意事项】

配置的 bfd 模板各参数按默认值除非有修改。

### 75.2.3 detect-multiplier

【功能描述】

**detect-multiplier** 命令用来检测时间倍数。

**no detect-multiplier** 命令用来恢复默认配置。

【命令格式】

**detect-multiplier** *COUNT*

**no detect-multiplier** *COUNT*

【视图】

templete 视图

【缺省情况】

缺省检测时间倍数为 3。

【参数说明】

*COUNT*：检测时间倍数，取值范围（3-15）。

【使用举例】

#配置模板 msy 的检测时间倍数为 5。

```
NOS# config bfd
NOS(bfd)# config templete msy
NOS(bfd/templete-msy)# detect-multiplier 5
```

【注意事项】

无。

### 75.2.4 receive-interval

【功能描述】

**receive-interval** 命令用来配置接收 bfd 控制报文的最小时间间隔。

**no receive-interval** 命令用来恢复默认配置。

【命令格式】

**receive-interval** *INTERVAL*

**no receive-interval**

【视图】

templete 视图

【缺省情况】

缺省接收 bfd 控制报文的最小时间间隔为 300 豪秒。

【参数说明】

*INTERVAL*：接收报文时间间隔，取值范围为(3-1000),单位为毫秒。

【使用举例】

#配置模板 msy 的接收报文时间间隔为 400 毫秒。

```
NOS# config bfd
NOS(bfd)# config templete msy
NOS(bfd/templete-msy)# receive-interval 400
```

【注意事项】

无。

### 75.2.5 transmit-interval

【功能描述】

**transmit-interval (3-1000)**命令用来配置发送 bfd 控制报文的最小时间间隔。

**no transmit-interval** 命令用来恢复默认配置。

【命令格式】

**transmit-interval** *INTERVAL*

**no transmit-interval**

【视图】

templete 视图

【缺省情况】

缺省发送 bfd 控制报文的 最小时间间隔为 300 毫秒。

【参数说明】

*INTERVAL*：发送 bfd 控制报文的最小时间间隔，取值范围为(3-1000),单位为毫秒。

【使用举例】

#配置发送 bfd 控制报文的最小时间间隔为 400 毫秒。

```
NOS# config bfd
NOS(bfd)# config templete msy
NOS(bfd/templete-msy)# transmit-interval 400
```

【注意事项】

无。

### 75.2.6 show bfd peers

【功能描述】

**show bfd peers** [brief|counters|] [json]命令显示当前会话信息。

【命令格式】

**show bfd peers** [brief|counters] [json]

【视图】

任意视图

【缺省情况】

无。

【参数说明】

brief:显示会话概要信息。

counters：显示会话收发报记数和会话状态事件等。

json:以 json 的格式显示会话信息。

【使用举例】

#显示已经配置的域名映射表

```
<NOS> show bfd peers
BFD Peers Total: 2    Up session: 2
----------------------------------------------------------------------
       peer 82.82.215.108 vrf default interface vlan215
Local ID        : 3360456581        Remote ID       : 34817
Init Mode       : Active             Peer Type       : dynamic
Session State    : up
Uptime          : 55 minutes,36 seconds
Source Port     : 49152            TTL             : 255
Min Tx Interval  : 300ms            ActualTxIntv    : 300ms
Min Rx Interval  : 300ms            Dectection Time  : 900ms
Local DetectMult : 3                Remote DetectMult: 3
Echo Tx Interval : 0ms
Diag Info       : ok
----------------------------------------------------------------------
       peer 82.82.216.108 vrf default interface vlan216
```

```
Local ID        : 2034930331        Remote ID       : 34818
Init Mode       : Active            Peer Type       : dynamic
Session State    : up
Uptime          : 54 minutes,8 seconds
Source Port     : 49153             TTL             : 255
Min Tx Interval  : 300ms             ActualTxIntv    : 300ms
Min Rx Interval  : 300ms             Dectection Time  : 900ms
Local DetectMult : 3                 Remote DetectMult: 3
Echo Tx Interval : 0ms
Diag Info       : ok
```

表75-1 参数说明

| 字段 | 描述 |
| --- | --- |
| peer | 对等方地址,动态会话bfd来区别会话 |
| interface | 始能bfd的接口，动态会话bfd来区别会话 |
| Local ID | 发送方产生的一个唯一的、非0鉴别值，用来区分两个协议之间的多个BFD会话 |
| Remote ID | 接收方收到的鉴别值“My Discriminator”，如果没有收到这个值就返回0 |
| Session State | BFD会话当前状态，取值为：0代表AdminDown，1代表Down，2代表Init，3代表Up |
| Diag Info | 本地会话最后一次从up状态转换到其他状态的原因 |
| ttl | 会话跳数 |
| Peer Type | 会话类型（configed, dynamic） |
| Local DetectMult | 检测时间倍数。即接收方允许发送方发送报文的最大连续丢包数，用来检测链路是否正常 |
| Min Rx Interval | 发送方能够支持的接收两个BFD控制报文之间的间隔，单位毫秒 |
| Min Tx Interval | 发送方发送BFD控制报文时想要采用的最小间隔，单位毫秒 |

## 75.3 配置举例

配置接口 vlan215,并配置接口地址 82.82.215.104，略

配置 ospf，接口 vlan215 开启 ospf，并建立完整的 ospf 邻居状态,略。

(1) 配置接口 vlan215 开启 bfd 链路检测功能。

```
NOS# config vlan 215
NOS(if-vlan215)# ospf bfd
```

(2) 验证，查看 ospf 邻居状态：

```
NOS# show ospf neighbor
Neighbor ID     Pri State         Dead Time Address         Interface
RXmtL RqstL DBsmL
6.6.6.6           1 Full/DR           1.193s 82.82.215.108   vlan215:82.82.215.104
0     0     0
```

```
6.6.6.6         1 Full/DR          1.193s 82.82.216.108   vlan216:82.82.216.104
0    0    0
```

(3) 查看 bfd 会话创建情况。

```
CTC# show bfd peers
BFD Peers Total: 2   Up session: 2
--------------------------------------------------------------------
       peer 82.82.215.108 vrf default interface vlan215
Local ID        : 3360456581       Remote ID       : 34817
Init Mode       : Active           Peer Type       : dynamic
Session State   : up
Uptime          : 55 minutes,36 seconds
Source Port     : 49152            TTL             : 255
Min Tx Interval  : 300ms            ActualTxIntv    : 300ms
Min Rx Interval  : 300ms            Dectection Time  : 900ms
Local DetectMult : 3                Remote DetectMult: 3
Echo Tx Interval : 0ms
Diag Info       : ok
--------------------------------------------------------------------
       peer 82.82.216.108 vrf default interface vlan216
Local ID        : 2034930331       Remote ID       : 34818
Init Mode       : Active           Peer Type       : dynamic
Session State   : up
Uptime          : 54 minutes,8 seconds
Source Port     : 49153            TTL             : 255
Min Tx Interval  : 300ms            ActualTxIntv    : 300ms
Min Rx Interval  : 300ms            Dectection Time  : 900ms
Local DetectMult : 3                Remote DetectMult: 3
Echo Tx Interval : 0ms
Diag Info       : ok
```

## 75.4 常见问题

在配置 BFD 基本功能之前，需完成以下任务：

1、配置接口的网络层地址，使相邻节点之间网络层可达。

2、配置可支持 BFD 的路由协议。

# 76 GLDP

## 76.1 功能介绍

GLDP（General Link Detection Protocol，通用链路检测协议） 可以监控光纤或者双绞线的链路状态，如果发现单向链路存在，GLDP 会根据用户配置，自动关闭或者通知用户手工关闭相关端口，防止网络问题的发生。

GLDP 是链路层协议，它与物理层协同工作来监控设备的链路状态，物理层的自动协商机制进行物理信号和故障的检测；GLDP 进行对端设备的识别，单向链路的识别和关闭不可达的端口，二者协同工作，可以检测和关闭物理或者逻辑的单向连接。

### 76.1.1 基本概念

#### 1. GLDP 邻居状态

表76-1 GLDP 邻居状态

| 状态 | 说明 |
| --- | --- |
| Confirmed（确定） | 链路双通时的GLDP邻居状态 |
| Unconfirmed（未确定） | 发现新邻居但未确认链路双通时的GLDP邻居状态 |

#### 2. GLDP 接口状态

表76-2 GLDP 接口状态

| 状态 | 说明 |
| --- | --- |
| Initial（初始） | 当接口已开启GLDP功能，但全局尚未开启GLDP功能时的接口状态 |
| Inactive（非活动） | 当接口和全局均已开启GLDP功能，但链路物理down时的接口状态 |
| Bidirectional（双通） | 当接口和全局均已开启GLDP功能，且有至少一个处于确定状态下的邻居时的接口状态 |
| Unidirectional（单通） | 当接口和全局均已开启GLDP功能，且没有处于确定状态下的邻居时的接口状态，处于此状态的接口只能收发GLDP报文 |

#### 3. GLDP 定时器

表76-3 GLDP 定时器

| 状态 | 说明 |
| --- | --- |
| Advertisement发送定时器 | Advertisement报文的发送间隔（缺省为5秒，可配） |
| Probe发送定时器 | Probe报文的发送间隔（固定为1秒） |
| Echo等待定时器 | 对邻居进行探测时会启动此定时器，该定时器超时则删除邻居信息（固定为10秒） |
| 邻居老化定时器 | 每个新邻居的加入都要建立邻居表项，当邻居处于确定状 |

| | |
|---|---|
| | 态时启动邻居老化定时器，当收到邻居的Advertisement报文时刷新邻居表项的邻居老化定时器。如果该定时器超时，则启动该邻居的加强探测定时器和Echo等待定时器。邻居老化定时器的值是Advertisement发送定时器的值的3倍 |
| 加强探测定时器 | Probe报文的发送间隔（固定为1秒）<br>若邻居老化定时器超时，则启动该邻居的加强探测定时器并发送Probe报文，同时启动Echo等待定时器 |
| DelayDown定时器 | 接口物理down时不会立即删除所有邻居，而是先启动DelayDown定时器（缺省为1秒），该定时器超时后再核对接口的物理状态：若为down，则删除GLDP邻居信息；若为up，则不进行任何处理 |
| 恢复探测定时器 | RecoverProbe报文的发送间隔（固定为2秒）。处于单通状态的接口会定期发送RecoverProbe报文来检测单向链路是否恢复 |

在实际组网中，有时会出现单通现象，即一条链路上的两个端口，有且只有一端可收到另一端发来的链路层报文，此链路便称为单向链路。两种单通情形：一种是光纤交叉相连，另一种是一条光纤未连接或断路。

## 76.2 命令手册

### 76.2.1 config gldp

【功能描述】

**config gldp** 命令用来进入 gldp 视图。

**no config gldp** 命令用来删除 gldp 视图及视图下的所有配置。

【命令格式】

**config gldp**

**no config gldp**

【视图】

根视图

【缺省情况】

不存在 gldp 视图。

【参数说明】

无。

【使用举例】

#配置 gldp 并进去 gldp 视图。

```
NOS# config gldp
NOS(gldp)#
```

【注意事项】

无。

### 76.2.2 interval

【功能描述】

**interval** 通过合理调整 Advertisement 报文的发送间隔，可使 GLDP 在不同的网络环境下都能够及时发现单向链路（建议采用缺省值）。

**no interval** 命令用来恢复缺省值。

【命令格式】

**interval** *INTERVAL*

**no interval** *INTERVAL*

【视图】

gldp 视图

【缺省情况】

缺省情况下，Advertisement 报文的发送间隔为 2 秒。

【参数说明】

*INTERVAL*：发送 Advertisement 报文的时间间隔，取值范围为(1-10),单位为秒。

【使用举例】

```
#进入 gldp 视图
NOS# config gldp
NOS(gldp)# interval 6
```

【注意事项】

无

### 76.2.3 gldp enable

【功能描述】

**gldp enable** 通过合理调整 Advertisement 报文的发送间隔，可使 GLDP 在不同的网络环境下都能够及时发现单向链路（建议采用缺省值）。

**no gldp enable** 命令用来恢复缺省值。

【命令格式】

**gldp enable**

**no gldp enable**

【视图】

二层接口视图

【缺省情况】

缺省情况下，接口上的 GLDP 功能处于关闭状态。

【参数说明】

无

【使用举例】

```
#进入 gldp 视图
NOS# config interface ge2
NOS(gldp)# gldp enable
```

【注意事项】

要启用 GLDP 功能，必须先全局使能 GLDP 功能，再在端口上使能 GLDP 功能

只能在以太网端口（包括光口和电口）上使能 GLDP 功能。

GLDP 功能只有在物理链路连通后才会起作用，因此在使能 GLDP 之前，请连接好光纤或铜质双绞线。

### 76.2.4 show gldp

【功能描述】

show gldp 命令用于查看 gldp 状态信息。

【命令格式】

**show gldp** [interface *ETH_IF*]

【视图】

任意视图

【缺省情况】

无

【参数说明】

ETH_IF：指定二层接口。

【使用举例】

#查看 gldp 信息

```
NOS# show  gldp
GLDP global status: Enabled
  GLDP advertisement interval: 2
  Number of enabled ports: 1
Interface ge1
  GLDP port state: Bidirectional
  Neighbor Msg:
    Neighbor MAC address: 08:68:8d:ab:22:01
    Neighbor port index : 4
NOS#
```

【注意事项】

无。

## 76.3 配置举例

(1) 设置发送 Advertisement 报文的时间间隔为 6 秒钟。

(2) 在 ge2 接口下使能 gldp 功能

```
NOS# config gldp
NOS(gldp)# interval 6
NOS(gldp)# interface ge2
NOS(if-ge2)# gldp enable
```

(3) 查看 gldp 配置

```
NOS# show  gldp
GLDP global status: Enabled
  GLDP advertisement interval: 6
```

```
  Number of enabled ports: 1
Interface ge2
  GLDP port state: Bidirectional
  Neighbor Msg:
    Neighbor MAC address: 08:68:8d:ab:22:01
    Neighbor port index : 4
```

## 76.4 常见问题

为确保 GLDP 功能正常工作，要保证两端设备的 GLDP 功能都处于开启状态，且 Advertisement 报文的发送间隔、GLDP 认证模式和密码都相同。

为确保 GLDP 功能正常工作，请将两端接口的双工模式配置为全双工、速率配置为相同的强制速率。

# 77 CID 定制

## 77.1 功能介绍

CID（Customer information Define）定制是指在系统软件不变的情况下，通过修改或导入客户定制信息来实现差异化呈现的一种方法。

本系统的大部分定制项不对客户开放，需要在出厂时一次性导入（具体请联系供应商）。少部分定制项支持客户自行修改。

## 77.2 命令手册

### 77.2.1 banner

【功能描述】

**banner** 命令用来修改系统的登录欢迎词。

**no banner** 命令用来恢复缺省情况。

【命令格式】

**banner**

**no banner**

【视图】

根视图

【缺省情况】

取决于出厂时的客户定制情况

【参数说明】

无

【使用举例】

# 修改欢迎词为如下两行内容：

Hello world!

Welcome to hangzhou!

配置如下：

```
NOS# banner
Please input banner content, finish by 'commit' (cancel by 'exit' or 'quit'):
Hello world!
Welcome to hangzhou!
commit
NOS#
```

【注意事项】

无

### 77.2.2 show banner

【功能描述】

show banner 命令用来显示当前生效的欢迎词。

【命令格式】

show banner

【视图】

任意视图

【缺省情况】

不涉及

【参数说明】

无

【使用举例】

```
# 显示当前生效的欢迎词：
NOS# show banner
Hello world!
Welcome to hangzhou!
NOS#
```

【注意事项】

无

## 77.3 配置举例

修改欢迎词为如下两行内容：

```
Hello world!
Welcome to hangzhou!
NOS# banner
Please input banner content, finish by 'commit' (cancel by 'exit' or 'quit'):
Hello world!
Welcome to hangzhou!
commit
NOS#
# 显示当前生效的欢迎词：
NOS# show banner
Hello world!
Welcome to hangzhou!
```

## 77.4 常见问题

待补充。

# 78 第三方应用管理

## 78.1 功能介绍

### 78.1.1 功能简介

本系统采用基于容器技术的沙箱方案来运行第三方应用，用户应用运行在独立的文件系统中，跟系统原有的文件系统完全隔离，有效地保障了系统的安全性。

第三方应用需要使用本系统发布的交叉编译工具链来生成程序，同时可使用系统自带的 lib 库（如 glibc 等），支持自有配置文件和 lib 库。

使用第三方应用功能时，应先通过 ftp/tftp 等方式将相关文件上传到设备根目录下的“usrapp”子文件夹下，如果有依赖的第三方 lib，还需要放到该目录下的 lib 子目录下。

本功能的支持情况取决于实际产品，部分资源较少的产品可能不支持该功能。

### 78.1.2 API介绍

系统对第三方应用公开了完整的 CLI 操作接口,包括配置和显示两类,可以实现对系统的完全控制。相关头文件定义如下：

```
/* Config api: return 0 means success */
typedef int (*USRAPP_CFG_PF)(int iCmdCnt, char **apcCmds);
/* Show api: return show result length */
typedef int (*USRAPP_SHOW_PF)(const char *pcCmd, char *pcOutBuf, int iOutBufLen);
/* Get api, return api-handle */
static void *usrapp_api_ref(USRAPP_CFG_PF *ppfCfg, USRAPP_SHOW_PF *ppfShow)
{
    void *pHandle = NULL;
    pHandle = dlopen("libusrapi.so", RTLD_LAZY);
    if (NULL != pHandle) {
        *ppfCfg = (USRAPP_CFG_PF)dlsym(pHandle, "usrapp_cfg_proc");
        *ppfShow = (USRAPP_SHOW_PF)dlsym(pHandle, "usrapp_show_proc");
        if ((NULL == *ppfCfg) || (NULL == *ppfShow)) {
            (void)dlclose(pHandle);
            pHandle = NULL;
        }
    }
    return pHandle;
}

/* Release api-handle */
static void usrapp_api_unref(void *pHandle)
{
    if (NULL != pHandle) {
        (void)dlclose(pHandle);
    }
    return;
}
```

API 接口的使用方式跟 CLI 类似（注意显示 API 只支持 json 类的显示命令，返回的是未缩进的 json 格式字符串），举例如下：

```
void test(void)
{
    int iLen;
    void *pHandle;
    USRAPP_CFG_PF pfCfg = NULL;
    USRAPP_SHOW_PF pfShow = NULL;
    char szShowBuf[512];
    char *apcCmds[2] = {"config interface mgt0", "ipv4-address 10.1.1.1/24"};
    // Init:
    if (NULL == (pHandle = usrapp_api_ref(&pfCfg, &pfShow))) {
        // Error process ...
    }
    // Config:
    if (0 != pfCfg(2, apcCmds)) {
        // Error process ...
    }
    // Show:
    iLen = pfShow("show version json", szShowBuf, sizeof(szShowBuf));
    if (iLen > 0) {
        // process show result of 'szShowBuf' ...
    }
    // Exit:
    usrapp_api_unref(pHandle);
}
```

## 78.2 命令手册

### 78.2.1 config third-party-app

【功能描述】

**config third-party-app** 命令用来进入第三方应用配置视图。

**no config third-party-app** 命令用来删除所有第三方应用配置。

【命令格式】

**config third-party-app**

**no config third-party-app**

【视图】

根视图

【缺省情况】

无第三方应用配置

【参数说明】

无

【使用举例】

#进入第三方应用视图。

```
NOS# config third-party-app
NOS(usrapp)#
```

【注意事项】

无

### 78.2.2 daemon

【功能描述】

**daemon** 命令用来以指定名称创建第三方应用并进入该业务视图。

**no daemon** 命令用来停止并删除第三方应用配置。

【命令格式】

**daemon** *NAME*

**no daemon** *NAME*

【视图】

第三方应用视图

【缺省情况】

无

【参数说明】

*NAME*：该第三方应用的名称。

【使用举例】

```
#配置名为“test”的第三方应用，并进入该模块视图。
NOS# config third-party-app
NOS(usrapp)# daemon test
NOS(usrapp/test)#
```

【注意事项】

无

### 78.2.3 data-file

【功能描述】

**data-file** 命令用来配置第三方应用需要使用的数据文件。

【命令格式】

**data-file** *FILE...*

【视图】

第三方应用业务视图

【缺省情况】

无

【参数说明】

*FILE*：需要使用的文件名称，可配置多个。

【使用举例】

```
# 配置依赖的数据文件为“config.ini”（必须已存在于“usrapp”目录下）。
NOS# config third-party-app
```

```
NOS(usrapp)# daemon test
NOS(usrapp/test)# data-file usrapp/config.ini
NOS(usrapp/test)#
```

【注意事项】

- 该配置不支持取消操作。
- 如果多次配置此命令，以最新配置为准。
- 只有通过该命令指定的文件(以及运行 exec-file 时所依赖的文件)才能被该第三方应用访问，其他文件均被隔离。
- 配置该命令会自动触发对应的业务重启，以获取访问新配置文件的权限。

### 78.2.4 exec-file

【功能描述】

**exec-file** 命令用来配置第三方应用的后台执行程序。

【命令格式】

**exec-file** *FILE*

【视图】

第三方应用模块视图

【缺省情况】

无

【参数说明】

*FILE*：后台执行程序的名称。

【使用举例】

```
#配置可执行文件名称为 testd（必须已存在于“usrapp”目录下）。
NOS# config third-party-app
NOS(usrapp)# daemon test
NOS(usrapp/test)# exec-file usrapp/testd
NOS(usrapp/test)#
```

【注意事项】

- 该配置不支持取消操作。
- 该命令执行完后，会立即启动对应程序，因此建议先配置完必要的 data-file 后再执行此命令。

## 78.3 配置举例

```
#配置名为“test”的第三方应用，并进入该模块视图。
NOS# config third-party-app
NOS(usrapp)# daemon test
NOS(usrapp/test)#
# 配置依赖的数据文件为“config.ini”（必须已存在于“usrapp”目录下）。
NOS(usrapp/test)# data-file usrapp/config.ini
NOS(usrapp/test)#
#配置可执行文件名称为 testd（必须已存在于“usrapp”目录下）。
NOS(usrapp/test)# exec-file usrapp/testd
NOS(usrapp/test)#
```

## 78.4 常见问题

待补充。