H3C CR16000-F 日志信息参考

Copyright © 2020 新华三技术有限公司 版权所有，保留一切权利。
非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。
除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。
本文档中的信息可能变动，恕不另行通知。

目 录

1 简介 1

1.1 日志格式说明 1

1.2 软件模块列表 3

1.3 文档使用说明 7

2 AAA 8

2.1 AAA_FAILURE 8

2.2 AAA_LAUNCH 9

2.3 AAA_SUCCESS 9

3 ACL 9

3.1 ACL_ACCELERATE_NO_RES 10

3.2 ACL_ACCELERATE_NONCONTIGUOUSMASK 10

3.3 ACL_ACCELERATE_NOT_SUPPORT 10

3.4 ACL_ACCELERATE_NOT_SUPPORTHOPBYHOP 11

3.5 ACL_ACCELERATE_NOT_SUPPORTMULTITCPFLAG 11

3.6 ACL_ACCELERATE_UNK_ERR 11

3.7 ACL_IPV6_STATIS_INFO 12

3.8 ACL_NO_MEM 12

3.9 ACL_STATIS_INFO 12

4 AFT 13

4.1 AFT_LOG_FLOW 13

4.2 AFT_V6TOV4_FLOW 14

4.3 AFT_V4TOV6_FLOW 15

5 ANCP 16

5.1 ANCP_INVALID_PACKET 16

6 API 16

6.1 API 17

7 APMGR 17

7.1 APMGR_ADDBAC_INFO 17

7.2 APMGR_AP_CFG_FAILED 18

7.3 APMGR_DELBAC_INFO 18

7.4 APMGR_LOG_ADD_AP_FAIL 18

7.5 APMGR_LOG_LACOFFLINE 19

7.6 APMGR_LOG_LACONLINE 19
7.7 APMGR_LOG_MEMALERT 19
7.8 APMGR_LOG_NOLICENSE 20
7.9 APMGR_LOG_OFFLINE 20
7.10 APMGR_LOG_ONLINE 20
7.11 APMGR_REACH_MAX_APNUMBER 21
7.12 CWC_AP_DOWN 21
7.13 CWC_AP_UP 22
7.14 CWC_AP_REBOOT 22
7.15 CWC_IMG_DOWNLOAD_COMPLETE 22
7.16 CWC_IMG_DOWNLOAD_START 23
7.17 CWC_IMG_NO_ENOUGH_SPACE 23
7.18 CWC_LOCALAC_DOWN 24
7.19 CWC_LOCALAC_UP 24
7.20 CWC_RUN_DOWNLOAD_COMPLETE 25
7.21 CWC_RUN_DOWNLOAD_START 25
7.22 CWC_RUN_NO_ENOUGH_SPACE 25
7.23 CWS_AP_DOWN 26
7.24 CWS_AP_UP 26
7.25 CWS_IMG_DOWNLOAD_COMPLETE 27
7.26 CWS_IMG_DOWNLOAD_FAILED 27
7.27 CWS_IMG_DOWNLOAD_START 27
7.28 CWS_LOCALAC_DOWN 28
7.29 CWS_LOCALAC_UP 28
7.30 CWS_RUN_DOWNLOAD_COMPLETE 29
7.31 CWS_RUN_DOWNLOAD_START 29
8 ARP 29
8.1 ARP_ACTIVE_ACK_NO_REPLY 30
8.2 ARP_ACTIVE_ACK_NOREQUESTED_REPLY 30
8.3 ARP_BINDRULETOHW_FAILED 31
8.4 ARP_DUPLICATE_IPADDR_DETECT 32
8.5 ARP_DYNAMIC 32
8.6 ARP_DYNAMIC_IF 33
8.7 ARP_DYNAMIC_SLOT 33
8.8 ARP_ENTRY_CONFLICT 34
8.9 ARP_HOST_IP_CONFLICT 34

8.10 ARP_RATE_EXCEEDED 35
8.11 ARP_RATELIMIT_NOTSUPPORT 35
8.12 ARP_SENDER_IP_INVALID 36
8.13 ARP_SENDER_MAC_INVALID 36
8.14 ARP_SRC_MAC_FOUND_ATTACK 36
8.15 ARP_TARGET_IP_INVALID 37
8.16 DUPIFIP 37
8.17 DUPIP 37
8.18 DUPVRRPIP 38
8.19 L3_COMMON 38
9 ATK 38
9.1 ATK_ICMP_ADDRMASK_REQ 39
9.2 ATK_ICMP_ADDRMASK_REQ_RAW 40
9.3 ATK_ICMP_ADDRMASK_REQ_RAW_SZ 40
9.4 ATK_ICMP_ADDRMASK_REQ_SZ 41
9.5 ATK_ICMP_ADDRMASK_RPL 42
9.6 ATK_ICMP_ADDRMASK_RPL_RAW 43
9.7 ATK_ICMP_ADDRMASK_RPL_RAW_SZ 43
9.8 ATK_ICMP_ADDRMASK_RPL_SZ 44
9.9 ATK_ICMP_ECHO_REQ 45
9.10 ATK_ICMP_ECHO_REQ_RAW 46
9.11 ATK_ICMP_ECHO_REQ_RAW_SZ 47
9.12 ATK_ICMP_ECHO_REQ_SZ 48
9.13 ATK_ICMP_ECHO_RPL 49
9.14 ATK_ICMP_ECHO_RPL_RAW 50
9.15 ATK_ICMP_ECHO_RPL_RAW_SZ 50
9.16 ATK_ICMP_ECHO_RPL_SZ 51
9.17 ATK_ICMP_FLOOD 52
9.18 ATK_ICMP_FLOOD_SZ 52
9.19 ATK_ICMP_INFO_REQ 53
9.20 ATK_ICMP_INFO_REQ_RAW 54
9.21 ATK_ICMP_INFO_REQ_RAW_SZ 54
9.22 ATK_ICMP_INFO_REQ_SZ 55
9.23 ATK_ICMP_INFO_RPL 56
9.24 ATK_ICMP_INFO_RPL_RAW 57
9.25 ATK_ICMP_INFO_RPL_RAW_SZ 57

9.26 ATK_ICMP_INFO_RPL_SZ 58
9.27 ATK_ICMP_LARGE 59
9.28 ATK_ICMP_LARGE_RAW 59
9.29 ATK_ICMP_LARGE_RAW_SZ 60
9.30 ATK_ICMP_LARGE_SZ 60
9.31 ATK_ICMP_PARAPROBLEM 61
9.32 ATK_ICMP_PARAPROBLEM_RAW 62
9.33 ATK_ICMP_PARAPROBLEM_RAW_SZ 62
9.34 ATK_ICMP_PARAPROBLEM_SZ 63
9.35 ATK_ICMP_PINGOFDEATH 64
9.36 ATK_ICMP_PINGOFDEATH_RAW 65
9.37 ATK_ICMP_PINGOFDEATH_RAW_SZ 65
9.38 ATK_ICMP_PINGOFDEATH_SZ 66
9.39 ATK_ICMP_REDIRECT 67
9.40 ATK_ICMP_REDIRECT_RAW 68
9.41 ATK_ICMP_REDIRECT_RAW_SZ 68
9.42 ATK_ICMP_REDIRECT_SZ 69
9.43 ATK_ICMP_SMURF 70
9.44 ATK_ICMP_SMURF_RAW 71
9.45 ATK_ICMP_SMURF_RAW_SZ 71
9.46 ATK_ICMP_SMURF_SZ 72
9.47 ATK_ICMP_SOURCEQUENCH 73
9.48 ATK_ICMP_SOURCEQUENCH_RAW 74
9.49 ATK_ICMP_SOURCEQUENCH_RAW_SZ 74
9.50 ATK_ICMP_SOURCEQUENCH_SZ 75
9.51 ATK_ICMP_TIMEEXCEED 76
9.52 ATK_ICMP_TIMEEXCEED_RAW 77
9.53 ATK_ICMP_TIMEEXCEED_RAW_SZ 77
9.54 ATK_ICMP_TIMEEXCEED_SZ 78
9.55 ATK_ICMP_TRACEROUTE 79
9.56 ATK_ICMP_TRACEROUTE_RAW 79
9.57 ATK_ICMP_TRACEROUTE_RAW_SZ 80
9.58 ATK_ICMP_TRACEROUTE_SZ 80
9.59 ATK_ICMP_TSTAMP_REQ 81
9.60 ATK_ICMP_TSTAMP_REQ_RAW 82
9.61 ATK_ICMP_TSTAMP_REQ_RAW_SZ 82

9.62 ATK_ICMP_TSTAMP_REQ_SZ 83
9.63 ATK_ICMP_TSTAMP_RPL 84
9.64 ATK_ICMP_TSTAMP_RPL_RAW 85
9.65 ATK_ICMP_TSTAMP_RPL_RAW_SZ 85
9.66 ATK_ICMP_TSTAMP_RPL_SZ 86
9.67 ATK_ICMP_TYPE 87
9.68 ATK_ICMP_TYPE_RAW 88
9.69 ATK_ICMP_TYPE_RAW_SZ 88
9.70 ATK_ICMP_TYPE_SZ 89
9.71 ATK_ICMP_UNREACHABLE 90
9.72 ATK_ICMP_UNREACHABLE_RAW 91
9.73 ATK_ICMP_UNREACHABLE_RAW_SZ 91
9.74 ATK_ICMP_UNREACHABLE_SZ 92
9.75 ATK_ICMPV6_DEST_UNREACH 93
9.76 ATK_ICMPV6_DEST_UNREACH_RAW 93
9.77 ATK_ICMPV6_DEST_UNREACH_RAW_SZ 94
9.78 ATK_ICMPV6_DEST_UNREACH_SZ 94
9.79 ATK_ICMPV6_ECHO_REQ 95
9.80 ATK_ICMPV6_ECHO_REQ_RAW 95
9.81 ATK_ICMPV6_ECHO_REQ_RAW_SZ 96
9.82 ATK_ICMPV6_ECHO_REQ_SZ 96
9.83 ATK_ICMPV6_ECHO_RPL 97
9.84 ATK_ICMPV6_ECHO_RPL_RAW 97
9.85 ATK_ICMPV6_ECHO_RPL_RAW_SZ 98
9.86 ATK_ICMPV6_ECHO_RPL_SZ 98
9.87 ATK_ICMPV6_FLOOD 99
9.88 ATK_ICMPV6_FLOOD_SZ 99
9.89 ATK_ICMPV6_GROUPQUERY 100
9.90 ATK_ICMPV6_GROUPQUERY_RAW 100
9.91 ATK_ICMPV6_GROUPQUERY_RAW_SZ 101
9.92 ATK_ICMPV6_GROUPQUERY_SZ 101
9.93 ATK_ICMPV6_GROUPREDUCTION 102
9.94 ATK_ICMPV6_GROUPREDUCTION_RAW 102
9.95 ATK_ICMPV6_GROUPREDUCTION_RAW_SZ 103
9.96 ATK_ICMPV6_GROUPREDUCTION_SZ 103
9.97 ATK_ICMPV6_GROUPREPORT 104

9.98 ATK_ICMPV6_GROUPREPORT_RAW 104
9.99 ATK_ICMPV6_GROUPREPORT_RAW_SZ 105
9.100 ATK_ICMPV6_GROUPREPORT_SZ 105
9.101 ATK_ICMPV6_LARGE 106
9.102 ATK_ICMPV6_LARGE_RAW 106
9.103 ATK_ICMPV6_LARGE_RAW_SZ 107
9.104 ATK_ICMPV6_LARGE_SZ 107
9.105 ATK_ICMPV6_PACKETTOOBIG 108
9.106 ATK_ICMPV6_PACKETTOOBIG_RAW 108
9.107 ATK_ICMPV6_PACKETTOOBIG_RAW_SZ 109
9.108 ATK_ICMPV6_PACKETTOOBIG_SZ 109
9.109 ATK_ICMPV6_PARAPROBLEM 110
9.110 ATK_ICMPV6_PARAPROBLEM_RAW 110
9.111 ATK_ICMPV6_PARAPROBLEM_RAW_SZ 111
9.112 ATK_ICMPV6_PARAPROBLEM_SZ 111
9.113 ATK_ICMPV6_TIMEEXCEED 112
9.114 ATK_ICMPV6_TIMEEXCEED_RAW 112
9.115 ATK_ICMPV6_TIMEEXCEED_RAW_SZ 113
9.116 ATK_ICMPV6_TIMEEXCEED_SZ 113
9.117 ATK_ICMPV6_TRACEROUTE 114
9.118 ATK_ICMPV6_TRACEROUTE_RAW 115
9.119 ATK_ICMPV6_TRACEROUTE_RAW_SZ 116
9.120 ATK_ICMPV6_TRACEROUTE_SZ 117
9.121 ATK_ICMPV6_TYPE 118
9.122 ATK_ICMPV6_TYPE _RAW 118
9.123 ATK_ICMPV6_TYPE _RAW_SZ 119
9.124 ATK_ICMPV6_TYPE_SZ 119
9.125 ATK_IP_OPTION 120
9.126 ATK_IP_OPTION_RAW 121
9.127 ATK_IP_OPTION_RAW_SZ 121
9.128 ATK_IP_OPTION_SZ 122
9.129 ATK_IP4_ACK_FLOOD 123
9.130 ATK_IP4_ACK_FLOOD_SZ 123
9.131 ATK_IP4_DIS_PORTSCAN 124
9.132 ATK_IP4_DIS_PORTSCAN_SZ 124
9.133 ATK_IP4_DNS_FLOOD 125

9.134 ATK_IP4_DNS_FLOOD_SZ 125
9.135 ATK_IP4_FIN_FLOOD 126
9.136 ATK_IP4_FIN_FLOOD_SZ 126
9.137 ATK_IP4_FRAGMENT 127
9.138 ATK_IP4_FRAGMENT_RAW 128
9.139 ATK_IP4_FRAGMENT_RAW_SZ 128
9.140 ATK_IP4_FRAGMENT_SZ 129
9.141 ATK_IP4_HTTP_FLOOD 129
9.142 ATK_IP4_HTTP_FLOOD_SZ 130
9.143 ATK_IP4_IMPOSSIBLE 131
9.144 ATK_IP4_IMPOSSIBLE_RAW 132
9.145 ATK_IP4_IMPOSSIBLE_RAW_SZ 132
9.146 ATK_IP4_IMPOSSIBLE_SZ 133
9.147 ATK_IP4_IPSWEEP 134
9.148 ATK_IP4_IPSWEEP_SZ 134
9.149 ATK_IP4_PORTSCAN 135
9.150 ATK_IP4_PORTSCAN_SZ 135
9.151 ATK_IP4_RST_FLOOD 136
9.152 ATK_IP4_RST_FLOOD_SZ 136
9.153 ATK_IP4_SYN_FLOOD 137
9.154 ATK_IP4_SYN_FLOOD_SZ 137
9.155 ATK_IP4_SYNACK_FLOOD 138
9.156 ATK_IP4_SYNACK_FLOOD_SZ 138
9.157 ATK_IP4_TCP_ALLFLAGS 139
9.158 ATK_IP4_TCP_ALLFLAGS_RAW 139
9.159 ATK_IP4_TCP_ALLFLAGS_RAW_SZ 140
9.160 ATK_IP4_TCP_ALLFLAGS_SZ 140
9.161 ATK_IP4_TCP_FINONLY 141
9.162 ATK_IP4_TCP_FINONLY_RAW 141
9.163 ATK_IP4_TCP_FINONLY_RAW_SZ 142
9.164 ATK_IP4_TCP_FINONLY_SZ 142
9.165 ATK_IP4_TCP_INVALIDFLAGS 143
9.166 ATK_IP4_TCP_INVALIDFLAGS_RAW 144
9.167 ATK_IP4_TCP_INVALIDFLAGS_RAW_SZ 144
9.168 ATK_IP4_TCP_INVALIDFLAGS_SZ 145
9.169 ATK_IP4_TCP_LAND 146

9.170 ATK_IP4_TCP_LAND_RAW 146
9.171 ATK_IP4_TCP_LAND_RAW_SZ 147
9.172 ATK_IP4_TCP_LAND_SZ 147
9.173 ATK_IP4_TCP_NULLFLAG 148
9.174 ATK_IP4_TCP_NULLFLAG_RAW 148
9.175 ATK_IP4_TCP_NULLFLAG_RAW_SZ 149
9.176 ATK_IP4_TCP_NULLFLAG_SZ 149
9.177 ATK_IP4_TCP_SYNFIN 150
9.178 ATK_IP4_TCP_SYNFIN_RAW 150
9.179 ATK_IP4_TCP_SYNFIN_RAW_SZ 151
9.180 ATK_IP4_TCP_SYNFIN_SZ 151
9.181 ATK_IP4_TCP_WINNUKE 152
9.182 ATK_IP4_TCP_WINNUKE_RAW 153
9.183 ATK_IP4_TCP_WINNUKE_RAW_SZ 153
9.184 ATK_IP4_TCP_WINNUKE_SZ 154
9.185 ATK_IP4_TEARDROP 155
9.186 ATK_IP4_TEARDROP_RAW 156
9.187 ATK_IP4_TEARDROP_RAW_SZ 156
9.188 ATK_IP4_TEARDROP_SZ 157
9.189 ATK_IP4_TINY_FRAGMENT 158
9.190 ATK_IP4_TINY_FRAGMENT_RAW 159
9.191 ATK_IP4_TINY_FRAGMENT_RAW_SZ 159
9.192 ATK_IP4_TINY_FRAGMENT_SZ 160
9.193 ATK_IP4_UDP_BOMB 161
9.194 ATK_IP4_UDP_BOMB_RAW 161
9.195 ATK_IP4_UDP_BOMB_RAW_SZ 162
9.196 ATK_IP4_UDP_BOMB_SZ 162
9.197 ATK_IP4_UDP_FLOOD 163
9.198 ATK_IP4_UDP_FLOOD_SZ 163
9.199 ATK_IP4_UDP_FRAGGLE 164
9.200 ATK_IP4_UDP_FRAGGLE_RAW 164
9.201 ATK_IP4_UDP_FRAGGLE_RAW_SZ 165
9.202 ATK_IP4_UDP_FRAGGLE_SZ 165
9.203 ATK_IP4_UDP_SNORK 166
9.204 ATK_IP4_UDP_SNORK_RAW 167
9.205 ATK_IP4_UDP_SNORK_RAW_SZ 167

9.206 ATK_IP4_UDP_SNORK_SZ 168
9.207 ATK_IP6_ACK_FLOOD 168
9.208 ATK_IP6_ACK_FLOOD_SZ 169
9.209 ATK_IP6_DIS_PORTSCAN 169
9.210 ATK_IP6_DIS_PORTSCAN_SZ 170
9.211 ATK_IP6_DNS_FLOOD 170
9.212 ATK_IP6_DNS_FLOOD_SZ 171
9.213 ATK_IP6_FIN_FLOOD 171
9.214 ATK_IP6_FIN_FLOOD_SZ 172
9.215 ATK_IP6_FRAGMENT 173
9.216 ATK_IP6_FRAGMENT_RAW 173
9.217 ATK_IP6_FRAGMENT_RAW_SZ 174
9.218 ATK_IP6_FRAGMENT_SZ 174
9.219 ATK_IP6_HTTP_FLOOD 175
9.220 ATK_IP6_HTTP_FLOOD_SZ 175
9.221 ATK_IP6_IMPOSSIBLE 176
9.222 ATK_IP6_IMPOSSIBLE_RAW 176
9.223 ATK_IP6_IMPOSSIBLE_RAW_SZ 177
9.224 ATK_IP6_IMPOSSIBLE_SZ 177
9.225 ATK_IP6_IPSWEEP 178
9.226 ATK_IP6_IPSWEEP_SZ 178
9.227 ATK_IP6_PORTSCAN 179
9.228 ATK_IP6_PORTSCAN_SZ 179
9.229 ATK_IP6_RST_FLOOD 180
9.230 ATK_IP6_RST_FLOOD_SZ 180
9.231 ATK_IP6_SYN_FLOOD 181
9.232 ATK_IP6_SYN_FLOOD_SZ 181
9.233 ATK_IP6_SYNACK_FLOOD 182
9.234 ATK_IP6_SYNACK_FLOOD_SZ 182
9.235 ATK_IP6_TCP_ALLFLAGS 183
9.236 ATK_IP6_TCP_ALLFLAGS_RAW 183
9.237 ATK_IP6_TCP_ALLFLAGS_RAW_SZ 184
9.238 ATK_IP6_TCP_ALLFLAGS_SZ 184
9.239 ATK_IP6_TCP_FINONLY 185
9.240 ATK_IP6_TCP_FINONLY_RAW 185
9.241 ATK_IP6_TCP_FINONLY_RAW_SZ 186

9.242 ATK_IP6_TCP_FINONLY_SZ 186
9.243 ATK_IP6_TCP_INVALIDFLAGS 187
9.244 ATK_IP6_TCP_INVALIDFLAGS_RAW 188
9.245 ATK_IP6_TCP_INVALIDFLAGS_RAW_SZ 188
9.246 ATK_IP6_TCP_INVALIDFLAGS_SZ 189
9.247 ATK_IP6_TCP_LAND 190
9.248 ATK_IP6_TCP_LAND_RAW 190
9.249 ATK_IP6_TCP_LAND_RAW_SZ 191
9.250 ATK_IP6_TCP_LAND_SZ 191
9.251 ATK_IP6_TCP_NULLFLAG 192
9.252 ATK_IP6_TCP_NULLFLAG_RAW 192
9.253 ATK_IP6_TCP_NULLFLAG_RAW_SZ 193
9.254 ATK_IP6_TCP_NULLFLAG_SZ 193
9.255 ATK_IP6_TCP_SYNFIN 194
9.256 ATK_IP6_TCP_SYNFIN_RAW 194
9.257 ATK_IP6_TCP_SYNFIN_RAW_SZ 195
9.258 ATK_IP6_TCP_SYNFIN_SZ 195
9.259 ATK_IP6_TCP_WINNUKE 196
9.260 ATK_IP6_TCP_WINNUKE_RAW 196
9.261 ATK_IP6_TCP_WINNUKE_RAW_SZ 197
9.262 ATK_IP6_TCP_WINNUKE_SZ 197
9.263 ATK_IP6_UDP_FLOOD 198
9.264 ATK_IP6_UDP_FLOOD_SZ 198
9.265 ATK_IP6_UDP_FRAGGLE 199
9.266 ATK_IP6_UDP_FRAGGLE_RAW 199
9.267 ATK_IP6_UDP_FRAGGLE_RAW_SZ 200
9.268 ATK_IP6_UDP_FRAGGLE_SZ 200
9.269 ATK_IP6_UDP_SNORK 201
9.270 ATK_IP6_UDP_SNORK_RAW 201
9.271 ATK_IP6_UDP_SNORK_RAW_SZ 202
9.272 ATK_IP6_UDP_SNORK_SZ 202
9.273 ATK_IPOPT_ABNORMAL 203
9.274 ATK_IPOPT_ABNORMAL_RAW 204
9.275 ATK_IPOPT_ABNORMAL_RAW_SZ 204
9.276 ATK_IPOPT_ABNORMAL_SZ 205
9.277 ATK_IPOPT_LOOSESRCROUTE 206

9.278 ATK_IPOPT_LOOSESRCROUTE_RAW 207
9.279 ATK_IPOPT_LOOSESRCROUTE_RAW_SZ 208
9.280 ATK_IPOPT_LOOSESRCROUTE_SZ 209
9.281 ATK_IPOPT_RECORDROUTE 210
9.282 ATK_IPOPT_RECORDROUTE_RAW 211
9.283 ATK_IPOPT_RECORDROUTE_RAW_SZ 212
9.284 ATK_IPOPT_RECORDROUTE_SZ 213
9.285 ATK_IPOPT_ROUTEALERT 214
9.286 ATK_IPOPT_ROUTEALERT_RAW 215
9.287 ATK_IPOPT_ROUTEALERT_RAW_SZ 216
9.288 ATK_IPOPT_ROUTEALERT_SZ 217
9.289 ATK_IPOPT_SECURITY 218
9.290 ATK_IPOPT_SECURITY_RAW 219
9.291 ATK_IPOPT_SECURITY_RAW_SZ 220
9.292 ATK_IPOPT_SECURITY_SZ 221
9.293 ATK_IPOPT_STREAMID 222
9.294 ATK_IPOPT_STREAMID_RAW 223
9.295 ATK_IPOPT_STREAMID_RAW_SZ 224
9.296 ATK_IPOPT_STREAMID_SZ 225
9.297 ATK_IPOPT_STRICTSRCROUTE 226
9.298 ATK_IPOPT_STRICTSRCROUTE_RAW 227
9.299 ATK_IPOPT_STRICTSRCROUTE_RAW_SZ 228
9.300 ATK_IPOPT_STRICTSRCROUTE_SZ 229
9.301 ATK_IPOPT_TIMESTAMP 230
9.302 ATK_IPOPT_TIMESTAMP_RAW 231
9.303 ATK_IPOPT_TIMESTAMP_RAW_SZ 232
9.304 ATK_IPOPT_TIMESTAMP_SZ 233
9.305 ATK_IPV6_EXT_HEADER 234
9.306 ATK_IPV6_EXT_HEADER_ABNORMAL 235
9.307 ATK_IPV6_EXT_HEADER_ABNORMAL_RAW 235
9.308 ATK_IPV6_EXT_HEADER_ABNORMAL_RAW_SZ 236
9.309 ATK_IPV6_EXT_HEADER_ABNORMAL_SZ 236
9.310 ATK_IPV6_EXT_HEADER_RAW 237
9.311 ATK_IPV6_EXT_HEADER_RAW_SZ 237
9.312 ATK_IPV6_EXT_HEADER_SZ 238

10 ATM 238
10.1 ATM_PVCDOWN 239
10.2 ATM_PVCUP 239
10.3 ATM _FAILURE 240
10.4 ATM_PVCDOWN 240
10.5 ATM_PVCUP 241
11 BFD 241
11.1 BFD_N 241
11.2 BFD_CHANGE_FSM (Severity 4) 242
11.3 BFD_CHANGE_FSM (Severity 5) 243
11.4 BFD_CHANGE_SESS 244
11.5 BFD_REACHED_UPPER_LIMIT 244
12 BGP 244
12.1 BGP_EXCEED_ROUTE_LIMIT 245
12.2 BGP_REACHED_THRESHOLD 245
12.3 BGP_LOG_ROUTE_FLAP 246
12.4 BGP_LABEL_CONFLICT 246
12.5 BGP_LABEL_OUTOFRANGE 246
12.6 BGP_MEM_ALERT 247
12.7 BGP_PEER_LICENSE_REACHED 247
12.8 BGP_ROUTE_LICENSE_REACHED 248
12.9 BGP_STATE_CHANGED 248
13 BLS 248
13.1 BLS_ENTRY_ADD 249
13.2 BLS_ENTRY_DEL 249
13.3 BLS_IPV6_ENTRY_ADD 250
13.4 BLS_IPV6_ENTRY_DEL 250
14 BRAS_COM 250
14.1 BRAS_FUNC 251
15 BRIPRO 251
15.1 API 251
15.2 API 251
15.3 API 252
15.4 API 252
15.5 TRUNK 252

16 CFD 253
16.1 API 253
16.2 L2MC_IPV4 253
16.3 CFD_CROSS_CCM 254
16.4 CFD_ERROR_CCM 254
16.5 CFD_LOST_CCM 255
16.6 CFD_RECEIVE_CCM 255
17 CFGMAN 255
17.1 CFGMAN_CFGCHANGED 256
17.2 CFGMAN_OPTCOMPLETION 257
18 CGN 258
18.1 INTE_CGNSOFTCTL 258
19 CLK 258
19.1 CLK 258
19.2 CLK 259
19.3 CLK 259
19.4 CLK 259
19.5 CLK 260
19.6 CLK 260
19.7 CLK 260
19.8 CLK 261
19.9 CLK 261
19.10 CLK 261
19.11 CLK 262
19.12 CLK 262
19.13 CLK 262
19.14 CLK 263
19.15 CLK 263
19.16 CLK 263
19.17 CLK 264
19.18 CLK 264
19.19 CLK 264
19.20 CLK 265
19.21 CLK 265
19.22 CLK 265
19.23 CLK 266

19.24 CLK 266
19.25 CLK 266
20 CONNLMT 266
20.1 CONNLMT_IPV4_OVERLOAD 267
20.2 CONNLMT_IPV4_RECOVER 268
20.3 CONNLMT_IPV6_OVERLOAD 269
20.4 CONNLMT_IPV6_RECOVER 270
21 DEV 270
21.1 DrvDebug 271
21.2 DrvDebug 271
21.3 DrvDebug 272
21.4 DrvDebug 272
21.5 DrvDebug 273
21.6 DrvDebug 273
21.7 DrvDebug 274
21.8 DrvDebug 274
21.9 DrvDebug 274
21.10 DrvDebug 275
21.11 DrvDebug 275
21.12 DrvDebug 275
21.13 DrvDebug 276
21.14 DrvDebug 276
21.15 DrvDebug 276
21.16 DrvDebug 277
21.17 DrvDebug 277
21.18 DrvDebug 278
21.19 DrvDebug 278
21.20 REBOOT 278
21.21 BOARD_REBOOT 279
21.22 BOARD_REMOVED 279
21.23 BOARD_STATE_FAULT 280
21.24 BOARD_STATE_NORMAL 280
21.25 CFCARD_FAILED 281
21.26 CFCARD_INSERTED 281
21.27 CFCARD_REMOVED 281
21.28 CHASSIS_REBOOT 282

21.29 CPU_STATE_NORMAL 282
21.30 DEV_CLOCK_CHANGE 282
21.31 DEV_FAULT_TOOLONG 283
21.32 DEV_REBOOT_UNSTABLE 283
21.33 DYINGGASP 283
21.34 FAN_ABSENT 284
21.35 FAN_DIRECTION_NOT_PREFERRED 284
21.36 FAN_FAILED 285
21.37 FAN_RECOVERED 285
21.38 MAD_DETECT 286
21.39 POWER_ABSENT 286
21.40 POWER_FAILED 287
21.41 POWER_MONITOR_ABSENT 287
21.42 POWER_MONITOR_FAILED 288
21.43 POWER_MONITOR_RECOVERED 288
21.44 POWER_RECOVERED 289
21.45 RPS_ABSENT 289
21.46 RPS_NORMAL 290
21.47 SUBCARD_FAULT 290
21.48 SUBCARD_INSERTED 291
21.49 SUBCARD_REBOOT 291
21.50 SUBCARD_REMOVED 291
21.51 SYSTEM_REBOOT 292
21.52 TEMPERATURE_ALARM 293
21.53 TEMPERATURE_LOW 294
21.54 TEMPERATURE_NORMAL 295
21.55 TEMPERATURE_POWEROFF 295
21.56 TEMPERATURE_SHUTDOWN 296
21.57 TEMPERATURE_WARNING 297
21.58 VCHK_VERSION_INCOMPATIBLE 297
22 DHCP 298
22.1 DHCP_NORESOURCES 298
22.2 DHCP_NOTSUPPORTED 298
23 DHCPR 298
23.1 DHCPR_SERVERCHANGE 299
23.2 DHCPR_SWITCHMASTER 299

24 DHCPS 299
24.1 DHCPS_ALLOCATE_IP 300
24.2 DHCPS_CONFLICT_IP 300
24.3 DHCPS_EXTEND_IP 301
24.4 DHCPS_FILE 301
24.5 DHCPS_RECLAIM_IP 302
24.6 DHCPS_THRESHOLD_EXCEED 302
24.7 DHCPS_THRESHOLD_RECOVER 302
24.8 DHCPS_VERIFY_CLASS 303
24.9 DHCPS_WARNING_EXHAUSTION 303
25 DHCPS6 303
25.1 DHCPS6_ALLOCATE_ADDRESS 304
25.2 DHCPS6_ALLOCATE_PREFIX 304
25.3 DHCPS6_CONFLICT_ADDRESS 305
25.4 DHCPS6_EXTEND_ADDRESS 305
25.5 DHCPS6_EXTEND_PREFIX 306
25.6 DHCPS6_FILE 306
25.7 DHCPS6_RECLAIM_ADDRESS 307
25.8 DHCPS6_RECLAIM_PREFIX 307
26 DHCPSP4 307
26.1 DHCPSP4_FILE 308
27 DHCPSP6 308
27.1 DHCPSP6_FILE 308
28 DIAG 308
28.1 CPU_MINOR_RECOVERY 309
28.2 CPU_MINOR_THRESHOLD 309
28.3 CPU_SEVERE_RECOVERY 309
28.4 CPU_SEVERE_THRESHOLD 310
28.5 DIAG_AI 310
28.6 DIAG_AI 310
28.7 FMEA 311
28.8 FMEA 311
28.9 FMEA 311
28.10 FMEA 312
28.11 DIAG_STORAGE_BELOW_THRESHOLD 312
28.12 DIAG_STORAGE_EXCEED_THRESHOLD 312

28.13 MEM_ALERT 313
28.14 MEM_BELOW_THRESHOLD 314
28.15 MEM_EXCEED_THRESHOLD 314
29 DLDP 314
29.1 DLDP_AUTHENTICATION_FAILED 315
29.2 DLDP_LINK_BIDIRECTIONAL 315
29.3 DLDP_LINK_SHUTMODECHG 315
29.4 DLDP_LINK_UNIDIRECTIONAL 316
29.5 DLDP_NEIGHBOR_AGED 316
29.6 DLDP_NEIGHBOR_CONFIRMED 317
29.7 DLDP_NEIGHBOR_DELETED 317
30 DOMAIN 317
30.1 DOMAIN_IP_LOWTHR_ALM 318
30.2 DOMAIN_IP_LOWTHR_ALM_REMOVE 318
30.3 DOMAIN_IP_UPTHR_ALM 319
30.4 DOMAIN_IP_UPTHR_ALM_REMOVE 319
30.5 DOMAIN_IPV6_LOWTHR_ALM 320
30.6 DOMAIN_IPV6_LOWTHR_ALM_REMOVE 320
30.7 DOMAIN_IPV6_UPTHR_ALM 321
30.8 DOMAIN_IPV6_UPTHR_ALM_REMOVE 321
30.9 DOMAIN_ND_PREF_LOWTHR_ALM 322
30.10 DOMAIN_ND_PREF_LOWTHR_ALM_REMOVE 322
30.11 DOMAIN_ND_PREF_UPTHR_ALM 323
30.12 DOMAIN_ND_PREF_UPTHR_ALM_REMOVE 323
30.13 DOMAIN_PD_PREF_LOWTHR_ALM 324
30.14 DOMAIN_PD_PREF_LOWTHR_ALM_REMOVE 324
30.15 DOMAIN_PD_PREF_UPTHR_ALM 325
30.16 DOMAIN_PD_PREF_UPTHR_ALM_REMOVE 325
31 DOT1X 325
31.1 DOT1X_LOGIN_FAILURE 326
31.2 DOT1X_LOGIN_SUCC 326
31.3 DOT1X_LOGOFF 327
31.4 DOT1X_NOTENOUGH_EADFREEIP_RES 327
31.5 DOT1X_NOTENOUGH_EADFREERULE_RES 327
31.6 DOT1X_NOTENOUGH_EADMACREDIR_RES 328
31.7 DOT1X_NOTENOUGH_EADPORTREDIR_RES 328

31.8 DOT1X_NOTENOUGH_ENABLEDOT1X_RES 328
31.9 DOT1X_SMARTON_FAILURE 329
31.10 DOT1X_UNICAST_NOT_EFFECTIVE 329
32 DP 329
32.1 DP_SWITCH_SUCCESS 330
33 DSTM 330
33.1 DrvDebug 330
33.2 DrvDebug 331
33.3 DrvDebug 331
33.4 DrvDebug 332
33.5 DrvDebug 332
33.6 DrvDebug 332
33.7 UTL 333
34 E&M 333
34.1 EM_CALLEDTALKING_IDLE 333
34.2 EM_CALLEDTALKING_SEIZE 334
34.3 EM_CALLERTALKING_IDLE 334
34.4 EM_CALLERTALKING_SEIZE 334
34.5 EM_SEND_IDLE 335
34.6 EM_SEND_SEIZE 335
35 EDEV 335
35.1 EDEV_FAILOVER_GROUP_STATE_CHANGE 335
36 EIGRP 336
36.1 RID_CHANGE 336
36.2 PEER_CHANGE 336
37 EKDM 337
37.1 EKDM 337
37.2 EKDM 338
38 ERPS 338
38.1 ERPS_STATE_CHANGED 338
39 ETH 338
39.1 ETH_VLAN_DEFAULT_TERMINATION_FAILED 339
39.2 ETH_VLAN_DEFAULT_TERMINATION_FAILED 339
39.3 ETH_VLAN_TERMINATION_FAILED 339
39.4 ETH_VLAN_TERMINATION_NOT_SUPPORT 340

39.5 ETH_VMAC_INEFFECTIVE 340
40 ETHOAM 340
40.1 ETHOAM_CONNECTION_FAIL_DOWN 340
40.2 ETHOAM_CONNECTION_FAIL_TIMEOUT 341
40.3 ETHOAM_CONNECTION_FAIL_UNSATISF 341
40.4 ETHOAM_CONNECTION_SUCCEED 341
40.5 ETHOAM_DISABLE 342
40.6 ETHOAM_DISCOVERY_EXIT 342
40.7 ETHOAM_ENABLE 342
40.8 ETHOAM_ENTER_LOOPBACK_CTRLLED 343
40.9 ETHOAM_ENTER_LOOPBACK_CTRLLING 343
40.10 ETHOAM_LOCAL_DYING_GASP 343
40.11 ETHOAM_LOCAL_ERROR_FRAME 344
40.12 ETHOAM_LOCAL_ERROR_FRAME_PERIOD 344
40.13 ETHOAM_LOCAL_ERROR_FRAME_SECOND 344
40.14 ETHOAM_LOCAL_LINK_FAULT 345
40.15 ETHOAM_LOOPBACK_EXIT 345
40.16 ETHOAM_LOOPBACK_EXIT_ERROR_STATU 345
40.17 ETHOAM_LOOPBACK_NO_RESOURCE 346
40.18 ETHOAM_LOOPBACK_NOT_SUPPORT 346
40.19 ETHOAM_NO_ENOUGH_RESOURCE 346
40.20 ETHOAM_NOT_CONNECTION_TIMEOUT 347
40.21 ETHOAM_QUIT_LOOPBACK_CTRLLED 347
40.22 ETHOAM_QUIT_LOOPBACK_CTRLLING 347
40.23 ETHOAM_REMOTE_CRITICAL 348
40.24 ETHOAM_REMOTE_DYING_GASP 348
40.25 ETHOAM_REMOTE_ERROR_FRAME 348
40.26 ETHOAM_REMOTE_ERROR_FRAME_PERIOD 349
40.27 ETHOAM_REMOTE_ERROR_FRAME_SECOND 349
40.28 ETHOAM_REMOTE_ERROR_SYMBOL 349
40.29 ETHOAM_REMOTE_EXIT 350
40.30 ETHOAM_REMOTE_FAILURE_RECOVER 350
40.31 ETHOAM_REMOTE_LINK_FAULT 350
41 EVB 350
41.1 EVB_AGG_FAILED 351
41.2 EVB_LICENSE_EXPIRE 351

41.3 EVB_VSI_OFFLINE 351
41.4 EVB_VSI_ONLINE 352
42 EVIISIS 352
42.1 EVIISIS_LICENSE 352
42.2 EVIISIS_NBR_CHG 353
43 FCLINK 353
43.1 FCLINK_FDISC_REJECT_NORESOURCE 353
43.2 FCLINK_FLOGI_REJECT_NORESOURCE 354
44 FCOE 354
44.1 FCOE_INTERFACE_NOTSUPPORT_FCOE 354
44.2 FCOE_LAGG_BIND_ACTIVE 355
44.3 FCOE_LAGG_BIND_DEACTIVE 355
45 FCZONE 355
45.1 FCZONE_DISTRIBUTE_FAILED 356
45.2 FCZONE_HARDZONE_DISABLED 356
45.3 FCZONE_HARDZONE_ENABLED 357
45.4 FCZONE_ISOLATE_ALLNEIGHBOR 357
45.5 FCZONE_ISOLATE_CLEAR_ALLVSAN 357
45.6 FCZONE_ISOLATE_CLEAR_VSAN 358
45.7 FCZONE_ISOLATE_NEIGHBOR 358
46 FDB 358
46.1 LRN 359
47 FIB 359
47.1 FIB_FILE 359
48 FILTER 359
48.1 FILTER_EXECUTION_ICMP 360
48.2 FILTER_EXECUTION_ICMPV6 361
48.3 FILTER_IPV4_EXECUTION 362
48.4 FILTER_IPV6_EXECUTION 363
49 FIPSNG 363
49.1 FIPSNG_HARD_RESOURCE_NOENOUGH 363
49.2 FIPSNG_HARD_RESOURCE_RESTORE 364
50 FTPD 364
50.1 FTP_ACL_DENY 364
50.2 FTP_REACH_SESSION_LIMIT 365

51 gRPC 365
51.1 GRPC_LOGIN 365
51.2 GRPC_LOGIN_FAILED 366
51.3 GRPC_LOGOUT 366
51.4 GRPC_SERVER_FAILED 366
51.5 GRPC_SUBSCRIBE_EVENT_FAILED 367
51.6 GRPC_RECEIVE_SUBSCRIPTION 367
52 HA 367
52.1 HA_BATCHBACKUP_FINISHED 367
52.2 HA_BATCHBACKUP_STARTED 368
52.3 HA_STANDBY_NOT_READY 368
52.4 HA_STANDBY_TO_MASTER 368
53 HQOS 368
53.1 HQOS_DP_SET_FAIL 369
53.2 HQOS_FP_SET_FAIL 369
53.3 HQOS_POLICY_APPLY_FAIL 369
53.4 HQOS_POLICY_RECOVER_FAIL 370
54 HTTPD 370
54.1 HTTPD_CONNECT 370
54.2 HTTPD_CONNECT_TIMEOUT 371
54.3 HTTPD_DISCONNECT 371
54.4 HTTPD_FAIL_FOR_ACL 371
54.5 HTTPD_FAIL_FOR_ACP 372
54.6 HTTPD_REACH_CONNECT_LIMIT 372
55 IF 372
55.1 IF 373
55.2 IF 373
55.3 IF 373
55.4 IF 374
55.5 IF 374
55.6 IF 375
55.7 IF 375
55.8 IF 376
55.9 IF 376

56 IFNET 376
56.1 VLAN_MODE_CHANGE 377
56.2 IF_JUMBOFRAME_WARN 377
56.3 INTERFACE_NOTSUPPRESSED 377
56.4 INTERFACE_SUPPRESSED 378
56.5 LINK_UPDOWN 378
56.6 PHY_UPDOWN 378
56.7 PROTOCOL_UPDOWN 379
56.8 VLAN_MODE_CHANGE 379
57 IKE 379
57.1 IKE_P1_SA_ESTABLISH_FAIL 380
57.2 IKE_P2_SA_ESTABLISH_FAIL 380
57.3 IKE_P2_SA_TERMINATE 381
58 INTRACE 381
58.1 WHITELIST 381
59 IP ROUTING 382
59.1 IPUC_ROUTE 382
59.2 IPUC_ROUTE 383
59.3 IPUC_ROUTE6 383
59.4 IPUC_VN 383
59.5 IPUC_VN 384
60 IP6ADDR 384
60.1 IP6ADDR_CREATEADDRESS_ERROR 384
60.2 IP6ADDR_CREATEADDRESS_INVALID 385
61 IP6FW 385
61.1 IP6FW_ABNORMAL_HEADERS 385
62 IP6FW 385
62.1 IP6FW_ABNORMAL_HEADERS 386
62.2 IP6FW_FAILED_TO_SET_MTU 386
63 IPADDR 386
63.1 IPADDR_HA_EVENT_ERROR 387
63.2 IPADDR_HA_STOP_EVENT 388
64 IPFW 388
64.1 IP_ADD_FLOW_ANTISYNFLD 388
64.2 IP_ADD_INTERFACE_ANTISYNFLD 389

64.3 IP_DEL_FLOW_ANTISYNFLD 389
64.4 IP_DEL_INTERFACE_ANTISYNFLD 390
64.5 IP_INSERT_FAILED_ANTISYNFLD 390
64.6 IP_NOTSUPPORT_ANTISYNFLD 390
64.7 IP_SETTING_FAILED_ANTISYNFLD 391
64.8 IPFW_BPA_NORESOURCE 391
64.9 IPFW_INFO 391
64.10 IPFW_FAILED_TO_SET_MTU 392
65 IPoE 392
65.1 DIAG 393
65.2 DIAG 393
65.3 IPOE_ENABLE_ERROR 394
65.4 IPOE_FREERULE_ERROR 395
65.5 IPOE_HTTP_DEFENSE 395
65.6 IPOE_IPV4_HTTP_ATTACK_EXCEED_ERROR 396
65.7 IPOE_IPV4_REMAIN_ACL_BELOW_ERROR 396
65.8 IPOE_IPV6_HTTP_ATTACK_EXCEED_ERROR 396
65.9 IPOE_IPV6_REMAIN_ACL_BELOW_ERROR 397
65.10 IPOE_REDIRECTRULE_ERROR 397
65.11 IPOE_SESSION_ERROR 398
65.12 IPOE_USER_LOGON_SUCCESS 398
65.13 IPOE_USER_LOGON_FAILED 399
65.14 IPOE_USER_LOGOFF 401
65.15 IPOE_USER_LOGOFF_ABNORMAL 402
65.16 USER_TRACEINFO 405
66 IPSEC 412
66.1 IPSEC_FAILED_ADD_FLOW_TABLE 412
66.2 IPSEC_PACKET_DISCARDED 413
66.3 IPSEC_SA_ESTABLISH 413
66.4 IPSEC_SA_ESTABLISH_FAIL 414
66.5 IPSEC_SA_INITINATION 414
66.6 IPSEC_SA_TERMINATE 415
67 IPSG 415
67.1 IPSG_ADDENTRY_ERROR 416
67.2 IPSG_DELENTRY_ERROR 417

68 IRDP 417
68.1 IRDP_EXCEED_ADVADDR_LIMIT 417
69 IRF 417
69.1 IRF 418
69.2 IRF 418
69.3 IRF_LINK_BLOCK 418
69.4 IRF_LINK_DOWN 419
69.5 IRF_LINK_UP 419
69.6 IRF_MEMBERID_CONFLICT 419
69.7 IRF_MERGE 420
69.8 IRF_MERGE_NEED_REBOOT 420
69.9 IRF_MERGE_NOT_NEED_REBOOT 420
70 ISIS 420
70.1 ISIS_LSP_CONFLICT 421
70.2 ISIS_MEM_ALERT 421
70.3 ISIS_NBR_CHG 422
71 ISSU 422
71.1 ISSU_PROCESSWITCHOVER 422
71.2 ISSU_ROLLBACKCHECKNORMAL 423
72 KHTTP 423
72.1 KHTTP_BIND_PORT_ALLOCETED 423
72.2 KHTTP_BIND_ADDRESS_INUSED 424
73 L2MC 424
73.1 L2MC_INIT 424
74 L2PT 424
74.1 L2PT_ADD_GROUPMEMBER_FAILED 425
74.2 L2PT_CREATE_TUNNELGROUP_FAILED 425
74.3 L2PT_ENABLE_DROP_FAILED 425
74.4 L2PT_SET_MULTIMAC_FAILED 426
75 L2TPV2 426
75.1 L2TPV2_TUNNEL_EXCEED_LIMIT 426
75.2 L2TPV2_SESSION_EXCEED_LIMIT 426
75.3 L2TPV2_SESSIONS_LOWER_THRESHOLD 427
75.4 L2TPV2_SESSIONS_RECOVER_NORMAL 427
75.5 L2TPV2_SESSIONS_UPPER_THRESHOLD 427

76 L2VPN 427
76.1 L2VPN_BGPVC_CONFLICT_LOCAL 428
76.2 L2VPN_BGPVC_CONFLICT_REMOTE 428
76.3 L2VPN_HARD_RESOURCE_NOENOUGH 428
76.4 L2VPN_HARD_RESOURCE_RESTORE 429
76.5 L2VPN_LABEL_DUPLICATE 429
76.6 L2VPN_MACLIMIT_FALL_AC 430
76.7 L2VPN_MACLIMIT_FALL_PW 430
76.8 L2VPN_MACLIMIT_FALL_VSI 431
76.9 L2VPN_MACLIMIT_MAX_AC 431
76.10 L2VPN_MACLIMIT_MAX_PW 432
76.11 L2VPN_MACLIMIT_MAX_VSI 432
77 L3 432
77.1 COMMON 433
77.2 COMMON 433
77.3 COMMON 433
77.4 COMMON 434
77.5 COMMON 434
77.6 COMMON 434
77.7 COMMON 435
77.8 L3_ARP 435
77.9 L3_ARP 435
77.10 L3_PAD 436
77.11 L3_PAD 436
77.12 L3_PAD 436
77.13 L3_PAD 437
77.14 L3_ARP 437
77.15 L3_COMMON 437
77.16 L3_P2C 438
77.17 L3_P2C 438
77.18 L3_P2C 438
77.19 L3_P2C 439
77.20 L3_MTU 439
78 L3MC 439
78.1 L3MC_IPv4 439
78.2 L3MC_IPv4 440

78.3 L3MC_BRAS 440
78.4 L3MC_IPv6 440
78.5 L3MC_IPv6 441
78.6 L3MC_MVPN 441
79 LAGG 441
79.1 LAGG_ACTIVE 441
79.2 LAGG_INACTIVE_AICFG 442
79.3 LAGG_INACTIVE_BFD 442
79.4 LAGG_INACTIVE_CONFIGURATION 443
79.5 LAGG_INACTIVE_DUPLEX 443
79.6 LAGG_INACTIVE_HARDWAREVALUE 443
79.7 LAGG_INACTIVE_LINKQUALITY_LOW 444
79.8 LAGG_INACTIVE_IRFSELECTMODE 444
79.9 LAGG_INACTIVE_LOWER_LIMIT 445
79.10 LAGG_INACTIVE_PARTNER 445
79.11 LAGG_INACTIVE_PHYSTATE 445
79.12 LAGG_INACTIVE_RESOURCE_INSUFICIE 446
79.13 LAGG_INACTIVE_SPEED 446
79.14 LAGG_INACTIVE_UPPER_LIMIT 446
80 LB 447
80.1 LB_SLB_LICENSE_INSTALLED 447
80.2 LB_SLB_LICENSE_UNINSTALLED 447
81 LDP 447
81.1 LDP_SESSION_CHG 448
81.2 LDP_SESSION_GR 449
81.3 LDP_SESSION_SP 449
82 LIF 450
82.1 API 450
82.2 API 450
82.3 DATA 451
82.4 EPOLL 451
82.5 IF 451
82.6 IF 452
82.7 IF 452
82.8 IF 452
82.9 IF 453

82.10 IF 453
82.11 IF 453
82.12 IF 454
82.13 IF 454
82.14 IF 455
82.15 QINQ 455
82.16 QINQ 456
82.17 QINQ 456
82.18 QINQ 457
82.19 QINQ 457
83 LLDP 457
83.1 LLDP_CREATE_NEIGHBOR 458
83.2 LLDP_DELETE_NEIGHBOR 458
83.3 LLDP_LESS_THAN_NEIGHBOR_LIMIT 459
83.4 LLDP_NEIGHBOR_AGE_OUT 459
83.5 LLDP_PVID_INCONSISTENT 460
83.6 LLDP_REACH_NEIGHBOR_LIMIT 460
84 LOAD 460
84.1 BOARD_LOADING 461
84.2 LOAD_FAILED 461
84.3 LOAD_FINISHED 461
85 LOCAL 462
85.1 LOCAL_CMDDENY 462
86 LOGIN 464
86.1 LOGIN_AUTHENTICATION_FAILED 465
86.2 LOGIN_FAILED 465
86.3 LOGIN_INVALID_USERNAME_PWD 466
87 LPDT 466
87.1 LPDT_LOOPED 466
87.2 LPDT_QINQ_LOOPED 466
87.3 LPDT_QINQ_RECOVERED 467
87.4 LPDT_RECOVERED 467
87.5 LPDT_VLAN_LOOPED 467
87.6 LPDT_VLAN_RECOVERED 468

88 LS 468
88.1 LS_ADD_USER_TO_GROUP 468
88.2 LS_AUTHEN_FAILURE 469
88.3 LS_AUTHEN_SUCCESS 469
88.4 LS_DEL_USER_FROM_GROUP 470
88.5 LS_DELETE_PASSWORD_FAIL 470
88.6 LS_PWD_ADDBLACKLIST 470
88.7 LS_PWD_CHGPWD_FOR_AGEDOUT 471
88.8 LS_PWD_CHGPWD_FOR_AGEOUT 471
88.9 LS_PWD_CHGPWD_FOR_COMPOSITION 471
88.10 LS_PWD_CHGPWD_FOR_FIRSTLOGIN 472
88.11 LS_PWD_CHGPWD_FOR_LENGTH 472
88.12 LS_PWD_FAILED2WRITEPASS2FILE 472
88.13 LS_PWD_MODIFY_FAIL 473
88.14 LS_PWD_MODIFY_SUCCESS 473
88.15 LS_REAUTHEN_FAILURE 474
88.16 LS_UPDATE_PASSWORD_FAIL 474
88.17 LS_USER_CANCEL 474
88.18 LS_USER_PASSWORD_EXPIRE 475
88.19 LS_USER_ROLE_CHANGE 475
88.20 LOCALSVR_PROMPTED_CHANGE_PWD 476
89 LSM 476
89.1 LSM_SR_LABEL_CONFLICT 477
89.2 LSM_SR_PREFIX_CONFLICT 477
90 LSPV 477
90.1 LSPV_PING_STATIS_INFO 478
91 MAC 478
91.1 MAC_TABLE_FULL_GLOBAL 478
91.2 MAC_TABLE_FULL_GLOBAL 479
91.3 MAC_TABLE_FULL_PORT 479
91.4 MAC_TABLE_FULL_VLAN 479
92 MACA 480
92.1 MACA_ENABLE_NOT_EFFECTIVE 480
92.2 MACA_LOGIN_FAILURE 480
92.3 MACA_LOGIN_SUCC 481
92.4 MACA_LOGOFF 481

93 MACSEC 481
93.1 MACSEC_MKA_KEEPALIVE_TIMEOUT 482
93.2 MACSEC_MKA_PRINCIPAL_ACTOR 482
93.3 MACSEC_MKA_SAK_REFRESH 482
93.4 MACSEC_MKA_SESSION_REAUTH 483
93.5 MACSEC_MKA_SESSION_SECURED 483
93.6 MACSEC_MKA_SESSION_START 484
93.7 MACSEC_MKA_SESSION_STOP 484
93.8 MACSEC_MKA_SESSION_UNSECURED 485
94 MBFD 485
94.1 MBFD_TRACEROUTE_FAILURE 485
95 MBUF 485
95.1 MBUF_DATA_BLOCK_CREATE_FAIL 486
96 MDC 486
96.1 MDC_CREATE 486
96.2 MDC_CREATE_ERR 487
96.3 MDC_DELETE 487
96.4 MDC_EVENT_ERROR 488
96.5 MDC_KERNEL_EVENT_TOOLONG 488
96.6 MDC_LICENSE_EXPIRE 489
96.7 MDC_NO_FORMAL_LICENSE 489
96.8 MDC_NO_LICENSE_EXIT 489
96.9 MDC_OFFLINE 490
96.10 MDC_ONLINE 490
96.11 MDC_STATE_CHANGE 490
97 MFIB 491
97.1 MFIB_CFG_NOT_SUPPORT 491
97.2 MFIB_MTI_NO_ENOUGH_RESOURCE 491
97.3 MFIB_OIF_NOT_SUPPORT 492
98 MGROUP 492
98.1 MGROUP_APPLY_SAMPLER_FAIL 492
98.2 MGROUP_RESTORE_CPUCFG_FAIL 493
98.3 MGROUP_RESTORE_IFCFG_FAIL 493
98.4 MGROUP_SYNC_CFG_FAIL 494

99 MPLS 494
99.1 MPLS_ILM 494
99.2 MPLS_NHLFE 494
99.3 MPLS_RSC 495
99.4 MPLS_VN 495
99.5 TE 495
99.6 VPLS_AC 496
99.7 VPLS_AC 496
99.8 VPLS_AC 496
99.9 VPLS_AC 497
99.10 VPLS_PW 497
99.11 VLL_FWD 497
99.12 VLL_FWD 498
99.13 VPLS_CFG 498
99.14 VPLS_CFG 498
99.15 VPLS_CFG 499
99.16 VPLS_CFG 499
99.17 VPLS_CFG 499
99.18 VPLS_CFG 500
99.19 MPLS_HARD_RESOURCE_NOENOUGH 500
99.20 MPLS_HARD_RESOURCE_RESTORE 500
100 MSC 500
100.1 MSC_NO_RTP_IN2SECS 501
100.2 MSC_NO_RTP_IN2XNSECS 501
100.3 MSC_NO_RTP_IN120SECS 501
101 MTLK 501
101.1 MTLK_UPLINK_STATUS_CHANGE 502
102 NAT 502
102.1 DSLITE_SYSLOG 502
102.2 EIM_MODE_PORT_USAGE_ALARM 503
102.3 NAT_ADDR_BIND_CONFLICT 503
102.4 NAT_EIM 504
102.5 NAT_FAILED_ADD_FLOW_RULE 504
102.6 NAT_FAILED_ADD_FLOW_TABLE 505
102.7 NAT_FLOW 506
102.8 NAT_INSTANCE_SERVER_INVALID 507

102.9 NAT_SERVER_INVALID 507
102.10 NAT_SERVICE_CARD_RECOVER_FAILURE 508
102.11 NAT444_SYSLOG 509
102.12 PORT_USAGE_ALARM 509
102.13 PORTBLOCK_ALARM 510
102.14 PORTBLOCKGRP_MEMORY_WARNING 510
103 ND 510
103.1 ND_CONFLICT 511
103.2 ND_DUPADDR 511
103.3 ND_HOST_IP_CONFLICT 512
103.4 ND_MAC_CHECK 512
103.5 ND_MAXNUM_DEV 512
103.6 ND_MAXNUM_IF 513
103.7 ND_RAGUARD_DROP 513
103.8 ND_SET_PORT_TRUST_NORESOURCE 513
103.9 ND_SET_VLAN_REDIRECT_NORESOURCE 514
104 NETCONF 514
104.1 CLI 514
104.2 EDIT-CONFIG 515
104.3 NETCONF_MSG_DEL 516
104.4 REPLY 516
104.5 THREAD 516
105 NP 517
105.1 NP 517
106 NPD 517
106.1 MONT 517
106.2 MONT 518
106.3 MONT 518
106.4 ECC_ERROR 518
106.5 ECC_ERROR 519
107 NQA 519
107.1 NQA_LOG_UNREACHABLE 519
107.2 NQA_PACKET_OVERSIZE 519
107.3 NQA_SCHEDULE_FAILURE 520
107.4 NQA_SEVER_FAILURE 520

108 NTP 520
108.1 NTP_CLOCK_CHANGE 521
108.2 NTP_LEAP_CHANGE 521
108.3 NTP_SOURCE_CHANGE 521
108.4 NTP_SOURCE_LOST 522
108.5 NTP_STRATUM_CHANGE 522
109 OBJP 522
109.1 OBJP_ACCELERATE_NO_RES 522
109.2 OBJP_ACCELERATE_NOT_SUPPORT 523
109.3 OBJP_ACCELERATE_UNK_ERR 523
110 OFP 523
110.1 OFC_DATAPATH_CHANNEL_CONNECT 523
110.2 OFC_DATAPATH_CHANNEL_DISCONNECT 524
110.3 OFC_FLOW_ADD 524
110.4 OFC_FLOW_DEL 524
110.5 OFC_FLOW_MOD 525
110.6 OFP_ACTIVE 525
110.7 OFP_ACTIVE_FAILED 525
110.8 OFP_CONNECT 526
110.9 OFP_FAIL_OPEN 526
110.10 OFP_FLOW_ADD 526
110.11 OFP_FLOW_ADD_DUP 527
110.12 OFP_FLOW_ADD_FAILED 527
110.13 OFP_FLOW_ADD_TABLE_MISS 528
110.14 OFP_FLOW_ADD_TABLE_MISS_FAILED 528
110.15 OFP_FLOW_DEL 529
110.16 OFP_FLOW_DEL_TABLE_MISS 529
110.17 OFP_FLOW_DEL_TABLE_MISS_FAILED 530
110.18 OFP_FLOW_MOD 530
110.19 OFP_FLOW_MOD_FAILED 531
110.20 OFP_FLOW_MOD_TABLE_MISS 531
110.21 OFP_FLOW_MOD_TABLE_MISS_FAILED 532
110.22 OFP_FLOW_RMV_GROUP 532
110.23 OFP_FLOW_RMV_HARDTIME 532
110.24 OFP_FLOW_RMV_IDLETIME 533
110.25 OFP_FLOW_RMV_METER 533

110.26 OFP_FLOW_UPDATE_FAILED 534
110.27 OFP_GROUP_ADD 534
110.28 OFP_GROUP_ADD_FAILED 535
110.29 OFP_GROUP_DEL 535
110.30 OFP_GROUP_MOD 535
110.31 OFP_GROUP_MOD_FAILED 536
110.32 OFP_METER_ADD 536
110.33 OFP_METER_ADD_FAILED 536
110.34 OFP_METER_DEL 537
110.35 OFP_METER_MOD 537
110.36 OFP_METER_MOD_FAILED 537
110.37 OFP_MISS_RMV_GROUP 538
110.38 OFP_MISS_RMV_HARDTIME 538
110.39 OFP_MISS_RMV_IDLETIME 538
110.40 OFP_MISS_RMV_METER 539
111 OPENSRC（RSYNC） 539
111.1 同步成功 539
111.2 同步失败 540
111.3 同步错误 540
112 OPTMOD 540
112.1 BIAS_HIGH 541
112.2 BIAS_LOW 541
112.3 BIAS_NORMAL 541
112.4 CFG_ERR 542
112.5 CHKSUM_ERR 542
112.6 FIBER_SFP MODULE_INVALID 542
112.7 FIBER_SFPMODULE_NOWINVALID 543
112.8 IO_ERR 543
112.9 MOD_ALM_OFF 543
112.10 MOD_ALM_ON 544
112.11 MODULE_IN 544
112.12 MODULE_OUT 544
112.13 PHONY_MODULE 545
112.14 RX_ALM_OFF 545
112.15 RX_ALM_ON 545
112.16 RX_POW_HIGH 546

112.17 RX_POW_LOW 546
112.18 RX_POW_NORMAL 546
112.19 TEMP_HIGH 547
112.20 TEMP_LOW 547
112.21 TEMP_NORMAL 547
112.22 TX_ALM_OFF 548
112.23 TX_ALM_ON 548
112.24 TX_POW_HIGH 548
112.25 TX_POW_LOW 549
112.26 TX_POW_NORMAL 549
112.27 TYPE_ERR 549
112.28 VOLT_HIGH 550
112.29 VOLT_LOW 550
112.30 VOLT_NORMAL 550
113 OSPF 551
113.1 OSPF_DUP_RTRID_NBR 551
113.2 OSPF_IP_CONFLICT_INTRA 551
113.3 OSPF_LAST_NBR_DOWN 552
113.4 OSPF_MEM_ALERT 552
113.5 OSPF_NBR_CHG 553
113.6 OSPF_RT_LMT 553
113.7 OSPF_RTRID_CHG 553
113.8 OSPF_RTRID_CONFLICT_INTER 554
113.9 OSPF_RTRID_CONFLICT_INTRA 554
113.10 OSPF_VLINKID_CHG 554
114 OSPFV3 554
114.1 OSPFV3_LAST_NBR_DOWN 555
114.2 OSPFV3_MEM_ALERT 555
114.3 OSPFV3_NBR_CHG 556
114.4 OSPFV3_RT_LMT 556
115 PBB 556
115.1 PBB_JOINAGG_WARNING 557
116 PBR 557
116.1 PBR_HARDWARE_BIND_ERROR 557
116.2 PBR_HARDWARE_ERROR 558
116.3 PBR_NEXTHOP_CHANGE 558

117 PCE 558
117.1 PCE_PCEP_SESSION_CHG 559
118 PEX（IRF3.1） 560
118.1 PEX_AUTOCONFIG_BAGG_ASSIGNMEMBER 560
118.2 PEX_AUTOCONFIG_BAGG_CREATE 560
118.3 PEX_AUTOCONFIG_BAGG_NORESOURCE 560
118.4 PEX_AUTOCONFIG_BAGG_REMOVEMEMBER 561
118.5 PEX_AUTOCONFIG_CAPABILITY_ENABLE 561
118.6 PEX_AUTOCONFIG_CASCADELIMIT 561
118.7 PEX_AUTOCONFIG_CONNECTION_ERROR 562
118.8 PEX_AUTOCONFIG_DIFFGROUPNUMBER 562
118.9 PEX_AUTOCONFIG_DYNAMICBAGG_STP 562
118.10 PEX_AUTOCONFIG_GROUP_CREATE 563
118.11 PEX_AUTOCONFIG_NONUMBERRESOURCE 563
118.12 PEX_AUTOCONFIG_NOT_CASCADEPORT 564
118.13 PEX_AUTOCONFIG_NUMBER_ASSIGN 564
118.14 PEX_LLDP_DISCOVER 565
118.15 PEX_MEMBERID_EXCEED 565
118.16 PEX_PECSP_OPEN_RCVD 565
118.17 PEX_PECSP_OPEN_SEND 566
118.18 PEX_PECSP_TIMEOUT 566
119 PEX（IRF3） 566
119.1 PEX_ASSOCIATEID_MISMATCHING 567
119.2 PEX_CONFIG_ERROR 567
119.3 PEX_CONNECTION_ERROR 568
119.4 PEX_FORBID_STACK 568
119.5 PEX_LINK_BLOCK 569
119.6 PEX_LINK_DOWN 569
119.7 PEX_LINK_FORWARD 570
119.8 PEX_REG_JOININ 570
119.9 PEX_REG_LEAVE 571
119.10 PEX_REG_REQUEST 571
119.11 PEX_STACKCONNECTION_ERROR 572
120 PFILTER 573
120.1 PFILTER_GLB_RES_CONFLICT 573
120.2 PFILTER_GLB_IPV4_DACT_NO_RES 573

120.3 PFILTER_GLB_IPV4_DACT_UNK_ERR 574
120.4 PFILTER_GLB_IPV6_DACT_NO_RES 574
120.5 PFILTER_GLB_IPV6_DACT_UNK_ERR 574
120.6 PFILTER_GLB_MAC_DACT_NO_RES 575
120.7 PFILTER_GLB_MAC_DACT_UNK_ERR 575
120.8 PFILTER_GLB_NO_RES 575
120.9 PFILTER_GLB_NOT_SUPPORT 576
120.10 PFILTER_GLB_UNK_ERR 576
120.11 PFILTER_IF_IPV4_DACT_NO_RES 577
120.12 PFILTER_IF_IPV4_DACT_UNK_ERR 577
120.13 PFILTER_IF_IPV6_DACT_NO_RES 577
120.14 PFILTER_IF_IPV6_DACT_UNK_ERR 578
120.15 PFILTER_IF_MAC_DACT_NO_RES 578
120.16 PFILTER_IF_MAC_DACT_UNK_ERR 578
120.17 PFILTER_IF_NO_RES 579
120.18 PFILTER_IF_NOT_SUPPORT 579
120.19 PFILTER_IF_RES_CONFLICT 580
120.20 PFILTER_IF_UNK_ERR 580
120.21 PFILTER_IPV6_STATIS_INFO 581
120.22 PFILTER_STATIS_INFO 581
120.23 PFILTER_VLAN_IPV4_DACT_NO_RES 582
120.24 PFILTER_VLAN_IPV4_DACT_UNK_ERR 582
120.25 PFILTER_VLAN_IPV6_DACT_NO_RES 582
120.26 PFILTER_VLAN_IPV6_DACT_UNK_ERR 583
120.27 PFILTER_VLAN_MAC_DACT_NO_RES 583
120.28 PFILTER_VLAN_MAC_DACT_UNK_ERR 583
120.29 PFILTER_VLAN_NO_RES 584
120.30 PFILTER_VLAN_NOT_SUPPORT 584
120.31 PFILTER_VLAN_RES_CONFLICT 585
120.32 PFILTER_VLAN_UNK_ERR 585
121 PIM 585
121.1 PIM_NBR_DOWN 586
121.2 PIM_NBR_UP 586
122 PING 586
122.1 PING_STATISTICS 587
122.2 PING_VPN_STATISTICS 588

123 PKI 588
123.1 REQUEST_CERT_FAIL 588
123.2 REQUEST_CERT_SUCCESS 589
124 PKT2CPU 589
124.1 PKT2CPU_NO_RESOURCE 589
125 PKTCPT 589
125.1 PKTCPT_AP_OFFLINE 590
125.2 PKTCPT_AREADY_EXIT 590
125.3 PKTCPT_CONN_FAIL 590
125.4 PKTCPT_INVALID_FILTER 591
125.5 PKTCPT_LOGIN_DENIED 591
125.6 PKTCPT_MEMORY_ALERT 591
125.7 PKTCPT_OPEN_FAIL 592
125.8 PKTCPT_OPERATION_TIMEOUT 592
125.9 PKTCPT_SERVICE_FAIL 592
125.10 PKTCPT_UNKNOWN_ERROR 593
125.11 PKTCPT_UPLOAD_ERROR 593
125.12 PKTCPT_WRITE_FAIL 593
126 PORT 594
126.1 OMA 594
127 PORTAL 594
127.1 PORTAL_INFO 594
127.2 PORTAL_DIAG 595
127.3 PORTAL_LIMIT_GLOBAL 595
127.4 PORTAL_LIMIT_IF 595
127.5 PORTAL_USER_LOGOFF 596
127.6 PORTAL_USER_LOGOFF_ABNORMAL 597
127.7 PORTAL_USER_LOGON_FAIL 599
127.8 PORTAL_USER_LOGON_SUCCESS 600
127.9 USER_TRACEINFO 601
128 PORTSEC 603
128.1 PORTSEC_ACL_FAILURE 604
128.2 PORTSEC_LEARNED_MACADDR 604
128.3 PORTSEC_NTK_NOT_EFFECTIVE 605
128.4 PORTSEC_PORTMODE_NOT_EFFECTIVE 605

128.5 PORTSEC_PROFILE_FAILURE 605
128.6 PORTSEC_VIOLATION 606
129 PPP 606
129.1 IPPOOL_ADDRESS_EXHAUSTED 606
129.2 PPP_USER_LOGON_SUCCESS 607
129.3 PPP_USER_LOGON_FAILED 607
129.4 PPP_USER_LOGOFF 609
129.5 PPP_USER_LOGOFF_ABNORMAL 610
129.6 PPPOES_LIMIT 612
129.7 PPPOES_LIMIT_VLAN 613
129.8 PPPOES_LIMIT_IF 613
129.9 PPPOES_LIMIT_MAC 614
129.10 PPPOES_MAC_THROTTLE 614
129.11 USER_TRACEINFO 615
130 PPPoE 621
130.1 PPPOE_DAPI 622
130.2 PPPOE_PADI 622
130.3 PADI_DEFEND 622
130.4 PPPOE_ENABLE 623
130.5 PPPOE_TABLE 623
131 PS 623
131.1 PS_SWITCH_WTOP 624
131.2 PS_SWITCH_PTOW 624
132 PTP 624
132.1 PTP_CLOCK_SOURCE_CLASS_BELOW_THRESHOLD 625
132.2 PTP_CLOCK_SOURCE_CLASS_RECOVER 625
132.3 PTP_EXT_TIME_PORT_DISCONNECT 626
132.4 PTP_EXT_TIME_PORT_RECOVER 626
132.5 PTP_FREQUENCY_LOCK 626
132.6 PTP_FREQUENCY_NOT_LOCK 627
132.7 PTP_MASTER_CLOCK_CHANGE 628
132.8 PTP_PKTLOST_RECOVER 629
132.9 PTP_PKTLOST 629
132.10 PTP_PORT_BMCINFO_CHANGE 630
132.11 PTP_PORT_STATE_CHANGE 631
132.12 PTP_SRC_CHANGE 632

132.13 PTP_SRC_SWITCH 633
132.14 PTP_TIME_LOCK 633
132.15 PTP_TIME_NOT_LOCK 633
132.16 PTP_TIME_OFFSE_EXCEED_THRESHOLD 634
132.17 PTP_TIME_OFFSET_RECOVER 634
132.18 PTP_TIME_SYNC 634
132.19 PTP_TIME_UNSYNC 635
132.20 PTP_TIMESTAMP_CHANGE 635
132.21 PTP_TIMESTAMP_UNCHANGE 636
133 PWDCTL 636
133.1 PWDCTL_ADD_BLACKLIST 636
133.2 PWDCTL_CHANGE_PASSWORD 637
133.3 PWDCTL_FAILED_TO_OPENFILE 637
133.4 PWDCTL_FAILED_TO_WRITEPWD 637
133.5 PWDCTL_UPDATETIME 638
134 QACL 638
134.1 ACL 638
134.2 ACL 639
134.3 DrvDebug 639
134.4 DrvDebug 640
134.5 DrvDebug 640
134.6 DrvDebug 641
134.7 QoS 641
134.8 QoS 642
134.9 QoS 642
134.10 QoS 642
134.11 QOS_CAR_APPLYIF_FAIL 643
134.12 QOS_QMPROFILE_RESTORE_FAIL 643
134.13 TE 644
135 QOS 644
135.1 EDSG_CONFIG_CONFLICT 644
135.2 EDSG_EXCEED_LIMIT 645
135.3 EDSG_LRMODE_CONFLICT 645
135.4 EDSG_MODE_CONFLICT 646
135.5 EDSG_NOT_SUPPORT 646
135.6 QOS_CAR_APPLYUSER_FAIL 647

135.7 QOS_CBWFQ_REMOVED 647
135.8 QOS_DIFFSERV_CFG_FAIL 648
135.9 QOS_GTS_APPLYINT_FAIL 648
135.10 QOS_GTS_APPLYUSER_FAIL 649
135.11 QOS_MEMORY_WARNING 649
135.12 QOS_NOT_ENOUGH_BANDWIDTH 650
135.13 QOS_POLICY_APPLYCOPP_CBFAIL 650
135.14 QOS_POLICY_APPLYCOPP_FAIL 651
135.15 QOS_POLICY_APPLYGLOBAL_CBFAIL 651
135.16 QOS_POLICY_APPLYGLOBAL_FAIL 652
135.17 QOS_POLICY_APPLYIF_CBFAIL 652
135.18 QOS_POLICY_APPLYIF_FAIL 653
135.19 QOS_POLICY_APPLYUSER_FAIL 653
135.20 QOS_POLICY_APPLYVLAN_CBFAIL 654
135.21 QOS_POLICY_APPLYVLAN_FAIL 654
135.22 QOS_QMPROFILE_APPLYINT_FAIL 655
135.23 QOS_QMPROFILE_APPLYUSER_FAIL 655
135.24 QOS_QMPROFILE_MODIFYQUEUE_FAIL 656
135.25 QOS_PRIORITY_APPLYUSER_FAIL 656
135.26 QOS_LR_APPLYIF_CONFIGFAIL 656
135.27 QOS_ITACAR_APPLYUSER_FAIL 657
135.28 QOS_WEIGHT_APPLYUSER_FAIL 657
136 RADIUS 657
136.1 RADIUS_AUTH_FAILURE 658
136.2 RADIUS_AUTH_SUCCESS 658
136.3 RADIUS_DELETE_HOST_FAIL 658
137 RDDC 658
137.1 RDDC_ACTIVENODE_CHANGE 659
138 RIP 659
138.1 RIP_MEM_ALERT 659
138.2 RIP_RT_LMT 660
139 RIPNG 660
139.1 RIPNG_MEM_ALERT 660
139.2 RIPNG_RT_LMT 660

140 RM 661
140.1 RM_ACRT_REACH_LIMIT 661
140.2 RM_ACRT_REACH_THRESVALUE 661
140.3 RM_THRESHLD_VALUE_REACH 662
141 RPR 662
141.1 RPR_EXCEED_MAX_SEC_MAC 662
141.2 RPR_EXCEED_MAX_SEC_MAC_OVER 663
141.3 RPR_EXCEED_MAX_STATION 663
141.4 RPR_EXCEED_MAX_STATION_OVER 663
141.5 RPR_EXCEED_RESERVED_RATE 664
141.6 RPR_EXCEED_RESERVED_RATE_OVER 664
141.7 RPR_IP_DUPLICATE 664
141.8 RPR_IP_DUPLICATE_OVER 665
141.9 RPR_JUMBO_INCONSISTENT 665
141.10 RPR_JUMBO_INCONSISTENT_OVER 665
141.11 RPR_LAGGCONFIG_INCONSISTENT 666
141.12 RPR_LAGGCONFIG_INCONSISTENT_OVER 666
141.13 RPR_MISCABLING 666
141.14 RPR_MISCABLING_OVER 667
141.15 RPR_PROTECTION_INCONSISTENT 667
141.16 RPR_PROTECTION_INCONSISTENT_OVER 667
141.17 RPR_SEC_MAC_DUPLICATE 668
141.18 RPR_SEC_MAC_DUPLICATE_OVER 668
141.19 RPR_TOPOLOGY_INCONSISTENT 668
141.20 RPR_TOPOLOGY_INCONSISTENT_OVER 669
141.21 RPR_TOPOLOGY_INSTABILITY 669
141.22 RPR_TOPOLOGY_INSTABILITY_OVER 669
141.23 RPR_TOPOLOGY_INVALID 670
141.24 RPR_TOPOLOGY_INVALID_OVER 670
142 RRPP 670
142.1 RRPP_RING_FAIL 670
142.2 RRPP_RING_RESTORE 671
143 RSVP 671
143.1 RSVP_FRR_SWITCH 671
143.2 RSVP_P2MP_FRR_SWITCH 672

144 RTM 672
144.1 RTM_ENVIRONMENT 672
144.2 RTM_TCL_LOAD_FAILED 672
144.3 RTM_TCL_MODIFY 673
144.4 RTM_TCL_NOT_EXIST 673
145 RXTX 673
145.1 INIT 674
146 SCM 674
146.1 PROCESS_ABNORMAL 675
146.2 PROCESS_ACTIVEFAILED 675
146.3 SCM_ABNORMAL_REBOOT 676
146.4 SCM_ABNORMAL_REBOOTMDC 677
146.5 SCM_ABORT_RESTORE 677
146.6 SCM_INSMOD_ADDON_TOOLONG 678
146.7 SCM_KERNEL_INIT_TOOLONG 678
146.8 SCM_PROCESS_STARTING_TOOLONG 679
146.9 SCM_PROCESS_STILL_STARTING 679
146.10 SCM_SKIP_PROCESS 680
146.11 SCM_SKIP_PROCESS 680
147 SCRLSP 680
147.1 SCRLSP_LABEL_DUPLICATE 681
148 SESSION 681
148.1 SESSION_DRV_EXCEED 681
148.2 SESSION_DRV_RECOVERY 682
148.3 SESSION_IPV4_FLOW 683
148.4 SESSION_IPV6_FLOW 685
149 SFLOW 685
149.1 SFLOW_HARDWARE_ERROR 686
150 SHELL 686
150.1 SHELL_CMD 686
150.2 SHELL_CMD_CONFIRM 687
150.3 SHELL_CMD_EXECUTEFAIL 687
150.4 SHELL_CMD_INPUT 688
150.5 SHELL_CMD_INPUT_TIMEOUT 688
150.6 SHELL_CMD_LOCKEDBYOTHER 689

150.7 SHELL_CMD_MATCHFAIL 689
150.8 SHELL_CMDDENY 689
150.9 SHELL_CMDFAIL 690
150.10 SHELL_COMMIT_FAIL 690
150.11 SHELL_COMMIT_ROLLBACK 690
150.12 SHELL_COMMIT_ROLLBACKDONE 691
150.13 SHELL_COMMIT_ROLLBACKFAIL 691
150.14 SHELL_COMMIT_SUCCESS 691
150.15 SHELL_CRITICAL_CMDFAIL 692
150.16 SHELL_LOGIN 692
150.17 SHELL_LOGOUT 692
150.18 SHELL_SAVE_FAILED 693
150.19 SHELL_SAVE_SUCCESS 693
150.20 SHELL_SAVEPOINT_EXIST 693
150.21 SHELL_SAVEPOINT_FAILED 694
150.22 SHELL_SAVEPOINT_SUCCESS 694
151 SLSP 694
151.1 SLSP_LABEL_DUPLICATE 694
152 SMLK 695
152.1 SMLK_LINK_SWITCH 695
153 SNMP 695
153.1 SNMP_ACL_RESTRICTION 695
153.2 SNMP_AUTHENTICATION_FAILURE 696
153.3 SNMP_GET 696
153.4 SNMP_INFORM_LOST 697
153.5 SNMP_NOTIFY 698
153.6 SNMP_SET 699
153.7 SNMP_USM_NOTINTIMEWINDOW 699
154 SSHC 699
154.1 SSHC_ALGORITHM_MISMATCH 700
155 SSHS 700
155.1 SSHS_ACL_DENY 700
155.2 SSHS_ALGORITHM_MISMATCH 701
155.3 SSHS_AUTH_EXCEED_RETRY_TIMES 701
155.4 SSHS_AUTH_FAIL 702

155.5 SSHS_AUTH_TIMEOUT 702
155.6 SSHS_CONNECT 702
155.7 SSHS_DECRYPT_FAIL 703
155.8 SSHS_DISCONNECT 703
155.9 SSHS_ENCRYPT_FAIL 703
155.10 SSHS_LOG 704
155.11 SSHS_MAC_ERROR 704
155.12 SSHS_REACH_SESSION_LIMIT 704
155.13 SSHS_REACH_USER_LIMIT 705
155.14 SSHS_SCP_OPER 705
155.15 SSHS_SFTP_OPER 706
155.16 SSHS_SRV_UNAVAILABLE 706
155.17 SSHS_VERSION_MISMATCH 707
156 STAMGR 707
156.1 STAMGR_ADD_FAILVLAN 707
156.2 STAMGR_ADDBAC_INFO 707
156.3 STAMGR_ADDSTA_INFO 708
156.4 STAMGR_AUTHORACL_FAILURE 708
156.5 STAMGR_AUTHORUSERPROFILE_FAILURE 709
156.6 STAMGR_CLIENT_OFFLINE 709
156.7 STAMGR_CLIENT_ONLINE 709
156.8 STAMGR_DELBAC_INFO 710
156.9 STAMGR_DELSTA_INFO 710
156.10 STAMGR_DOT1X_LOGIN_FAILURE 710
156.11 STAMGR_DOT1X_LOGIN_SUCC 711
156.12 STAMGR_DOT1X_LOGOFF 711
156.13 STAMGR_MACA_LOGIN_FAILURE 712
156.14 STAMGR_MACA_LOGIN_SUCC 712
156.15 STAMGR_MACA_LOGOFF 713
156.16 STAMGR_STAIPCHANGE_INFO 713
156.17 STAMGR_TRIGGER_IP 714
157 STM 714
157.1 STM_AUTO_UPDATE_FAILED 715
157.2 STM_AUTO_UPDATE_FINISHED 716
157.3 STM_AUTO_UPDATING 716
157.4 STM_LINK_DOWN 717

157.5 STM_LINK_TIMEOUT 717
157.6 STM_LINK_UP 717
157.7 STM_MERGE 718
157.8 STM_MERGE_NEED_REBOOT 718
157.9 STM_MERGE_NOT_NEED_REBOOT 718
157.10 STM_SAMEMAC 719
157.11 STM_SOMER_CHECK 719
158 STP 719
158.1 STP_BPDU_PROTECTION 719
158.2 STP_BPDU_RECEIVE_EXPIRY 720
158.3 STP_CONSISTENCY_RESTORATION 720
158.4 STP_DETECTED_TC 720
158.5 STP_DISABLE 721
158.6 STP_DISCARDING 721
158.7 STP_ENABLE 721
158.8 STP_FORWARDING 722
158.9 STP_LOOP_PROTECTION 722
158.10 STP_NOT_ROOT 722
158.11 STP_NOTIFIED_TC 723
158.12 STP_PORT_TYPE_INCONSISTENCY 723
158.13 STP_PVID_INCONSISTENCY 723
158.14 STP_PVST_BPDU_PROTECTION 724
158.15 STP_ROOT_PROTECTION 724
159 SWFA 724
159.1 FWD 724
159.2 FWD 725
160 SYSEVENT 725
160.1 EVENT_TIMEOUT 725
161 SYSLOG 725
161.1 SYSLOG_FILE_DECOMPRESS_ERROR 726
161.2 SYSLOG_LOGFILE_FULL 726
161.3 SYSLOG_RESTART 726
161.4 SYSLOG_RTM_EVENT_BUFFER_FULL 727
162 SYSM 727
162.1 DrvDebug 727

162.2 DrvDebug 728
162.3 DrvDebug 728
162.4 DrvDebug 729
162.5 DrvDebug 729
162.6 DrvDebug 729
162.7 DrvDebug 730
162.8 DrvDebug 730
162.9 DrvDebug 730
162.10 DrvDebug 731
162.11 DrvDebug 731
162.12 DrvDebug 731
162.13 DrvDebug 732
162.14 DrvDebug 732
162.15 DrvDebug 733
162.16 DrvDebug 733
162.17 DrvDebug 734
162.18 DrvDebug 734
162.19 DrvDebug 734
162.20 DrvDebug 735
162.21 DrvDebug 736
162.22 DrvDebug 737
162.23 DrvDebug 737
162.24 DrvDebug 737
162.25 DrvDebug 738
162.26 DrvDebug 738
162.27 DrvDebug 738
162.28 DrvDebug 739
162.29 DrvDebug 739
162.30 DrvDebug 739
162.31 DrvDebug 740
162.32 DrvDebug 740
162.33 FUNCMV 740
162.34 SUBCARD 741
162.35 SUBCARD 741
162.36 SUBCARD 742
162.37 SUBCARD 742

162.38 SUBCARD 743
162.39 SUBCARD 743
162.40 SUBCARD 743
163 TACACS 744
163.1 TACACS_AUTH_FAILURE 744
163.2 TACACS_AUTH_SUCCESS 744
163.3 TACACS_DELETE_HOST_FAIL 744
164 TBDL 745
164.1 TBDL_SWICH_P 745
164.2 TBDL_SWICH_W 745
165 TE 745
165.1 TE_BACKUP_SWITCH 746
165.2 TE_MBB_SWITCH 746
166 TELNETD 747
166.1 TELNETD_ACL_DENY 747
166.2 TELNETD_REACH_SESSION_LIMIT 747
167 TRILL 747
167.1 TRILL_DUP_SYSTEMID 748
167.2 TRILL_INTF_CAPABILITY 748
167.3 TRILL_LICENSE_EXPIRED 748
167.4 TRILL_MEM_ALERT 749
167.5 TRILL_NBR_CHG 749
167.6 TRILL_NO_LICENSE 749
168 TUNNEL 750
168.1 L3_TUNNEL 750
168.2 L3_TUNNEL 750
169 USER 750
169.1 USER_RECOVER_NORMAL 751
169.2 USER_UPPER_THRESHOLD 751
170 VLAN 752
170.1 VLAN_FAILED 752
170.2 VLAN_VLANMAPPING_FAILED 752
170.3 VLAN_VLANTRANSPARENT_FAILED 752
171 VRRP 753
171.1 VRRP_STATUS_CHANGE 753

171.2 VRRP_VF_STATUS_CHANGE 754
171.3 VRRP_VMAC_INEFFECTIVE 754
172 VSRP 754
172.1 VSRP_BIND_FAILED 755
173 VXLAN 755
173.1 VXLAN_LICENSE_UNAVAILABLE 755
174 WAN 755
174.1 ALARM 756
174.2 ALARM 757
174.3 ALARM 758
174.4 ALARM 759
174.5 ALARM 760
174.6 ALARM 761
174.7 ALARM 762
174.8 ATM 762
175 WIPS 762
175.1 APFLOOD 763
175.2 AP_CHANNEL_CHANGE 763
175.3 ASSOCIATEOVERFLOW 763
175.4 HONEYPOT 764
175.5 HTGREENMODE 764
175.6 MAN_IN_MIDDLE 764
175.7 WIPS_DOS 765
175.8 WIPS_FLOOD 765
175.9 WIPS_MALF 766
175.10 WIPS_ROGUE 767
175.11 WIPS_SPOOF 767
175.12 WIPS_UNAUTH 768
175.13 WIPS_WEAKIV 768
175.14 WIRELESSBRIDGE 768

1 简介

本文包含日志的参数介绍、产生原因、处理建议等，为用户进行系统诊断和维护提供参考。

除了 CR16000-F 特有的日志信息外，本文还包含 Comware V7 平台版本的日志信息，其中的部分日志信息本产品可能并不支持，请以设备的实际情况为准。

本文假设您已具备数据通信技术知识，并熟悉 H3C 网络产品。

1.1 日志格式说明

缺省情况下，日志信息根据输出方向不同，采用如下格式：

- 日志主机方向（RFC 3164 定义的格式）：

```
<PRI>TIMESTAMP Sysname %%vendorMODULE/severity/MNEMONIC: location; CONTENT
```

- 非日志主机方向：

```
Prefix TIMESTAMP Sysname MODULE/severity/MNEMONIC: CONTENT
```

表1-1 日志字段说明

字段	描述
<PRI>	优先级标识符，仅存在于输出方向为日志主机的日志信息。优先级的计算公式为：facility×8＋severity • facility 表示日志主机的记录工具，由 **info-center loghost** 命令设置，主要用于在日志主机端标志不同的日志来源，查找、过滤对应日志源的日志。 • severity 表示日志信息的严重等级，具体含义请参见表 1-2
Prefix	信息类型标识符，仅存在于输出方向为非日志主机方向的日志信息 • 百分号（%）：表示该日志信息为 Informational 级别及以上级别的日志 • 星号（*）：表示该日志信息为 Debug 级别的日志
TIMESTAMP	时间戳记录了日志信息产生的时间，方便用户查看和定位系统事件 • 日志主机方向：时间戳精确到秒，用户可以通过 **info-center timestamp loghost** 命令自定义时间显示格式 • 非日志主机方向：时间戳精确到毫秒，用户可以通过 **info-center timestamp** 命令自定义时间显示格式
Sysname	生成该日志信息的设备的名称或IP地址
%%vendor	厂家标志，%%10表示本日志信息由H3C设备生成 只有发往日志主机的日志中携带该字段
MODULE	生成该日志信息的功能模块的名称
severity	日志信息的等级，具体说明请参见表1-2
MNEMONIC	助记符，本字段为该日志信息的概述，是一个不超过32个字符的字符串
location	定位信息，用来标识该日志信息的产生者。本字段为可选字段，只有在日志信息发往日志主机时才会存在，可能包含以下参数： • -MDC=XX，表示生成该日志的 MDC 的编号 • -DevIp=XXX.XXX.XXX.XXX，表示日志发送者的源 IP

字段	描述
	• -Slot=XX，表示生成该日志的 Slot 编号 • -Chassis=XX-Slot=XX，表示生成该日志的 Chassis 编号和 Slot 编号 格式如下： -attribute1=x-attribute2=y…-attributeN=z 定位信息和日志描述之间用分号和空格“; ”分隔 说明 日志手册中以输出到非日志主机方向的日志为例，不提供 location 字段。
CONTENT	该日志的具体内容，包含事件或错误发生的详细信息 对于本字段中的可变参数域，本文使用表1-3定义的方式表示

日志信息按严重性可划分为如表 1-2 所示的八个等级，各等级的严重性依照数值从 0～7 依次降低。

表1-2 日志严重等级说明

级别	严重程度	描述
0	Emergency	表示设备不可用的信息，如系统授权已到期
1	Alert	表示设备出现重大故障，需要立刻做出反应的信息，如流量超出接口上限
2	Critical	表示严重信息，如设备温度已经超过预警值，设备电源、风扇出现故障等
3	Error	表示错误信息，如接口链路状态变化，存储卡拔出等
4	Warning	表示警告信息，如接口连接断开，内存耗尽告警等
5	Notification	表示正常出现但是重要的信息，如通过终端登录设备，设备重启等
6	Informational	表示需要记录的通知信息，如通过命令行输入命令的记录信息，执行ping命令的日志信息等
7	Debug	表示调试过程产生的信息

本文使用表 1-3 定义的方式表示日志描述字段中的可变参数域。

表1-3 可变参数域

参数标识	参数类型
INT16	有符号的16位整数
UINT16	无符号的16位整数
INT32	有符号的32位整数
UINT32	无符号的32位整数
INT64	有符号的64位整数
UINT64	无符号的64位整数
DOUBLE	有符号的双32位整数，格式为：[INT32].[INT32]
HEX	十六进制数

参数标识	参数类型
CHAR	字节类型
STRING	字符串类型
IPADDR	IP地址
MAC	MAC地址
DATE	日期
TIME	时间

1.2 软件模块列表

表 1-4 列出了所有可能生成系统日志信息的软件模块。其中，“OPENSRC”代表所有开源软件模块的日志，本文使用“OPENSRC（开源软件名称）”表示不同开源软件模块输出的日志信息。

表1-4 软件模块列表

模块名	模块全称
AAA	Authentication, Authorization and Accounting
ACL	Access Control List
AFT	Address Family Translation
ANCP	Access Node Control Protocol
APMGR	Access Point Management
ARP	Address Resolution Protocol
ATK	ATK Detect and Defense
ATM	Asynchronous Transfer Mode
BFD	Bidirectional Forwarding Detection
BGP	Border Gateway Protocol
BLS	Blacklist
CFD	Connectivity Fault Detection
CFGMAN	Configuration Management
CLKM	Clock Management
CONNLMT	Connect Limit
DEV	Device Management
DHCP	Dynamic Host Configuration Protocol
DHCPR	IPv4 DHCP Relay
DHCPS	IPv4 DHCP Server
DHCPS6	IPv6 DHCP Server
DHCPSP4	IPv4 DHCP snooping

模块名	模块全称
DHCPSP6	IPv6 DHCP snooping
DIAG	Diagnosis
DLDP	Device Link Detection Protocol
DOT1X	802.1X
DP	Data plane backup
EDEV	Extender Device Management
EIGRP	Enhanced Interior Gateway Routing Protocol
ERPS	Ethernet Ring Protection Switching
ETH	Ethernet
ETHOAM	Ethernet Operation, Administration and Maintenance
EVB	Ethernet Virtual Bridging
EVIISIS	Ethernet Virtual Interconnect Intermediate System-to-Intermediate System
FCLINK	Fibre Channel Link
FCOE	Fibre Channel Over Ethernet
FCZONE	Fibre Channel Zone
FIB	Forwarding Information Base
FILTER	Filter
FIPSNG	FIP Snooping
FTPD	File Transfer Protocol Daemon
gRPC	Google Remote Procedure Call
HA	High Availability
HQOS	Hierarchical QoS
HTTPD	Hypertext Transfer Protocol Daemon
IFNET	Interface Net Management
IKE	Internet Key Exchange
IP6ADDR	IPv6 address
IP6FW	IPv6 Forwarding
IPADDR	IP address
IPFW	IP Forwarding
IPOE	IP Over Ethernet
IPSEC	IP Security
IPSG	IP Source Guard
IRDP	ICMP Router Discovery Protocol
IRF	Intelligent Resilient Framework

模块名	模块全称
ISIS	Intermediate System-to-Intermediate System
ISSU	In-Service Software Upgrade
L2PT	Layer 2 Protocol Tunneling
L2TPV2	Layer 2 Tunneling Protocol Version 2
L2VPN	Layer 2 VPN
LAGG	Link Aggregation
LB	Load Balance
LDP	Label Distribution Protocol
LLDP	Link Layer Discovery Protocol
LOAD	Load Management
LOCAL	Local
LOGIN	Login
LPDT	Loopback Detection
LS	Local Server
LSM	Label Switch Management
LSPV	LSP Verification
MAC	Media Access Control
MACA	MAC Authentication
MACSEC	MAC Security
MBFD	MPLS BFD
MBUF	Memory Buffer
MDC	Multitenant Device Context
MFIB	Multicast Forwarding Information Base
MGROUP	Mirroring group
MPLS	Multiprotocol Label Switching
MTLK	Monitor Link
MTP	Maintain Probe
NAT	Network Address Translate
ND	Neighbor Discovery
NETCONF	Network Configuration Protocol
NQA	Network Quality Analyzer
NTP	Network Time Protocol
OBJP	Object Policy
OFP	OpenFlow Protocol
OPENSRC(RSYNC)	Open Source(Remote Synchronize)

模块名	模块全称
OPTMOD	Optical Module
OSPF	Open Shortest Path First
OSPFV3	Open Shortest Path First Version 3
PBB	Provider Backbone Bridge
PBR	Policy Based Route
PCE	Path Computation Element
PEX	Port Extender
PFILTER	Packet Filter
PIM	Protocol Independent Multicast
PING	Packet Internet Groper
PKI	Public Key Infrastructure
PKT2CPU	Packet to CPU
PKTCPT	Packet Capture
PORTAL	Portal
PORTSEC	Port Security
PPP	Point to Point Protocol
PTP	Precision Time Protocol
PWDCTL	Password Control
QOS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RDDC	Redundancy
REDISDBM	Redis Database Manager
RIP	Routing Information Protocol
RIPNG	Routing Information Protocol Next Generation
RM	Routing Management
RPR	Resilient Packet Ring
RRPP	Rapid Ring Protect Protocol
RSVP	Resource Reservation Protocol
RTM	Real-Time Management
SCM	Service Control Manager
SCRLSP	Static CRLSP
SESSION	Session
SFLOW	Sampler Flow
SHELL	Shell
SLSP	Static LSP

模块名	模块全称
SMLK	Smart Link
SNMP	Simple Network Management Protocol
SSHC	Secure Shell Client
SSHS	Secure Shell Server
STAMGR	Station Management
STM	Stack Topology Management
STP	Spanning Tree Protocol
STRUNK	Smart Trunk
SYSEVENT	System Event
SYSLOG	System Log
TACACS	Terminal Access Controller Access Control System
TE	Traffic Engineering
TELNETD	Telnet Daemon
TRILL	Transparent Interconnect of Lots of Links
UCM	User Connection Management
UPMGR	User Plane Management
VLAN	Virtual Local Area Network
VRRP	Virtual Router Redundancy Protocol
VSRP	Virtual Service Redundancy Protocol
VXLAN	Virtual eXtensible LAN
WEB	Web
WIPS	Wireless Intrusion Prevention System

1.3 文档使用说明

本文将系统日志信息按照软件模块分类，每个模块以字母顺序排序，在每个模块中，系统日志信息按照助记符的名称，以字母顺序排序。在开源软件模块输出的日志信息中，助记符均为 SYSLOG，本文使用日志简要描述作为该类日志信息标题，不做特殊排序。

本文以表格的形式对日志信息进行介绍。有关表中各项的含义请参考表 1-5。

表1-5 日志信息表内容说明

表项	说明	举例
日志内容	显示日志信息的具体内容	ACL [UINT32] [STRING] [COUNTER64] packet(s).
参数解释	按照参数在日志中出现的顺序对参数进行解释 参数顺序用“$数字”表示，例如“$1”表示在该日志中出现的第一个参数	$1：ACL编号 $2：ACL规则的ID和内容 $3：与ACL规则匹配的数据包个数
日志等级	日志严重等级	6
举例	一个真实的日志信息举例。由于不同的系统设置，日志信息中的“<Int_16>TIMESTAMP HOSTNAME %%vendor”部分也会不同，本文表格中的日志信息举例不包含这部分内容	ACL/6/ACL_STATIS_INFO: ACL 2000 rule 0 permit source 1.1.1.1 0 logging 10000 packet(s).
日志说明	解释日志信息和日志生成的原因	匹配一条ACL规则的数据包个数。该日志会在数据包个数发生变化时输出
处理建议	建议用户应采取哪些处理措施。级别为6的“Informational”日志信息是正常运行的通知信息，用户无需处理	系统正常运行时产生的信息，无需处理

2 AAA

本节介绍 AAA 模块输出的日志信息。

2.1 AAA_FAILURE

日志内容	-AAAType=[STRING]-AAADomain=[STRING]-Service=[STRING]-UserName=[STRING]; AAA failed.
参数解释	$1：AAA类型 $2：AAA方案 $3：服务 $4：用户名称
日志等级	5
举例	AAA/5/AAA_FAILURE: -AAAType=AUTHOR-AAADomain=domain1-Service=login-UserName=cwf@system; AAA failed.
日志说明	由于未收到服务器响应，用户名/密码错误，或其他原因（例如用户申请的服务类型不正确），用户的AAA请求被拒绝
处理建议	• 检查设备与服务器的连接 • 重新输入用户名和密码 • 检查服务器上的设置（例如服务类型）是否正确

2.2 AAA_LAUNCH

日志内容	-AAAType=[STRING]-AAADomain=[STRING]-Service=[STRING]-UserName=[STRING]; AAA launched.
参数解释	$1：AAA类型 $2：AAA方案 $3：服务 $4：用户名称
日志等级	6
举例	AAA/6/AAA_LAUNCH: -AAAType=AUTHEN-AAADomain=domain1-Service=login-UserName=cwf@system; AAA launched.
日志说明	用户发送AAA请求
处理建议	无

2.3 AAA_SUCCESS

日志内容	-AAAType=[STRING]-AAADomain=[STRING]-Service=[STRING]-UserName=[STRING]; AAA succeeded.
参数解释	$1：AAA类型 $2：AAA方案 $3：服务 $4：用户名称
日志等级	6
举例	AAA/6/AAA_SUCCESS: -AAAType=AUTHOR-AAADomain=domain1-Service=login-UserName=cwf@system; AAA succeeded.
日志说明	接受用户的AAA请求
处理建议	无

3 ACL

本节介绍 ACL 模块输出的日志信息。

3.1 ACL_ACCELERATE_NO_RES

日志内容	Failed to accelerate [STRING] ACL [UINT32]. The resources are insufficient.
参数解释	$1：ACL类型 $2：ACL编号
日志等级	4
举例	ACL/4/ACL_ACCELERATE_NO_RES: Failed to accelerate IPv6 ACL 2001. The resources are insufficient.
日志说明	因硬件资源不足，系统加速ACL失败
处理建议	删除一些规则或者关闭其他ACL的加速功能，释放硬件资源

3.2 ACL_ACCELERATE_NONCONTIGUOUSMASK

日志内容	Failed to accelerate ACL [UINT32]. ACL acceleration supports only contiguous wildcard masks.
参数解释	$1：ACL编号
日志等级	4
举例	ACL/4/ACL_ACCELERATE_NONCONTIGUOUSMASK: Failed to accelerate ACL 2001. ACL acceleration supports only contiguous wildcard masks.
日志说明	因IPv4 ACL中的规则指定了非连续的掩码，导致ACL加速失败
处理建议	检查ACL规则并删除不支持的配置

3.3 ACL_ACCELERATE_NOT_SUPPORT

日志内容	Failed to accelerate [STRING] ACL [UINT32]. The operation is not supported.
参数解释	$1：ACL类型 $2：ACL编号
日志等级	4
举例	ACL/4/ACL_ACCELERATE_NOT_SUPPORT: Failed to accelerate IPv6 ACL 2001. The operation is not supported.
日志说明	因系统不支持ACL加速而导致ACL加速失败
处理建议	无

3.4 ACL_ACCELERATE_NOT_SUPPORTHOPBYHOP

日志内容	Failed to accelerate IPv6 ACL [UINT32]. ACL acceleration does not support the rules that contain the hop-by-hop keywords.
参数解释	$1：ACL编号
日志等级	4
举例	ACL/4/ACL_ACCELERATE_NOT_SUPPORTHOPBYHOP: Failed to accelerate IPv6 ACL 2001. ACL acceleration does not support the rules that contain the hop-by-hop keywords.
日志说明	因IPv6 ACL中的规则指定了hop-by-hop参数，导致ACL加速失败
处理建议	检查ACL规则并删除不支持的配置

3.5 ACL_ACCELERATE_NOT_SUPPORTMULTITCPFLAG

日志内容	Failed to accelerate IPv6 ACL [UINT32]. ACL acceleration does not support specifying multiple TCP flags in one rule.
参数解释	$1：ACL编号
日志等级	4
举例	ACL/4/ACL_ACCELERATE_NOT_SUPPORTMULTITCPFLAG: Failed to accelerate IPv6 ACL 2001. ACL acceleration does not support specifying multiple TCP flags in one rule.
日志说明	因IPv6 ACL中的规则指定了多个Tcp Flag参数，导致ACL加速失败
处理建议	检查ACL规则并删除不支持的配置

3.6 ACL_ACCELERATE_UNK_ERR

日志内容	Failed to accelerate [STRING] ACL [UINT32].
参数解释	$1：ACL类型 $2：ACL编号
日志等级	4
举例	ACL/4/ACL_ACCELERATE_UNK_ERR: Failed to accelerate IPv6 ACL 2001.
日志说明	因系统故障导致ACL加速失败
处理建议	无

3.7 ACL_IPV6_STATIS_INFO

日志内容	IPv6 ACL [UINT32] [STRING] [UINT64] packet(s).
参数解释	$1：ACL编号 $2：IPv6 ACL规则的ID及内容 $3：匹配上规则的报文个数
日志等级	6
举例	ACL6/6/ACL_IPV6_STATIS_INFO: IPv6 ACL 2000 rule 0 permit source 1:1::/64 logging 1000 packet(s).
日志说明	匹配上IPv6 ACL规则的报文数量发生变化
处理建议	无

3.8 ACL_NO_MEM

日志内容	Failed to configure [STRING] ACL [UINT] due to lack of memory
参数解释	$1：ACL类型 $2：ACL编号
日志等级	3
举例	ACL/3/ACL_NO_MEM: Failed to configure ACL 2001 due to lack of memory.
日志说明	内存不足导致配置ACL失败
处理建议	使用**display memory-threshold**命令检查内存使用情况

3.9 ACL_STATIS_INFO

日志内容	ACL [UINT32] [STRING] [UINT64] packet(s).
参数解释	$1：ACL编号 $2：IPv4 ACL规则的ID及内容 $3：匹配上规则的报文个数
日志等级	6
举例	ACL/6/ACL_STATIS_INFO: ACL 2000 rule 0 permit source 1.1.1.1 0 logging 10000 packet(s).
日志说明	匹配上IPv4 ACL规则的报文数量发生变化
处理建议	无

4 AFT

本节介绍 AFT 模块输出的日志信息。

4.1 AFT_LOG_FLOW

日志内容	AFT PORTBLOCK was [STRING]: IPv6addr=[IPADDR]; VPNNameV6=[STRING]; ipv4addr=[IPADDR]; VPNNameV4=[STRING]; PortBlockSize=[UINT16]-[UINT16]; BeginTime_e=[STRING]; EndTime_e=[STRING].
参数解释	$1：事件类型 • allocated：端口块分配 • released：端口块释放 $2：IPv6地址 $3：IPv6所属VPN名称 $4：IPv4地址 $5：IPv4所属VPN名称 $6：分配的端口块中的起始值 $7：分配的端口块中的结束值 $8：端口块分配时间 $9：端口块删除时间
日志等级	6
举例	AFT/6/AFT_LOG_FLOW: AFT PORTBLOCK was free: IPv6addr=1000::1b; VPNNameV6=-; IPv4addr=10.0.0.140; VPNNameV4=-; PortBlockSize=1024-1535; BeginTime_e=03232017053558; EndTime_e=03232017065040.
日志说明	释放端口块时发送该日志
处理建议	无

4.2 AFT_V6TOV4_FLOW

日志内容	Protocol(1001)= [STRING];SrcIPv6Addr(1036)= [IPADDR];SrcPort(1004)= [UINT16];NatSrcIPAddr(1005)= [IPADDR];NatSrcPort(1006)= [UINT16];DstIPv6Addr(1037)= [IPADDR];DstPort(1008)= [UINT16];NatDstIPAddr(1009)= [IPADDR];NatDstPort(1010)= [UINT16];InitPktCount(1044)= [UINT32];InitByteCount(1046)= [UINT32];RplyPktCount(1045)= [UINT32];RplyByteCount(1047)= [UINT32];RcvVPNInstance(1042)= [STRING];SndVPNInstance(1043)= [STRING];BeginTime_e(1013)= [STRING];EndTime_e(1014)= [STRING];Event(1048)= ([UNIT16])[STRING].
参数解释	$1：协议类型 $2：源IPv6地址 $3：源端口号 $4：转换后的源IP地址 $5：转换后的源端口号 $6：目的IPv6地址 $7：目的端口号 $8：转换后的目的IP地址 $9：转换后的目的端口号 $10：入方向的报文总数 $11：入方向的字节总数 $12：出方向的报文总数 $13：出方向的字节总数 $14：源VPN名称 $15：目的VPN名称 $16：创建会话的时间 $17：会话删除时间 $18：日志类型 $19：日志类型描述信息，包括： • Session created：AFT 会话创建 • Session ended：正常流结束，AFT 会话删除 • Session aged out：AFT 会话老化删除 • Session deleted through configuration：通过配置删除 AFT 会话 • Other：其他原因删除 AFT 会话，如由其他模块删除
日志等级	6
举例	AFT/6/AFT_V6TOV4_FLOW: Protocol(1001)=IPv6-ICMP;SrcIPv6Addr(1036)=1000::10;SrcPort(1004)=1;NatSrcIPAddr(1005)=9.9.9.9;NatSrcPort(1006)=1027;DstIPv6Addr(1037)=2000::201:102;DstPort(1008)=32768;NatDstIPAddr(1009)=2.1.1.2;NatDstPort(1010)=2048;InitPktCount(1044)=177411959;InitByteCount(1046)=2122604543;RplyPktCount(1045)=1895856127;RplyByteCount(1047)=30720;RcvVPNInstance(1042)=;SndVPNInstance(1043)=;BeginTime_e(1013)=05052017134514;EndTime_e(1014)=;Event(1048)=(8)Session created.
日志说明	创建、删除IPv6侧发起的会话时发送该日志
处理建议	无

4.3 AFT_V4TOV6_FLOW

日志内容	Protocol(1001)= [STRING]; SrcIPAddr(1003)= [IPADDR];SrcPort(1004)= [UINT16]; NatSrcIPv6Addr(1038)= [IPADDR];NatSrcPort(1006)= [UINT16]; DstIPAddr(1003)= [IPADDR];DstPort(1008)= [UINT16]; NatDstIPv6Addr(1039)= [IPADDR];NatDstPort(1010)= [UINT16];InitPktCount(1044)= [UINT32];InitByteCount(1046)= [UINT32];RplyPktCount(1045)= [UINT32];RplyByteCount(1047)= [UINT32];RcvVPNInstance(1042)= [STRING];SndVPNInstance(1043)= [STRING];BeginTime_e(1013)= [STRING];EndTime_e(1014)= [STRING];Event(1048)= ([UNIT16])[STRING].
参数解释	$1：协议类型 $2：源IPv6地址 $3：源端口号 $4：转换后的源IP地址 $5：转换后的源端口号 $6：目的IPv6地址 $7：目的端口号 $8：转换后的目的IP地址 $9：转换后的目的端口号 $10：入方向的报文总数 $11：入方向的字节总数 $12：出方向的报文总数 $13：出方向的字节总数 $14：源VPN名称 $15：目的VPN名称 $16：创建会话的时间 $17：会话删除时间 $18：日志类型 $19：日志类型描述信息，包括： • Session created：AFT 会话创建 • Session ended：正常流结束，AFT 会话删除 • Session aged out：AFT 会话老化删除 • Session deleted through configuration：通过配置删除 AFT 会话 • Other：其他原因删除 AFT 会话，如由其他模块删除
日志等级	6
举例	AFT/6/AFT_V4TOV6_FLOW: Protocol(1001)=ICMP;SrcIPAddr(1003)=2.1.1.4;SrcPort(1004)=197;NatSrcIPv6Addr(1038)=2000::201:104;NatSrcPort(1006)=197;DstIPAddr(1003)=5.5.5.5;DstPort(1008)=2048;NatDstIPv6Addr(1039)=1000::;NatDstPort(1010)=32768;InitPktCount(1044)=2092588805;InitByteCount(1046)=1166331903;RplyPktCount(1045)=1895856127;RplyByteCount(1047)=30720;RcvVPNInstance(1042)=;SndVPNInstance(1043)=;BeginTime_e(1013)=05052017152731;EndTime_e(1014)=;Event(1048)=(8)Session created.
日志说明	创建、删除IPv4侧发起的会话时发送该日志
处理建议	无

5 ANCP

本节介绍 ANCP（Access Node Control Protocol）模块输出的 日志信息。

5.1 ANCP_INVALID_PACKET

日志内容	-NeighborName=[STRING]-State=[STRING]-MessageType=[STRING]; The [STRING] value [STRING] is wrong, and the value [STRING] is expected.
参数解释	$1：ANCP邻居名 $2：邻居状态 $3：报文类型 $4：错误字段 $5：错误字段值 $6：期望值
日志等级	6
举例	ANCP/6/ANCP_INVALID_PACKET: -NeighborName=Dslam-State=SYNSENT-MessageType=SYNACK; The Sender Instance value 0 is wrong, and the value 1 is expected.
日志说明	系统收到一个错误的ANCP邻接报文，报文中指定字段与预期值不一致
处理建议	无需处理

6 API

本节介绍 API 模块输出的日志信息

6.1 API

日志内容	[STRING] state error. Please check the subcard [UINT16].
参数解释	$1：检测到错误的部件，取值包括： • Tm Spi4A：子卡槽位 1 和业务底板之间的接口 • Tm Spi4B：子卡槽位 2 和业务底板之间的接口 • ILKEN：单板内部器件连接接口状态 $2：子卡所在的槽位号，取值范围为1～2
日志等级	3
举例	PORT/3/API: -MDC=1-Slot=2; ILKEN state error. Please check the subcard 2.
日志说明	CSPEX类单板（除CSPEX-1204之外）上检测到PIC子卡的SPI通道或ILKEN通道的信号同步状态错误
处理建议	1. 请重新插拔子卡，确保子卡安装到位 2. 更换故障槽位上的子卡，如故障消失，则表示子卡故障；如故障仍然存在，则表示单板连接故障或者子卡槽位故障，请联系技术支持

7 APMGR

本节介绍 AP 管理模块输出的日志信息。

7.1 APMGR_ADDBAC_INFO

日志内容	Add BAS AC [STRING].
参数解释	$1：BAS AC的MAC地址
日志等级	6
举例	APMGR/6/APMGR_ADDBAC_INFO: Add BAS AC 3ce5-a616-28cd.
日志说明	Master AC与BAS AC建立连接
处理建议	无

7.2 APMGR_AP_CFG_FAILED

日志内容	Failed to reset AP [STRING]. Reason: The AP is writing an image file into the flash.
参数解释	$1：AP的名称
日志等级	4
举例	APMGR/6/APMGR_CFG_FAILD; Failed to reset AP ap2. Reason: The AP is writing an image file into the flash.
日志说明	当AP从AC下载文件时，在AC上重启AP失败
处理建议	AP完成从AC下载文件后，再重启AP

7.3 APMGR_DELBAC_INFO

日志内容	Delete BAS AC [STRING].
参数解释	$1：BAS AC的MAC地址
日志等级	6
举例	APMGR/6/APMGR_DELBAC_INFO: Delete BAS AC 3ce5-a616-28cd.
日志说明	Master AC断开与BAS AC的连接
处理建议	无

7.4 APMGR_LOG_ADD_AP_FAIL

日志内容	AP [STRING] failed to come online using serial ID [STRING]: MAC address [STRING] is being used by AP [STRING].
参数解释	$1：AP的名称 $2：AP的序列号 $3：AP的MAC地址 $4：AP的名称
日志等级	4
举例	APMGR/4/ APMGR_ADD_AP_FAIL: AP ap1 failed to come online using serial ID 01247ef96: MAC address 0023-7961-5201 is being used by AP ap2.
日志说明	AP上线过程中，由于MAC地址已存在，添加MAC地址失败，AP不能上线
处理建议	将此AP的MAC地址或serial ID对应的手工AP删除一个，AP方能正常上线

7.5 APMGR_LOG_LACOFFLINE

日志内容	Local AC [STRING] went offline. State changed to Idle.
参数解释	$1：Local AC的名称
日志等级	6
举例	APMGR/6/APMGR_LOCAL_AC_OFFLINE: Local AC ac1 went offline. State changed to Idle.
日志说明	Local AC下线，状态变为Idle状态
处理建议	• 若 Local AC 主动下线，则不用排查问题 • 若 Local AC 异常下线，需要根据调试信息定位并解决问题

7.6 APMGR_LOG_LACONLINE

日志内容	Local AC [STRING] went online. State changed to Run.
参数解释	$1：Local AC的名称
日志等级	6
举例	APMGR/6/APMGR_LOCAL_AC_ONLINE: Local AC ac1 went online. State changed to Run.
日志说明	Local AC上线，状态变为运行状态
处理建议	无

7.7 APMGR_LOG_MEMALERT

日志内容	The memory usage of the AC has reached the threshold.
参数解释	无
日志等级	4
举例	APMGR/4/APMGR_AC_MEM_ALERT: The memory usage of the AC has reached the threshold.
日志说明	创建手工AP成功时触发，但由于达到内存门限值，AP不能上线
处理建议	此时不应该继续创建AP，且不允许有新AP上线

7.8 APMGR_LOG_NOLICENSE

日志内容	AP failed to come online in [STRING]. Reason: No license for the [STRING].
参数解释	$1：AP的状态 • discover：discover 阶段 • join：join 阶段 $2：AP类型 • common AP：普通的 FIT AP • WTU AP：分体 AP
日志等级	6
举例	APMGR/6/APMGR_LOG_NOLICENSE: AP failed to come online in discover. Reason: No license for the common AP.
日志说明	已上线的普通AP或分体AP已经达到license所允许的最大值，因此AP上线失败
处理建议	购买license扩充AP数量

7.9 APMGR_LOG_OFFLINE

日志内容	AP [STRING] went offline. State changed to Idle.
参数解释	$1：AP的名称
日志等级	6
举例	APMGR/6/APMGR_AP_OFFLINE: AP ap1 went offline. State changed to Idle.
日志说明	AP下线，状态变为Idle状态
处理建议	• 若 AP 主动下线，则不用排查问题 • 若 AP 异常下线，需要根据调试信息定位并解决问题

7.10 APMGR_LOG_ONLINE

日志内容	AP [STRING] came online. State changed to Run.
参数解释	$1：AP的名称
日志等级	6
举例	APMGR/6/APMGR_AP_ONLINE: AP ap1 came online. State changed to Run.
日志说明	AP上线，状态变为运行状态
处理建议	无

7.11 APMGR_REACH_MAX_APNUMBER

日志内容	An AP failed to come online: Maximum number of APs already reached.
参数解释	无
日志等级	4
举例	APMGR/4/APMGR_REACH_MAX_APNEMBER: An AP failed to come online: Maximum number of APs already reached.
日志说明	由于接入AC的AP个数达到上限，新AP不能上线
处理建议	无

7.12 CWC_AP_DOWN

日志内容	CAPWAP tunnel to AC [STRING] went down. Reason: [STRING].
参数解释	$1：AC的IP地址 $2：隧道断开原因 • Added AP IP address：添加新的 AP IP 地址 • Deleted AP IP address：AP IP 地址被删除 • AP interface used for CAPWAP tunnel went down：CAPWAP 隧道使用的 AP 接口 DOWN • AP config changed：AP 配置改变 • AP was reset：AP 重启 • Number of echo retransmission attempts exceeded the limit：超过 echo 报文重传次数 • No license for the AP：没有足够的 AP 数量 license • Full retransmission queue：重传队列满 • Data channel timer expired：数据隧道定时器超时 • Backup AC IP address changed：备 AC IP 地址改变 • Backup tunnel changed to master tunnel：备隧道切换成主隧道 • Failed to change backup tunnel to master tunnel：备切主失败 • Backup method changed：备份模式改变 • N/A：不涉及
日志等级	6
举例	CWC/6/CWC_AP_DOWN: CAPWAP tunnel to AC 192.168.10.1 went down. Reason: AP was reset.
日志说明	AP与AC之间CAPWAP隧道断开以及断开原因
处理建议	请检查AP与AC之间的网络连接是否正常

7.13 CWC_AP_UP

日志内容	[STRING] CAPWAP tunnel to AC [STRING] went up.
参数解释	$1：与AC连接的隧道的主备类型 • Master：主隧道 • Backup：备隧道 $2：AC的IP地址
日志等级	6
举例	CWC/6/CWC_AP_UP: Master CAPWAP tunnel to AC 192.168.10.1 went up.
日志说明	AP成功连接到AC，即AP已进入Run状态
处理建议	无

7.14 CWC_AP_REBOOT

日志内容	AP in state [STRING] is rebooting. Reason: [STRING]
参数解释	$1：AP的当前状态 $2：重启原因。原因如下： • AP was reset：AP 重启 • Image was downloaded successfully：版本文件下载成功 • Stayed in idle state for a long time：长时间处于 idle 状态
日志等级	6
举例	CWC/6/CWC_AP_REBOOT: AP in State Run is rebooting. Reason: AP was reset.
日志说明	AP重启及重启原因
处理建议	无

7.15 CWC_IMG_DOWNLOAD_COMPLETE

日志内容	System software image file [STRING] downloading through the CAPWAP tunnel to AC [STRING] completed.
参数解释	$1：镜像文件名 $2：AC的IP地址
日志等级	6
举例	CWC/6/CWC_IMG_DOWNLOAD_COMPLETE: System software image file 5800.ipe downloading through the CAPWAP tunnel to AC 192.168.10.1 completed.
日志说明	AP从AC下载系统镜像成功
处理建议	无

7.16 CWC_IMG_DOWNLOAD_START

日志内容	Started to download the system software image file [STRING] through the CAPWAP tunnel to AC [STRING].
参数解释	$1：下载的镜像文件名 $2：AC的IP地址
日志等级	6
举例	CWC/6/CWC_IMG_DOWNLOAD_START: Started to download the system software image file 5800.ipe through the CAPWAP tunnel to AC 192.168.10.1.
日志说明	AP开始进行版本文件下载
处理建议	保持AP和AC之间正常的网络连接使AP能够正常升级

7.17 CWC_IMG_NO_ENOUGH_SPACE

日志内容	Insufficient flash memory space for downloading system software image file [STRING].
参数解释	$1：下载的镜像文件名
日志等级	6
举例	CWC/6/CWC_IMG_NO_ENOUGH_SPACE: Insufficient flash memory space for downloading system software image file 5800.ipe.
日志说明	由于AP上的Flash剩余空间不足导致AP进行版本升级不成功
处理建议	建议删除AP上无用的文件以进行版本升级

7.18 CWC_LOCALAC_DOWN

日志内容	CAPWAP tunnel to Central AC [STRING] went down. Reason: [STRING].
参数解释	$1：Central AC的IP地址 $2：隧道断开的原因 • Added local AC IP address：添加新的 Local AC IP 地址 • Deleted local AC IP address：Local AC IP 地址被删除 • Local AC interface used for CAPWAP tunnel went down：CAPWAP 隧道使用的 Local AC 接口 DOWN • Local AC config changed：Local AC 配置改变 • N/A：不涉及
日志等级	4
举例	CWC/4/CWC_LOCAL_AC_DOWN: CAPWAP tunnel to Central AC 2.2.2.1 went down. Reason: Added local AC IP address.
日志说明	Central AC与Local AC之间隧道断开及断开原因
处理建议	• 检查 Central AC 与 Local AC 的连接是否正常 • 检查 Central AC 上的配置 • 检查 Local AC 上的配置

7.19 CWC_LOCALAC_UP

日志内容	CAPWAP tunnel to Central AC [STRING] went up.
参数解释	$1：Central AC的IP地址
日志等级	6
举例	CWC/6/CWC_LOCAL_AC_UP: CAPWAP tunnel to Central AC 2.2.2.1 went up.
日志说明	Central AC与Local AC建立CAPWAP隧道
处理建议	无

7.20 CWC_RUN_DOWNLOAD_COMPLETE

日志内容	File [STRING] successfully downloaded through the CAPWAP tunnel to AC [STRING].
参数解释	$1：下载文件的文件名 $2：AC的IP地址
日志等级	6
举例	CWC/6/CWC_RUN_DOWNLOAD_COMPLETE: File ac.cfg successfully downloaded through the CAPWAP tunnel to AC 192.168.10.1.
日志说明	AP从AC下载文件成功
处理建议	无

7.21 CWC_RUN_DOWNLOAD_START

日志内容	Started to download the file [STRING] through the CAPWAP tunnel to AC [STRING].
参数解释	$1：下载文件的文件名 $2：AC的IP地址
日志等级	6
举例	CWC/6/CWC_RUN_DOWNLOAD_START: Started to download the file ac.cfg through the CAPWAP tunnel to AC 192.168.10.1.
日志说明	AP开始进行版本文件下载
处理建议	保持AP和AC之间都处于RUN状态，AC才能够正常下载文件到AP

7.22 CWC_RUN_NO_ENOUGH_SPACE

日志内容	Insufficient flash memory space for downloading file [STRING].
参数解释	$1：下载文件的文件名
日志等级	6
举例	CWC/6/CWC_RUN_NO_ENOUGH_SPACE: Insufficient flash memory space for downloading file ac.cfg.
日志说明	由于AP上的Flash剩余空间不足导致AP进行文件下载不成功
处理建议	建议删除AP上无用的文件以进行文件下载

7.23 CWS_AP_DOWN

日志内容	CAPWAP tunnel to AP [STRING] went down. Reason: [STRING].
参数解释	$1：AC端配置的AP名称 $2：隧道断开原因 • Neighbor dead timer expired：邻居截止定时器超时 • AP was reset：AP 重启 • AP was deleted：AP 被删除 • Serial number changed：序列号改变 • Processed join request in Run state：在 Run 状态下处理 join request 报文 • Failed to retransmit message：处理重传消息失败 • Received WTP tunnel down event from AP：接收到来自 AP 的 WTP DOWN 隧道事件 • Backup AC closed the backup tunnel：备 AC DOWN 自身的隧道 • Backup AP upgrade failed：备份 AP 升级失败 • AC is inactive：AC 由活跃状态转变为非活跃 • Tunnel switched：由于隧道切换 • N/A：不涉及
日志等级	6
举例	CWS/6/CWS_AP_DOWN: CAPWAP tunnel to AP ap1 went down. Reason: AP was reset.
日志说明	AP下线及下线原因
处理建议	• 检查设备 AP 与设备 AC 的连接是否正常 • 检查 AP 上的配置 • 检查 AC 上的配置

7.24 CWS_AP_UP

日志内容	[STRING] CAPWAP tunnel to AP [STRING] went up.
参数解释	$1：与AP连接的隧道的主备类型 • Master：主隧道 • Backup：备隧道 $2：AP的名称或序列号
日志等级	6
举例	CWS/6/CWS_AP_UP: Backup CAPWAP tunnel to AP ap1 went up.
日志说明	AC端配置的AP成功上线，即此AP进入Run状态
处理建议	无

7.25 CWS_IMG_DOWNLOAD_COMPLETE

日志内容	System software image file [STRING] downloading through the CAPWAP tunnel for AP [STRING] completed.
参数解释	$1：AP已经下载完成的版本文件名 $2：AP名称
日志等级	6
举例	CWS/6/CWS_IMG_DOWNLOAD_COMPLETE: System software image file 5800.ipe downloading through the CAPWAP tunnel for AP ap2 completed.
日志说明	AP已经成功完成版本文件下载
处理建议	无

7.26 CWS_IMG_DOWNLOAD_FAILED

日志内容	Failed to download image file [STRING] for the AP. AC memory is not enough.
参数解释	$1：AP从AC上下载的版本文件名
日志等级	6
举例	CWS/6/CWS_IMG_DOWNLOAD_FAILED: Failed to download image file wa4300anchor.ipe for the AP. AC memory is not enough.
日志说明	AC内存不足，下发版本到AP失败
处理建议	无

7.27 CWS_IMG_DOWNLOAD_START

日志内容	AP [STRING] started to download the system software image file [STRING].
参数解释	$1：AC端配置的AP名称 $2：AP正在下载升级的版本文件名
日志等级	6
举例	CWS/6/CWS_IMG_DOWNLOAD_START: AP ap1 started to download the system software image file 5800.ipe.
日志说明	AP开始进行版本文件下载
处理建议	无

7.28 CWS_LOCALAC_DOWN

日志内容	CAPWAP tunnel to local AC [STRING] went down. Reason: [STRING].
参数解释	$1：Local AC的IP地址 $2：隧道断开的原因 • Neighbor dead timer expired：邻居截止定时器超时 • Local AC was deleted：Local AC 被删除 • Serial number changed：序列号改变 • Processed join request in Run state：在 Run 状态下处理 join request 报文 • Failed to retransmit message：处理重传消息失败 • N/A：不涉及
日志等级	4
举例	CWS/4/CWS_LOCAL_AC_DOWN: CAPWAP tunnel to local AC 1.1.1.1 went down. Reason: Local AC was deleted.
日志说明	Central AC与Local AC之间隧道断开及断开原因
处理建议	• 检查 Central AC 与 Local AC 的连接是否正常 • 检查 Central AC 上的配置 • 检查 Local AC 上的配置

7.29 CWS_LOCALAC_UP

日志内容	CAPWAP tunnel to local AC [STRING] went up.
参数解释	$1：Local AC的IP地址
日志等级	6
举例	CWS/6/CWS_LOCAL_AC_UP: CAPWAP tunnel to local AC 1.1.1.1 went up.
日志说明	Central AC与 Local AC建立CAPWAP隧道
处理建议	无

7.30 CWS_RUN_DOWNLOAD_COMPLETE

日志内容	File [STRING] successfully downloaded through the CAPWAP tunnel for AP [STRING].
参数解释	$1：AP已经下载完成的文件的文件名 $2：AC端配置的AP名称
日志等级	6
举例	CWS/6/CWS_RUN_DOWNLOAD_COMPLETE: File ac.cfg successfully downloaded through the CAPWAP tunnel for AP ap2.
日志说明	AP已经成功完成文件下载
处理建议	无

7.31 CWS_RUN_DOWNLOAD_START

日志内容	AP [STRING] started to download the file [STRING].
参数解释	$1：AC端配置的AP名称 $2：AP正在下载的文件的文件名
日志等级	6
举例	CWS/6/CWS_RUN_DOWNLOAD_START: AP ap1 started to download the file ac.cfg.
日志说明	AP开始进行配置文件下载
处理建议	无

8 ARP

本节介绍 ARP 模块输出的日志信息。

8.1 ARP_ACTIVE_ACK_NO_REPLY

日志内容	No ARP reply from IP [STRING] was received on interface [STRING].
参数解释	$1：IP 地址 $2：接口名称
日志等级	6
举例	ARP/6/ARP_ACTIVE_ACK_NO_REPLY: No ARP reply from IP 192.168.10.1 was received on interface GigabitEthernet1/0/1.
日志说明	ARP主动确认功能检测到攻击 接口向所收到ARP报文的发送端IP发送ARP请求，未收到ARP应答
处理建议	**1.** 检查设备上学习到的 ARP 表项中的 IP 和 MAC 是否对应（如果网络部署中存在网关和服务器，优先检查网关和服务器的 IP 和 MAC 是否对应） **2.** 请联系系统支持

8.2 ARP_ACTIVE_ACK_NOREQUESTED_REPLY

日志内容	Interface [STRING] received from IP [STRING] an ARP reply that was not requested by the device.
参数解释	$1：接口名称 $2：IP地址
日志等级	6
举例	ARP/6/ARP_ACTIVE_ACK_NOREQUESTED_REPLY: Interface Ethernet0/1/0 received from IP 192.168.10.1 an ARP reply that was not requested by the device.
日志说明	ARP主动确认功能检测到攻击 接口在未向ARP报文发送端IP地址发送ARP请求的情况下，收到ARP应答
处理建议	设备丢弃该ARP应答

8.3 ARP_BINDRULETOHW_FAILED

日志内容	Failed to download binding rule to hardware on the interface [STRING], SrcIP [IPADDR], SrcMAC [MAC], VLAN [UINT16], Gateway MAC [MAC].
参数解释	$1：接口名称. $2：源IP地址 $3：源MAC地址. $4：VLAN编号. $5：网关MAC地址.
日志等级	5
举例	ARP/5/ARP_BINDRULETOHW_FAILED: Failed to download binding rule to hardware on the interface Ethernet1/0/1, SrcIP 1.1.1.132, SrcMAC 0015-E944-A947, VLAN 1, Gateway MAC 00A1-B812-1108.
日志说明	由于硬件资源不足、内存不足或其他硬件错误导致绑定规则下发失败
处理建议	**1.** 使用 **`display qos-acl resource`** 查看硬件 ACL 资源是否充足 ○ 如果充足，则请执行步骤 2 ○ 如果不充足，则请取消部分 ACL 配置或接受当前结果 **2.** 使用 **`display memory`** 查看内存资源是否充足 ○ 如果充足，则请执行步骤 3 ○ 如果不充足，则请取消部分配置或接受当前结果 **3.** **硬件发生错误，请取消最后一次相关配置，并重新尝试**

8.4 ARP_DUPLICATE_IPADDR_DETECT

日志内容	Detected an IP address conflict. The device with MAC address [STRING] connected to interface [STRING] in VSI [STRING] and the device with MAC address [STRING] connected to interface [STRING] in VSI [STRING] were using the same IP address [IPADDR].
参数解释	$1：MAC 地址 $2：接口名称（包括Tunnel口、三层接口和以太网服务实例等） $3：VSI名称 $4：冲突对端的源MAC地址 $5：冲突对端的源接口名称（包括Tunnel口、三层接口和以太网服务实例等） $6：冲突对端的VSI名称 $7：冲突的IP地址
日志等级	6
举例	ARP/6/ARP_DUPLICATE_IPADDR_DETECT: Detected an IP address conflict. The device with MAC address 00-00-01 connected to interface Ethernet0/0/1 service-instance 1000 in VSI vpna and the device with MAC address 00-00-02 connected to interface tunnel 10 in VSI vpna were using the same IP address 192.168.1.1.
日志说明	ARP检测到重复地址 接口收到ARP报文中发送端的IP地址，与本设备学习到的ARP表项中的IP地址冲突
处理建议	修改IP地址

8.5 ARP_DYNAMIC

日志内容	The maximum number of dynamic ARP entries for the device reached.
参数解释	无
日志等级	3
举例	ARP/3/ARP_DYNAMIC: The maximum number of dynamic ARP entries for the device reached.
日志说明	设备学到的ARP表项总数到达最大值，打印该提示日志
处理建议	无需处理

8.6 ARP_DYNAMIC_IF

日志内容	The maximum number of dynamic ARP entries for interface [STRING] reached.
参数解释	$1：接口名
日志等级	3
举例	ARP/3/ARP_DYNAMIC_IF: The maximum number of dynamic ARP entries for interface GigabitEthernet3/0/1 reached.
日志说明	接口学到的ARP表项总数到达最大值，打印该提示日志
处理建议	无需处理

8.7 ARP_DYNAMIC_SLOT

日志内容	形式一： The maximum number of dynamic ARP entries for slot [INT32] reached. 形式二： The maximum number of dynamic ARP entries for chassis [INT32] slot [INT32] reached.
参数解释	形式一： $1：slot编号 形式二： $1：chassis编号 $2：slot编号
日志等级	3
举例	ARP/3/ARP_DYNAMIC_SLOT: The maximum number of dynamic ARP entries for slot 2 reached. ARP/3/ARP_DYNAMIC_SLOT: The maximum number of dynamic ARP entries for chassis 1 slot 2 reached.
日志说明	形式一： 指定slot学到的动态ARP表项数达到最大值 形式二： 指定chassis内slot上学到的动态ARP表项数达到最大值
处理建议	无需处理

8.8 ARP_ENTRY_CONFLICT

日志内容	The software entry for [STRING] on [STRING] and the hardware entry did not have the same [STRING].
参数解释	$1：IP地址 $2：VPN实例名。如果该ARP属于公网，显示为the public network $3：不一致的表项参数类型 • MAC address：MAC 地址 • output interface：ARP 表项的出接口 • output port ：ARP 表项的出端口 • outermost layer VLAN ID：第一层 VLAN 标签 • second outermost layer VLAN ID：第二层 VLAN 标签 • VSI index：VSI 索引 • link ID：VSI 出链路标识符
日志等级	6
举例	ARP/6/ARP_ENTRY_CONFLICT: The software entry for 1.1.1.1 on the VPN a and the hardware entry did not have the same MAC address, output port, VSI index, and link ID. ARP/6/ARP_ENTRY_CONFLICT: The software entry for 1.1.1.2 on the public network and the hardware entry did not have the same MAC address, output port, VSI index, and link ID.
日志说明	ARP软件表项与硬件表项不一致，比如ARP表项的出接口
处理建议	不需要处理，ARP会主动重刷硬件表项

8.9 ARP_HOST_IP_CONFLICT

日志内容	The host [STRING] connected to interface [STRING] cannot communicate correctly, because it uses the same IP address as the host connected to interface [STRING].
参数解释	$1：IP地址 $2：接口名 $3：接口名
日志等级	4
举例	ARP/4/ARP_HOST_IP_CONFLICT: The host 1.1.1.1 connected to interface GigabitEthernet1/0/1 cannot communicate correctly, because it uses the same IP address as the host connected to interface GigabitEthernet1/0/2.
日志说明	接口收到主机ARP报文中的源IP与其他接口连接的主机的IP地址冲突
处理建议	检查发送ARP报文的主机的合法性。如果非法，需要断开该主机网络

8.10 ARP_RATE_EXCEEDED

日志内容	The ARP packet rate ([UINT32] pps) exceeded the rate limit ([UINT32] pps) on interface [STRING] in the last [UINT32] seconds.
参数解释	$1：ARP报文速率 $2：ARP报文限速速率 $3：接口名称 $4：间隔时间
日志等级	4
举例	ARP/4/ARP_RATE_EXCEEDED: The ARP packet rate (100 pps) exceeded the rate limit (80 pps) on interface Ethernet0/1/0 in the last 10 seconds.
日志说明	接口接收ARP报文速率超过了接口的限速值
处理建议	检查ARP报文发送主机的合法性

8.11 ARP_RATELIMIT_NOTSUPPORT

日志内容	形式一： ARP packet rate limit is not support on slot [INT32]. 形式二： ARP packet rate limit is not support on chassis [INT32] slot [INT32].
参数解释	形式一： $1：slot编号 形式二： $1：chassis编号 $2：slot编号
日志等级	6
举例	ARP/6/ARP_RATELIMIT_NOTSUPPORT: ARP packet rate limit is not support on slot 2.
日志说明	形式一： 指定slot不支持ARP报文限速功能 形式二： 指定chassis内slot不支持ARP报文限速功能
处理建议	无需处理

8.12 ARP_SENDER_IP_INVALID

日志内容	Sender IP [STRING] was not on the same network as the receiving interface [STRING].
参数解释	$1：IP地址 $2：接口名称
日志等级	6
举例	ARP/6/ARP_SENDER_IP_INVALID: Sender IP 192.168.10.2 was not on the same network as the receiving interface GigabitEthernet1/0/1.
日志说明	接口收到ARP报文中发送端IP与本接口不在同一网段
处理建议	检查发送端IP对应主机的合法性

8.13 ARP_SENDER_MAC_INVALID

日志内容	Sender MAC [STRING] was not identical to Ethernet source MAC [STRING] on interface [STRING].
参数解释	$1：MAC 地址 $2：MAC 地址 $3：接口名称
日志等级	6
举例	ARP/6/ARP_SENDER_MAC_INVALID: Sender MAC 0000-5E14-0E00 was not identical to Ethernet source MAC 0000-5C14-0E00 on interface GigabitEthernet1/0/1.
日志说明	接口收到ARP报文的以太网数据帧首部中的源MAC地址和ARP报文中的发送端MAC地址不同
处理建议	检查发送端MAC地址对应主机的合法性

8.14 ARP_SRC_MAC_FOUND_ATTACK

日志内容	An attack from MAC [STRING] was detected on interface [STRING].
参数解释	$1：MAC 地址 $2：接口名称
日志等级	6
举例	ARP/6/ARP_SRC_MAC_FOUND_ATTACK: An attack from MAC 0000-5E14-0E00 was detected on interface GigabitEthernet1/0/1.
日志说明	源MAC地址固定的ARP攻击检测功能检测到攻击 5秒内，收到同一源MAC地址（源MAC地址固定）的ARP报文超过一定的阈值
处理建议	检查该源MAC地址对应主机的合法性

8.15 ARP_TARGET_IP_INVALID

日志内容	Target IP [STRING] was not the IP of the receiving interface [STRING].
参数解释	$1：IP 地址 $2：接口名称
日志等级	6
举例	ARP/6/ARP_TARGET_IP_INVALID: Target IP 192.168.10.2 was not the IP of the receiving interface Ethernet0/1/0.
日志说明	接口收到ARP报文中的目标IP与本接口IP不一致
处理建议	检查发送ARP报文的主机的合法性

8.16 DUPIFIP

日志内容	Duplicate address [STRING] on interface [STRING], sourced from [STRING].
参数解释	$1：IP 地址 $2：接口名称 $3：MAC 地址
日志等级	6
举例	ARP/6/DUPIFIP: Duplicate address 1.1.1.1 on interface Ethernet1/1/1, sourced from 0015-E944-A947.
日志说明	ARP检测到重复地址 接口收到ARP报文的发送端IP地址与该接口的IP地址重复
处理建议	修改IP地址配置

8.17 DUPIP

日志内容	IP address [STRING] conflicted with global or imported IP address, sourced from [STRING].
参数解释	$1：IP 地址 $2：MAC 地址
日志等级	6
举例	ARP/6/DUPIP: IP address 30.1.1.1 conflicted with global or imported IP address, sourced from 0000-0000-0001.
日志说明	收到ARP报文中的发送端IP地址与全局或导入的IP地址冲突
处理建议	修改IP地址配置

8.18 DUPVRRPIP

日志内容	IP address [STRING] conflicted with VRRP virtual IP address on interface [STRING], sourced from [STRING].
参数解释	$1：IP 地址 $2：接口名称 $3：MAC 地址
日志等级	6
举例	ARP/6/DUPVRRPIP: IP address 1.1.1.1 conflicted with VRRP virtual IP address on interface Ethernet1/1/1, sourced from 0015-E944-A947.
日志说明	收到ARP报文中的发送端IP与VRRP虚拟IP地址冲突
处理建议	修改IP地址配置

8.19 L3_COMMON

日志内容	形式一： The Board on slot [INT32] doesn't support the ARP safe-guard function. 形式二： The Board on chassis t [INT32] slot [INT32] doesn't support the ARP safe-guard function.
参数解释	形式一： $1：slot编号 形式二： $1：chassis编号 $2：slot编号
日志等级	4
举例	L3/4/L3_COMMON: -MDC=1-Slot=5; The Board on slot 5 doesn't support the ARP safe-guard function.
日志说明	形式一： 指定slot不支持ARP双向分离功能 形式二： 指定chassis内slot不支持ARP双向分离功能
处理建议	使用支持ARP双向分离功能的单板的接口

9 ATK

本节介绍 ATK 模块输出的日志信息。

9.1 ATK_ICMP_ADDRMASK_REQ

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMP_ADDRMASK_REQ: IcmpType(1058)=17; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP地址掩码请求报文数超过1，聚合后触发日志
处理建议	无

9.2 ATK_ICMP_ADDRMASK_REQ_RAW

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_ADDRMASK_REQ_RAW: IcmpType(1058)=17; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP地址掩码请求报文首包触发日志；日志聚合开关关闭，每个ICMP地址掩码请求报文触发一个日志
处理建议	无

9.3 ATK_ICMP_ADDRMASK_REQ_RAW_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_ADDRMASK_REQ_RAW_SZ: IcmpType(1058)=17; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP地址掩码请求报文首包触发日志；日志聚合开关关闭，每个ICMP地址掩码请求报文触发一个日志
处理建议	无

9.4 ATK_ICMP_ADDRMASK_REQ_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMP_ADDRMASK_REQ_SZ: IcmpType(1058)=17; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP地址掩码请求报文数超过1，聚合后触发日志
处理建议	无

9.5 ATK_ICMP_ADDRMASK_RPL

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMP_ADDRMASK_RPL: IcmpType(1058)=18; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP地址掩码应答报文数超过1，聚合后触发日志
处理建议	无

9.6 ATK_ICMP_ADDRMASK_RPL_RAW

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_ADDRMASK_RPL_RAW: IcmpType(1058)=18; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP地址掩码应答报文首包触发日志；日志聚合开关关闭，每个ICMP地址掩码应答报文触发一个日志
处理建议	无

9.7 ATK_ICMP_ADDRMASK_RPL_RAW_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_ADDRMASK_RPL_RAW_SZ: IcmpType(1058)=18; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP地址掩码应答报文首包触发日志；日志聚合开关关闭，每个ICMP地址掩码应答报文触发一个日志
处理建议	无

9.8 ATK_ICMP_ADDRMASK_RPL_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMP_ADDRMASK_RPL_SZ: IcmpType(1058)=18; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP地址掩码应答报文数超过1，聚合后触发日志
处理建议	无

9.9 ATK_ICMP_ECHO_REQ

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMP_ECHO_REQ: IcmpType(1058)=8; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP请求回显报文数超过1，聚合后触发日志
处理建议	无

9.10 ATK_ICMP_ECHO_REQ_RAW

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; DstPort(1004)=[UINT16]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：目的端口 $7：VPN名称 $8：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_ECHO_REQ_RAW: IcmpType(1058)=8; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DstPort(1004)=22; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP请求回显报文首包触发日志；日志聚合开关关闭，每个ICMP请求回显报文触发一个日志
处理建议	无

9.11 ATK_ICMP_ECHO_REQ_RAW_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; DstPort(1004)=[UINT16]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：目的端口 $7：VPN名称 $8：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_ECHO_REQ_RAW_SZ: IcmpType(1058)=8; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DstPort(1004)=22; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP请求回显报文首包触发日志；日志聚合开关关闭，每个ICMP请求回显报文触发一个日志
处理建议	无

9.12 ATK_ICMP_ECHO_REQ_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMP_ECHO_REQ_SZ: IcmpType(1058)=8; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP请求回显报文数超过1，聚合后触发日志
处理建议	无

9.13 ATK_ICMP_ECHO_RPL

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMP_ECHO_RPL: IcmpType(1058)=0; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP回显应答报文数超过1，聚合后触发日志
处理建议	无

9.14 ATK_ICMP_ECHO_RPL_RAW

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_ECHO_RPL_RAW: IcmpType(1058)=0; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP回显应答报文首包触发日志；日志聚合开关关闭，每个ICMP回显应答报文触发一个日志
处理建议	无

9.15 ATK_ICMP_ECHO_RPL_RAW_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_ECHO_RPL_RAW_SZ: IcmpType(1058)=0; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP回显应答报文首包触发日志；日志聚合开关关闭，每个ICMP回显应答报文触发一个日志
处理建议	无

9.16 ATK_ICMP_ECHO_RPL_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMP_ECHO_RPL_SZ: IcmpType(1058)=0; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP回显应答报文数超过1，聚合后触发日志
处理建议	无

9.17 ATK_ICMP_FLOOD

日志内容	RcvIfName(1023)=[STRING]; DstIPAddr(1007)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：目的IP地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_ICMP_FLOOD: RcvIfName(1023)=Ethernet0/0/2; DstIPAddr(1007)=6.1.1.5; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	单位时间内指定目的地址的ICMP报文数超过阈值，触发日志
处理建议	无

9.18 ATK_ICMP_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING]; DstIPAddr(1007)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：目的IP地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_ICMP_FLOOD_SZ: SrcZoneName(1025)=Trust; DstIPAddr(1007)=6.1.1.5; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	单位时间内指定目的地址的ICMP报文数超过阈值，触发日志
处理建议	无

9.19 ATK_ICMP_INFO_REQ

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMP_INFO_REQ: IcmpType(1058)=15; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP信息请求的报文数超过1，聚合后触发日志
处理建议	无

9.20 ATK_ICMP_INFO_REQ_RAW

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_INFO_REQ_RAW: IcmpType(1058)=15; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP信息请求的报文首包触发日志；日志聚合开关关闭，每个ICMP信息请求的报文触发一个日志
处理建议	无

9.21 ATK_ICMP_INFO_REQ_RAW_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_INFO_REQ_RAW_SZ: IcmpType(1058)=15; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP信息请求的报文首包触发日志；日志聚合开关关闭，每个ICMP信息请求的报文触发一个日志
处理建议	无

9.22 ATK_ICMP_INFO_REQ_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMP_INFO_REQ_SZ: IcmpType(1058)=15; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP信息请求的报文数超过1，聚合后触发日志
处理建议	无

9.23 ATK_ICMP_INFO_RPL

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMP_INFO_RPL: IcmpType(1058)=16; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP信息应答的报文数超过1，聚合后触发日志
处理建议	无

9.24 ATK_ICMP_INFO_RPL_RAW

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_INFO_RPL_RAW: IcmpType(1058)=16; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP信息应答的报文首包触发日志；日志聚合开关关闭，每个ICMP信息应答的报文触发一个日志
处理建议	无

9.25 ATK_ICMP_INFO_RPL_RAW_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_INFO_RPL_RAW_SZ: IcmpType(1058)=16; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP信息应答的报文首包触发日志；日志聚合开关关闭，每个ICMP信息应答的报文触发一个日志
处理建议	无

9.26 ATK_ICMP_INFO_RPL_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMP_INFO_RPL_SZ: IcmpType(1058)=16; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP信息应答的报文数超过1，聚合后触发日志
处理建议	无

9.27 ATK_ICMP_LARGE

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_ICMP_LARGE: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP超大报文数超过1，聚合后触发日志
处理建议	无

9.28 ATK_ICMP_LARGE_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_ICMP_LARGE_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP超大报文首包触发日志；日志聚合开关关闭，每个ICMP超大报文触发一个日志
处理建议	无

9.29 ATK_ICMP_LARGE_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_LARGE_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP超大报文首包触发日志；日志聚合开关关闭，每个ICMP超大报文触发一个日志
处理建议	无

9.30 ATK_ICMP_LARGE_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_ICMP_LARGE_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP超大报文数超过1，聚合后触发日志
处理建议	无

9.31 ATK_ICMP_PARAPROBLEM

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMP_PARAPROBLEM: IcmpType(1058)=12; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP参数错误的报文数超过1，聚合后触发日志
处理建议	无

9.32 ATK_ICMP_PARAPROBLEM_RAW

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_PARAPROBLEM_RAW: IcmpType(1058)=12; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP参数错误的报文首包触发日志；日志聚合开关关闭，每个ICMP参数错误的报文触发一个日志
处理建议	无

9.33 ATK_ICMP_PARAPROBLEM_RAW_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_PARAPROBLEM_RAW_SZ: IcmpType(1058)=12; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP参数错误的报文首包触发日志；日志聚合开关关闭，每个ICMP参数错误的报文触发一个日志
处理建议	无

9.34 ATK_ICMP_PARAPROBLEM_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMP_PARAPROBLEM_SZ: IcmpType(1058)=12; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP参数错误的报文数超过1，聚合后触发日志
处理建议	无

9.35 ATK_ICMP_PINGOFDEATH

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_ICMP_PINGOFDEATH: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，标志位设置为最后一片并且(IP offset * 8) + (IP data lenth) > 65535 的ICMP报文数超过1，聚合后触发日志
处理建议	无

9.36 ATK_ICMP_PINGOFDEATH_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_ICMP_PINGOFDEATH_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，标志位设置为最后一片并且(IP offset * 8) + (IP data lenth) > 65535 的ICMP报文首包触发日志；日志聚合开关关闭，每个标志位设置为最后一片并且(IP offset * 8) + (IP data lenth) > 65535 的ICMP报文触发一个日志
处理建议	无

9.37 ATK_ICMP_PINGOFDEATH_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_ICMP_PINGOFDEATH_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，标志位设置为最后一片并且(IP offset * 8) + (IP data lenth) > 65535 的ICMP报文首包触发日志；日志聚合开关关闭，每个标志位设置为最后一片并且(IP offset * 8) + (IP data lenth) > 65535 的ICMP报文触发一个日志
处理建议	无

9.38 ATK_ICMP_PINGOFDEATH_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_ICMP_PINGOFDEATH_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，标志位设置为最后一片并且(IP offset * 8) + (IP data lenth) > 65535 的ICMP报文数超过1，聚合后触发日志
处理建议	无

9.39 ATK_ICMP_REDIRECT

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMP_REDIRECT: IcmpType(1058)=5; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP重定向报文数超过1，聚合后触发日志
处理建议	无

9.40 ATK_ICMP_REDIRECT_RAW

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_REDIRECT_RAW: IcmpType(1058)=5; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP重定向报文首包触发日志；日志聚合开关关闭，每个ICMP重定向报文触发一个日志
处理建议	无

9.41 ATK_ICMP_REDIRECT_RAW_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_REDIRECT_RAW_SZ: IcmpType(1058)=5; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP重定向报文首包触发日志；日志聚合开关关闭，每个ICMP重定向报文触发一个日志
处理建议	无

9.42 ATK_ICMP_REDIRECT_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMP_REDIRECT_SZ: IcmpType(1058)=5; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP重定向报文数超过1，聚合后触发日志
处理建议	无

9.43 ATK_ICMP_SMURF

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_ICMP_SMURF: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP请求回显报文，目的IP为：(1)A、B、C类广播地址或者网络地址；D类或者E类地址；(2)入接口IP地址对应的广播地址或者网络地址特征的报文数超过1，聚合后触发日志
处理建议	无

9.44 ATK_ICMP_SMURF_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_ICMP_SMURF_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP请求回显报文，目的IP为：(1)A、B、C类广播地址或者网络地址；D类或者E类地址；(2)入接口IP地址对应的广播地址或者网络地址特征的报文首包触发日志 日志聚合开关关闭，符合上述条件的ICMP请求回显报文，每个报文触发一个日志
处理建议	无

9.45 ATK_ICMP_SMURF_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_ICMP_SMURF_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP请求回显报文，目的IP为：(1)A、B、C类广播地址或者网络地址；D类或者E类地址；(2)入接口IP地址对应的广播地址或者网络地址特征的报文首包触发日志 日志聚合开关关闭，符合上述条件的ICMP请求回显报文，每个报文触发一个日志
处理建议	无

9.46 ATK_ICMP_SMURF_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_ICMP_SMURF_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP请求回显报文，目的IP为：(1)A、B、C类广播地址或者网络地址；D类或者E类地址；(2)入接口IP地址对应的广播地址或者网络地址特征的报文数超过1，聚合后触发日志
处理建议	无

9.47 ATK_ICMP_SOURCEQUENCH

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMP_SOURCEQUENCH: IcmpType(1058)=4; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP源端被关闭的报文数超过1，聚合后触发日志
处理建议	无

9.48 ATK_ICMP_SOURCEQUENCH_RAW

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_SOURCEQUENCH_RAW: IcmpType(1058)=4; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP源端被关闭的报文首包触发日志；日志聚合开关关闭，每个ICMP源端被关闭的报文触发一个日志
处理建议	无

9.49 ATK_ICMP_SOURCEQUENCH_RAW_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_SOURCEQUENCH_RAW_SZ: IcmpType(1058)=4; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP源端被关闭的报文首包触发日志；日志聚合开关关闭，每个ICMP源端被关闭的报文触发一个日志
处理建议	无

9.50 ATK_ICMP_SOURCEQUENCH_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMP_SOURCEQUENCH_SZ: IcmpType(1058)=4; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP源端被关闭的报文数超过1，聚合后触发日志
处理建议	无

9.51 ATK_ICMP_TIMEEXCEED

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMP_TIMEEXCEED: IcmpType(1058)=11; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP超时的报文数超过1，聚合后触发日志
处理建议	无

9.52 ATK_ICMP_TIMEEXCEED_RAW

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_TIMEEXCEED_RAW: IcmpType(1058)=11; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP超时的报文首包触发日志；日志聚合开关关闭，每个ICMP超时的报文触发一个日志
处理建议	无

9.53 ATK_ICMP_TIMEEXCEED_RAW_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_TIMEEXCEED_RAW_SZ: IcmpType(1058)=11; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP超时的报文首包触发日志；日志聚合开关关闭，每个ICMP超时的报文触发一个日志
处理建议	无

9.54 ATK_ICMP_TIMEEXCEED_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMP_TIMEEXCEED_SZ: IcmpType(1058)=11; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP超时的报文数超过1，聚合后触发日志
处理建议	无

9.55 ATK_ICMP_TRACEROUTE

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_ICMP_TRACEROUTE: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP类型为11且代码为0的报文数超过1，聚合后触发日志
处理建议	无

9.56 ATK_ICMP_TRACEROUTE_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_ICMP_TRACEROUTE_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP类型为11且代码为0的报文首包触发日志；日志聚合开关关闭，每个ICMP类型为11且代码为0的报文触发一个日志
处理建议	无

9.57 ATK_ICMP_TRACEROUTE_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_ICMP_TRACEROUTE_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP类型为11且代码为0的报文首包触发日志；日志聚合开关关闭，每个ICMP类型为11且代码为0的报文触发一个日志
处理建议	无

9.58 ATK_ICMP_TRACEROUTE_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_ICMP_TRACEROUTE_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP类型为11且代码为0的报文数超过1，聚合后触发日志
处理建议	无

9.59 ATK_ICMP_TSTAMP_REQ

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMP_TSTAMP_REQ: IcmpType(1058)=13; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP时间戳请求的报文数超过1，聚合后触发日志
处理建议	无

9.60 ATK_ICMP_TSTAMP_REQ_RAW

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_TSTAMP_REQ_RAW: IcmpType(1058)=13; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP时间戳请求的报文首包触发日志；日志聚合开关关闭，每个ICMP时间戳请求的报文触发一个日志
处理建议	无

9.61 ATK_ICMP_TSTAMP_REQ_RAW_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_TSTAMP_REQ_RAW_SZ: IcmpType(1058)=13; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP时间戳请求的报文首包触发日志；日志聚合开关关闭，每个ICMP时间戳请求的报文触发一个日志
处理建议	无

9.62 ATK_ICMP_TSTAMP_REQ_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMP_TSTAMP_REQ_SZ: IcmpType(1058)=13; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP时间戳请求的报文数超过1，聚合后触发日志
处理建议	无

9.63 ATK_ICMP_TSTAMP_RPL

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMP_TSTAMP_RPL: IcmpType(1058)=14; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP时间戳应答的报文数超过1，聚合后触发日志
处理建议	无

9.64 ATK_ICMP_TSTAMP_RPL_RAW

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_TSTAMP_RPL_RAW: IcmpType(1058)=14; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP时间戳应答的报文首包触发日志；日志聚合开关关闭，每个ICMP时间戳应答的报文触发一个日志
处理建议	无

9.65 ATK_ICMP_TSTAMP_RPL_RAW_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_TSTAMP_RPL_RAW_SZ: IcmpType(1058)=14; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP时间戳应答的报文首包触发日志；日志聚合开关关闭，每个ICMP时间戳应答的报文触发一个日志
处理建议	无

9.66 ATK_ICMP_TSTAMP_RPL_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMP_TSTAMP_RPL_SZ: IcmpType(1058)=14; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP时间戳应答的报文数超过1，聚合后触发日志
处理建议	无

9.67 ATK_ICMP_TYPE

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMP_TYPE: IcmpType(1058)=38; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP用户自定义类型的报文数超过1，聚合后触发日志
处理建议	无

9.68 ATK_ICMP_TYPE_RAW

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_TYPE_RAW: IcmpType(1058)=38; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP用户自定义类型的报文首包触发日志；日志聚合开关关闭，每个ICMP用户自定义类型的报文触发一个日志
处理建议	无

9.69 ATK_ICMP_TYPE_RAW_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_TYPE_RAW_SZ: IcmpType(1058)=38; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP用户自定义类型的报文首包触发日志；日志聚合开关关闭，每个ICMP用户自定义类型的报文触发一个日志
处理建议	无

9.70 ATK_ICMP_TYPE_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMP_TYPE_SZ: IcmpType(1058)=38; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP用户自定义类型的报文数超过1，聚合后触发日志
处理建议	无

9.71 ATK_ICMP_UNREACHABLE

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMP_UNREACHABLE: IcmpType(1058)=3; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP目的不可达的报文数超过1，聚合后触发日志
处理建议	无

9.72 ATK_ICMP_UNREACHABLE_RAW

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_UNREACHABLE_RAW: IcmpType(1058)=3; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP目的不可达的报文首包触发日志；日志聚合开关关闭，每个ICMP目的不可达的报文触发一个日志
处理建议	无

9.73 ATK_ICMP_UNREACHABLE_RAW_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_UNREACHABLE_RAW_SZ: IcmpType(1058)=3; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP目的不可达的报文首包触发日志；日志聚合开关关闭，每个ICMP目的不可达的报文触发一个日志
处理建议	无

9.74 ATK_ICMP_UNREACHABLE_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMP_UNREACHABLE_SZ: IcmpType(1058)=3; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP目的不可达的报文数超过1，聚合后触发日志
处理建议	无

9.75 ATK_ICMPV6_DEST_UNREACH

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMPV6_DEST_UNREACH: Icmpv6Type(1059)=133; RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMPV6目的不可达的报文数超过1，聚合后触发日志
处理建议	无

9.76 ATK_ICMPV6_DEST_UNREACH_RAW

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_DEST_UNREACH_RAW: Icmpv6Type(1059)=133; RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMPV6目的不可达的报文首包触发日志；日志聚合开关关闭，每个ICMPV6目的不可达的报文触发一个日志
处理建议	无

9.77 ATK_ICMPV6_DEST_UNREACH_RAW_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_DEST_UNREACH_RAW_SZ: Icmpv6Type(1059)=133; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMPV6目的不可达的报文首包触发日志；日志聚合开关关闭，每个ICMPV6目的不可达的报文触发一个日志
处理建议	无

9.78 ATK_ICMPV6_DEST_UNREACH_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMPV6_DEST_UNREACH_SZ: Icmpv6Type(1059)=133; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMPV6目的不可达的报文数超过1，聚合后触发日志
处理建议	无

9.79 ATK_ICMPV6_ECHO_REQ

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMPV6_ECHO_REQ: Icmpv6Type(1059)=128; RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMPV6请求回显的报文数超过1，聚合后触发日志
处理建议	无

9.80 ATK_ICMPV6_ECHO_REQ_RAW

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_ECHO_REQ_RAW: Icmpv6Type(1059)=128; RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMPV6请求回显的报文首包触发日志；日志聚合开关关闭，每个ICMPV6请求回显的报文触发一个日志
处理建议	无

9.81 ATK_ICMPV6_ECHO_REQ_RAW_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_ECHO_REQ_RAW_SZ: Icmpv6Type(1059)=128; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMPV6请求回显的报文首包触发日志；日志聚合开关关闭，每个ICMPV6请求回显的报文触发一个日志
处理建议	无

9.82 ATK_ICMPV6_ECHO_REQ_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMPV6_ECHO_REQ_SZ: Icmpv6Type(1059)=128; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMPV6请求回显的报文数超过1，聚合后触发日志
处理建议	无

9.83 ATK_ICMPV6_ECHO_RPL

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMPV6_ECHO_RPL: Icmpv6Type(1059)=129; RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMPV6回显应答的报文数超过1，聚合后触发日志
处理建议	无

9.84 ATK_ICMPV6_ECHO_RPL_RAW

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_ECHO_RPL_RAW: Icmpv6Type(1059)=129; RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMPV6回显应答的报文首包触发日志；日志聚合开关关闭，每个ICMPV6回显应答的报文触发一个日志
处理建议	无

9.85 ATK_ICMPV6_ECHO_RPL_RAW_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_ECHO_RPL_RAW_SZ: Icmpv6Type(1059)=129; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMPV6回显应答的报文首包触发日志；日志聚合开关关闭，每个ICMPV6回显应答的报文触发一个日志
处理建议	无

9.86 ATK_ICMPV6_ECHO_RPL_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMPV6_ECHO_RPL_SZ: Icmpv6Type(1059)=129; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMPV6回显应答的报文数超过1，聚合后触发日志
处理建议	无

9.87 ATK_ICMPV6_FLOOD

日志内容	RcvIfName(1023)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：目的IPv6地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_ICMPV6_FLOOD: RcvIfName(1023)=Ethernet0/0/2; DstIPv6Addr(1007)=2002::2; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	单位时间内指定目的地址的ICMPV6报文数超过阈值，触发日志
处理建议	无

9.88 ATK_ICMPV6_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：目的IPv6地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_ICMPV6_FLOOD_SZ: SrcZoneName(1025)=Trust; DstIPv6Addr(1007)=2002::2; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	单位时间内指定目的地址的ICMPV6报文数超过阈值，触发日志
处理建议	无

9.89 ATK_ICMPV6_GROUPQUERY

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMPV6_GROUPQUERY: Icmpv6Type(1059)=130; RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMPV6组播侦听者查询的报文数超过1，聚合后触发日志
处理建议	无

9.90 ATK_ICMPV6_GROUPQUERY_RAW

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_GROUPQUERY_RAW: Icmpv6Type(1059)=130; RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMPV6组播侦听者查询的报文首包触发日志；日志聚合开关关闭，每个每个ICMPV6组播侦听者查询的报文触发一个日志
处理建议	无

9.91 ATK_ICMPV6_GROUPQUERY_RAW_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_GROUPQUERY_RAW_SZ: Icmpv6Type(1059)=130; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMPV6组播侦听者查询的报文首包触发日志；日志聚合开关关闭，每个每个ICMPV6组播侦听者查询的报文触发一个日志
处理建议	无

9.92 ATK_ICMPV6_GROUPQUERY_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMPV6_GROUPQUERY_SZ: Icmpv6Type(1059)=130; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMPV6组播侦听者查询的报文数超过1，聚合后触发日志
处理建议	无

9.93 ATK_ICMPV6_GROUPREDUCTION

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMPV6_GROUPREDUCTION: Icmpv6Type(1059)=132; RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMPV6组播侦听者Done的报文数超过1，聚合后触发日志
处理建议	无

9.94 ATK_ICMPV6_GROUPREDUCTION_RAW

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_GROUPREDUCTION_RAW: Icmpv6Type(1059)=132; RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMPV6组播侦听者Done的报文首包触发日志；日志聚合开关关闭，每个每个ICMPV6组播侦听者Done的报文触发一个日志
处理建议	无

9.95 ATK_ICMPV6_GROUPREDUCTION_RAW_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_GROUPREDUCTION_RAW_SZ: Icmpv6Type(1059)=132; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMPV6组播侦听者Done的报文首包触发日志；日志聚合开关关闭，每个每个ICMPV6组播侦听者Done的报文触发一个日志
处理建议	无

9.96 ATK_ICMPV6_GROUPREDUCTION_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMPV6_GROUPREDUCTION_SZ: Icmpv6Type(1059)=132; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMPV6组播侦听者Done的报文数超过1，聚合后触发日志
处理建议	无

9.97 ATK_ICMPV6_GROUPREPORT

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMPV6_GROUPREPORT: Icmpv6Type(1059)=131; RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMPV6组播侦听者报告的报文数超过1，聚合后触发日志
处理建议	无

9.98 ATK_ICMPV6_GROUPREPORT_RAW

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_GROUPREPORT_RAW: Icmpv6Type(1059)=131; RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMPV6组播侦听者报告的报文首包触发日志；日志聚合开关关闭，每个每个ICMPV6组播侦听者报告的报文触发一个日志
处理建议	无

9.99 ATK_ICMPV6_GROUPREPORT_RAW_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_GROUPREPORT_RAW_SZ: Icmpv6Type(1059)=131; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMPV6组播侦听者报告的报文首包触发日志；日志聚合开关关闭，每个每个ICMPV6组播侦听者报告的报文触发一个日志
处理建议	无

9.100 ATK_ICMPV6_GROUPREPORT_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMPV6_GROUPREPORT_SZ: Icmpv6Type(1059)=131; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMPV6组播侦听者报告的报文数超过1，聚合后触发日志
处理建议	无

9.101 ATK_ICMPV6_LARGE

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_ICMPV6_LARGE: RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMPV6超长报文数超过1，聚合后触发日志
处理建议	无

9.102 ATK_ICMPV6_LARGE_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_ICMPV6_LARGE_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMPV6超长报文首包触发日志；日志聚合开关关闭，每个每个ICMPV6超长报文触发一个日志
处理建议	无

9.103 ATK_ICMPV6_LARGE_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_ICMPV6_LARGE_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMPV6超长报文首包触发日志；日志聚合开关关闭，每个每个ICMPV6超长报文触发一个日志
处理建议	无

9.104 ATK_ICMPV6_LARGE_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_ICMPV6_LARGE_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMPV6超长报文数超过1，聚合后触发日志
处理建议	无

9.105 ATK_ICMPV6_PACKETTOOBIG

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMPV6_PACKETTOOBIG: Icmpv6Type(1059)=136; RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMPV6数据超长的报文数超过1，聚合后触发日志
处理建议	无

9.106 ATK_ICMPV6_PACKETTOOBIG_RAW

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_PACKETTOOBIG_RAW: Icmpv6Type(1059)=136; RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMPV6数据超长的报文首包触发日志；日志聚合开关关闭，每个ICMPV6数据超长的报文触发一个日志
处理建议	无

9.107 ATK_ICMPV6_PACKETTOOBIG_RAW_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_PACKETTOOBIG_RAW_SZ: Icmpv6Type(1059)=136; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMPV6数据超长的报文首包触发日志；日志聚合开关关闭，每个ICMPV6数据超长的报文触发一个日志
处理建议	无

9.108 ATK_ICMPV6_PACKETTOOBIG_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMPV6_PACKETTOOBIG_SZ: Icmpv6Type(1059)=136; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMPV6数据超长的报文数超过1，聚合后触发日志
处理建议	无

9.109 ATK_ICMPV6_PARAPROBLEM

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMPV6_PARAPROBLEM: Icmpv6Type(1059)=135; RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMPV6参数问题的报文数超过1，聚合后触发日志
处理建议	无

9.110 ATK_ICMPV6_PARAPROBLEM_RAW

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_PARAPROBLEM_RAW: Icmpv6Type(1059)=135; RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMPV6参数问题的报文首包触发日志；日志聚合开关关闭，每个ICMPV6参数问题的报文触发一个日志
处理建议	无

9.111 ATK_ICMPV6_PARAPROBLEM_RAW_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_PARAPROBLEM_RAW_SZ: Icmpv6Type(1059)=135; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMPV6参数问题的报文首包触发日志；日志聚合开关关闭，每个ICMPV6参数问题的报文触发一个日志
处理建议	无

9.112 ATK_ICMPV6_PARAPROBLEM_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMPV6_PARAPROBLEM_SZ: Icmpv6Type(1059)=135; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMPV6参数问题的报文数超过1，聚合后触发日志
处理建议	无

9.113 ATK_ICMPV6_TIMEEXCEED

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMPV6_TIMEEXCEED: Icmpv6Type(1059)=134; RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMPV6超时的报文数超过1，聚合后触发日志
处理建议	无

9.114 ATK_ICMPV6_TIMEEXCEED_RAW

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_TIMEEXCEED_RAW: Icmpv6Type(1059)=134; RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMPV6超时的报文首包触发日志；日志聚合开关关闭，每个ICMPV6超时的报文触发一个日志
处理建议	无

9.115 ATK_ICMPV6_TIMEEXCEED_RAW_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_TIMEEXCEED_RAW_SZ: Icmpv6Type(1059)=134; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMPV6超时的报文首包触发日志；日志聚合开关关闭，每个ICMPV6超时的报文触发一个日志
处理建议	无

9.116 ATK_ICMPV6_TIMEEXCEED_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMPV6_TIMEEXCEED_SZ: Icmpv6Type(1059)=134; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMPV6超时的报文数超过1，聚合后触发日志
处理建议	无

9.117 ATK_ICMPV6_TRACEROUTE

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_ICMPV6_TRACEROUTE: RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP类型为3的报文数超过1，聚合后触发日志
处理建议	无

9.118 ATK_ICMPV6_TRACEROUTE_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_ICMPV6_TRACEROUTE_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435.
日志说明	日志聚合开关开启，ICMP类型为3的报文首包触发日志；日志聚合开关关闭，每个ICMP类型为3的报文触发一个日志
处理建议	无

9.119 ATK_ICMPV6_TRACEROUTE_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_ICMPV6_TRACEROUTE_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435.
日志说明	日志聚合开关开启，ICMP类型为3的报文首包触发日志；日志聚合开关关闭，每个ICMP类型为3的报文触发一个日志
处理建议	无

9.120 ATK_ICMPV6_TRACEROUTE_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_ICMPV6_TRACEROUTE_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP类型为3的报文数超过1，聚合后触发日志
处理建议	无

9.121 ATK_ICMPV6_TYPE

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMPV6_TYPE: Icmpv6Type(1059)=38; RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMPV6用户自定义类型的报文数超过1，聚合后触发日志
处理建议	无

9.122 ATK_ICMPV6_TYPE _RAW

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_TYPE_RAW: Icmpv6Type(1059)=38; RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMPV6用户自定义类型的报文首包触发日志；日志聚合开关关闭，每个ICMPV6用户自定义类型的报文触发一个日志
处理建议	无

9.123 ATK_ICMPV6_TYPE _RAW_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_TYPE_RAW_SZ: Icmpv6Type(1059)=38; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMPV6用户自定义类型的报文首包触发日志；日志聚合开关关闭，每个ICMPV6用户自定义类型的报文触发一个日志
处理建议	无

9.124 ATK_ICMPV6_TYPE_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMPV6_TYPE_SZ: Icmpv6Type(1059)=38; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMPV6用户自定义类型的报文数超过1，聚合后触发日志
处理建议	无

9.125 ATK_IP_OPTION

日志内容	IPOptValue(1057)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：IP选项值 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5
举例	ATK/5/ATK_IP_OPTION: IPOptValue(1057)=38; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging; BeginTime_c(1011)=20131011063123; EndTime_c(1012)=20131011063623; AtkTimes(1050)=3.
日志说明	日志聚合开关打开，用户自定义IP选项的报文数超过1，聚合后触发日志
处理建议	无

9.126 ATK_IP_OPTION_RAW

日志内容	IPOptValue(1057)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：IP选项值 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型
日志等级	5
举例	ATK/5/ATK_IP_OPTION_RAW: IPOptValue(1057)=38; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging.
日志说明	日志聚合开关开启，用户自定义IP选项的报文首包触发日志；日志聚合开关关闭，每个用户自定义IP选项的报文触发一个日志
处理建议	无

9.127 ATK_IP_OPTION_RAW_SZ

日志内容	IPOptValue(1057)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：IP选项值 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型
日志等级	5
举例	ATK/5/ATK_IP_OPTION_RAW_SZ: IPOptValue(1057)=38; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging.
日志说明	日志聚合开关开启，用户自定义IP选项的报文首包触发日志；日志聚合开关关闭，每个用户自定义IP选项的报文触发一个日志
处理建议	无

9.128 ATK_IP_OPTION_SZ

日志内容	IPOptValue(1057)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：IP选项值 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5
举例	ATK/5/ATK_IP_OPTION_SZ: IPOptValue(1057)=38; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging; BeginTime_c(1011)=20131011063123; EndTime_c(1012)=20131011063623; AtkTimes(1050)=3.
日志说明	日志聚合开关打开，用户自定义IP选项的报文数超过1，聚合后触发日志
处理建议	无

9.129 ATK_IP4_ACK_FLOOD

日志内容	RcvIfName(1023)=[STRING]; DstIPAddr(1007)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：目的IP地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP4_ACK_FLOOD: RcvIfName(1023)=Ethernet0/0/2; DstIPAddr(1007)=6.1.1.5; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	单位时间内指定目的地址的TCP标志位为ACK的IPV4报文数超过阈值，触发日志
处理建议	无

9.130 ATK_IP4_ACK_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING]; DstIPAddr(1007)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：目的IP地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP4_ACK_FLOOD_SZ: SrcZoneName(1025)=Trust; DstIPAddr(1007)=6.1.1.5; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	单位时间内指定目的地址的TCP标志位为ACK的IPV4报文数超过阈值，触发日志
处理建议	无

9.131 ATK_IP4_DIS_PORTSCAN

日志内容	RcvIfName(1023)=[STRING]; Protocol(1001)=[STRING]; TcpFlag(1074)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：协议名称 $3：TCP类型（仅在TCP报文中显示该字段） $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP4_DIS_PORTSCAN: RcvIfName(1023)=Ethernet0/0/2; Protocol(1001)=TCP; TcpFlag(1074)=[SYN]; DstIPAddr(1007)=6.1.1.5; RcvVPNInstance(1041)=vpn1; Action(1049)=logging,block-source; BeginTime_c(1011)=20131009052955.
日志说明	报文满足分布式port scan时触发日志
处理建议	无

9.132 ATK_IP4_DIS_PORTSCAN_SZ

日志内容	SrcZoneName(1025)=[STRING]; Protocol(1001)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：协议名称 $3：目的IP地址 $4：VPN名称 $5：动作类型 $6：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP4_DIS_PORTSCAN_SZ: SrcZoneName(1025)=Trust; Protocol(1001)=TCP; DstIPAddr(1007)=6.1.1.5; RcvVPNInstance(1041)=vpn1; Action(1049)=logging,block-source; BeginTime_c(1011)=20131009052955.
日志说明	报文满足分布式port scan时触发日志
处理建议	无

9.133 ATK_IP4_DNS_FLOOD

日志内容	RcvIfName(1023)=[STRING]; DstIPAddr(1007)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：目的IP地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP4_DNS_FLOOD: RcvIfName(1023)=Ethernet0/0/2; DstIPAddr(1007)=6.1.1.5; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	单位时间内向指定目的IP发送DNS Query的报文数超过阈值，触发日志发送
处理建议	无

9.134 ATK_IP4_DNS_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING]; DstIPAddr(1007)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：目的IP地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP4_DNS_FLOOD_SZ: SrcZoneName(1025)=Trust; DstIPAddr(1007)=6.1.1.5; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	单位时间内向指定目的IP发送DNS Query的报文数超过阈值，触发日志发送
处理建议	无

9.135 ATK_IP4_FIN_FLOOD

日志内容	RcvIfName(1023)=[STRING]; DstIPAddr(1007)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：目的IP地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP4_FIN_FLOOD: RcvIfName(1023)=Ethernet0/0/2; DstIPAddr(1007)=6.1.1.5; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	单位时间内向指定目的IP发送的TCP标志位为SYN+ACK的报文数超过阈值，触发日志发送
处理建议	无

9.136 ATK_IP4_FIN_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING]; DstIPAddr(1007)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：目的IP地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP4_FIN_FLOOD_SZ: SrcZoneName(1025)=Trust; DstIPAddr(1007)=6.1.1.5; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	单位时间内向指定目的IP发送的TCP标志位为SYN+ACK的报文数超过阈值，触发日志发送
处理建议	无

9.137 ATK_IP4_FRAGMENT

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：协议类型 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	3
举例	ATK/3/ATK_IP4_FRAGMENT: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=TCP; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=3.
日志说明	日志聚合开关开启，偏移量OffSet值在(0,5)之间的IPV4报文数超过1，聚合后触发日志
处理建议	无

9.138 ATK_IP4_FRAGMENT_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：协议类型 $7：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_FRAGMENT_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=TCP; Action(1049)=logging.
日志说明	日志聚合开关开启，偏移量OffSet值在(0,5)之间的IPV4报文首包触发日志；日志聚合开关关闭，每个偏移量OffSet值在(0,5)之间的IPV4报文触发一个日志
处理建议	无

9.139 ATK_IP4_FRAGMENT_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：协议类型 $7：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_FRAGMENT_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=TCP; Action(1049)=logging.
日志说明	日志聚合开关开启，偏移量OffSet值在(0,5)之间的IPV4报文首包触发日志；日志聚合开关关闭，每个偏移量OffSet值在(0,5)之间的IPV4报文触发一个日志
处理建议	无

9.140 ATK_IP4_FRAGMENT_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：协议类型 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	3
举例	ATK/3/ATK_IP4_FRAGMENT_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=TCP; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=3.
日志说明	日志聚合开关开启，偏移量OffSet值在(0,5)之间的IPV4报文数超过1，聚合后触发日志
处理建议	无

9.141 ATK_IP4_HTTP_FLOOD

日志内容	RcvIfName(1023)=[STRING]; DstIPAddr(1007)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：目的IP地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP4_HTTP_FLOOD: RcvIfName(1023)=Ethernet0/0/2; DstIPAddr(1007)=6.1.1.5; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	单位时间内向指定目的IP发送的HTTP的Get报文数超过阈值，触发日志发送
处理建议	无

9.142 ATK_IP4_HTTP_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING]; DstIPAddr(1007)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：目的IP地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP4_HTTP_FLOOD_SZ: SrcZoneName(1025)=Trust; DstIPAddr(1007)=6.1.1.5; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	单位时间内向指定目的IP发送的HTTP的Get报文数超过阈值，触发日志发送
处理建议	无

9.143 ATK_IP4_IMPOSSIBLE

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：协议类型 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	3
举例	ATK/3/ATK_IP4_IMPOSSIBLE: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=TCP; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=3.
日志说明	日志聚合开关开启，源目的地址相同的IPV4报文数超过1，聚合后触发日志
处理建议	无

9.144 ATK_IP4_IMPOSSIBLE_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：协议类型 $7：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_IMPOSSIBLE_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=TCP; Action(1049)=logging.
日志说明	日志聚合开关开启，源目的地址相同的IPV4报文首包触发日志；日志聚合开关关闭，每个源目的地址相同的IPV4报文触发一个日志
处理建议	无

9.145 ATK_IP4_IMPOSSIBLE_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：协议类型 $7：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_IMPOSSIBLE_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=TCP; Action(1049)=logging.
日志说明	日志聚合开关开启，源目的地址相同的IPV4报文首包触发日志；日志聚合开关关闭，每个源目的地址相同的IPV4报文触发一个日志
处理建议	无

9.146 ATK_IP4_IMPOSSIBLE_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：协议类型 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	3
举例	ATK/3/ATK_IP4_IMPOSSIBLE_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=TCP; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=3.
日志说明	日志聚合开关开启，源目的地址相同的IPV4报文数超过1，聚合后触发日志
处理建议	无

9.147 ATK_IP4_IPSWEEP

日志内容	RcvIfName(1023)=[STRING]; Protocol(1001)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：协议名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP4_IPSWEEP: RcvIfName(1023)=Ethernet0/0/2; Protocol(1001)=TCP; SrcIPAddr(1003)=9.1.1.5; DSLiteTunnelPeer(1040)=--; RcvVPNInstance(1041)=vpn1; Action(1049)=logging,block-source; BeginTime_c(1011)=20131009060657.
日志说明	报文满足ip sweep时触发日志
处理建议	无

9.148 ATK_IP4_IPSWEEP_SZ

日志内容	SrcZoneName(1025)=[STRING]; Protocol(1001)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：协议名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP4_IPSWEEP_SZ: SrcZoneName(1025)=Trust; Protocol(1001)=TCP; SrcIPAddr(1003)=9.1.1.5; DSLiteTunnelPeer(1040)=--; RcvVPNInstance(1041)=vpn1; Action(1049)=logging,block-source; BeginTime_c(1011)=20131009060657.
日志说明	报文满足ip sweep时触发日志
处理建议	无

9.149 ATK_IP4_PORTSCAN

日志内容	RcvIfName(1023)=[STRING]; Protocol(1001)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; RcvVPNInstance(1041)=[STRING]; DstIPAddr(1007)=[IPADDR]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：协议名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：VPN名称 $6：目的IP地址 $7：动作类型 $8：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP4_PORTSCAN: RcvIfName(1023)=Ethernet0/0/2; Protocol(1001)=TCP; SrcIPAddr(1003)=9.1.1.5; DSLiteTunnelPeer(1040)=--; RcvVPNInstance(1041)=vpn1; DstIPAddr(1007)=6.1.1.5; Action(1049)=logging,block-source; BeginTime_c(1011)=20131009052955.
日志说明	报文满足port scan时触发日志
处理建议	无

9.150 ATK_IP4_PORTSCAN_SZ

日志内容	SrcZoneName(1025)=[STRING]; Protocol(1001)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; RcvVPNInstance(1041)=[STRING]; DstIPAddr(1007)=[IPADDR]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：协议名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：VPN名称 $6：目的IP地址 $7：动作类型 $8：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP4_PORTSCAN_SZ: SrcZoneName(1025)=Trust; Protocol(1001)=TCP; SrcIPAddr(1003)=9.1.1.5; DSLiteTunnelPeer(1040)=--; RcvVPNInstance(1041)=vpn1; DstIPAddr(1007)=6.1.1.5; Action(1049)=logging,block-source; BeginTime_c(1011)=20131009052955.
日志说明	报文满足port scan时触发日志
处理建议	无

9.151 ATK_IP4_RST_FLOOD

日志内容	RcvIfName(1023)=[STRING]; DstIPAddr(1007)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：目的IP地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP4_RST_FLOOD: RcvIfName(1023)=Ethernet0/0/2; DstIPAddr(1007)=6.1.1.5; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	单位时间内指定目的地址的TCP标志位为RST的IPV4报文数超过阈值，触发日志
处理建议	无

9.152 ATK_IP4_RST_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING]; DstIPAddr(1007)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：目的IP地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP4_RST_FLOOD_SZ: SrcZoneName(1025)=Trust; DstIPAddr(1007)=6.1.1.5; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	单位时间内指定目的地址的TCP标志位为RST的IPV4报文数超过阈值，触发日志
处理建议	无

9.153 ATK_IP4_SYN_FLOOD

日志内容	RcvIfName(1023)=[STRING]; DstIPAddr(1007)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：目的IP地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP4_SYN_FLOOD: RcvIfName(1023)=Ethernet0/0/2; DstIPAddr(1007)=6.1.1.5; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	单位时间内指定目的地址的TCP标志位为SYN的IPV4报文数超过阈值，触发日志
处理建议	无

9.154 ATK_IP4_SYN_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：目的IP地址 $3：VPN名称 $4：速率上限 $5：动作类型 $6：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP4_SYN_FLOOD_SZ: SrcZoneName(1025)=Trust; DstIPAddr(1007)=6.1.1.5; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	单位时间内指定目的地址的TCP标志位为SYN的IPV4报文数超过阈值，触发日志
处理建议	无

9.155 ATK_IP4_SYNACK_FLOOD

日志内容	RcvIfName(1023)=[STRING]; DstIPAddr(1007)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：目的IP地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP4_SYNACK_FLOOD: RcvIfName(1023)=Ethernet0/0/2; DstIPAddr(1007)=6.1.1.5; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	单位时间内指定目的地址的TCP标志位为SYN+ACK的IPV4报文数超过阈值，触发日志
处理建议	无

9.156 ATK_IP4_SYNACK_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING]; DstIPAddr(1007)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：目的IP地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP4_SYNACK_FLOOD_SZ: SrcZoneName(1025)=Trust; DstIPAddr(1007)=6.1.1.5; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	单位时间内指定目的地址的TCP标志位为SYN+ACK的IPV4报文数超过阈值，触发日志
处理建议	无

9.157 ATK_IP4_TCP_ALLFLAGS

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_IP4_TCP_ALLFLAGS: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=3.
日志说明	日志聚合开关开启，TCP标志位全置位的IPV4报文数超过1，聚合后触发日志
处理建议	无

9.158 ATK_IP4_TCP_ALLFLAGS_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TCP_ALLFLAGS_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，TCP标志位全置位的IPV4报文首包触发日志；日志聚合开关关闭，每个TCP标志位全置位的IPV4报文触发一个日志
处理建议	无

9.159 ATK_IP4_TCP_ALLFLAGS_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TCP_ALLFLAGS_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，TCP标志位全置位的IPV4报文首包触发日志；日志聚合开关关闭，每个TCP标志位全置位的IPV4报文触发一个日志
处理建议	无

9.160 ATK_IP4_TCP_ALLFLAGS_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_IP4_TCP_ALLFLAGS_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=3.
日志说明	日志聚合开关开启，TCP标志位全置位的IPV4报文数超过1，聚合后触发日志
处理建议	无

9.161 ATK_IP4_TCP_FINONLY

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_IP4_TCP_FINONLY: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=3.
日志说明	日志聚合开关开启，TCP标志位为FIN的IPV4报文数超过1，聚合后触发日志
处理建议	无

9.162 ATK_IP4_TCP_FINONLY_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TCP_FINONLY_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，TCP标志位为FIN的IPV4报文首包触发日志；日志聚合开关关闭，每个TCP标志位为FIN的IPV4报文触发一个日志
处理建议	无

9.163 ATK_IP4_TCP_FINONLY_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TCP_FINONLY_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，TCP标志位为FIN的IPV4报文首包触发日志；日志聚合开关关闭，每个TCP标志位为FIN的IPV4报文触发一个日志
处理建议	无

9.164 ATK_IP4_TCP_FINONLY_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_IP4_TCP_FINONLY_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=3.
日志说明	日志聚合开关开启，TCP标志位为FIN的IPV4报文数超过1，聚合后触发日志
处理建议	无

9.165 ATK_IP4_TCP_INVALIDFLAGS

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_IP4_TCP_INVALIDFLAGS: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=3.
日志说明	日志聚合开关开启，TCP标志位为无效（RST+FIN、RST+SYN、RST+FIN+SYN、PSH+RST+FIN、PSH+RST+SYN、PSH+RST+SYN+FIN、ACK+RST+FIN、ACK+RST+SYN、ACK+RST+SYN+FIN、ACK+PSH+SYN+FIN、ACK+PSH+RST+FIN、ACK+PSH+RST+SYN）时的IPV4报文数超过1，聚合后触发日志
处理建议	无

9.166 ATK_IP4_TCP_INVALIDFLAGS_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TCP_INVALIDFLAGS_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，TCP标志位为无效（RST+FIN、RST+SYN、RST+FIN+SYN、PSH+RST+FIN、PSH+RST+SYN、PSH+RST+SYN+FIN、ACK+RST+FIN、ACK+RST+SYN、ACK+RST+SYN+FIN、ACK+PSH+SYN+FIN、ACK+PSH+RST+FIN、ACK+PSH+RST+SYN）时的IPV4 TCP报文触发日志 日志聚合开关关闭，每个TCP标志位无效的IPv4 TCP报文触发一个日志
处理建议	无

9.167 ATK_IP4_TCP_INVALIDFLAGS_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TCP_INVALIDFLAGS_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，TCP标志位为无效（RST+FIN、RST+SYN、RST+FIN+SYN、PSH+RST+FIN、PSH+RST+SYN、PSH+RST+SYN+FIN、ACK+RST+FIN、ACK+RST+SYN、ACK+RST+SYN+FIN、ACK+PSH+SYN+FIN、ACK+PSH+RST+FIN、ACK+PSH+RST+SYN）时的IPV4 TCP报文触发日志 日志聚合开关关闭，每个TCP标志位无效的IPv4 TCP报文触发一个日志
处理建议	无

9.168 ATK_IP4_TCP_INVALIDFLAGS_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_IP4_TCP_INVALIDFLAGS_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=3.
日志说明	日志聚合开关开启，TCP标志位为无效（RST+FIN、RST+SYN、RST+FIN+SYN、PSH+RST+FIN、PSH+RST+SYN、PSH+RST+SYN+FIN、ACK+RST+FIN、ACK+RST+SYN、ACK+RST+SYN+FIN、ACK+PSH+SYN+FIN、ACK+PSH+RST+FIN、ACK+PSH+RST+SYN）时的IPV4报文数超过1，聚合后触发日志
处理建议	无

9.169 ATK_IP4_TCP_LAND

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_IP4_TCP_LAND: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=3.
日志说明	日志聚合开关开启，IPV4源目的地址相同的TCP报文数超过1，聚合后触发日志
处理建议	无

9.170 ATK_IP4_TCP_LAND_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TCP_LAND_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，IPV4源目的地址相同的TCP报文首包触发日志；日志聚合开关关闭，每个IPV4源目的地址相同的TCP报文触发一个日志
处理建议	无

9.171 ATK_IP4_TCP_LAND_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TCP_LAND_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，IPV4源目的地址相同的TCP报文首包触发日志；日志聚合开关关闭，每个IPV4源目的地址相同的TCP报文触发一个日志
处理建议	无

9.172 ATK_IP4_TCP_LAND_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_IP4_TCP_LAND_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=3.
日志说明	日志聚合开关开启，IPV4源目的地址相同的TCP报文数超过1，聚合后触发日志
处理建议	无

9.173 ATK_IP4_TCP_NULLFLAG

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_IP4_TCP_NULLFLAG: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=4.
日志说明	日志聚合开关开启，TCP标志位未置位的IPV4报文数超过1，聚合后触发日志
处理建议	无

9.174 ATK_IP4_TCP_NULLFLAG_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TCP_NULLFLAG_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，TCP标志位未置位的IPV4报文首包触发日志；日志聚合开关关闭，每个TCP标志位未置位的IPV4报文触发一个日志
处理建议	无

9.175 ATK_IP4_TCP_NULLFLAG_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TCP_NULLFLAG_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，TCP标志位未置位的IPV4报文首包触发日志；日志聚合开关关闭，每个TCP标志位未置位的IPV4报文触发一个日志
处理建议	无

9.176 ATK_IP4_TCP_NULLFLAG_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_IP4_TCP_NULLFLAG_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=4.
日志说明	日志聚合开关开启，TCP标志位未置位的IPV4报文数超过1，聚合后触发日志
处理建议	无

9.177 ATK_IP4_TCP_SYNFIN

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_IP4_TCP_SYNFIN: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，TCP标志位为SYN+FIN的IPV4报文数超过1，聚合后触发日志
处理建议	无

9.178 ATK_IP4_TCP_SYNFIN_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TCP_SYNFIN_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，TCP标志位为SYN+FIN的IPV4报文首包触发日志；日志聚合开关关闭，每个TCP标志位为SYN+FIN的IPV4报文触发一个日志
处理建议	无

9.179 ATK_IP4_TCP_SYNFIN_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TCP_SYNFIN_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，TCP标志位为SYN+FIN的IPV4报文首包触发日志；日志聚合开关关闭，每个TCP标志位为SYN+FIN的IPV4报文触发一个日志
处理建议	无

9.180 ATK_IP4_TCP_SYNFIN_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_IP4_TCP_SYNFIN_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，TCP标志位为SYN+FIN的IPV4报文数超过1，聚合后触发日志
处理建议	无

9.181 ATK_IP4_TCP_WINNUKE

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_IP4_TCP_WINNUKE: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=5.
日志说明	日志聚合开关开启，TCP目的端口为139，标志位为URG且紧急指针非零的IPV4报文数超过1，聚合后触发日志
处理建议	无

9.182 ATK_IP4_TCP_WINNUKE_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TCP_WINNUKE_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，TCP目的端口为139，标志位为URG且紧急指针非零的IPV4报文首包触发日志；日志聚合开关关闭，每个TCP目的端口为139，标志位为URG且紧急指针非零的IPV4报文触发一个日志
处理建议	无

9.183 ATK_IP4_TCP_WINNUKE_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TCP_WINNUKE_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，TCP目的端口为139，标志位为URG且紧急指针非零的IPV4报文首包触发日志；日志聚合开关关闭，每个TCP目的端口为139，标志位为URG且紧急指针非零的IPV4报文触发一个日志
处理建议	无

9.184 ATK_IP4_TCP_WINNUKE_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_IP4_TCP_WINNUKE_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=5.
日志说明	日志聚合开关开启，TCP目的端口为139，标志位为URG且紧急指针非零的IPV4报文数超过1，聚合后触发日志
处理建议	无

9.185 ATK_IP4_TEARDROP

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：协议类型 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	3
举例	ATK/3/ATK_IP4_TEARDROP: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=TCP; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=3.
日志说明	日志聚合开关开启，重叠偏移的报文数超过1，聚合后触发日志
处理建议	无

9.186 ATK_IP4_TEARDROP_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：协议类型 $7：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TEARDROP_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=TCP; Action(1049)=logging.
日志说明	日志聚合开关开启，重叠偏移的报文首包触发日志；日志聚合开关关闭，每个重叠偏移的报文触发一个日志
处理建议	无

9.187 ATK_IP4_TEARDROP_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：协议类型 $7：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TEARDROP_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=TCP; Action(1049)=logging.
日志说明	日志聚合开关开启，重叠偏移的报文首包触发日志；日志聚合开关关闭，每个重叠偏移的报文触发一个日志
处理建议	无

9.188 ATK_IP4_TEARDROP_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：协议类型 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	3
举例	ATK/3/ATK_IP4_TEARDROP_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=TCP; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=3.
日志说明	日志聚合开关开启，重叠偏移的报文数超过1，聚合后触发日志
处理建议	无

9.189 ATK_IP4_TINY_FRAGMENT

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：协议类型 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	3
举例	ATK/3/ATK_IP4_TINY_FRAGMENT: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=TCP; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=6.
日志说明	日志聚合开关开启，分片标志位IP_MF置位且IP数据包的长度小于68的报文数超过1，聚合后触发日志
处理建议	无

9.190 ATK_IP4_TINY_FRAGMENT_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：协议类型 $7：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TINY_FRAGMENT_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=TCP; Action(1049)=logging.
日志说明	日志聚合开关开启，分片标志位IP_MF置位且IP数据包的长度小于68的报文首包触发日志；日志聚合开关关闭，每个分片标志位IP_MF置位且IP数据包的长度小于68的报文触发一个日志
处理建议	无

9.191 ATK_IP4_TINY_FRAGMENT_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：协议类型 $7：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TINY_FRAGMENT_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=TCP; Action(1049)=logging.
日志说明	日志聚合开关开启，分片标志位IP_MF置位且IP数据包的长度小于68的报文首包触发日志；日志聚合开关关闭，每个分片标志位IP_MF置位且IP数据包的长度小于68的报文触发一个日志
处理建议	无

9.192 ATK_IP4_TINY_FRAGMENT_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：协议类型 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	3
举例	ATK/3/ATK_IP4_TINY_FRAGMENT_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=TCP; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=6.
日志说明	日志聚合开关开启，分片标志位IP_MF置位且IP数据包的长度小于68的报文数超过1，聚合后触发日志
处理建议	无

9.193 ATK_IP4_UDP_BOMB

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_IP4_UDP_BOMB: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，满足IP报文长度-IP首部>数据报长度的UDP报文数超过1，聚合后触发日志
处理建议	无

9.194 ATK_IP4_UDP_BOMB_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_UDP_BOMB_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，满足IP报文长度-IP首部>数据报长度的UDP报文首包触发日志；日志聚合开关关闭，每个满足IP报文长度-IP首部>数据报长度的UDP报文触发一个日志
处理建议	无

9.195 ATK_IP4_UDP_BOMB_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_UDP_BOMB_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，满足IP报文长度-IP首部>数据报长度的UDP报文首包触发日志；日志聚合开关关闭，每个满足IP报文长度-IP首部>数据报长度的UDP报文触发一个日志
处理建议	无

9.196 ATK_IP4_UDP_BOMB_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_IP4_UDP_BOMB_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，满足IP报文长度-IP首部>数据报长度的UDP报文数超过1，聚合后触发日志
处理建议	无

9.197 ATK_IP4_UDP_FLOOD

日志内容	RcvIfName(1023)=[STRING]; DstIPAddr(1007)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：目的IP地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP4_UDP_FLOOD: RcvIfName(1023)=Ethernet0/0/2; DstIPAddr(1007)=6.1.1.5; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	单位时间内指定IPV4目的地址的UDP报文数超过阈值，触发日志
处理建议	无

9.198 ATK_IP4_UDP_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING]; DstIPAddr(1007)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：目的IP地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP4_UDP_FLOOD_SZ: SrcZoneName(1025)=Trust; DstIPAddr(1007)=6.1.1.5; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	单位时间内指定IPV4目的地址的UDP报文数超过阈值，触发日志
处理建议	无

9.199 ATK_IP4_UDP_FRAGGLE

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_IP4_UDP_FRAGGLE: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=11.
日志说明	日志聚合开关开启，满足IPV4源端口为7，目的端口为19的UDP报文数超过1，聚合后触发日志
处理建议	无

9.200 ATK_IP4_UDP_FRAGGLE_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_UDP_FRAGGLE_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，IPV4源端口为7，目的端口为19的UDP报文首包触发日志；日志聚合开关关闭，每个IPV4源端口为7，目的端口为19的UDP报文触发一个日志
处理建议	无

9.201 ATK_IP4_UDP_FRAGGLE_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_UDP_FRAGGLE_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，IPV4源端口为7，目的端口为19的UDP报文首包触发日志；日志聚合开关关闭，每个IPV4源端口为7，目的端口为19的UDP报文触发一个日志
处理建议	无

9.202 ATK_IP4_UDP_FRAGGLE_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_IP4_UDP_FRAGGLE_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=11.
日志说明	日志聚合开关开启，满足IPV4源端口为7，目的端口为19的UDP报文数超过1，聚合后触发日志
处理建议	无

9.203 ATK_IP4_UDP_SNORK

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_IP4_UDP_SNORK: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，IPV4源端口为7、19或135，目的端口为135的UDP报文数超过1，聚合后触发日志
处理建议	无

9.204 ATK_IP4_UDP_SNORK_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_UDP_SNORK_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，IPV4源端口为7、19或135，目的端口为135的UDP报文首包触发日志；日志聚合开关关闭，每个IPV4源端口为7、19或135，目的端口为135的UDP报文触发一个日志
处理建议	无

9.205 ATK_IP4_UDP_SNORK_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_UDP_SNORK_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，IPV4源端口为7、19或135，目的端口为135的UDP报文首包触发日志；日志聚合开关关闭，每个IPV4源端口为7、19或135，目的端口为135的UDP报文触发一个日志
处理建议	无

9.206 ATK_IP4_UDP_SNORK_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_IP4_UDP_SNORK_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，IPV4源端口为7、19或135，目的端口为135的UDP报文数超过1，聚合后触发日志
处理建议	无

9.207 ATK_IP6_ACK_FLOOD

日志内容	RcvIfName(1023)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：目的IPv6地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP6_ACK_FLOOD: RcvIfName(1023)=Ethernet0/0/2; DstIPv6Addr(1037)=2::2; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009100434.
日志说明	单位时间内指定目的地址的TCP标志位为ACK的IPV6报文数超过阈值，触发日志
处理建议	无

9.208 ATK_IP6_ACK_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：目的IPv6地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP6_ACK_FLOOD_SZ: SrcZoneName(1025)=Trust; DstIPv6Addr(1037)=2::2; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009100434.
日志说明	单位时间内指定目的地址的TCP标志位为ACK的IPV6报文数超过阈值，触发日志
处理建议	无

9.209 ATK_IP6_DIS_PORTSCAN

日志内容	RcvIfName(1023)=[STRING]; Protocol(1001)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：协议名称 $3：目的IPv6地址 $4：VPN名称 $5：动作类型 $6：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP6_DIS_PORTSCAN: RcvIfName(1023)=Ethernet0/0/2; Protocol(1001)=UDP; DstIPv6Addr(1037)=2::2; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009100928.
日志说明	IPV6报文满足分布式port scan时触发日志
处理建议	无

9.210 ATK_IP6_DIS_PORTSCAN_SZ

日志内容	SrcZoneName(1025)=[STRING]; Protocol(1001)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：协议名称 $3：目的IPv6地址 $4：VPN名称 $5：动作类型 $6：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP6_DIS_PORTSCAN_SZ: SrcZoneName(1025)=Trust; Protocol(1001)=TCP; DstIPv6Addr(1037)=2::2; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009100928.
日志说明	IPV6报文满足分布式port scan时触发日志
处理建议	无

9.211 ATK_IP6_DNS_FLOOD

日志内容	RcvIfName(1023)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：目的IPv6地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP6_DNS_FLOOD: RcvIfName(1023)=Ethernet0/0/2; DstIPv6Addr(1037)=2::2; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009100434.
日志说明	单位时间内向指定目的IP发送DNS Query的IPV6报文数超过阈值，触发日志发送
处理建议	无

9.212 ATK_IP6_DNS_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：目的IPv6地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP6_DNS_FLOOD_SZ: SrcZoneName(1025)=Trust; DstIPv6Addr(1037)=2::2; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009100434.
日志说明	单位时间内向指定目的IP发送DNS Query的IPV6报文数超过阈值，触发日志发送
处理建议	无

9.213 ATK_IP6_FIN_FLOOD

日志内容	RcvIfName(1023)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：目的IPv6地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP6_FIN_FLOOD: RcvIfName(1023)=Ethernet0/0/2; DstIPv6Addr(1037)=2::2; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009100434.
日志说明	单位时间内向指定目的IP发送的TCP标志位为SYN+ACK的IPV6报文数超过阈值，触发日志发送
处理建议	无

9.214 ATK_IP6_FIN_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：目的IPv6地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP6_FIN_FLOOD_SZ: SrcZoneName(1025)=Trust; DstIPv6Addr(1037)=2::2; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009100434.
日志说明	单位时间内向指定目的IP发送的TCP标志位为SYN+ACK的IPV6报文数超过阈值，触发日志发送
处理建议	无

9.215 ATK_IP6_FRAGMENT

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：协议类型 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_FRAGMENT: RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=1::1; RcvVPNInstance(1041)=--; Protocol(1001)=IPv6-ICMP; Action(1049)=logging; BeginTime_c(1011)=20131011103335; EndTime_c(1012)=20131011103835; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，偏移量OffSet值在(0,5)之间的IPV6报文数超过1，聚合后触发日志
处理建议	无

9.216 ATK_IP6_FRAGMENT_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：协议名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_FRAGMENT_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=1::1; RcvVPNInstance(1041)=--; Protocol(1001)=IPv6-ICMP; Action(1049)=logging.
日志说明	日志聚合开关开启，偏移量OffSet值在(0,5)之间的IPV6报文首包触发日志；日志聚合开关关闭，每个偏移量OffSet值在(0,5)之间的IPV6报文触发一个日志
处理建议	无

9.217 ATK_IP6_FRAGMENT_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：协议名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_FRAGMENT_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=1::1; RcvVPNInstance(1041)=--; Protocol(1001)=IPv6-ICMP; Action(1049)=logging.
日志说明	日志聚合开关开启，偏移量OffSet值在(0,5)之间的IPV6报文首包触发日志；日志聚合开关关闭，每个偏移量OffSet值在(0,5)之间的IPV6报文触发一个日志
处理建议	无

9.218 ATK_IP6_FRAGMENT_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：协议类型 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_FRAGMENT_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=1::1; RcvVPNInstance(1041)=--; Protocol(1001)=IPv6-ICMP; Action(1049)=logging; BeginTime_c(1011)=20131011103335; EndTime_c(1012)=20131011103835; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，偏移量OffSet值在(0,5)之间的IPV6报文数超过1，聚合后触发日志
处理建议	无

9.219 ATK_IP6_HTTP_FLOOD

日志内容	RcvIfName(1023)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：目的IPv6地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP6_HTTP_FLOOD: RcvIfName(1023)=Ethernet0/0/2; DstIPv6Addr(1037)=2::2; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009100434.
日志说明	单位时间内向指定目的IP发送的HTTP的IPV6 Get报文数超过阈值，触发日志发送
处理建议	无

9.220 ATK_IP6_HTTP_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：目的IPv6地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP6_HTTP_FLOOD_SZ: SrcZoneName(1025)=Trust; DstIPv6Addr(1037)=2::2; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009100434.
日志说明	单位时间内向指定目的IP发送的HTTP的IPV6 Get报文数超过阈值，触发日志发送
处理建议	无

9.221 ATK_IP6_IMPOSSIBLE

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：协议类型 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_IMPOSSIBLE: RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=1::1; RcvVPNInstance(1041)=--; Protocol(1001)=IPv6-ICMP; Action(1049)=logging; BeginTime_c(1011)=20131011103335; EndTime_c(1012)=20131011103835; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，源目的地址相同的IPV6报文数超过1，聚合后触发日志
处理建议	无

9.222 ATK_IP6_IMPOSSIBLE_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：协议名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_IMPOSSIBLE_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=1::1; RcvVPNInstance(1041)=--; Protocol(1001)=IPv6-ICMP; Action(1049)=logging.
日志说明	日志聚合开关开启，源目的地址相同的IPV4报文首包触发日志；日志聚合开关关闭，每个源目的地址相同的IPV4报文触发一个日志
处理建议	无

9.223 ATK_IP6_IMPOSSIBLE_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：协议名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_IMPOSSIBLE_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=1::1; RcvVPNInstance(1041)=--; Protocol(1001)=IPv6-ICMP; Action(1049)=logging.
日志说明	日志聚合开关开启，源目的地址相同的IPV4报文首包触发日志；日志聚合开关关闭，每个源目的地址相同的IPV4报文触发一个日志
处理建议	无

9.224 ATK_IP6_IMPOSSIBLE_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：协议类型 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_IMPOSSIBLE_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=1::1; RcvVPNInstance(1041)=--; Protocol(1001)=IPv6-ICMP; Action(1049)=logging; BeginTime_c(1011)=20131011103335; EndTime_c(1012)=20131011103835; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，源目的地址相同的IPV6报文数超过1，聚合后触发日志
处理建议	无

9.225 ATK_IP6_IPSWEEP

日志内容	RcvIfName(1023)=[STRING]; Protocol(1001)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：协议名称 $3：源IPv6地址 $4：VPN名称 $5：动作类型 $6：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP6_IPSWEEP: RcvIfName(1023)=Ethernet0/0/2; Protocol(1001)=UDP; SrcIPv6Addr(1036)=1::5; RcvVPNInstance(1041)=--; Action(1049)=logging,block-source; BeginTime_c(1011)=20131009100639.
日志说明	IPV6报文满足ip sweep时触发日志
处理建议	无

9.226 ATK_IP6_IPSWEEP_SZ

日志内容	SrcZoneName(1025)=[STRING]; Protocol(1001)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：协议名称 $3：源IPv6地址 $4：VPN名称 $5：动作类型 $6：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP6_IPSWEEP_SZ: SrcZoneName(1025)=Trust; Protocol(1001)=TCP; SrcIPv6Addr(1036)=1::5; RcvVPNInstance(1041)=--; Action(1049)=logging,block-source; BeginTime_c(1011)=20131009100639.
日志说明	IPV6报文满足ip sweep时触发日志
处理建议	无

9.227 ATK_IP6_PORTSCAN

日志内容	RcvIfName(1023)=[STRING]; Protocol(1001)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：协议名称 $3：源IPv6地址 $4：VPN名称 $5：目的IPv6地址 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP6_PORTSCAN: RcvIfName(1023)=Ethernet0/0/2; Protocol(1001)=UDP; SrcIPv6Addr(1036)=1::5; RcvVPNInstance(1041)=--; DstIPv6Addr(1037)=2::2; Action(1049)=logging,block-source; BeginTime_c(1011)=20131009100455.
日志说明	IPV6报文满足port scan时触发日志
处理建议	无

9.228 ATK_IP6_PORTSCAN_SZ

日志内容	SrcZoneName(1025)=[STRING]; Protocol(1001)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：协议名称 $3：源IPv6地址 $4：VPN名称 $5：目的IPv6地址 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP6_PORTSCAN_SZ: SrcZoneName(1025)=Trust; Protocol(1001)=TCP; SrcIPv6Addr(1036)=1::5; RcvVPNInstance(1041)=--; DstIPv6Addr(1037)=2::2; Action(1049)=logging,block-source; BeginTime_c(1011)=20131009100455.
日志说明	IPV6报文满足port scan时触发日志
处理建议	无

9.229 ATK_IP6_RST_FLOOD

日志内容	RcvIfName(1023)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：目的IPv6地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP6_RST_FLOOD: RcvIfName(1023)=Ethernet0/0/2; DstIPv6Addr(1037)=2::2; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009100434.
日志说明	单位时间内指定目的地址的TCP标志位为RST的IPV6报文数超过阈值，触发日志
处理建议	无

9.230 ATK_IP6_RST_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：目的IPv6地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP6_RST_FLOOD_SZ: SrcZoneName(1025)=Trust; DstIPv6Addr(1037)=2::2; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009100434.
日志说明	单位时间内指定目的地址的TCP标志位为RST的IPV6报文数超过阈值，触发日志
处理建议	无

9.231 ATK_IP6_SYN_FLOOD

日志内容	RcvIfName(1023)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：目的IPv6地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP6_SYN_FLOOD: RcvIfName(1023)=Ethernet0/0/2; DstIPv6Addr(1037)=2::2; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009100434.
日志说明	满足周期内指定目的地址的TCP标志位为SYN的IPV6报文数超过阈值，触发日志
处理建议	无

9.232 ATK_IP6_SYN_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：目的IPv6地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP6_SYN_FLOOD_SZ: SrcZoneName(1025)=Trust; DstIPv6Addr(1037)=2::2; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009100434.
日志说明	满足周期内指定目的地址的TCP标志位为SYN的IPV6报文数超过阈值，触发日志
处理建议	无

9.233 ATK_IP6_SYNACK_FLOOD

日志内容	RcvIfName(1023)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：目的IPv6地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP6_SYNACK_FLOOD: RcvIfName(1023)=Ethernet0/0/2; DstIPv6Addr(1037)=2::2; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009100434.
日志说明	单位时间内指定目的地址的TCP标志位为SYN+ACK的IPV6报文数超过阈值，触发日志
处理建议	无

9.234 ATK_IP6_SYNACK_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：目的IPv6地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP6_SYNACK_FLOOD_SZ: SrcZoneName(1025)=Trust; DstIPv6Addr(1037)=2::2; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009100434.
日志说明	单位时间内指定目的地址的TCP标志位为SYN+ACK的IPV6报文数超过阈值，触发日志
处理建议	无

9.235 ATK_IP6_TCP_ALLFLAGS

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_TCP_ALLFLAGS: RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，TCP标志位全置位的IPV6报文数超过1，聚合后触发日志
处理建议	无

9.236 ATK_IP6_TCP_ALLFLAGS_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_TCP_ALLFLAGS_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=2000::1; DstIPv6Addr(1037)=2003::200; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，TCP标志位全置位的IPV6报文首包触发日志；日志聚合开关关闭，每个TCP标志位全置位的IPV6报文触发一个日志
处理建议	无

9.237 ATK_IP6_TCP_ALLFLAGS_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_TCP_ALLFLAGS_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=2000::1; DstIPv6Addr(1037)=2003::200; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，TCP标志位全置位的IPV6报文首包触发日志；日志聚合开关关闭，每个TCP标志位全置位的IPV6报文触发一个日志
处理建议	无

9.238 ATK_IP6_TCP_ALLFLAGS_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_TCP_ALLFLAGS_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，TCP标志位全置位的IPV6报文数超过1，聚合后触发日志
处理建议	无

9.239 ATK_IP6_TCP_FINONLY

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_TCP_FINONLY: RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，TCP标志位为FIN的IPV6报文数超过1，聚合后触发日志
处理建议	无

9.240 ATK_IP6_TCP_FINONLY_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_TCP_FINONLY_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=2000::1; DstIPv6Addr(1037)=2003::200; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，TCP标志位为FIN的IPV6报文首包触发日志；日志聚合开关关闭，每个TCP标志位为FIN的IPV6报文触发一个日志
处理建议	无

9.241 ATK_IP6_TCP_FINONLY_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_TCP_FINONLY_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=2000::1; DstIPv6Addr(1037)=2003::200; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，TCP标志位为FIN的IPV6报文首包触发日志；日志聚合开关关闭，每个TCP标志位为FIN的IPV6报文触发一个日志
处理建议	无

9.242 ATK_IP6_TCP_FINONLY_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_TCP_FINONLY_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，TCP标志位为FIN的IPV6报文数超过1，聚合后触发日志
处理建议	无

9.243 ATK_IP6_TCP_INVALIDFLAGS

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_TCP_INVALIDFLAGS: RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，TCP标志位为无效（RST+FIN、RST+SYN、RST+FIN+SYN、PSH+RST+FIN、PSH+RST+SYN、PSH+RST+SYN+FIN、ACK+RST+FIN、ACK+RST+SYN、ACK+RST+SYN+FIN、ACK+PSH+SYN+FIN、ACK+PSH+RST+FIN、ACK+PSH+RST+SYN）时的IPV6报文数超过1，聚合后触发日志
处理建议	无

9.244 ATK_IP6_TCP_INVALIDFLAGS_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_TCP_INVALIDFLAGS_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=2000::1; DstIPv6Addr(1037)=2003::200; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，TCP标志位为无效（RST+FIN、RST+SYN、RST+FIN+SYN、PSH+RST+FIN、PSH+RST+SYN、PSH+RST+SYN+FIN、ACK+RST+FIN、ACK+RST+SYN、ACK+RST+SYN+FIN、ACK+PSH+SYN+FIN、ACK+PSH+RST+FIN、ACK+PSH+RST+SYN）时的IPV6 TCP报文首包触发日志 日志聚合开关关闭，每个TCP标志位为无效时的IPV6 TCP报文触发一个日志
处理建议	无

9.245 ATK_IP6_TCP_INVALIDFLAGS_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_TCP_INVALIDFLAGS_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=2000::1; DstIPv6Addr(1037)=2003::200; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，TCP标志位为无效（RST+FIN、RST+SYN、RST+FIN+SYN、PSH+RST+FIN、PSH+RST+SYN、PSH+RST+SYN+FIN、ACK+RST+FIN、ACK+RST+SYN、ACK+RST+SYN+FIN、ACK+PSH+SYN+FIN、ACK+PSH+RST+FIN、ACK+PSH+RST+SYN）时的IPV6 TCP报文首包触发日志 日志聚合开关关闭，每个TCP标志位为无效时的IPV6 TCP报文触发一个日志
处理建议	无

9.246 ATK_IP6_TCP_INVALIDFLAGS_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_TCP_INVALIDFLAGS_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，TCP标志位为无效（RST+FIN、RST+SYN、RST+FIN+SYN、PSH+RST+FIN、PSH+RST+SYN、PSH+RST+SYN+FIN、ACK+RST+FIN、ACK+RST+SYN、ACK+RST+SYN+FIN、ACK+PSH+SYN+FIN、ACK+PSH+RST+FIN、ACK+PSH+RST+SYN）时的IPV6报文数超过1，聚合后触发日志
处理建议	无

9.247 ATK_IP6_TCP_LAND

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_TCP_LAND: RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，IPV6源目的地址相同的TCP报文数超过1，聚合后触发日志
处理建议	无

9.248 ATK_IP6_TCP_LAND_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_TCP_LAND_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=2000::1; DstIPv6Addr(1037)=2003::200; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，IPV6源目的地址相同的TCP报文首包触发日志；日志聚合开关关闭，每个IPV6源目的地址相同的TCP报文触发一个日志
处理建议	无

9.249 ATK_IP6_TCP_LAND_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_TCP_LAND_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=2000::1; DstIPv6Addr(1037)=2003::200; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，IPV6源目的地址相同的TCP报文首包触发日志；日志聚合开关关闭，每个IPV6源目的地址相同的TCP报文触发一个日志
处理建议	无

9.250 ATK_IP6_TCP_LAND_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_TCP_LAND_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，IPV6源目的地址相同的TCP报文数超过1，聚合后触发日志
处理建议	无

9.251 ATK_IP6_TCP_NULLFLAG

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_TCP_NULLFLAG: RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，TCP标志位未置位的IPV6报文数超过1，聚合后触发日志
处理建议	无

9.252 ATK_IP6_TCP_NULLFLAG_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_TCP_NULLFLAG_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=2000::1; DstIPv6Addr(1037)=2003::200; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，TCP标志位未置位的IPV6报文首包触发日志；日志聚合开关关闭，每个TCP标志位未置位的IPV6报文触发一个日志
处理建议	无

9.253 ATK_IP6_TCP_NULLFLAG_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_TCP_NULLFLAG_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=2000::1; DstIPv6Addr(1037)=2003::200; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，TCP标志位未置位的IPV6报文首包触发日志；日志聚合开关关闭，每个TCP标志位未置位的IPV6报文触发一个日志
处理建议	无

9.254 ATK_IP6_TCP_NULLFLAG_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_TCP_NULLFLAG_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，TCP标志位未置位的IPV6报文数超过1，聚合后触发日志
处理建议	无

9.255 ATK_IP6_TCP_SYNFIN

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_TCP_SYNFIN: RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，TCP标志位为SYN+FIN的IPV6报文数超过1，聚合后触发日志
处理建议	无

9.256 ATK_IP6_TCP_SYNFIN_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_TCP_SYNFIN_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=2000::1; DstIPv6Addr(1037)=2003::200; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，TCP标志位为SYN+FIN的IPV6报文首包触发日志；日志聚合开关关闭，每个TCP标志位为SYN+FIN的IPV6报文触发一个日志
处理建议	无

9.257 ATK_IP6_TCP_SYNFIN_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_TCP_SYNFIN_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=2000::1; DstIPv6Addr(1037)=2003::200; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，TCP标志位为SYN+FIN的IPV6报文首包触发日志；日志聚合开关关闭，每个TCP标志位为SYN+FIN的IPV6报文触发一个日志
处理建议	无

9.258 ATK_IP6_TCP_SYNFIN_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_TCP_SYNFIN_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，TCP标志位为SYN+FIN的IPV6报文数超过1，聚合后触发日志
处理建议	无

9.259 ATK_IP6_TCP_WINNUKE

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_TCP_WINNUKE: RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，TCP目的端口为139，标志位为URG且紧急指针非零的IPV6报文数超过1，聚合后触发日志
处理建议	无

9.260 ATK_IP6_TCP_WINNUKE_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_TCP_WINNUKE_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，TCP目的端口为139，标志位为URG且紧急指针非零的IPV6报文首包触发日志；日志聚合开关关闭，每个TCP目的端口为139，标志位为URG且紧急指针非零的IPV6报文触发一个日志
处理建议	无

9.261 ATK_IP6_TCP_WINNUKE_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_TCP_WINNUKE_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，TCP目的端口为139，标志位为URG且紧急指针非零的IPV6报文首包触发日志；日志聚合开关关闭，每个TCP目的端口为139，标志位为URG且紧急指针非零的IPV6报文触发一个日志
处理建议	无

9.262 ATK_IP6_TCP_WINNUKE_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_TCP_WINNUKE_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，TCP目的端口为139，标志位为URG且紧急指针非零的IPV6报文数超过1，聚合后触发日志
处理建议	无

9.263 ATK_IP6_UDP_FLOOD

日志内容	RcvIfName(1023)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：目的IPv6地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP6_UDP_FLOOD: RcvIfName(1023)=Ethernet0/0/2; DstIPv6Addr(1037)=2::2; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009100434.
日志说明	单位时间内指定IPV6目的地址的UDP报文数超过阈值，触发日志
处理建议	无

9.264 ATK_IP6_UDP_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：目的IPv6地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP6_UDP_FLOOD_SZ: SrcZoneName(1025)=Trust; DstIPv6Addr(1037)=2::2; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009100434.
日志说明	单位时间内指定IPV6目的地址的UDP报文数超过阈值，触发日志
处理建议	无

9.265 ATK_IP6_UDP_FRAGGLE

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_UDP_FRAGGLE: RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，IPV6源端口为7，目的端口为19的UDP报文数超过1，聚合后触发日志
处理建议	无

9.266 ATK_IP6_UDP_FRAGGLE_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_UDP_FRAGGLE_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，IPV6源端口为7，目的端口为19的UDP报文首包触发日志；日志聚合开关关闭，每个IPV6源端口为7，目的端口为19的UDP报文触发一个日志
处理建议	无

9.267 ATK_IP6_UDP_FRAGGLE_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_UDP_FRAGGLE_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，IPV6源端口为7，目的端口为19的UDP报文首包触发日志；日志聚合开关关闭，每个IPV6源端口为7，目的端口为19的UDP报文触发一个日志
处理建议	无

9.268 ATK_IP6_UDP_FRAGGLE_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_UDP_FRAGGLE_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，IPV6源端口为7，目的端口为19的UDP报文数超过1，聚合后触发日志
处理建议	无

9.269 ATK_IP6_UDP_SNORK

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_UDP_SNORK: RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，IPV6源端口为7、19或135，目的端口为135的UDP报文数超过1，聚合后触发日志
处理建议	无

9.270 ATK_IP6_UDP_SNORK_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_UDP_SNORK_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，IPV6源端口为7、19或135，目的端口为135的UDP报文首包触发日志；日志聚合开关关闭，每个IPV6源端口为7、19或135，目的端口为135的UDP报文触发一个日志
处理建议	无

9.271 ATK_IP6_UDP_SNORK_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_UDP_SNORK_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，IPV6源端口为7、19或135，目的端口为135的UDP报文首包触发日志；日志聚合开关关闭，每个IPV6源端口为7、19或135，目的端口为135的UDP报文触发一个日志
处理建议	无

9.272 ATK_IP6_UDP_SNORK_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_UDP_SNORK_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，IPV6源端口为7、19或135，目的端口为135的UDP报文数超过1，聚合后触发日志
处理建议	无

9.273 ATK_IPOPT_ABNORMAL

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：协议类型 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	3
举例	ATK/3/ATK_IPOPT_ABNORMAL: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging; BeginTime_c(1011)=20131011072002; EndTime_c(1012)=20131011072502; AtkTimes(1050)=3.
日志说明	日志聚合开关打开，两个以上IP选项置位的报文数超过1，聚合后触发日志
处理建议	无

9.274 ATK_IPOPT_ABNORMAL_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：协议类型 $7：动作类型
日志等级	3
举例	ATK/3/ATK_IPOPT_ABNORMAL_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging.
日志说明	日志聚合开关开启，两个以上IP选项置位的报文首包触发日志；日志聚合开关关闭，每个两个以上IP选项置位的报文触发一个日志
处理建议	无

9.275 ATK_IPOPT_ABNORMAL_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：协议类型 $7：动作类型
日志等级	3
举例	ATK/3/ATK_IPOPT_ABNORMAL_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging.
日志说明	日志聚合开关开启，两个以上IP选项置位的报文首包触发日志；日志聚合开关关闭，每个两个以上IP选项置位的报文触发一个日志
处理建议	无

9.276 ATK_IPOPT_ABNORMAL_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：协议类型 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	3
举例	ATK/3/ATK_IPOPT_ABNORMAL_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging; BeginTime_c(1011)=20131011072002; EndTime_c(1012)=20131011072502; AtkTimes(1050)=3.
日志说明	日志聚合开关打开，两个以上IP选项置位的报文数超过1，聚合后触发日志
处理建议	无

9.277 ATK_IPOPT_LOOSESRCROUTE

日志内容	IPOptValue(1057)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：IP选项值 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5
举例	ATK/5/ATK_IPOPT_LOOSESRCROUTE: IPOptValue(1057)=131; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging; BeginTime_c(1011)=20131011063123; EndTime_c(1012)=20131011063623; AtkTimes(1050)=3.
日志说明	日志聚合开关打开，IP选项为131的报文数超过1，聚合后触发日志
处理建议	无

9.278 ATK_IPOPT_LOOSESRCROUTE_RAW

日志内容	IPOptValue(1057)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：IP选项值 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型
日志等级	5
举例	ATK/5/ATK_IPOPT_LOOSESRCROUTE_RAW: IPOptValue(1057)=131; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging.
日志说明	日志聚合开关开启，IP选项为131的报文首包触发日志；日志聚合开关关闭，每个IP选项为131的报文触发一个日志
处理建议	无

9.279 ATK_IPOPT_LOOSESRCROUTE_RAW_SZ

日志内容	IPOptValue(1057)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：IP选项值 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型
日志等级	5
举例	ATK/5/ATK_IPOPT_LOOSESRCROUTE_RAW_SZ: IPOptValue(1057)=131; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging.
日志说明	日志聚合开关开启，IP选项为131的报文首包触发日志；日志聚合开关关闭，每个IP选项为131的报文触发一个日志
处理建议	无

9.280 ATK_IPOPT_LOOSESRCROUTE_SZ

日志内容	IPOptValue(1057)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)= [UINT32].
参数解释	$1：IP选项值 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5
举例	ATK/5/ATK_IPOPT_LOOSESRCROUTE_SZ: IPOptValue(1057)=131; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging; BeginTime_c(1011)=20131011063123; EndTime_c(1012)=20131011063623; AtkTimes(1050)=3.
日志说明	日志聚合开关打开，IP选项为131的报文数超过1，聚合后触发日志
处理建议	无

9.281 ATK_IPOPT_RECORDROUTE

日志内容	IPOptValue(1057)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：IP选项值 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5
举例	ATK/5/ATK_IPOPT_RECORDROUTE: IPOptValue(1057)=7; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging; BeginTime_c(1011)=20131011063123; EndTime_c(1012)=20131011063623; AtkTimes(1050)=3.
日志说明	日志聚合开关打开，IP选项为7的报文数超过1，聚合后触发日志
处理建议	无

9.282 ATK_IPOPT_RECORDROUTE_RAW

日志内容	IPOptValue(1057)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：IP选项值 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型
日志等级	5
举例	ATK/5/ATK_IPOPT_RECORDROUTE_RAW: IPOptValue(1057)=7; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging.
日志说明	日志聚合开关开启，IP选项为7的报文首包触发日志；日志聚合开关关闭，每个IP选项为7的报文触发一个日志
处理建议	无

9.283 ATK_IPOPT_RECORDROUTE_RAW_SZ

日志内容	IPOptValue(1057)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：IP选项值 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型
日志等级	5
举例	ATK/5/ATK_IPOPT_RECORDROUTE_RAW_SZ: IPOptValue(1057)=7; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging.
日志说明	日志聚合开关开启，IP选项为7的报文首包触发日志；日志聚合开关关闭，每个IP选项为7的报文触发一个日志
处理建议	无

9.284 ATK_IPOPT_RECORDROUTE_SZ

日志内容	IPOptValue(1057)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：IP选项值 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5
举例	ATK/5/ATK_IPOPT_RECORDROUTE_SZ: IPOptValue(1057)=7; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging; BeginTime_c(1011)=20131011063123; EndTime_c(1012)=20131011063623; AtkTimes(1050)=3.
日志说明	日志聚合开关打开，IP选项为7的报文数超过1，聚合后触发日志
处理建议	无

9.285 ATK_IPOPT_ROUTEALERT

日志内容	IPOptValue(1057)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：IP选项值 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5
举例	ATK/5/ATK_IPOPT_ROUTEALERT: IPOptValue(1057)=148; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging; BeginTime_c(1011)=20131011063123; EndTime_c(1012)=20131011063623; AtkTimes(1050)=3.
日志说明	日志聚合开关打开，IP选项为148的报文数超过1，聚合后触发日志
处理建议	无

9.286 ATK_IPOPT_ROUTEALERT_RAW

日志内容	IPOptValue(1057)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：IP选项值 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型
日志等级	5
举例	ATK/5/ATK_IPOPT_ROUTEALERT_RAW: IPOptValue(1057)=148; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging.
日志说明	日志聚合开关开启，IP选项为148的报文首包触发日志；日志聚合开关关闭，每个IP选项为148的报文触发一个日志
处理建议	无

9.287 ATK_IPOPT_ROUTEALERT_RAW_SZ

日志内容	IPOptValue(1057)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：IP选项值 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型
日志等级	5
举例	ATK/5/ATK_IPOPT_ROUTEALERT_RAW_SZ: IPOptValue(1057)=148; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging.
日志说明	日志聚合开关开启，IP选项为148的报文首包触发日志；日志聚合开关关闭，每个IP选项为148的报文触发一个日志
处理建议	无

9.288 ATK_IPOPT_ROUTEALERT_SZ

日志内容	IPOptValue(1057)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：IP选项值 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5
举例	ATK/5/ATK_IPOPT_ROUTEALERT_SZ: IPOptValue(1057)=148; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging; BeginTime_c(1011)=20131011063123; EndTime_c(1012)=20131011063623; AtkTimes(1050)=3.
日志说明	日志聚合开关打开，IP选项为148的报文数超过1，聚合后触发日志
处理建议	无

9.289 ATK_IPOPT_SECURITY

日志内容	IPOptValue(1057)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：IP选项值 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5
举例	ATK/5/ATK_IPOPT_SECURITY: IPOptValue(1057)=130; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging; BeginTime_c(1011)=20131009091022; EndTime_c(1012)=20131009091522; AtkTimes(1050)=2.
日志说明	日志聚合开关打开，IP选项为130的报文数超过1，聚合后触发日志
处理建议	无

9.290 ATK_IPOPT_SECURITY_RAW

日志内容	IPOptValue(1057)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：IP选项值 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型
日志等级	5
举例	ATK/5/ATK_IPOPT_SECURITY_RAW: IPOptValue(1057)=130; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging.
日志说明	日志聚合开关开启，IP选项为130的报文首包触发日志；日志聚合开关关闭，每个IP选项为130的报文触发一个日志
处理建议	无

9.291 ATK_IPOPT_SECURITY_RAW_SZ

日志内容	IPOptValue(1057)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：IP选项值 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型
日志等级	5
举例	ATK/5/ATK_IPOPT_SECURITY_RAW_SZ: IPOptValue(1057)=130; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging.
日志说明	日志聚合开关开启，IP选项为130的报文首包触发日志；日志聚合开关关闭，每个IP选项为130的报文触发一个日志
处理建议	无

9.292 ATK_IPOPT_SECURITY_SZ

日志内容	IPOptValue(1057)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：IP选项值 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5
举例	ATK/5/ATK_IPOPT_SECURITY_SZ: IPOptValue(1057)=130; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging; BeginTime_c(1011)=20131009091022; EndTime_c(1012)=20131009091522; AtkTimes(1050)=2.
日志说明	日志聚合开关打开，IP选项为130的报文数超过1，聚合后触发日志
处理建议	无

9.293 ATK_IPOPT_STREAMID

日志内容	IPOptValue(1057)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：IP选项值 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5
举例	ATK/5/ATK_IPOPT_STREAMID: IPOptValue(1057)=136; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging; BeginTime_c(1011)=20131011063123; EndTime_c(1012)=20131011063623; AtkTimes(1050)=3.
日志说明	日志聚合开关打开，IP选项为136的报文数超过1，聚合后触发日志
处理建议	无

9.294 ATK_IPOPT_STREAMID_RAW

日志内容	IPOptValue(1057)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：IP选项值 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型
日志等级	5
举例	ATK/5/ATK_IPOPT_STREAMID_RAW: IPOptValue(1057)=136; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging.
日志说明	日志聚合开关开启，IP选项为136的报文首包触发日志；日志聚合开关关闭，每个IP选项为136的报文触发一个日志
处理建议	无

9.295 ATK_IPOPT_STREAMID_RAW_SZ

日志内容	IPOptValue(1057)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：IP选项值 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型
日志等级	5
举例	ATK/5/ATK_IPOPT_STREAMID_RAW_SZ: IPOptValue(1057)=136; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging.
日志说明	日志聚合开关开启，IP选项为136的报文首包触发日志；日志聚合开关关闭，每个IP选项为136的报文触发一个日志
处理建议	无

9.296 ATK_IPOPT_STREAMID_SZ

日志内容	IPOptValue(1057)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：IP选项值 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5
举例	ATK/5/ATK_IPOPT_STREAMID_SZ: IPOptValue(1057)=136; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging; BeginTime_c(1011)=20131011063123; EndTime_c(1012)=20131011063623; AtkTimes(1050)=3.
日志说明	日志聚合开关打开，IP选项为136的报文数超过1，聚合后触发日志
处理建议	无

9.297 ATK_IPOPT_STRICTSRCROUTE

日志内容	IPOptValue(1057)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：IP选项值 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5
举例	ATK/5/ATK_IPOPT_STRICTSRCROUTE: IPOptValue(1057)=137; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging; BeginTime_c(1011)=20131011063123; EndTime_c(1012)=20131011063623; AtkTimes(1050)=3.
日志说明	日志聚合开关打开，IP选项为137的报文数超过1，聚合后触发日志
处理建议	无

9.298 ATK_IPOPT_STRICTSRCROUTE_RAW

日志内容	IPOptValue(1057)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：IP选项值 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型
日志等级	5
举例	ATK/5/ATK_IPOPT_STRICTSRCROUTE_RAW: IPOptValue(1057)=137; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging.
日志说明	日志聚合开关开启，IP选项为137的报文首包触发日志；日志聚合开关关闭，每个IP选项为137的报文触发一个日志
处理建议	无

9.299 ATK_IPOPT_STRICTSRCROUTE_RAW_SZ

日志内容	IPOptValue(1057)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：IP选项值 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型
日志等级	5
举例	ATK/5/ATK_IPOPT_STRICTSRCROUTE_RAW_SZ: IPOptValue(1057)=137; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging.
日志说明	日志聚合开关开启，IP选项为137的报文首包触发日志；日志聚合开关关闭，每个IP选项为137的报文触发一个日志
处理建议	无

9.300 ATK_IPOPT_STRICTSRCROUTE_SZ

日志内容	IPOptValue(1057)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：IP选项值 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5
举例	ATK/5/ATK_IPOPT_STRICTSRCROUTE_SZ: IPOptValue(1057)=137; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging; BeginTime_c(1011)=20131011063123; EndTime_c(1012)=20131011063623; AtkTimes(1050)=3.
日志说明	日志聚合开关打开，IP选项为137的报文数超过1，聚合后触发日志
处理建议	无

9.301 ATK_IPOPT_TIMESTAMP

日志内容	IPOptValue(1057)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：IP选项值 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5
举例	ATK/5/ATK_IPOPT_TIMESTAMP: IPOptValue(1057)=68; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging; BeginTime_c(1011)=20131011063123; EndTime_c(1012)=20131011063623; AtkTimes(1050)=3.
日志说明	日志聚合开关打开，IP选项为68的报文数超过1，聚合后触发日志
处理建议	无

9.302 ATK_IPOPT_TIMESTAMP_RAW

日志内容	IPOptValue(1057)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：IP选项值 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型
日志等级	5
举例	ATK/5/ATK_IPOPT_TIMESTAMP_RAW: IPOptValue(1057)=68; RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging.
日志说明	日志聚合开关开启，IP选项为68的报文首包触发日志；日志聚合开关关闭，每个IP选项为68的报文触发一个日志
处理建议	无

9.303 ATK_IPOPT_TIMESTAMP_RAW_SZ

日志内容	IPOptValue(1057)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：IP选项值 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型
日志等级	5
举例	ATK/5/ATK_IPOPT_TIMESTAMP_RAW_SZ: IPOptValue(1057)=68; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging.
日志说明	日志聚合开关开启，IP选项为68的报文首包触发日志；日志聚合开关关闭，每个IP选项为68的报文触发一个日志
处理建议	无

9.304 ATK_IPOPT_TIMESTAMP_SZ

日志内容	IPOptValue(1057)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：IP选项值 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5
举例	ATK/5/ATK_IPOPT_TIMESTAMP_SZ: IPOptValue(1057)=68; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging; BeginTime_c(1011)=20131011063123; EndTime_c(1012)=20131011063623; AtkTimes(1050)=3.
日志说明	日志聚合开关打开，IP选项为68的报文数超过1，聚合后触发日志
处理建议	无

9.305 ATK_IPV6_EXT_HEADER

日志内容	IPv6ExtHeader(1060)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：IPv6 扩展头 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：入接口VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	5
举例	ATK/5/ATK_IPV6_EXT_HEADER: IPv6ExtHeader(1060)=43; RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	日志聚合开关打开，自定义扩展头的IPV6报文数超过1，聚合后触发日志
处理建议	无

9.306 ATK_IPV6_EXT_HEADER_ABNORMAL

日志内容	RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_IPV6_EXT_HEADER_ABNORMAL: RcvIfName(1023)=Ethernet0/0/2;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=--;Action(1053)=logging;BeginTime_c(1011)=20131009103631;EndTime_c(1012)=20131009104131;AtkTimes(1054)=2.
日志说明	日志聚合开关开启，扩展头个数超过配置的最大数目或者出现不允许重复扩展头的IPv6报文数超过1，触发一个日志
处理建议	无

9.307 ATK_IPV6_EXT_HEADER_ABNORMAL_RAW

日志内容	RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_IPV6_EXT_HEADER_RAW: IPv6ExtHeader(1066)=43;RcvIfName(1023)=Ethernet0/0/2;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=--;Action(1053)=logging.
日志说明	日志聚合开关关闭，扩展头个数超过配置的最大数目的每个IPv6报文触发一个日志
处理建议	无

9.308 ATK_IPV6_EXT_HEADER_ABNORMAL_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_IPV6_EXT_HEADER_ABNORMAL_RAW_SZ: SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=--;Action(1053)=logging.
日志说明	日志聚合开关关闭，扩展头个数超过配置的最大数目的每个IPv6报文触发一个日志
处理建议	无

9.309 ATK_IPV6_EXT_HEADER_ABNORMAL_SZ

日志内容	SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_IPV6_EXT_HEADER_ABNORMAL_SZ: SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=--;Action(1053)=logging;BeginTime_c(1011)=20131009103631;EndTime_c(1012)=20131009104131;AtkTimes(1054)=2.
日志说明	日志聚合开关开启，扩展头个数超过配置的最大数目或者出现不允许重复扩展头的IPv6报文数超过1，触发一个日志
处理建议	无

9.310 ATK_IPV6_EXT_HEADER_RAW

日志内容	IPv6ExtHeader(1060)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：IPv6 扩展头 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型
日志等级	5
举例	ATK/5/ATK_IPV6_EXT_HEADER_RAW: IPv6ExtHeader(1060)=43; RcvIfName(1023)=Ethernet0/0/2; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，自定义扩展头的IPV6报文首包触发日志；日志聚合开关关闭，每个自定义扩展头的IPV6报文触发一个日志
处理建议	无

9.311 ATK_IPV6_EXT_HEADER_RAW_SZ

日志内容	IPv6ExtHeader(1060)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：IPv6 扩展头 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型
日志等级	5
举例	ATK/5/ATK_IPV6_EXT_HEADER_RAW_SZ: IPv6ExtHeader(1060)=43; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，自定义扩展头的IPV6报文首包触发日志；日志聚合开关关闭，每个自定义扩展头的IPV6报文触发一个日志
处理建议	无

9.312 ATK_IPV6_EXT_HEADER_SZ

日志内容	IPv6ExtHeader(1060)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：IPv6 扩展头 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：入接口VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	5
举例	ATK/5/ATK_IPV6_EXT_HEADER_SZ: IPv6ExtHeader(1060)=43; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	日志聚合开关打开，自定义扩展头的IPV6报文数超过1，聚合后触发日志
处理建议	无

10 ATM

本节介绍 ATM 模块输出的日志信息。

10.1 ATM_PVCDOWN

日志内容	Interface [STRING] PVC [UINT16]/[UINT16] status is down.
参数解释	$1：PVC所属接口的名称 $2：PVC的VPI值 $3：PVC的VCI值
日志等级	5
举例	ATM/5/ATM_PVCDOWN: Interface ATM2/0/2 PVC 0/100 status is down.
日志说明	PVC的状态转变为down。触发该日志的原因可能有：PVC所属ATM接口状态转变为down、PVC的OAM状态转变为down或该PVC被shutdown

处理建议	1. 使用 **display atm pvc-info** 命令查看指定接口的 PVC 详细信息，根据显示信息进行如下处理：
	2. 如果 Interface State 字段显示为 DOWN
	• 使用 display interface atm 命令分别检查本端和对端的 ATM 接口是否被手动 shutdown，若是，可通过在接口上执行 undo shutdown 命令解决该问题
	• 检查接口之间的连线是否插好
	3. 如果 OAM State 字段显示为 DOWN
	• 当两台路由器直连时：
	  ○ 检查对端接口上创建的 PVC 的 *vpi/vci* 是否与本端相同
	  ○ 检查对端接口上 PVC 的 OAM 配置是否与本端一致（比如本端配置了 oam cc sink，对端需配置 oam cc source）
	  ○ 检查对端的 PVC 是否被手动 shutdown，若是，可通过在 PVC 视图上执行 undo shutdown 命令解决该问题
	  ○ 检查两端连线是否正确
	• 当两台路由器通过 ATM 交换网络连接时，除检查上述几点外，还需要检查交换网络中转发规则配置是否正确，如果两端 PVC 在交换网络中不可达，PVC 状态同样为 down
	4. 如果 PVC State 字段显示为 DOWN，请检查本端的 PVC 是否被手动 shutdown，若是，可通过在 PVC 视图上执行 undo shutdown 命令解决该问题

10.2 ATM_PVCUP

日志内容	Interface [STRING] PVC [UINT16]/[UINT16] status is up.
参数解释	$1：PVC所属接口的名称 $2：PVC的VPI值 $3：PVC的VCI值
日志等级	5
举例	ATM/5/ATM_PVCUP: Interface ATM2/0/2 PVC 0/100 status is up.
日志说明	PVC的状态转变为up
处理建议	1. 无需处理

10.3 ATM _FAILURE

日志内容	Operation Failed on pvc [UINT16]/[UINT16].
参数解释	$1: PVC的VPI/VCI
日志等级	3
举例	WAN/3/ATM: -MDC=1-Slot=4; Operation Failed on pvc 43/43
日志说明	在指定PVC上配置**service** { **cbrs** | **ubr** | **vbr-nrt** | **vbr-rt** }命令失败
处理建议	请联系H3C技术支持

10.4 ATM_PVCDOWN

日志内容	Interface$1 PVC$2/$3 status is down.
参数解释	$1：PVC所属接口的名称 $2：PVC的VPI值 $3：PVC的VCI值
日志等级	5
举例	ATM/5/ATM_PVCDOWN: Interface ATM2/0/2 PVC 0/100 status is down.
日志说明	PVC的状态转变为down。触发该日志的原因可能有：PVC所属ATM接口状态转变为down、PVC的OAM状态转变为down或该PVC被shutdown

处理建议	使用**display atm pvc-info interface** *interface-type* **pvc** *vpi/vci*命令查看指定接口的PVC详细信息，根据显示信息进行如下处理：
	1. 如果 Interface State 字段显示为 DOWN
	• 使用 **display interface atm** 命令分别检查本端和对端的 ATM 接口是否被手动 shutdown，可通过在接口上执行 **undo shutdown** 命令解决该问题
	• 检查接口之间的连线是否插好
	2. 如果 OAM State 字段显示为 DOWN
	• 当两台路由器直连时：
	  ○ 检查对端接口上创建的 PVC 的 *vpi/vci* 是否与本端相同
	  ○ 检查对端接口上 PVC 的 OAM 配置是否与本端一致（比如本端配置了 **oam cc sink**，对端需配置 **oam cc source**）
	  ○ 检查对端的 PVC 是否被手动 shutdown，可通过在 PVC 视图上执行 **undo shutdown** 命令解决该问题
	  ○ 检查两端连线是否正确
	• 当两台路由器通过 ATM 交换网络连接时，除检查上述几点外，还需要检查交换网络中转发规则配置是否正确，如果两端 PVC 在交换网络中不可达，PVC 状态同样为 down
	3. 如果 PVC State 字段显示为 DOWN，请检查本端的 PVC 是否被手动 shutdown，可通过在 PVC 视图上执行 **undo shutdown** 命令解决该问题

10.5 ATM_PVCUP

日志内容	Interface$1 PVC$2/$3 status is up.
参数解释	$1：PVC所属接口的名称 $2：PVC的VPI值 $3：PVC的VCI值
日志等级	5
举例	ATM/5/ATM_PVCUP: Interface ATM2/0/2 PVC 0/100 status is up.
日志说明	PVC的状态转变为up
处理建议	无

11 BFD

11.1 BFD_N

日志内容	Interface [STRING] has been configured as a dedicated BFD MAD port.
参数解释	$1：物理端口
日志等级	5
举例	BFD/5/BFD_N: -MDC=1-Chassis=1-Slot=9; Interface GE1/9/2/2 has been configured as a dedicated BFD MAD port.
日志说明	在IRF模式下，对于CSPEX类单板（除CSPEX-1204单板）和CEPC类单板，若单板上存在IRF物理口，则该单板仅有一个接口支持配置mad bfd dedicated功能
处理建议	**1.** 在该接口上执行 undo mad bfd dedicated 命令

11.2 BFD_CHANGE_FSM (Severity 4)

日志内容	Sess[STRING], Ver, Sta: [STRING]->[STRING], Diag: [UINT32]
参数解释	$1：BFD会话的源地址、目的地址、接口、消息类型和MPLS FEC信息。LSP会话中包含LSP目的IP、掩码及下一跳IP；PW会话中包含Peer IP和PW ID；TE Tunnel会话中包含源IP、目的IP、Tunnel ID及LSP ID $2：变化前会话状态的名称 $3：变化后会话状态的名称，包括UP和DOWN $4：诊断信息，包括 • 0 (No Diagnostic)：表示无诊断信息 • 1 (Control Detection Time Expired)：表示 Ctrl 会话本端检测时间超时，会话 down • 2 (Echo Function Failed)：表示 Echo 会话本端检测时间超时或 echo 报文的源 IP 地址被删除，会话 down • 3 (Neighbor Signaled Session Down)：表示对端通知本端 BFD 会话 down • 7 (Administratively Down)：表示本端系统阻止 BFD 会话的建立
日志等级	4
举例	BFD/4/BFD_CHANGE_FSM: Sess[20.0.4.2/20.0.4.1,LD/RD:533/532, Interface:Vlan204, SessType:Ctrl, LinkType:INET], Ver.1, Sta: INIT->UP, Diag: 0 (No Diagnostic). BFD/4/BFD_CHANGE_FSM: Sess[20.0.4.2/20.0.4.1,LD/RD:533/532, Interface: Vlan204, SessType: Ctrl, LinkType: LSP, FEC: LSP, 20.0.4.0/24/10.1.1.1], Ver.1, Sta: INIT->UP, Diag: 0 (No Diagnostic). BFD/4/BFD_CHANGE_FSM: Sess[20.0.4.2/20.0.4.1,LD/RD:533/532, Interface: Vlan204, SessType: Ctrl, LinkType: LSP, FEC: PW FEC-128, 20.0.4.2/1], Ver.1, Sta: INIT->UP, Diag: 0 (No Diagnostic). BFD/4/BFD_CHANGE_FSM: Sess[20.0.4.2/20.0.4.1,LD/RD:533/532, Interface: Vlan204, SessType: Ctrl, LinkType: LSP, FEC: TE Tunnel, 20.0.4.2/20.0.4.1/100/100], Ver.1, Sta: INIT->UP, Diag: 0 (No Diagnostic).
日志说明	BFD会话的状态发生变化。当BFD会话up或down时出现此信息。如果出现会话异常丢失的情况，可能由高错误率或高丢包率导致
处理建议	需要检查是否BFD配置的问题或网络出现拥塞

11.3 BFD_CHANGE_FSM (Severity 5)

日志内容	Sess[STRING], Ver, Sta: [STRING]->[STRING], Diag: [UINT32]
参数解释	$1：BFD会话的源地址、目的地址、接口、消息类型和MPLS FEC信息。LSP会话中包含LSP目的IP、掩码及下一跳IP；PW会话中包含Peer IP和PW ID；TE Tunnel会话中包含源IP、目的IP、Tunnel ID及LSP ID $2：变化前会话状态的名称 $3：变化后会话状态的名称，包括INIT、ADMIN-DOWN和FAIL $4：诊断信息，包括 • 0 (No Diagnostic)：表示无诊断信息 • 1 (Control Detection Time Expired)：表示 Ctrl 会话本端检测时间超时，会话 down • 2 (Echo Function Failed)：表示 Echo 会话本端检测时间超时或 echo 报文的源 IP 地址被删除，会话 down • 3 (Neighbor Signaled Session Down)：表示对端通知本端 BFD 会话 down • 7 (Administratively Down)：表示本端系统阻止 BFD 会话的建立
日志等级	5
举例	BFD/5/BFD_CHANGE_FSM: Sess[20.0.4.2/20.0.4.1,LD/RD:533/532, Interface:Vlan204, SessType:Ctrl, LinkType:INET], Ver.1, Sta: DOWN->INIT, Diag: 0 (No Diagnostic). BFD/5/BFD_CHANGE_FSM: Sess[20.0.4.2/20.0.4.1,LD/RD:533/532, Interface: Vlan204, SessType: Ctrl, LinkType: LSP, FEC: LSP, 20.0.4.0/24/10.1.1.1], Ver.1, Sta: DOWN->INIT, Diag: 0 (No Diagnostic). BFD/5/BFD_CHANGE_FSM: Sess[20.0.4.2/20.0.4.1,LD/RD:533/532, Interface: Vlan204, SessType: Ctrl, LinkType: LSP, FEC: PW FEC-128, 20.0.4.2/1], Ver.1, Sta: DOWN->INIT, Diag: 0 (No Diagnostic). BFD/5/BFD_CHANGE_FSM: Sess[20.0.4.2/20.0.4.1,LD/RD:533/532, Interface: Vlan204, SessType: Ctrl, LinkType: LSP, FEC: TE Tunnel, 20.0.4.2/20.0.4.1/100/100], Ver.1, Sta: DOWN->INIT, Diag: 0 (No Diagnostic).
日志说明	BFD会话的状态发生变化。当BFD会话状态变为INIT、ADMIN-DOWN或FAIL时出现此信息。如果出现会话异常丢失的情况，可能由高错误率或高丢包率导致
处理建议	需要检查是否BFD配置的问题或网络出现拥塞

11.4 BFD_CHANGE_SESS

日志内容	Sess[STRING], Ver, Sta: [STRING], Diag: [UINT32]
参数解释	$1：BFD会话的源地址、目的地址、接口、消息类型和MPLS FEC信息。LSP会话中包含LSP目的IP、掩码及下一跳IP；PW会话中包含Peer IP和PW ID；TE Tunnel会话中包含源IP、目的IP、Tunnel ID及LSP ID $2：会话状态 $3：诊断码
日志等级	5
举例	BFD/5/BFD_CHANGE_SESS: Sess[17.1.1.2/17.1.1.1, LD/RD:1537/1537, Interface:GE1/0/1, SessType:Ctrl, LinkType:INET], Ver:1, Sta: Deleted, Diag: 7 (Administratively Down)
日志说明	当BFD会话删除时出现此信息
处理建议	请检查BFD会话配置

11.5 BFD_REACHED_UPPER_LIMIT

日志内容	The total number of BFD sessions [ULONG] reached the upper limit. Can’t create a new session.
参数解释	$1：BFD会话总数
日志等级	3
举例	BFD/5/BFD_REACHED_UPPER_LIMIT: The total number of BFD session 100 reached upper limit.
日志说明	BFD会话总数达到上限
处理建议	请检查BFD会话配置

12 BGP

本节介绍 BGP 模块输出的日志信息。

12.1 BGP_EXCEED_ROUTE_LIMIT

日志内容	BGP [STRING].[STRING]: The number of routes ([UINT32]) from peer [STRING] ([STRING]) exceeds the limit [UINT32].
参数解释	$1：BGP实例名称 $2：VPN实例名称。如果是公网内的日志信息，则显示为空 $3：从对等体已接收到的路由前缀数量 $4：BGP对等体的IP地址 $5：BGP对等体的地址族 $6：允许从对等体接收的最大路由前缀数量
日志等级	4
举例	BGP/4/BGP_EXCEED_ROUTE_LIMIT: BGP default.vpn1: The number of routes (101) from peer 1.1.1.1 (IPv4-UNC) exceeds the limit 100.
日志说明	从对等体学到的路由数量超过了允许的最大路由数量
处理建议	检查是否是攻击导致，如果是，需要管理员找到问题原因，对攻击进行防御 否则，查看是否需要增大允许的最大路由数量

12.2 BGP_REACHED_THRESHOLD

日志内容	BGP [STRING].[STRING]: The ratio of the number of routes ([UINT32]) received from peer [STRING] ([STRING]) to the number of allowed routes ([UINT32]) has reached the threshold ([UINT32]%).
参数解释	$1：BGP实例名称 $2：VPN实例名称。如果是公网内的日志信息，则显示为空 $3：从对等体已接收到的路由数量 $4：BGP对等体的IP地址 $5：BGP对等体的地址族 $6：允许从对等体接收的最大路由数量 $7：接收的路由数量占允许的最大路由数量百分比的阈值
日志等级	4
举例	BGP/4/BGP_REACHED_THRESHOLD: BGP default.vpn1: The ratio of the number of routes (3) received from peer 1.1.1.1 (IPv4-UNC) to the number of allowed routes (2) has reached the threshold (75%).
日志说明	接收的路由数量占允许的最大路由数量的百分比达到了阈值
处理建议	检查是否是攻击导致，如果是，需要管理员找到问题原因，对攻击进行防御 否则，查看是否需要增大以下数值： • 允许的最大路由数量 • 接收的路由数量占允许的最大路由数量百分比的阈值

12.3 BGP_LOG_ROUTE_FLAP

日志内容	BGP [STRING].[STRING]: The route [STRING] [STRING]/[UINT32] learned from peer [STRING] ([STRING]) flapped.
参数解释	$1：BGP实例名称 $2：VPN实例名称。如果是公网内的日志信息，则显示为空 $3：BGP路由的RD值。不带RD的路由则显示为空 $4：BGP路由的前缀地址 $5：BGP路由的前缀掩码 $6：BGP对等体的IP地址 $7：BGP对等体的地址族
日志等级	4
举例	BGP/4/BGP_LOG_ROUTE_FLAP: BGP default.vpn1: The route 15.1.1.1/24 learned from peer 1.1.1.1 (IPv4-UNC) flapped.
日志说明	从对等体学到的路由发生抖动
处理建议	检查路由抖动是否不正常，如果是，需要管理员找到路由抖动的源头，并制定解决方案

12.4 BGP_LABEL_CONFLICT

日志内容	BGP egress-engineering incoming label [STRING] conflicts with current configuration.
参数解释	$1：标签值
日志等级	4
举例	BGP/4/BGP_LABEL_CONFLICT: BGP egress-engineering incoming label 3000 conflicts with current configuration.
日志说明	通过BGP-EPE功能为对等体分配的标签值已被占用
处理建议	检查配置BGP-EPE功能时指定的路由策略中应用的标签值是否与其他功能中使用的标签值相同

12.5 BGP_LABEL_OUTOFRANGE

日志内容	BGP egress-engineering incoming label [STRING] is out of range.
参数解释	$1：标签值
日志等级	4
举例	BGP/4/BGP_LABEL_OUTOFRANGE: BGP egress-engineering incoming label 1024 is out of range.
日志说明	通过BGP-EPE功能为对等体分配的标签值超出正常范围
处理建议	检查配置BGP-EPE功能时指定的路由策略中应用的标签取值是否合法

12.6 BGP_MEM_ALERT

日志内容	BGP [STRING] instance received system memory alert [STRING] event.
参数解释	$1：BGP实例名称 $2：内存告警的类型，包括stop、start
日志等级	5
举例	BGP/5/BGP_MEM_ALERT: BGP default instance received system memory alert start event.
日志说明	BGP模块收到内存告警信息
处理建议	如果内存告警类型为start，请检查系统内存占用情况，对占用内存较多的模块进行调整，尽量释放可用内存

12.7 BGP_PEER_LICENSE_REACHED

日志内容	BGP [STRING]: Number of peers in Established state reached the license limit.
参数解释	$1：BGP实例名称
日志等级	3
举例	BGP/3/BGP_PEER_LICENSE_REACHED: BGP default: Number of peers in Established state reached the license limit.
日志说明	处于established状态的邻居数量已达到license规格限制
处理建议	检查license安装情况，判断是否需要安装新的license

12.8 BGP_ROUTE_LICENSE_REACHED

日志内容	BGP [STRING]: Number of [STRING] routes reached the license limit.
参数解释	$1：BGP实例名称 $2：BGP地址族，取值包括： • IPv4-UNC public：表示公网 IPv4 单播路由 • IPv6-UNC public：表示公网 IPv6 单播路由 • IPv4 private：表示私网 IPv4 单播路由，VPNv4 路由和嵌套 VPN 路由 • IPv6 private：表示私网 IPv6 单播路由，VPNv6 路由
日志等级	3
举例	BGP/3/BGP_ROUTE_LICENSE_REACHED: BGP default: Number of IPv4-UNC public routes reached the license limit.
日志说明	指定类型的路由数量已达到license规格限制
处理建议	检查license安装情况，判断是否需要安装新的license 当指定类型的路由数量降低到License的规格限制以下或者License规格限制扩大时，之前被丢弃的路由不能自动恢复，需要用户手工配置，以便重新学习路由

12.9 BGP_STATE_CHANGED

日志内容	BGP [STRING].[STRING]: [STRING] state has changed from [STRING] to [STRING].
参数解释	$1：BGP实例名称 $2：VPN实例名称。如果是公网内的日志信息，则显示为空 $3：BGP对等体的IP地址 $4：变化前的状态名称 $5：变化后的状态名称
日志等级	3
举例	BGP/3/BGP_STATE_CHANGED: BGP default.vpn1: 192.99.0.2 state has changed from ESTABLISHED to IDLE.
日志说明	BGP对等体的状态发生变化 此日志信息当BGP对等体从其他状态进入Established状态或者从Established状态进入其他状态时产生
处理建议	如果BGP对等体意外Down，请检查网络是否发生故障或丢包

13 BLS

本节介绍 BLS 模块输出的日志信息。

13.1 BLS_ENTRY_ADD

日志内容	SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; RcvVPNInstance(1041)=[STRING]; TTL(1051)=[STRING]; Reason(1052)=[STRING].
参数解释	$1：黑名单IP地址 $2：DS-Lite Tunnel 对端地址 $3：VPN名称 $4：老化时间 $5：添加原因
日志等级	5
举例	BLS/5/BLS_ENTRY_ADD: SrcIPAddr(1003)=1.1.1.6; DSLiteTunnelPeer(1040)=--; RcvVPNInstance(1041)=; TTL(1051)=; Reason(1052)=Configuration. BLS/5/BLS_ENTRY_ADD: SrcIPAddr(1003)=9.1.1.5; DSLiteTunnelPeer(1040)=--; RcvVPNInstance(1041)=vpn1; TTL(1051)=10; Reason(1052)=Scan behavior detected.
日志说明	日志开关打开；手动配置一个黑名单；scan检测添加一个黑名单；触发日志发送
处理建议	无

13.2 BLS_ENTRY_DEL

日志内容	SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; RcvVPNInstance(1041)=[STRING]; Reason(1052)=[STRING].
参数解释	$1：黑名单IP地址 $2：DS-Lite Tunnel对端地址 $3：VPN名称 $4：删除原因
日志等级	5
举例	BLS/5/BLS_ENTRY_DEL: SrcIPAddr(1003)=1.1.1.3; DSLiteTunnelPeer(1040)=--; RcvVPNInstance(1041)=; Reason(1052)=Configuration. BLS/5/BLS_ENTRY_DEL: SrcIPAddr(1003)=9.1.1.5; DSLiteTunnelPeer(1040)=--; RcvVPNInstance(1041)=vpn1; Reason(1052)=Aging.
日志说明	日志开关打开；手动删除一个黑名单；老化删除一个黑名单；触发日志发送
处理建议	无

13.3 BLS_IPV6_ENTRY_ADD

日志内容	SrcIPv6Addr(1036)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; TTL(1051)=[STRING]; Reason(1052)=[STRING].
参数解释	$1：黑名单IPv6地址 $2：VPN名称 $3：老化时间 $4：添加原因
日志等级	5
举例	BLS/5/BLS_IPV6_ENTRY_ADD: SrcIPv6Addr(1036)=2::2; RcvVPNInstance(1041)=; TTL(1051)=; Reason(1052)=Configuration. BLS/5/BLS_IPV6_ENTRY_ADD: SrcIPv6Addr(1036)=1::5; RcvVPNInstance(1041)=--; TTL(1051)=10; Reason(1052)=Scan behavior detected.
日志说明	日志开关打开；手动配置一个黑名单；scan检测添加一个黑名单；触发日志发送
处理建议	无

13.4 BLS_IPV6_ENTRY_DEL

日志内容	SrcIPv6Addr(1036)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Reason(1052)=[STRING].
参数解释	$1：黑名单IPv6地址 $2：VPN名称 $3：删除原因
日志等级	5
举例	BLS/5/BLS_IPV6_ENTRY_DEL: SrcIPv6Addr(1036)=2::2; RcvVPNInstance(1041)=; Reason(1052)=Configuration.
日志说明	日志开关打开；手动删除一个黑名单；老化删除一个黑名单；触发日志发送
处理建议	无

14 BRAS_COM

本节介绍 BRAS 模块输出的通用日志信息。

14.1 BRAS_FUNC

日志内容	Not enough resources.
参数解释	N/A
日志等级	4
举例	DBRAS/4/BRAS_FUNC: -MDC=1 -Slot=4; Not enough resources.
日志说明	配置单个帐号允许接入的最大用户数时，BRAS业务限速模板资源不足，导致限速功能无法生效
处理建议	1. 在系统视图下执行 display qos-acl resource slot 4 命令查看当前单板上 BRAS 业务限速模板的使用情况 2. 请联系技术支持

15 BRIPRO

15.1 API

日志内容	PVST is not supported on this board.
参数解释	无
日志等级	6
举例	BRIPRO/6/API: -MDC=1-Slot=5; PVST is not supported on this board.
日志说明	某些单板不支持PVST协议
处理建议	请不要在该单板上配置PVST相关业务

15.2 API

日志内容	PVST is not supported on this board because it conflicts with the OAP configuration.
参数解释	无
日志等级	6
举例	BRIPRO/6/API: -MDC=1-Slot=5; PVST is not supported on this board because it conflicts with the OAP configuration.
日志说明	某些单板上PVST和OAP协议互斥；同时配置OAP和PVST时，PVST不生效
处理建议	1. 关闭该单板所有接口上的 OAP 功能 2. 通过执行 **undo stp mode**、**stp mode pvst** 命令重新配置生成树的工作模式为 RSTP 模式，该单板上的 PVST 协议才能生效

15.3 API

日志内容	OAP is not supported on this board because it conflicts with the PVST configuration.
参数解释	无
日志等级	6
举例	BRIPRO/6/API: -MDC=1-Slot=5; OAP is not supported on this board because it conflicts with the PVST configuration.
日志说明	某些单板上PVST和OAP协议互斥；已配置PVST时，该单板接口上配置的OAP功能不生效
处理建议	1. 通过 **undo stp mode** 命令，不再使用 PVST 协议 2. 通过 **undo oap enable**、**oap enable** 重新开启该单板接口的 OAP 功能

15.4 API

日志内容	Operation failed because TPID value [INT32] was configured on [STRING]. Restore TPID value to default on this interface and try again.
参数解释	$1：外层VLAN Tag的TPID值 $2：接口名称
日志等级	2
举例	BRIPRO/2/API: -MDC=1-Slot=4; Operation failed because TPID value 2000 was configured on Bridge-Aggregation200. Restore TPID value to default on this interface and try again.
日志说明	对于CSPEX类单板、CEPC类单板的接口，系统仅支持配置一个报文外层VLAN Tag的TPID值（缺省值除外） 只有将提示信息中的接口恢复TPID值为缺省值，才能在其他接口上修改TPID值
处理建议	二层接口使用**qinq ethernet-type service-tag**命令或三层接口使用**dot1q ethernet-type**命令配置报文外层VLAN Tag的TPID值为非缺省值后，如果要在其他接口上再通过这些命令修改外层VLAN Tag的TPID值，请先在已修改外层VLAN Tag的TPID值的接口上通过**undo**命令恢复TPID值为缺省值

15.5 TRUNK

日志内容	Link aggregation load sharing not supported.
参数解释	无
日志等级	6
举例	BRIPRO/6/TRUNK: -MDC=1-Slot=2; Link aggregation load sharing not supported.
日志说明	成员端口属于CSPC类单板、CMPE-1104单板的聚合组不支持当前全局配置的聚合负载分担类型
处理建议	无

16 CFD

16.1 API

日志内容	Interface [STRING] does not support CFD. Please check your configuration.
参数解释	$1：物理端口
日志等级	6
举例	BRIPRO/6/API: -MDC=1; Interface GigabitEthernet2/1/3 does not support CFD. Please check your configuration.
日志说明	CSPEX-1204单板不支持CFD功能
处理建议	请用户在支持CFD功能的单板接口下进行配置，详情请参见“可靠性配置指导”中的“CFD”

16.2 L2MC_IPV4

日志内容	Interface [STRING] does not support CFD. Please check your configuration.
参数解释	$1：物理端口
日志等级	6
举例	L2MC/6/L2MC_IPV4: -MDC=1-Slot=2; Interface GigabitEthernet2/1/3 does not support CFD. Please check your configuration.
日志说明	CSPEX-1204单板不支持CFD功能
处理建议	请用户在支持CFD功能的单板接口下进行配置，详情请参见“可靠性配置指导”中的“CFD”

16.3 CFD_CROSS_CCM

日志内容	MEP [UINT16] in SI [INT32] received a cross-connect CCM. It's SrcMAC is [MAC], SeqNum is [INT32], RMEP is [UINT16], MD ID is [STRING], MA ID is [STRING].
参数解释	$1：服务实例的ID $2：本地MEP的ID $3：源MAC地址 $4：序列号 $5：远端MEP的ID $6：MD的ID。如果不存在，会显示“without ID” $7：MA的ID
日志等级	6
举例	CFD/6/CFD_CROSS_CCM: MEP 13 in SI 10 received a cross-connect CCM. Its SrcMAC is 0011-2233-4401, SeqNum is 78, RMEP is 12, MD ID is without ID, MA ID is 0.
日志说明	MEP收到交叉连接的CCM报文，该报文包含与本端不同的MA ID或MD ID
处理建议	检查两端MEP的配置。让MEP所属的MD和MA的配置一致，且两端MEP级别相同、方向都相同

16.4 CFD_ERROR_CCM

日志内容	MEP [UINT16] in SI [INT32] received an error CCM. It's SrcMAC is [MAC], SeqNum is [INT32], RMEP is [UINT16], MD ID is [STRING], MA ID is [STRING].
参数解释	$1：服务实例的ID $2：本地MEP的ID $3：源MAC地址 $4：序列号 $5：远端MEP的ID $6：MD的ID。如果不存在，会显示“without ID” $7：MA的ID
日志等级	6
举例	CFD/6/CFD_ERROR_CCM: MEP 2 in SI 7 received an error CCM. Its SrcMAC is 0011-2233-4401, SeqNum is 21, RMEP is 2, MD ID is 7, MA ID is 1.
日志说明	MEP收到错误的CCM报文，该报文包含错误的MEP ID或生存时间
处理建议	检查CCM配置。让两端的CC检测周期配置一致，并配置远端MEP ID在本端允许的MEP列表中

16.5 CFD_LOST_CCM

日志内容	MEP [UINT16] in SI [INT32] failed to receive CCMs from RMEP [UINT16].
参数解释	$1：本地MEP的ID $2：服务实例ID $3：远端MEP的ID
日志等级	6
举例	CFD/6/CFD_LOST_CCM: MEP 1 in SI 7 failed to receive CCMs from RMEP 2.
日志说明	MEP在3.5个CCM报文发送周期内没有收到CCM报文，可能的原因是链路故障或远端MEP在此期间没有发送CCM报文
处理建议	检查链路状态和远端MEP的配置。如果链路down了或有其它的故障，例如单通故障，则恢复此链路。如果远端配置了同一服务实例的MEP，则确认两端的CC发送周期是一致的

16.6 CFD_RECEIVE_CCM

日志内容	MEP [UINT16] in SI [INT32] received CCMs from RMEP [UINT16]
参数解释	$1：本地MEP的ID $2：服务实例ID $3：远端MEP的ID
日志等级	6
举例	CFD/6/CFD_RECEIVE_CCM: MEP 1 in SI 7 received CCMs from RMEP 2.
日志说明	MEP收到远端MEP发送的CCM报文
处理建议	无

17 CFGMAN

本节介绍配置管理模块输出的日志信息。

17.1 CFGMAN_CFGCHANGED

日志内容	-EventIndex=[INT32]-CommandSource=[INT32]-ConfigSource=[INT32]-ConfigDestination=[INT32]; Configuration changed.
参数解释	$1：事件索引，取值范围为1到2147483647 $2：引起配置变化的来源，取值为： • cli：表示引起配置变化的来源为命令行 • snmp：表示引起配置变化的来源为 MIB • other：表示引起配置变化的来源为其它途径 $3：源配置，取值为： • erase：配置删除或重命名 • running：保存正在运行的配置 • commandSource：拷贝配置文件 • startup：保存运行配置到下次启动配置文件 • local：保存运行配置到本地文件 • networkFtp：通过 FTP 方式将网络上的某个配置文件保存到设备作为运行配置或者下次启动配置 • hotPlugging：热插拔板卡导致配置被删除或者失效 $4：目的配置，取值为： • erase：配置删除或重命名 • running：保存正在运行的配置 • commandSource：拷贝配置文件 • startup：保存运行配置到下次启动配置文件 • local：保存运行配置到本地文件 • networkFtp：通过 FTP 方式将网络上的某个配置文件保存到设备作为运行配置或者下次启动配置 • hotPlugging：热插拔板卡导致配置被删除或者失效
日志等级	5
举例	CFGMAN/5/CFGMAN_CFGCHANGED: -EventIndex=[6]-CommandSource=[snmp]-ConfigSource=[startup]-ConfigDestination=[running]; Configuration changed.
日志说明	如果配置在过去的十分钟内发生了变化，设备将记录事件索引、引起配置变化的来源、源配置以及目的配置
处理建议	无

17.2 CFGMAN_OPTCOMPLETION

日志内容	-OperateType=[INT32]-OperateTime=[INT32]-OperateState=[INT32]-OperateEndTime=[INT32]; Operation completed.
参数解释	$1：操作类型，取值为： • running2startup：将运行配置保存为下次启动配置 • startup2running：将下次启动配置设置为运行配置 • running2net：将运行配置保存到网络 • net2running：将网络上的配置文件上传到设备，并作为当前配置运行 • net2startup：将网络上的配置文件上传到设备，并保存为下次启动配置文件 • startup2net：将下次启动配置文件保存到网络 $2：操作时间 $3：操作状态，取值为： • InProcess：正在执行 • success：执行成功 • InvalidOperation：无效的操作 • InvalidProtocol：无效的协议 • InvalidSource：无效的源文件名 • InvalidDestination：无效的目的文件名 • InvalidServer：无效的服务器地址 • DeviceBusy：设备繁忙 • InvalidDevice：设备地址无效 • DeviceError：设备出错 • DeviceNotWritable：设备不可写 • DeviceFull：设备的存储空间不足 • FileOpenError：文件打开出错 • FileTransferError：文件传输出错 • ChecksumError：文件校验和错误 • LowMemory：没有内存 • AuthFailed：用户验证失败 • TransferTimeout：传输超时 • UnknownError：未知原因 • invalidConfig：无效配置 $4：操作结束时间
日志等级	5
举例	CFGMAN/5/CFGMAN_OPTCOMPLETION: -OperateType=[running2startup]-OperateTime=[248]-OperateState=[success]-OperateEndTime=[959983]; Operation completed.

日志说明	操作完成后记录操作的类型、状态以及时间
处理建议	请根据OperateState的值定位、处理问题

18 CGN

18.1 INTE_CGNSOFTCTL

日志内容	No enough resource for Ds-Lite tunnel!
参数解释	无
日志等级	4
举例	INTE_CGN/4/INTE_CGNSOFTCTL: -MDC=1-Slot=5; No enough resource for Ds-Lite tunnel!
日志说明	CGN单板上的DS-Lite隧道资源不足，后续从此单板上通过DS-Lite隧道接入的用户创建的NAT会话将无法执行硬件转发
处理建议	**1.** 在 Probe 视图下执行 **display hardware internal indexq all** 命令，查看单板上 CGN TUNNEL INDEX 对应的 Handle 值 **2.** 在 Probe 视图下执行 **display hardware internal indexq handle** 命令，收集 DS-Lite 资源的使用情况，包括 IndexLeft 值查当前 DS-Lite 资源的剩余情况 **3.** 联系技术支持

19 CLK

19.1 CLK

日志内容	Get clock global config succeed.
参数解释	无
日志等级	5
举例	DSYSM/5/CLK: Get clock global config succeed.
日志说明	成功获取时钟局配置，即获取SSM级别是否参与控制和时钟监控的工作模式等配置信息
处理建议	无

19.2 CLK

日志内容	Traced reference change alarm, current traced reference of chassis [INT32] is PTP.
参数解释	$1：设备在IRF中的成员编号
日志等级	5
举例	DRIVER/5/CLK: Traced reference change alarm, current traced reference of chassis 1 is PTP.
日志说明	设备当前选中的参考源为PTP协议时钟源，即设备以该PTP协议时钟源作为生效时钟源进行时钟同步
处理建议	无

19.3 CLK

日志内容	Traced reference change alarm, current traced reference is PTP.
参数解释	无
日志等级	5
举例	DRIVER/5/CLK: Traced reference change alarm, current traced reference is PTP.
日志说明	设备当前选中的参考源为PTP协议时钟源，即设备以该PTP协议时钟源作为生效时钟源进行时钟同步
处理建议	无

19.4 CLK

日志内容	Traced reference change alarm, no reference of chassis [INT32] traced now.
参数解释	$1：设备在IRF中的成员编号
日志等级	5
举例	DRIVER/5/CLK:Traced reference change alarm, no reference of chassis 1 traced now.
日志说明	设备当前没有生效的时钟源
处理建议	**1.** 通过命令 display network-clock status 检查时钟监控的工作状态： • 如果为自动模式，请检查设备与时钟源之间的链路是否正常 • 如果为手工模式，请先通过命令 display network-clock source 查看所有参考源的工作状态，然后再通过命令 network-clock work-mode manual source 配置一个处于正常工作状态的参考时钟源作为设备的生效时钟源 **2.** 如以上步骤均未解决，请联系技术支持

19.5 CLK

日志内容	Traced reference change alarm, no reference traced now.
参数解释	无
日志等级	5
举例	DRIVER/5/CLK:Traced reference change alarm, no reference traced now.
日志说明	设备当前没有生效的时钟源
处理建议	1. 通过命令 display network-clock status 检查时钟监控的工作状态： • 如果为自动模式，请检查设备与时钟源之间的链路是否正常 • 如果为手工模式，请先通过命令 display network-clock source 查看所有参考源的工作状态，然后再通过命令 network-clock work-mode manual source 配置一个处于正常工作状态的参考时钟源作为设备的生效时钟源 2. 如以上步骤均未解决，请联系技术支持

19.6 CLK

日志内容	Traced reference change alarm, current traced reference of chassis [INT32] is [INT32].
参数解释	$1：设备在IRF中的成员编号 $2：当前生效时钟源的编号
日志等级	5
举例	DRIVER/5/CLK: Traced reference change alarm, current traced reference of chassis 1 is 5.
日志说明	当前时钟源被锁定，即设备以该选中的时钟源作为生效时钟源
处理建议	无

19.7 CLK

日志内容	Traced reference change alarm, current traced reference is [INT32].
参数解释	$1：当前生效时钟源的编号
日志等级	5
举例	DRIVER/5/CLK: Traced reference change alarm, current traced reference is 5.
日志说明	当前时钟源被锁定，即设备以该选中的时钟源作为生效时钟源
处理建议	无

19.8 CLK

日志内容	Reference [INT32] of chassis [INT32] is recovered.
参数解释	$1：丢失后重新恢复正常的时钟源的编号 $2：设备在IRF中的成员编号
日志等级	5
举例	DRIVER/5/CLK: References 5 of chassis 1 is recovered.
日志说明	时钟源恢复，即该时钟源从丢失状态恢复到正常工作状态；只有处于正常工作状态的时钟源才有可能成为设备的生效时钟源，时钟源的工作状态可以通过命令**display network-clock source**查看
处理建议	无

19.9 CLK

日志内容	Reference [INT32] is recovered.
参数解释	$1：丢失恢复时钟源的编号
日志等级	5
举例	DRIVER/5/CLK: References 5 is recovered.
日志说明	时钟源恢复，即该时钟源从丢失状态恢复到正常工作状态；只有处于正常工作状态的时钟源才有可能成为设备的生效时钟源，时钟源的工作状态可以通过命令**display network-clock source**查看
处理建议	无

19.10 CLK

日志内容	Reference [INT32] of chassis [INT32] is lost.
参数解释	$1：发生状态丢失时钟源的编号 $2：设备在IRF中的成员编号
日志等级	5
举例	DRIVER/5/CLK: References 5 of chassis 1 is lost.
日志说明	因时钟源链路断开或端口down掉导致设备上某一编号的时钟源丢失
处理建议	**1.** 检查设备与时钟源之间的链路是否断开； **2.** 如果是线路时钟源，再检查本设备的时钟源输入端口是否处于 down 状态 **3.** 如以上步骤均未解决，请联系技术支持

19.11 CLK

日志内容	Reference [INT32] is lost.
参数解释	$1：发生状态丢失时钟源的编号
日志等级	5
举例	DRIVER/5/CLK: References 5 is lost.
日志说明	因时钟源链路断开或端口down掉导致设备上某一编号的时钟源丢失
处理建议	1. 检查设备与时钟源之间的链路是否断开 2. 如果是线路时钟源，再检查本设备的时钟源输入端口是否处于 down 状态 3. 如以上步骤均未解决，请联系技术支持

19.12 CLK

日志内容	All references of chassis [INT32] are lost.
参数解释	$1：设备在IRF中的成员编号
日志等级	5
举例	DRIVER/5/CLK: All references of chassis 1 are lost.
日志说明	因时钟源链路断开或端口down掉导致设备上所有时钟源丢失
处理建议	1. 检查设备与时钟源之间的链路是否断开 2. 如果是线路时钟源，再检查本设备的时钟源输入端口是否处于 down 状态 3. 如以上步骤均未解决，请联系技术支持

19.13 CLK

日志内容	All references are lost.
参数解释	无
日志等级	5
举例	DRIVER/5/CLK: All references are lost.
日志说明	因时钟源链路断开或端口down掉导致设备上所有时钟源丢失
处理建议	1. 检查设备与时钟源之间的链路是否断开 2. 如果是线路时钟源，再检查本设备的时钟源输入端口是否处于 down 状态 3. 如以上步骤均未解决，请联系技术支持

19.14 CLK

日志内容	Priority alarm, current priority of PTP of chassis [INT32] is [INT32].
参数解释	$1：设备在IRF中的成员编号 $2：当前PTP时钟源的优先级
日志等级	5
举例	DRIVER/5/CLK: Priority alarm, current priority of PTP of chassis 1 is 8.
日志说明	设备的PTP时钟源的优先级更改为了其它设置值
处理建议	无

19.15 CLK

日志内容	Priority alarm, current priority of PTP is [INT32].
参数解释	$1：当前PTP时钟源的优先级
日志等级	5
举例	DRIVER/5/CLK: Priority alarm, current priority of PTP is 8.
日志说明	设备的PTP时钟源的优先级更改为了其它设置值
处理建议	无

19.16 CLK

日志内容	Priority alarm, current priority of reference [INT32] of chassis [INT32] is [INT32]
参数解释	$1：时钟源编号: $2：设备在IRF中的成员编号 $3：当前时钟的优先级
日志等级	5
举例	DRIVER/5/CLK: Priority alarm, current priority of reference 2 of chassis 1 is 8
日志说明	设备的某个时钟源的优先级更改为了其它设置值
处理建议	无

19.17 CLK

日志内容	Priority alarm, current priority of reference [INT32] is [INT32]
参数解释	$1：时钟源编号: $2：当前时钟的优先级
日志等级	5
举例	DRIVER/5/CLK: Priority alarm, current priority of reference 2 is 8
日志说明	设备的某个时钟源的优先级更改为了其它设置值
处理建议	无

19.18 CLK

日志内容	SSM level alarm, current SSM level of reference [INT32] of chassis [INT32] is [STRING].
参数解释	$1：时钟源编号 $2：设备在IRF中的成员编号 $3：存放的SSM等级字符串
日志等级	5
举例	DRIVER/5/CLK: SSM level alarm, current SSM level of reference 2 of chassis 1 is SSUB.
日志说明	设备的某个时钟源的SSM级别更改为了其它设置值
处理建议	无

19.19 CLK

日志内容	SSM level alarm, current SSM level of reference [INT32] is [STRING].
参数解释	$1：时钟源编号 $2：存放的SSM等级字符串
日志等级	5
举例	DRIVER/5/CLK: SSM level alarm, current SSM level of reference 2 is SSUB.
日志说明	设备的某个时钟源的SSM级别更改为了其它设置值
处理建议	无

19.20 CLK

日志内容	SSM level alarm, current SSM level of PTP of chassis [INT32] is [STRING].
参数解释	$1：设备在IRF中的成员编号 $2：存放的SSM等级字符串
日志等级	5
举例	DRIVER/5/CLK: SSM level alarm, current SSM level of PTP of chassis 1 is SSUA.
日志说明	设备的PTP时钟源的SSM级别更改为了其它设置值
处理建议	无

19.21 CLK

日志内容	SSM level alarm, current SSM level of PTP is [STRING].
参数解释	$1：存放的SSM等级字符串
日志等级	5
举例	DRIVER/5/CLK: SSM level alarm, current SSM level of PTP is SSUA.
日志说明	设备的PTP时钟源的SSM级别更改为了其它设置值
处理建议	无

19.22 CLK

日志内容	Phase lock alarm, current phase lock mode of chassis [INT32] is [STRING].
参数解释	$1：设备在IRF中的成员编号 $2：存放锁相状态字符串
日志等级	5
举例	DRIVER/5/CLK: Phase lock alarm, current phase lock mode of chassis 1 is Locked.
日志说明	设备的时钟锁相状态进入被锁定状态，即设备获取到生效的时钟源进行时钟同步
处理建议	无

19.23 CLK

日志内容	Phase lock alarm, current phase lock mode is [STRING].
参数解释	$1：存放锁相状态字符串
日志等级	5
举例	DRIVER/5/CLK: Phase lock alarm, current phase lock mode is Locked.
日志说明	设备的时钟锁相状态进入被锁定状态，即设备获取到生效的时钟源进行时钟同步
处理建议	无

19.24 CLK

日志内容	SSM out level alarm, current SSM out level of chassis [INT32] is [STRING].
参数解释	$1：设备在IRF中的成员编号 $2：存放SSM等级字符串
日志等级	5
举例	DRIVER/5/CLK: SSM out level alarm, current SSM out level of chassis 1 is SSUB.
日志说明	某个IRF成员设备整框同步输入时钟源的SSM级别改变
处理建议	无

19.25 CLK

日志内容	SSM out level alarm, current SSM out level is [STRING].
参数解释	$1：存放SSM等级字符串
日志等级	5
举例	DRIVER/5/CLK: SSM out level alarm, current SSM out level is SSUB.
日志说明	设备整框同步输入时钟源的SSM级别改变
处理建议	无

20 CONNLMT

本节介绍连接数限制模块输出的日志信息。

20.1 CONNLMT_IPV4_OVERLOAD

日志内容	RcvIfName(1023)=[STRING];Protocol(1001)=[STRING];SrcIPAddr(1003)=[IPADDR];DstIPAddr(1007)=[IPADDR];ServicePort(1071)=[UINT16];RcvVPNInstance(1042)=[STRING];SndVPNInstance(1043)=[STRING];SndDSLiteTunnelPeer(1041)=[STRING];UpperLimit(1049)=[UINT32];LimitRuleNum(1051)=[UINT16];Event(1048)=[STRING];
参数解释	$1：全局或接口名称 $2：传输层协议类型 $3：源IP地址 $4：目的IP地址 $5：服务端口号 $6：源VPN名称 $7：目的VPN名称 $8：对端隧道ID $9：上限值 $10：规则ID $11：Event信息
日志等级	6
举例	CONNLMT/6/CONNLMT_IPV4_OVERLOAD: RcvIfName(1023)=Global;Protocol(1001)=;SrcIPAddr(1003)=10.10.10.1;DstIPAddr(1007)=;ServicePort(1071)=;RcvVPNInstance(1042)=;SndVPNInstance(1043)=;SndDSLiteTunnelPeer(1041)=;UpperLimit(1049)=1000;LimitRuleNum(1051)=1;Event(1048)=Exceeded upper threshold;
日志说明	当连接数的并发数超过策略中配置的上限时触发日志输出
处理建议	无

20.2 CONNLMT_IPV4_RECOVER

日志内容	RcvIfName(1023)=[STRING];Protocol(1001)=[STRING];SrcIPAddr(1003)=[IPADDR];DstIPAddr(1007)=[IPADDR];ServicePort(1071)=[UINT16];RcvVPNInstance(1042)=[STRING];SndVPNInstance(1043)=[STRING];SndDSLiteTunnelPeer(1041)=[STRING];DropPktCount(1052)=[UINT32];LowerLimit(1050)=[UINT32];LimitRuleNum(1051)=[UINT16];Event(1048)=[STRING];
参数解释	$1：全局或接口名称 $2：传输层协议类型 $3：源IP地址 $4：目的IP地址 $5：服务端口号 $6：源VPN名称 $7：目的VPN名称 $8：对端隧道ID $9：丢包数 $10：下限值 $11：规则ID $12：Event信息
日志等级	6
举例	CONNLMT/6/CONNLMT_IPV4_RECOVER: RcvIfName(1023)=Global;Protocol(1001)=;SrcIPAddr(1003)=10.10.10.1;DstIPAddr(1007)=;ServicePort(1071)=;RcvVPNInstance(1042)=;SndVPNInstance(1043)=;SndDSLiteTunnelPeer(1041)=;DropPktCount(1052)=306004;LowerLimit(1050)=10;LimitRuleNum(1051)=1;Event(1048)=Dropped below lower threshold;
日志说明	当连接数的并发数从达到上限恢复到下限时触发日志输出
处理建议	无

20.3 CONNLMT_IPV6_OVERLOAD

日志内容	RcvIfName(1023)=[STRING];Protocol(1001)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];ServicePort(1071)=[UINT16];RcvVPNInstance(1042)=[STRING];SndVPNInstance(1043)=[STRING];SndDSLiteTunnelPeer(1041)=[STRING];UpperLimit(1049)=[UINT32];LimitRuleNum(1051)=[UINT16];Event(1048)=[STRING];
参数解释	$1：全局或接口名称 $2：传输层协议类型 $3：源IPv6地址 $4：目的IPv6地址 $5：服务端口号 $6：源VPN名称 $7：目的VPN名称 $8：对端隧道ID $9：上限值 $10：规则ID $11：Event信息
日志等级	6
举例	CONNLMT/6/CONNLMT_IPV6_OVERLOAD: RcvIfName(1023)=Global;Protocol(1001)=;SrcIPv6Addr(1036)=2001::1;DstIPv6Addr(1037)=;ServicePort(1071)=;RcvVPNInstance(1042)=;SndVPNInstance(1043)=;SndDSLiteTunnelPeer(1041)=;UpperLimit(1049)=1000;LimitRuleNum(1051)=1;Event(1048)=Exceeded upper threshold;
日志说明	当连接数的并发数超过策略中配置的上限时触发日志输出
处理建议	无

20.4 CONNLMT_IPV6_RECOVER

日志内容	RcvIfName(1023)=[STRING];Protocol(1001)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];ServicePort(1071)=[UINT16];RcvVPNInstance(1042)=[STRING];SndVPNInstance(1043)=[STRING];SndDSLiteTunnelPeer(1041)=[STRING];DropPktCount(1052)=[UINT32];LowerLimit(1050)=[UINT32];LimitRuleNum(1051)=[UINT16];Event(1048)=[STRING];
参数解释	$1：全局或接口名称 $2：传输层协议类型 $3：源IPv6地址 $4：目的IPv6地址 $5：服务端口号 $6：源VPN名称 $7：目的VPN名称 $8：对端隧道ID $9：丢包数 $10：下限值 $11：规则ID $12：Event信息
日志等级	6
举例	CONNLMT/6/CONNLMT_IPV6_RECOVER: RcvIfName(1023)=Global;Protocol(1001)=;SrcIPAddr(1003)=2001::1;DstIPAddr(1007)=;ServicePort(1071)=;RcvVPNInstance(1042)=;SndVPNInstance(1043)=;SndDSLiteTunnelPeer(1041)=;DropPktCount(1052)=306004;LowerLimit(1050)=10;LimitRuleNum(1051)=1;Event(1048)=Dropped below lower threshold;
日志说明	当连接数的并发数从达到上限恢复到下限时触发日志输出
处理建议	无

21 DEV

本节介绍 DEV（Device）模块输出的日志信息。

21.1 DrvDebug

日志内容	Over-current occurred to the USB port on the MPU. Please remove and check the USB device.
参数解释	无
日志等级	4
举例	DRVPLAT/4/DrvDebug: -MDC=1; Over-current occurred to the USB port on the MPU. Please remove and check the USB device.
日志说明	外接的USB设备故障，导致主控板的USB口电流过大
处理建议	**1.** 拔出并更换 USB 设备 **2.** 请联系技术支持

21.2 DrvDebug

日志内容	Temperature of the board is too high!
参数解释	无
日志等级	4
举例	DRVPLAT/4/DrvDebug: Temperature of the board is too high!
日志说明	由于风扇故障、环境温度过高等原因导致单板温度过高
处理建议	**1.** 如果环境温度较高，请检查设备所在机房的空调运行是否正常 **2.** 请检查设备出风口或入风口是否被阻塞 **3.** 请检查设备风扇是否正常运行 **4.** 请检查是否所有槽位上都正确插了单板或者假面板 **5.** 请联系技术支持

21.3 DrvDebug

日志内容	At least one fabric module slot is empty. Make sure a blank filler module has been installed in each empty slot so the switch can work correctly.
参数解释	无
日志等级	5
举例	DRVPLAT/5/DrvDebug: At least one fabric module slot is empty. Make sure a blank filler module has been installed in each empty slot so the switch can work correctly.
日志说明	4块A类交换网板未同时在位
处理建议	请将4块A类交换网板全部插入到CR16006-F对应的4个交换网板槽位，即CSFC-04-1需插在6号槽位（CSFC-04-1前面板上有提示“Notes:Please insert to Slot 6”），依次类推

21.4 DrvDebug

日志内容	The non-stack SFP module cannot be used on a STACK enabled port!
参数解释	无
日志等级	5
举例	DRVPLAT/5/DrvDebug: The non-stack SFP module cannot be used on a STACK enabled port!
日志说明	IRF堆叠口插入了不合适的光模块
处理建议	**1.** IRF 堆叠口上不能使用光电转换模块，请更换光模块 **2.** 请联系技术支持

21.5 DrvDebug

日志内容	Warning: Chip [INT32] temperature([STRING]) in slot [INT32] is too high, please check it.
参数解释	$1：单板上的芯片编号 $2：温度 $3：单板所在的全局槽位号（独立运行模式为单板所在的槽位号，IRF模式为（IRF中的成员编号-1）x 18+单板所在的槽位号）
日志等级	5
举例	DRVPLAT/5/DrvDebug: Warning:Chip 1 temperature(80) in slot 2 is too high, please check it.
日志说明	检测到单板上的某块芯片温度过高，需要关注并进行检查
处理建议	**1.** 如果环境温度较高，请检查设备所在机房的空调运行是否正常 **2.** 请检查设备出风口是否被阻塞 **3.** 请检查设备风扇是否正常运行 **4.** 请检查是否所有槽位上都正确插了单板或者假面板 **5.** 请联系技术支持

21.6 DrvDebug

日志内容	hotspot [STRING] in slot [INT32] temperature([STRING]) is too high, please check it.
参数解释	$1：温度观察点 $2：单板所在的全局槽位号（独立运行模式为单板所在的槽位号，IRF模式为（IRF中的成员编号-1）x 18+单板所在的槽位号） $3：温度
日志等级	5
举例	DRVPLAT/5/DrvDebug: hotspot 1 in slot 2 temperature(80) is too high, please check it.
日志说明	检测到单板上的某一温度观察点的温度过高，需要关注并进行检查
处理建议	**1.** 如果环境温度较高，请检查设备所在机房的空调运行是否正常 **2.** 请检查设备出风口是否被阻塞 **3.** 请检查设备风扇是否正常运行 **4.** 请检查是否所有槽位上都正确插了单板或者假面板 **5.** 请联系技术支持

21.7 DrvDebug

日志内容	Warning: cpu temperature([STRING]) in slot [INT32] is too high, please check it.
参数解释	$1：温度 $2：单板所在的全局槽位号（独立运行模式为单板所在的槽位号，IRF模式为（IRF中的成员编号-1）x 18+单板所在的槽位号）
日志等级	5
举例	DRVPLAT/5/DrvDebug: Warning: cpu temperature(80) in slot 2 is too high, please check it.
日志说明	出风口、入风口或芯片等温度过高，导致CPU温度过高
处理建议	**1.** 如果环境温度较高，请检查设备所在机房的空调运行是否正常 **2.** 请检查设备出风口是否被阻塞 **3.** 请检查设备风扇是否正常运行 **4.** 请检查是否所有槽位上都正确插了单板或者假面板 **5.** 请联系技术支持

21.8 DrvDebug

日志内容	Warning: The LPU board on chassis [STRING] slot [STRING] is not compatible with MPU board.
参数解释	$1：设备在IRF中的成员编号 $2：单板所在的槽位号
日志等级	2
举例	DRVPLAT/2/DrvDebug: -MDC=1-Chassis=3-Slot=6; Warning: The LPU board on chassis 3 slot 8 is not compatible with MPU board.
日志说明	当前单板槽位号的业务板或网板与本地主用主控板的设备标识不一致
处理建议	请联系技术支持

21.9 DrvDebug

日志内容	Warning: The LPU board on slot [STRING] is not compatible with MPU board.
参数解释	$1：单板所在的槽位号
日志等级	2
举例	DRVPLAT/2/DrvDebug: -MDC=1; Warning: The LPU board on slot 4 is not compatible with MPU board.
日志说明	当前单板槽位号的业务板或网板与主用主控板的设备标识不一致
处理建议	请联系技术支持

21.10 DrvDebug

日志内容	Warning: Standby board on chassis [STRING] slot [STRING] is not compatible with MPU board.
参数解释	$1：设备在IRF中的成员编号 $2：单板所在的槽位号
日志等级	2
举例	DRVPLAT/2/DrvDebug: -MDC=1-Chassis=3-Slot=1; Warning: Standby board on chassis 3 slot 1 is not compatible with MPU board.
日志说明	当前单板槽位号的备用主控板与本地主用主控板的设备标识不一致
处理建议	请联系技术支持

21.11 DrvDebug

日志内容	Warning: Standby board on slot [STRING] is not compatible with MPU board.
参数解释	$1：单板所在的槽位号
日志等级	2
举例	DRVPLAT/2/DrvDebug: -MDC=1; Warning: Standby board on slot 1 is not compatible with MPU board.
日志说明	当前单板槽位号的备用主控板与主用主控板的设备标识不一致
处理建议	请联系技术支持

21.12 DrvDebug

日志内容	IRF setup failed. The member devices have MPUs with different device identifiers.
参数解释	无
日志等级	4
举例	DRVPLAT/4/DrvDebug: IRF setup failed. The member devices have MPUs with different device identifiers.
日志说明	组建IRF时，各成员设备使用的主控板设备标识必须相同，否则无法形成IRF
处理建议	请联系技术支持

21.13 DrvDebug

日志内容	IRF setup failed. The member devices have MPUs of different models.
参数解释	无
日志等级	4
举例	DRVPLAT/4/DrvDebug: IRF setup failed. The member devices have MPUs of different models.
日志说明	组建IRF时，各成员设备使用的主控板丝印必须相同，否则无法形成IRF
处理建议	• 请将各成员设备上的主控板更换成相同丝印的主控板 • 请联系技术支持

21.14 DrvDebug

日志内容	IRF setup failed. The member devices are operating in different VLAN modes.
参数解释	无
日志等级	4
举例	DRVPLAT/4/DrvDebug: IRF setup failed. The member devices are operating in different VLAN modes.
日志说明	组建IRF时，各成员设备的VLAN模式必须保持一致，否则无法形成IRF
处理建议	请使用**system-vlan-mode**命令将各成员设备的VLAN模式配置成一致

21.15 DrvDebug

日志内容	IRF setup failed. The MPUs on member devices have different MAC address table sizes.
参数解释	无
日志等级	4
举例	DRVPLAT/4/DrvDebug: IRF setup failed. The MPUs on member devices have different MAC address table sizes.
日志说明	组建IRF时，各成员设备上的主控板MAC地址表项大小需要一致，否则无法形成IRF
处理建议	请联系技术支持

21.16 DrvDebug

日志内容	形式一： Current temperature on slot [STRING] is [STRING] degrees centigrade, which is higher than the shutdown threshold. The board is being shut down. 形式二： Current temperature on chassis [STRING] slot [STRING] is [STRING] degrees centigrade, which is higher than the shutdown threshold. The board is being shut down.
参数解释	形式一： $1：单板所在的槽位号 $2：温度值 形式二： $1：设备在IRF中的成员编号 $2：单板所在的槽位号 $3：温度值
日志等级	2
举例	DRVPLAT/2/DrvDebug: -MDC=1; Current temperature on slot 4 is 101 degrees centigrade, which is higher than the shutdown threshold. The board is being shut down.
日志说明	单板当前温度超过温度传感器的断电门限，该单板即将被下电
处理建议	• 检查风扇状态,风扇是否故障或者被拔出，风扇故障请执行步骤 2，风扇拔出请执行步骤 3 • 风扇故障请更换新风扇，更换新风扇仍然故障请联系技术人员 • 将风扇插回框内，风扇正常后再为单板进行上电，上电请执行步骤 4 • 更换插入新的正常单板，或者等过温的单板温度降下来，然后拔插该单板使该单板上电

21.17 DrvDebug

日志内容	The card in slot [UINT32] failed to start up. The card is not compatible with the chassis.
参数解释	$1：单板所在的槽位号
日志等级	2
举例	DRVPLAT/2/DrvDebug: -MDC=1; The card in slot 4 failed to start up. The card is not compatible with the chassis.
日志说明	当前单板与主机不适配，单板无法正常启动
处理建议	• 请将单板安装到适配的主机上 • 请联系技术支持

21.18 DrvDebug

日志内容	The card in chassis [UINT32] slot [UINT32] failed to start up. The card is not compatible with the chassis.
参数解释	$1：设备在IRF中的成员编号 $2：单板所在的槽位号
日志等级	2
举例	DRVPLAT/2/DrvDebug: -MDC=1; The card in chassis 0 slot 4 failed to start up. The card is not compatible with the chassis.
日志说明	当前单板与主机不适配，单板无法正常启动
处理建议	• 请将单板安装到适配的主机上 • 请联系技术支持

21.19 DrvDebug

日志内容	Chassis [UINT32] slot [UINT32] is using a different operating mode than the global active MPU. Please save the running configuration and reboot the card.
参数解释	$1：设备在IRF中的成员编号 $2：单板所在的槽位号
日志等级	2
举例	DRVPLAT/2/DrvDebug: -MDC=1-Chassis=4-Slot=5;Chassis 4 slot 5 is using a different operating mode than the global active MPU. Please save the running configuration and reboot the card.
日志说明	当前槽位上的单板的工作模式与全局主用主控板的模式不一致，请保存配置并重启该单板
处理建议	保存配置，并重启对应槽位的单板

21.20 REBOOT

日志内容	The subcard cannot be rebooted. The system is not operating stably. Please try again later.
参数解释	无
日志等级	6
举例	DEVD/6/REBOOT: -MDC=1-Slot=1; The subcard cannot be rebooted. The system is not operating stably. Please try again later.
日志说明	当前系统不稳定，暂时不能重启子卡。请在系统稳定后重新尝试
处理建议	通过display system stable state 命令查看系统的稳定状态，待系统稳定后再重新尝试

21.21 BOARD_REBOOT

日志内容	Board is rebooting on [STRING].
参数解释	$1：chassis编号+slot编号或slot编号
日志等级	5
举例	DEV/5/BOARD_REBOOT: Board is rebooting on slot 1.
日志说明	用户在重启指定slot，或者指定slot因为异常而重启
处理建议	1. 检查是否有用户在重启指定 slot 2. 如果没有用户重启，等待指定 slot 重新启动后，通过 **display version** 命令、对应指定 slot 信息中的 Last reboot reason 字段，查看重启原因 3. 如果重启原因为异常重启，请联系技术支持

21.22 BOARD_REMOVED

日志内容	Board was removed from [STRING], type is [STRING].
参数解释	$1：chassis编号+slot编号或slot编号 $2：单板类型
日志等级	3
举例	DEV/3/BOARD_REMOVED: Board was removed from slot 1, type is LSQ1FV48SA.
日志说明	一块LPU或者备用MPU被拔出。设备退出IRF
处理建议	1. 检查对应单板是否插紧 2. 检查对应单板是否损坏 3. 重新插入单板或更换单板 4. 重新将设备加入 IRF

21.23 BOARD_STATE_FAULT

日志内容	Board state changed to Fault on [STRING], type is [STRING].
参数解释	$1：chassis编号+slot编号或slot编号 $2：单板类型
日志等级	2
举例	DEV/2/BOARD_STATE_FAULT: Board state changed to Fault on slot 1, type is LSQ1FV48SA.
日志说明	单板在以下情况会处于Fault（故障）状态： • 单板处于启动阶段（正在初始化或者加载软件版本），单板不可用 • 单板不能正常工作
处理建议	根据日志产生的情况，处理建议如下： • 对于第一种情况：单板型号不同，加载的软件版本不同，启动所需的时间不同。一般不超过 10 分钟，请以设备的实际情况为准 • 对于第二种情况：请联系技术支持

21.24 BOARD_STATE_NORMAL

日志内容	Board state changed to Normal on [STRING], type is [STRING].
参数解释	$1：chassis编号+slot编号或slot编号 $2：单板类型
日志等级	5
举例	DEV/5/BOARD_STATE_NORMAL: Board state changed to Normal on slot 1, type is LSQ1FV48SA.
日志说明	一块新插入的LPU或者备用MPU完成了初始化
处理建议	无

21.25 CFCARD_FAILED

日志内容	CF card state changed to Fault in [STRING] [STRING].
参数解释	$1：the device或chassis编号+slot编号或slot编号 $2：CF卡所在的槽位号（仅支持多个CF卡的产品支持该字段）
日志等级	3
举例	DEV/3/CFCARD_FAILED: CF card state changed to Fault in slot 1 CF card slot 1.
日志说明	CF卡故障
处理建议	**1.** 检查 CF 卡是否损坏 **2.** 重新安装 CF 卡或更换 CF 卡

21.26 CFCARD_INSERTED

日志内容	CF card was inserted in [STRING] [STRING].
参数解释	$1：the device或chassis编号+slot编号或slot编号 $2：CF卡所在的槽位号（仅支持多个CF卡的产品支持该字段）
日志等级	4
举例	DEV/4/CFCARD_INSERTED: CF card was inserted in slot 1 CF card slot 1.
日志说明	CF卡安装到了指定槽位
处理建议	无

21.27 CFCARD_REMOVED

日志内容	CF card was removed from [STRING] [STRING].
参数解释	$1：the device或chassis编号+slot编号或slot编号 $2：CF卡所在的槽位号（仅支持多个CF卡的产品支持该字段）
日志等级	3
举例	DEV/3/CFCARD_REMOVED: CF card was removed from slot 1 CF card slot 1.
日志说明	CF卡被拔出
处理建议	**1.** 检查 CF 卡是否插紧 **2.** 检查 CF 卡是否损坏 **3.** 重新安装 CF 卡或更换 CF 卡

21.28 CHASSIS_REBOOT

日志内容	Chassis [STRING] is rebooting now.
参数解释	$1：chassis编号
日志等级	5
举例	DEV/5/CHASSIS_REBOOT: Chassis 1 is rebooting now.
日志说明	用户在重启成员设备，或者成员设备因为异常而重启
处理建议	1. 检查是否有用户在重启成员设备 2. 如果没有用户重启，等待成员设备重新启动后，通过 **display version** 命令、对应成员设备单板信息中的 Last reboot reason 字段，查看重启原因 3. 如果重启原因为异常重启，请联系技术支持

21.29 CPU_STATE_NORMAL

日志内容	Cpu state changed to Normal on [STRING].
参数解释	$1：chassis编号+slot编号+CPU编号或slot编号+CPU编号，只有slot支持多CPU时，才显示CPU编号
日志等级	5
举例	DEV/5/CPU_STATE_NORMAL: Cpu state changed to Normal on slot 1 cpu 1.
日志说明	CPU状态变成正常
处理建议	无

21.30 DEV_CLOCK_CHANGE

日志内容	-User=[STRING]-IPAddr=[IPADDR]; System clock changed from [STRING] to [STRING].
参数解释	$1：当前登录用户的用户名 $2：当前登录用户的IP地址 $3：老时间 $4：新时间
日志等级	5
举例	DEV/5/DEV_CLOCK_CHANGE: -User=admin-IPAddr=192.168.1.2; System clock changed from 15:49:52 01/02/2013 to 15:50:00 01/02/2013.
日志说明	系统时间发生了变更
处理建议	无

21.31 DEV_FAULT_TOOLONG

日志内容	Card in [STRING] is still in Fault state for [INT32] minutes.
参数解释	$1：chassis编号+slot编号或slot编号 $2：状态的持续时间
日志等级	4
举例	DEV/4/DEV_FAULT_TOOLONG: Card in slot 1 is still in Fault state for 60 minutes.
日志说明	单板长期处于Fault状态
处理建议	1. 重启单板尝试恢复 2. 联系工程师分析解决

21.32 DEV_REBOOT_UNSTABLE

日志内容	A reboot command was executed while the system status was not Stable.
参数解释	无
日志等级	5
举例	DEV/5/DEV_REBOOT_UNSTABLE: A reboot command was executed while the system status was not Stable.
日志说明	设备处于非稳定状态时，用户执行了**reboot**命令
处理建议	系统启动需要一定的时间，才能达到Stable状态。所以，在系统启动过程中请不要执行重启操作。如果系统长时间未能进入Stable状态，可通过**display system stable state**命令的显示信息找出未稳定的对象，根据其具体状态，采取进一步措施

21.33 DYINGGASP

日志内容	Power failure or manual power-off occurred.
参数解释	无
日志等级	0
举例	DYINGGASP/0/DYINGGASP: Power failure or manual power-off occurred.
日志说明	设备掉电，发送断电告警
处理建议	1. 检查设备电源连接是否正确 2. 如果为电源模块故障，请更换电源模块 3. 联系工程师定位解决

21.34 FAN_ABSENT

日志内容	形式一： Fan [INT32] is absent. 形式二： Chassis [STRING] fan [INT32] is absent.
参数解释	形式一： $1：风扇ID 形式二： $1：chassis编号 $2：风扇ID
日志等级	3
举例	DEV/3/FAN_ABSENT: Fan 2 is absent.
日志说明	指定位置没有风扇，或风扇被拔出
处理建议	**1.** 如果指定位置没有风扇，则可能因散热不好，引起设备温度升高，建议安装风扇 **2.** 如果有风扇，检查风扇框是否插紧 **3.** 检查风扇框是否损坏 **4.** 重新安装风扇框或更换风扇框

21.35 FAN_DIRECTION_NOT_PREFERRED

日志内容	Fan [INT32] airflow direction is not preferred on [STRING], please check it.
参数解释	$1：风扇ID $2：chassis编号+slot编号或slot编号
日志等级	1
举例	DEV/1/FAN_DIRECTION_NOT_PREFERRED: Fan 1 airflow direction is not preferred on slot 1, please check it.
日志说明	风扇的风道方向不是用户期望的方向。风扇方向配置出错或者插错风扇
处理建议	**1.** 根据机房通风系统的风向，选择风向一致的型号的风扇 **2.** 如果风扇风向和机房通风系统风向一致，请调整风扇风向的配置

21.36 FAN_FAILED

日志内容	形式一： Fan [INT32] failed. 形式二： Chassis [STRING] fan [INT32] failed.
参数解释	形式一： $1：风扇ID 形式二： $1：chassis编号 $2：风扇ID
日志等级	2
举例	DEV/2/FAN_FAILED: Fan 2 failed.
日志说明	风扇出现了故障，停止工作
处理建议	更换风扇

21.37 FAN_RECOVERED

日志内容	形式一： Fan [INT32] recovered. 形式二： Chassis [INT32] fan [INT32] recovered.
参数解释	形式一： $1：风扇ID 形式二： $1：chassis编号 $2：风扇ID
日志等级	2
举例	DEV/2/FAN_RECOVERED: Fan 2 recovered.
日志说明	插入风扇，稍后，风扇转入正常工作状态
处理建议	无

21.38 MAD_DETECT

日志内容	Multi-active devices detected, please fix it.
参数解释	无
日志等级	1
举例	DEV/1/MAD_DETECT: Multi-active devices detected, please fix it.
日志说明	当收到冲突消息的时候，检测到冲突，需要解决冲突问题
处理建议	1. 使用 **display irf** 查看当前 IRF 中有哪些成员设备，以便确定哪些成员设备分裂了 2. 使用 **display irf link** 查看 IRF 链路信息，确认故障的 IRF 链路 3. 手工修复状态为 DOWN 的 IRF 链路

21.39 POWER_ABSENT

日志内容	形式一： Power [INT32] is absent. 形式二： Chassis [INT32] power [INT32] is absent.
参数解释	形式一： $1：电源模块ID 形式二： $1：chassis编号 $2：电源模块ID
日志等级	3
举例	DEV/3/POWER_ABSENT: Power 1 is absent.
日志说明	电源模块被拔出
处理建议	1. 检查电源是否插紧 2. 检查电源是否损坏 3. 重新安装电源或更换电源

21.40 POWER_FAILED

日志内容	形式一： Power [INT32] failed. 形式二： Chassis [INT32] power [INT32] failed.
参数解释	形式一： $1：电源模块ID 形式二： $1：chassis编号 $2：电源模块ID
日志等级	2
举例	DEV/2/POWER_FAILED: Power 1 failed.
日志说明	电源模块出现故障
处理建议	更换电源

21.41 POWER_MONITOR_ABSENT

日志内容	形式一： Power monitor unit [INT32] is absent. 形式二： Chassis [INT32] power monitor unit [INT32] is absent.
参数解释	形式一： $1：电源监控模块ID 形式二： $1：chassis编号 $2：电源监控模块ID
日志等级	3
举例	DEV/3/POWER_MONITOR_ABSENT: Power monitor unit 1 is absent.
日志说明	电源监控模块被拔出
处理建议	**1.** 检查电源监控模块是否插紧 **2.** 检查电源监控模块是否损坏 **3.** 重新安装电源监控模块或更换电源监控模块

21.42 POWER_MONITOR_FAILED

日志内容	形式一： Power monitor unit [INT32] failed. 形式二： Chassis [INT32] power monitor unit [INT32] failed.
参数解释	形式一： $1：电源监控模块ID 形式二： $1：chassis编号 $2：电源监控模块ID
日志等级	2
举例	DEV/2/POWER_MONITOR_FAILED: Power monitor unit 1 failed.
日志说明	电源监控模块出现故障
处理建议	更换电源监控模块

21.43 POWER_MONITOR_RECOVERED

日志内容	形式一： Power monitor unit [INT32] recovered. 形式二： Chassis [INT32] power monitor unit [INT32] recovered.
参数解释	形式一： $1：电源监控模块ID 形式二： $1：chassis编号 $2：电源监控模块ID
日志等级	2
举例	DEV/2/POWER_MONITOR_RECOVERED: Power monitor unit 1 recovered.
日志说明	电源监控模块插入后，状态从Failed或者Absent状态转换为OK
处理建议	无

21.44 POWER_RECOVERED

日志内容	形式一： Power [INT32] recovered. 形式二： Chassis [INT32] power [INT32] recovered.
参数解释	形式一： $1：电源模块ID 形式二： $1：chassis编号 $2：电源模块ID
日志等级	2
举例	DEV/2/POWER_RECOVERED: Power 1 recovered.
日志说明	电源模块插入后，状态从Failed或者Absent状态转换为OK
处理建议	无

21.45 RPS_ABSENT

日志内容	形式一： RPS [INT32] is absent. 形式二： Chassis [INT32] RPS [INT32] is absent.
参数解释	形式一： $1：冗余电源模块ID 形式二： $1：chassis编号 $2：冗余电源模块ID
日志等级	3
举例	DEV/3/RPS_ABSENT: RPS 1 is absent.
日志说明	冗余电源模块被拔出
处理建议	**1.** 检查冗余电源模块是否插紧 **2.** 检查冗余电源模块是否损坏 **3.** 重新安装冗余电源模块或更换冗余电源模块

21.46 RPS_NORMAL

日志内容	形式一： RPS [INT32] is normal. 形式二： Chassis [INT32] RPS [INT32] is normal.
参数解释	形式一： $1：冗余电源模块ID 形式二： $1：chassis编号 $2：冗余电源模块ID
日志等级	5
举例	DEV/5/RPS_NORMAL: RPS 1 is normal.
日志说明	冗余电源模块插入后，状态正常
处理建议	无

21.47 SUBCARD_FAULT

日志内容	Subcard state changed to Fault on [STRING] subslot [INT32], type is [STRING].
参数解释	$1：chassis编号+slot编号或slot编号 $2：子卡所在的子槽位号 $3：子卡类型
日志等级	2
举例	DEV/2/SUBCARD_FAULT: Subcard state changed to Fault on slot 1 subslot 1, type is MIM-1ATM-OC3SML.
日志说明	子卡重启，稍后，子卡状态转换为Fault，或者子卡故障
处理建议	**1.** 如果后续子卡状态可以变为 Normal，则无需处理 **2.** 如果子卡一直处于 Falut 状态，则子卡故障，更换子卡

21.48 SUBCARD_INSERTED

日志内容	Subcard was inserted in [STRING] subslot [INT32], type is [STRING].
参数解释	$1：chassis编号+slot编号或slot编号 $2：子卡所在的子槽位号 $3：子卡类型
日志等级	4
举例	DEV/4/SUBCARD_INSERTED: Subcard was inserted in slot 1 subslot 1, type is MIM-1ATM-OC3SML.
日志说明	一块子卡安装到了指定槽位
处理建议	无

21.49 SUBCARD_REBOOT

日志内容	Subcard is rebooting on [STRING] subslot [INT32].
参数解释	$1：chassis编号+slot编号或slot编号 $2：子卡所在的子槽位号
日志等级	5
举例	DEV/5/SUBCARD_REBOOT: Subcard is rebooting on slot 1 subslot 1.
日志说明	用户在重启子卡或者子卡因为运行异常自动重启
处理建议	如果子卡重启后能正常运行，则无需处理。如果您想进一步了解异常重启的原因或者子卡不断自动重启，请联系技术支持

21.50 SUBCARD_REMOVED

日志内容	Subcard was removed from [STRING] subslot [INT32], type is [STRING].
参数解释	$1：chassis编号+slot编号或slot编号 $2：子卡所在的子槽位号 $3：子卡类型
日志等级	3
举例	DEV/3/SUBCARD_REMOVED: Subcard was removed from slot 1 subslot 1, type is MIM-1ATM-OC3SML.
日志说明	一块子卡被拔出
处理建议	**1.** 检查子卡是否插紧 **2.** 检查子卡是否损坏 **3.** 重新安装子卡或更换子卡

21.51 SYSTEM_REBOOT

日志内容	System is rebooting now.
参数解释	无
日志等级	4
举例	DEV/4/SYSTEM_REBOOT: System is rebooting now.
日志说明	用户在重启系统，或者系统因为异常而重启
处理建议	1. 检查是否有用户在重启系统 2. 如果没有用户重启，等待系统重新启动后，通过 **display version** 命令显示信息中的 Last reboot reason 字段，查看重启原因 3. 如果重启原因为异常重启，请联系技术支持

21.52 TEMPERATURE_ALARM

日志内容	形式一： Temperature is greater than the high-temperature alarming threshold on sensor [STRING] [USHOT]. 形式二： Temperature is greater than the high-temperature alarming threshold on [STRING] sensor [STRING] [USHOT]. 形式三： Temperature is greater than the high-temperature alarming threshold on [STRING] [STRING] sensor [STRING] [USHOT].
参数解释	形式一： $1：传感器类型 $2：传感器ID 形式二： $1：slot编号 $2：传感器类型 $3：传感器ID 形式三： $1：chassis编号 $2：slot编号 $3：传感器类型 $4：传感器ID
日志等级	4
举例	DEV/4/TEMPERATURE_ALARM: Temperature is greater than the high-temperature alarming threshold on slot 1 sensor inflow 1.
日志说明	传感器温度超过严重级（Alarm）高温告警门限。环境温度太高或者风扇异常
处理建议	1. 检查环境温度是否过高，保持设备环境正常通风 2. **display fan** 命令检查风扇是否不在或故障，以及检查风扇实际是否运转。如果风扇不在位，安装风扇；如果风扇故障，更换风扇

21.53 TEMPERATURE_LOW

日志内容	形式一： Temperature is less than the low-temperature threshold on sensor [STRING] [INT32]. 形式二： Temperature is less than the low-temperature threshold on [STRING] sensor [STRING] [INT32]. 形式三： Temperature is less than the low-temperature threshold on [STRING] [STRING] sensor [STRING] [INT32].
参数解释	形式一： $1：传感器类型 $2：传感器ID 形式二： $1：slot编号 $2：传感器类型 $3：传感器ID 形式三： $1：chassis编号 $2：slot编号 $3：传感器类型 $4：传感器ID
日志等级	4
举例	DEV/4/TEMPERATURE_LOW: Temperature is less than the low-temperature threshold on slot 1 sensor inflow 1.
日志说明	传感器温度低于低温告警门限
处理建议	环境温度过低，改善环境温度

21.54 TEMPERATURE_NORMAL

日志内容	形式一： Temperature changed to normal on sensor [STRING] [INT32]. 形式二： Temperature changed to normal on [STRING] sensor [STRING] [INT32]. 形式三： Temperature changed to normal on [STRING] [STRING] sensor [STRING] [INT32].
参数解释	形式一： $1：传感器类型 $2：传感器ID 形式二： $1：slot编号 $2：传感器类型 $3：传感器ID 形式三： $1：chassis编号 $2：slot编号 $3：传感器类型 $4：传感器ID
日志等级	4
举例	DEV/4/TEMPERATURE_NORMAL: Temperature changed to normal on slot 1 sensor inflow 1.
日志说明	传感器温度指示正常（大于低温告警门限，小于一般级高温告警门限）
处理建议	无

21.55 TEMPERATURE_POWEROFF

日志内容	Powering off [STRING]: Temperature exceeded the shutdown threshold.
参数解释	$1：chassis编号+slot编号或slot编号
日志等级	5
举例	DEV/2/TEMPERATURE_POWEROFF: Powering off slot 1: Temperature exceeded the shutdown threshold.
日志说明	传感器温度指示正常（大于低温告警门限，小于一般级高温告警门限）
处理建议	1. 检查环境温度是否过高，保持设备环境通风正常 2. **display fan** 命令检查风扇是否拔出或故障，以及检查风扇实际是否运转。如果风扇不在位，安装风扇；如果风扇故障，更换风扇 3. 手动给单板上电

21.56 TEMPERATURE_SHUTDOWN

日志内容	形式一： Temperature is greater than the high-temperature shutdown threshold on sensor [STRING] [INT32]. The slot will be powered off automatically. 形式二： Temperature is greater than the high-temperature shutdown threshold on [STRING] sensor [STRING] [INT32]. The slot will be powered off automatically. 形式三： Temperature is greater than the high-temperature shutdown threshold on [STRING] [STRING] sensor [STRING] [INT32]. The slot will be powered off automatically.
参数解释	形式一： $1：传感器类型 $2：传感器ID 形式二： $1：slot编号 $2：传感器类型 $3：传感器ID 形式三： $1：chassis编号 $2：slot编号 $3：传感器类型 $4：传感器ID
日志等级	2
举例	DEV/2/TEMPERATURE_SHUTDOWN: Temperature is greater than the high-temperature shutdown threshold on slot 1 sensor inflow 1. The slot will be powered off automatically.
日志说明	传感器温度超过关断级高温告警门限。环境温度太高或者风扇异常
处理建议	1. 检查环境温度是否过高，保持设备环境通风正常 2. **display fan** 命令检查风扇是否不在或故障，以及检查风扇实际是否运转。如果风扇不在位，安装风扇；如果风扇故障，更换风扇

21.57 TEMPERATURE_WARNING

日志内容	形式一： Temperature is greater than the high-temperature warning threshold on sensor [STRING] [INT32]. 形式二： Temperature is greater than the high-temperature warning threshold on [STRING] sensor [STRING] [INT32]. 形式三： Temperature is greater than the high-temperature warning threshold on [STRING] [STRING] sensor [STRING] [INT32].
参数解释	形式一： $1：传感器类型 $2：传感器ID 形式二： $1：slot编号 $2：传感器类型 $3：传感器ID 形式三： $1：chassis编号 $2：slot编号 $3：传感器类型 $4：传感器ID
日志等级	4
举例	DEV/4/TEMPERATURE_WARNING: Temperature is greater than the high-temperature warning threshold on slot 1 sensor inflow 1.
日志说明	传感器温度超过一般级高温告警门限。环境温度太高或者风扇异常
处理建议	1. 检查环境温度是否过高，保持设备环境通风正常 2. **display fan** 命令检查风扇是否不在或故障，以及检查风扇实际是否运转。如果风扇不在位，安装风扇；如果风扇故障，更换风扇

21.58 VCHK_VERSION_INCOMPATIBLE

日志内容	Software version of [STRING] is incompatible with that of the MPU.
参数解释	$1：chassis编号+slot编号或slot编号
日志等级	1
举例	DEV/1/VCHK_VERSION_INCOMPATIBLE: Software version of slot 1 is incompatible with that of the MPU.
日志说明	PEX在启动过程中，检测到自己的启动软件包和父设备上运行的软件包版本不兼容，PEX会打印该信息并重启
处理建议	请设置与父设备当前版本兼容的软件包作为该PEX的下次启动软件包/加载软件包

22 DHCP

本节介绍 DHCP（Dynamic Host Configuration Protocol）模块输出的日志信息。

22.1 DHCP_NORESOURCES

日志内容	Failed to apply filtering rules for DHCP packets because hardware resources are insufficient.
参数解释	无
日志等级	3
举例	DHCP/3/DHCP_NORESOURCES: Failed to apply filtering rules for DHCP packets because hardware resources are insufficient.
日志说明	配置DHCP功能需要针对DHCP报文下发报文过滤规则。由于设备硬件资源不足，导致设置DHCP报文过滤规则失败
处理建议	如果设备业务占用硬件资源过多，可能会导致资源不足，需要释放一些资源，重新配置DHCP功能

22.2 DHCP_NOTSUPPORTED

日志内容	Failed to apply filtering rules for DHCP packets because some rules are not supported.
参数解释	无
日志等级	3
举例	DHCP/3/DHCP_NOTSUPPORTED: Failed to apply filtering rules for DHCP packets because some rules are not supported.
日志说明	配置DHCP功能需要针对DHCP报文下发DHCP报文过滤规则。由于设备不支持某些报文过滤规则，导致设置DHCP报文过滤规则失败
处理建议	无

23 DHCPR

本节介绍 DHCPR（IPv4 DHCP Relay）模块输出的日志信息。

23.1 DHCPR_SERVERCHANGE

日志内容	Switched to the server at [IPADDR] because the current server did not respond.
参数解释	$1：切换到下一个DHCP服务器的IP地址
日志等级	3
举例	DHCPR/3/DHCPR_SERVERCHANGE: -MDC=1; Switched to the server at *2.2.2.2* because the current server did not respond.
日志说明	因为DHCP中继无法从当前的DHCP服务器得到应答，所以DHCP中继切换到下一台DHCP服务器申请IP地址
处理建议	无需处理

23.2 DHCPR_SWITCHMASTER

日志内容	Switched to the master DHCP server at [IPADDR].
参数解释	$1：主用DHCP服务器的IP地址
日志等级	3
举例	DHCPR/3/DHCPR_SWITCHMASTER: -MDC=1; Switched to the master DHCP server at 2.2.2.2.
日志说明	DHCP中继可以配置延迟回切时间，如果当时生效的为备用服务器，在经过延迟时间，DHCP中继会切换到主用DHCP服务器来执行申请IP地址的操作
处理建议	无需处理

24 DHCPS

本节介绍 DHCPS（ipv4 DHCP server）模块输出的日志信息。

24.1 DHCPS_ALLOCATE_IP

日志内容	DHCP server received a DHCP client's request packet on interface [STRING], and allocated an IP address [IPADDR](lease [UINT32] seconds) for the DHCP client(MAC [MAC]) from [STRING] pool.
参数解释	$1：IPv4 DHCP服务器所在接口的接口名 $2：分配给IPv4 DHCP客户端的IPv4地址 $3：分配给IPv4 DHCP客户端的IPv4地址租约时长 $4：IPv4 DHCP客户端的MAC地址 $5：IPv4 DHCP服务器地址池名
日志等级	5
举例	DHCPS/5/DHCPS_ALLOCATE_IP: DHCP server received a DHCP client's request packet on interface GigabitEthernet1/0/2, and allocated an IP address 1.0.0.91(lease 86400 seconds) for the DHCP client(MAC 0000-0000-905a) from p1 pool.
日志说明	IPv4 DHCP服务器为IPv4 DHCP客户端分配一个IPv4地址租约
处理建议	无

24.2 DHCPS_CONFLICT_IP

日志内容	A conflict IP [IPADDR] from [STRING] pool was detected by DHCP server on interface [STRING].
参数解释	$1：冲突的IPv4地址 $2：IPv4 DHCP服务器地址池名 $3：IPv4 DHCP服务器所在接口的接口名
日志等级	5
举例	DHCPS/5/DHCPS_CONFLICT_IP: A conflict IP 100.1.1.1 from p1 pool was detected by DHCP server on interface GigabitEthernet1/0/2.
日志说明	IPv4 DHCP服务器从地址池中删除一个冲突地址
处理建议	无

24.3 DHCPS_EXTEND_IP

日志内容	DHCP server received a DHCP client's request packet on interface [STRING], and extended lease from [STRING] pool for the DHCP client (IP [IPADDR], MAC [MAC]).
参数解释	$1：IPv4 DHCP服务器所在接口的接口名 $2：IPv4 DHCP服务器地址池名 $3：分配给IPv4 DHCP客户端的IPv4地址 $4：IPv4 DHCP客户端的MAC地址
日志等级	5
举例	DHCPS/5/DHCPS_EXTEND_IP: DHCP server received a DHCP client's request packet on interface GigabitEthernet1/0/2, and extended lease from p1 pool for the DHCP client (IP 1.0.0.91, MAC 0000-0000-905a).
日志说明	IPv4 DHCP服务器为IPv4 DHCP客户端续约
处理建议	无

24.4 DHCPS_FILE

日志内容	Failed to save DHCP client information due to lack of storage resources.
参数解释	无
日志等级	4
举例	DHCPS/4/DHCPS_FILE: Failed to save DHCP client information due to lack of storage resources.
日志说明	因为磁盘空间不足导致DHCP server保存客户端信息到文件失败
处理建议	删除其他文件，使有空间保存此文件

24.5 DHCPS_RECLAIM_IP

日志内容	DHCP server reclaimed a [STRING] pool's lease(IP [IPADDR], lease [UINT32] seconds), which is allocated for the DHCP client (MAC [MAC]).
参数解释	$1：IPv4 DHCP服务器地址池名 $2：分配给IPv4 DHCP客户端的IPv4地址 $3：分配给IPv4 DHCP客户端的IPv4地址租约时长 $4：IPv4 DHCP客户端的MAC地址
日志等级	5
举例	DHCPS/5/DHCPS_RECLAIM_IP: DHCP server reclaimed a p1 pool's lease(IP 1.0.0.91, lease 86400 seconds), which is allocated for the DHCP client (MAC 0000-0000-905a).
日志说明	IPv4 DHCP服务器回收一个分配给IPv4 DHCP客户端的地址租约
处理建议	无

24.6 DHCPS_THRESHOLD_EXCEED

日志内容	The IP address utilization of the address pool [STRING] has exceeded the threshold.
参数解释	$1：地址池名称
日志等级	4
举例	DHCPS/4/DHCPS_THRESHOLD_EXCEED: The IP address utilization of the address pool 1 has exceeded the threshold.
日志说明	DHCP地址池中的地址使用率已经高于指定阈值
处理建议	管理员需要重新规划地址池中的地址资源

24.7 DHCPS_THRESHOLD_RECOVER

日志内容	The IP address usage of pool [STRING] has descended to 90% of the threshold.
参数解释	$1：地址池名称
日志等级	4
举例	DHCPS/4/DHCPS_THRESHOLD_RECOVER: The IP address usage of pool 1 has descended to 90% of the threshold.
日志说明	DHCP地址池中的地址使用率已经下降到指定阈值的90%
处理建议	无

24.8 DHCPS_VERIFY_CLASS

日志内容	Illegal DHCP client-PacketType=[STRING]-ClientAddress=[MAC];
参数解释	$1：报文类型 $2：IPv4 DHCP客户端的硬件地址
日志等级	5
举例	DHCPS/5/DHCPS_VERIFY_CLASS: Illegal DHCP client-PacketType= DHCPDISCOVER-ClientAddress=0000-5e01-0104;
日志说明	IPv4 DHCP服务器对客户端报文白名单验证不通过
处理建议	确认该DHCP客户端是否合法

24.9 DHCPS_WARNING_EXHAUSTION

日志内容	Address pool [STRING] has run out of IP addresses.
参数解释	$1：地址池名称
日志等级	3
举例	DHCPS/3/DHCPS_WARNING_EXHAUSTION: Address pool 1 has run out of IP addresses.
日志说明	DHCP地址池中的地址资源已耗尽
处理建议	管理员需要重新规划地址池中的地址资源

25 DHCPS6

本节介绍 DHCPS6（IPv6 DHCP server）模块输出的 日志信息。

25.1 DHCPS6_ALLOCATE_ADDRESS

日志内容	DHCPv6 server received a DHCPv6 client's request packet on interface [STRING], and allocated an IPv6 address [IPADDR] (lease [UINT32] seconds) for the DHCP client(DUID [HEX], IAID [HEX]) from [STRING] pool.
参数解释	$1：IPv6 DHCP服务器所在接口的接口名 $2：分配给IPv6 DHCP客户端的ipv6地址 $3：分配给IPv6 DHCP客户端的ipv6地址租约时长 $4：IPv6 DHCP客户端的DUID $5：IPv6 DHCP客户端的IAID $6：IPv6 DHCP服务器地址池名
日志等级	5
举例	DHCPS6/5/DHCPS6_ALLOCATE_ADDRESS: DHCPv6 server received a DHCPv6 client's request packet on interface Ethernet0/2, and allocated an IPv6 address 2000::3(lease 60 seconds) for the DHCP client(DUID 0001000118137c37b4b52facab5a, IAID 10b4b52f) from p1 pool.
日志说明	IPv6 DHCP服务器为IPv6 DHCP客户端分配一个IPv6地址租约
处理建议	无

25.2 DHCPS6_ALLOCATE_PREFIX

日志内容	DHCPv6 server received a DHCPv6 client's request packet on interface [STRING], and allocated an IPv6 prefix [IPADDR] (lease [UINT32] seconds) for the DHCP client(DUID [HEX], IAID [HEX]) from [STRING] pool.
参数解释	$1：IPv6 DHCP服务器所在接口的接口名 $2：分配给IPv6 DHCP客户端的IPv6前缀地址 $3：分配给IPv6 DHCP客户端的IPv6前缀地址租约时长 $4：IPv6 DHCP客户端的DUID $5：IPv6 DHCP客户端的IAID $6：IPv6 DHCP服务器地址池名
日志等级	5
举例	DHCPS6/5/DHCPS6_ALLOCATE_PREFIX: DHCPv6 server received a DHCPv6 client's request packet on interface Ethernet0/2, and allocated an IPv6 prefix 2000::(lease 60 seconds) for the DHCP client(DUID 0001000118137c37b4b52facab5a, IAID 10b4b52f) from p1 pool.
日志说明	IPv6 DHCP服务器为IPv6 DHCP客户端分配一个IPv6前缀地址租约
处理建议	无

25.3 DHCPS6_CONFLICT_ADDRESS

日志内容	A conflict IPv6 address [IPADDR] from [STRING] pool was detected by DHCPv6 server on interface [STRING].
参数解释	$1：冲突的IPv6地址 $2：IPv6 DHCP服务器地址池名 $3：IPv6 DHCP服务器所在接口的接口名
日志等级	5
举例	DHCPS6/5/DHCPS6_CONFLICT_ADDRESS: A conflict IPv6 address 33::1 from p1 pool was detected by DHCPv6 server on interface Ethernet0/2.
日志说明	IPv6 DHCP服务器从地址池删除一个冲突地址
处理建议	无

25.4 DHCPS6_EXTEND_ADDRESS

日志内容	DHCPv6 server received a DHCP client's request packet on interface [STRING], and extended lease from [STRING] pool for the DHCP client (IPv6 address [IPADDR], DUID [HEX], IAID [HEX]).
参数解释	$1：IPv6 DHCP服务器所在接口的接口名 $2：IPv6 DHCP服务器地址池名 $3：分配给IPv6 DHCP客户端的IPv6地址 $4：IPv6 DHCP客户端的DUID $5：IPv6 DHCP客户端的IAID
日志等级	5
举例	DHCPS6/5/DHCPS6_EXTEND_ADDRESS: DHCPv6 server received a DHCP client's request packet on interface Ethernet0/2, and extended lease from p1 pool for the DHCP client (IPv6 address 2000::3, DUID 0001000118137c37b4b52facab5a, IAID 10b4b52f).
日志说明	IPv6 DHCP服务器为IPv6 DHCP客户端地址续约
处理建议	无

25.5 DHCPS6_EXTEND_PREFIX

日志内容	DHCPv6 server received a DHCP client's request packet on interface [STRING], and extended lease from [STRING] pool for the DHCP client (IPv6 prefix [IPADDR], DUID [HEX], IAID [HEX]).
参数解释	$1：IPv6 DHCP服务器所在接口的接口名 $2：IPv6 DHCP服务器地址池名 $3：分配给IPv6 DHCP客户端的IPv6前缀地址 $4：IPv6 DHCP客户端的DUID $5：IPv6 DHCP客户端的IAID
日志等级	5
举例	DHCPS6/5/DHCPS6_EXTEND_PREFIX: DHCPv6 server received a DHCP client's request packet on interface Ethernet0/2, and extended lease from p1 pool for the DHCP client (IPv6 prefix 2000::, DUID 0001000118137c37b4b52facab5a, IAID 10b4b52f).
日志说明	IPv6 DHCP服务器为IPv6 DHCP客户端前缀地址续约
处理建议	无

25.6 DHCPS6_FILE

日志内容	Failed to save DHCP client information due to lack of storage resources.
参数解释	无
日志等级	4
举例	DHCPS6/4/DHCPS6_FILE: Failed to save DHCP client information due to lack of storage resources.
日志说明	因为磁盘空间不足导致DHCPv6 server保存客户端信息到文件失败
处理建议	删除其他文件，使有空间保存此文件

25.7 DHCPS6_RECLAIM_ADDRESS

日志内容	DHCPv6 server reclaimed a [STRING] pool's lease(IPv6 address [IPADDR], lease [UINT32] seconds), which is allocated for the DHCPv6 client (DUID [HEX], IAID [HEX]).
参数解释	$1：IPv6 DHCP服务器地址池名 $2：分配给IPv6 DHCP客户端的IPv6地址 $3：分配给IPv6 DHCP客户端的IPv6地址租约时长 $4：IPv6 DHCP客户端的DUID $5：IPv6 DHCP客户端的IAID
日志等级	5
举例	DHCPS6/5/DHCPS6_RECLAIM_ADDRESS: DHCPv6 server reclaimed a p1 pool's lease(IPv6 address 2000::3, lease 60 seconds), which is allocated for the DHCPv6 client (DUID 0001000118137c37b4b52facab5a, IAID 10b4b52f).
日志说明	IPv6 DHCP服务器回收一个分配给IPv6客户端的地址租约
处理建议	无

25.8 DHCPS6_RECLAIM_PREFIX

日志内容	DHCPv6 server reclaimed a [STRING] pool's lease(IPv6 prefix [IPADDR], lease [INTEGER] seconds), which is allocated for the DHCPv6 client (DUID [HEX], IAID [HEX]).
参数解释	$1：IPv6 DHCP服务器所在接口的接口名 $2：分配给IPv6 DHCP客户端的IPv6前缀地址 $3：分配给IPv6 DHCP客户端的IPv6前缀地址租约时长 $4：IPv6 DHCP客户端的DUID $5：IPv6 DHCP客户端的IAID
日志等级	5
举例	DHCPS6/5/DHCPS6_RECLAIM_PREFIX: DHCPv6 server reclaimed a p1 pool's lease(IPv6 prefix 2000::, lease 60 seconds), which is allocated for the DHCPv6 client (DUID 0001000118137c37b4b52facab5a, IAID 10b4b52f).
日志说明	IPv6 DHCP服务器回收一个分配给IPv6客户端的前缀地址租约
处理建议	无

26 DHCPSP4

本节介绍 DHCPSP4 模块输出的 日志信息。

26.1 DHCPSP4_FILE

日志内容	Failed to save DHCP client information due to lack of storage resources.
参数解释	无
日志等级	4
举例	DHCPSP4/4/DHCPSP4_FILE: Failed to save DHCP client information due to lack of storage resources.
日志说明	因为磁盘空间不足导致DHCPv4 snooping保存客户端信息到文件失败
处理建议	删除其他文件，使有空间保存此文件

27 DHCPSP6

本节介绍 DHCPSP6 模块输出的日志信息。

27.1 DHCPSP6_FILE

日志内容	Failed to save DHCP client information due to lack of storage resources.
参数解释	无
日志等级	4
举例	DHCPSP6/4/DHCPSP6_FILE: Failed to save DHCP client information due to lack of storage resources.
日志说明	因为磁盘空间不足导致DHCPv6 snooping保存客户端信息到文件失败
处理建议	删除其他文件，使有空间保存此文件

28 DIAG

本节介绍 DIAG 综合诊断模块输出的日志信息，当 hardware-failure-detection { board | chip | forwarding }级别在 isolate/reset/warning 时，才会输出日志信息。

28.1 CPU_MINOR_RECOVERY

日志内容	CPU usage recovered to normal state.
参数解释	无
日志等级	4
举例	DIAG/4/CPU_MINOR_THRESHOLD: CPU usage recovered to normal state.
日志说明	当设备处于CPU低级别告警状态，并且采样值小于或等于恢复门限时，解除CPU低级别告警状态，CPU使用率恢复到正常
处理建议	根据提示信息操作设备，合理使用CPU资源

28.2 CPU_MINOR_THRESHOLD

日志内容	CPU usage is in minor alarm state.
参数解释	无
日志等级	4
举例	DIAG/4/CPU_MINOR_THRESHOLD: CPU usage is in minor alarm state.
日志说明	当CPU使用率的采样值从小于/等于变成大于低级别告警门限时，设备进入CPU低级别告警状态，并定期输出该日志，直到CPU低级别告警状态解除
处理建议	根据提示信息操作设备，合理使用CPU资源

28.3 CPU_SEVERE_RECOVERY

日志内容	CPU usage severe alarm removed.
参数解释	无
日志等级	3
举例	DIAG/3/CPU_RECOVERY: CPU usage severe alarm removed.
日志说明	当设备处于CPU高级别告警状态，并且采样值小于或等于低级别告警门限时，解除CPU高级别告警状态，输出该日志
处理建议	无

28.4 CPU_SEVERE_THRESHOLD

日志内容	CPU usage is in severe alarm state.
参数解释	无
日志等级	3
举例	DIAG/3/CPU_THRESHOLD: CPU usage is in severe alarm state.
日志说明	当CPU使用率的采样值从小于/等于变成大于高级别告警门限时，设备进入CPU高级别告警状态，并定期输出该日志，直到CPU高级别告警状态解除
处理建议	请使用display current-configuration | include "monitor cpu-usage"命令查看CPU的告警门限，如果门限设置不合适，请使用monitor cpu-usage命令修改

28.5 DIAG_AI

日志内容	Board fault: chassis [STRING] slot [STRING], please check it
参数解释	无
日志等级	3
举例	DIAG/3/ DIAG_AI: -MDC=1; Board fault: chassis 2 slot 1, please check it
日志说明	DIAG综合诊断发现单点故障
处理建议	联系技术支持

28.6 DIAG_AI

日志内容	Board fault: chassis [STRING] slot [STRING], chassis [STRING] slot [STRING] or chassis [STRING] slot [STRING], please check them
参数解释	无
日志等级	3
举例	DIAG/3/DIAG_AI: -MDC=1; Board fault: chassis 1 slot 4, chassis 1 slot 10 or chassis 1 slot 0, please check them
日志说明	DIAG综合诊断发现多点故障
处理建议	联系技术支持

28.7 FMEA

日志内容	Hardware error detected on chassis [UINT32] slot [UINT32]. Rebooting the card…
参数解释	$1：设备在IRF中的成员编号 $2：单板所在的槽位号
日志等级	2
举例	DIAG/2/FMEA: Hardware error detected on chassis 1 slot 2. Rebooting the card…
日志说明	FMEA检测到接口板硬件故障，该接口板即将重启
处理建议	请联系技术支持

28.8 FMEA

日志内容	Hardware error detected on slot [UINT32]. Rebooting the card…
参数解释	$1：单板所在的槽位号
日志等级	2
举例	DIAG/2/FMEA: Hardware error detected on slot 2. Rebooting the card…
日志说明	FMEA检测到接口板硬件故障，该接口板即将重启
处理建议	请联系技术支持

28.9 FMEA

日志内容	Hardware error detected on chassis [UINT32] slot [UINT32].
参数解释	$1：设备在IRF中的成员编号 $2：单板所在的槽位号
日志等级	3
举例	DIAG/3/FMEA: Hardware error detected on chassis 1 slot 2.
日志说明	FMEA检测到接口板硬件故障，设备仅发送Syslog信息，不会修复故障
处理建议	请联系技术支持

28.10 FMEA

日志内容	Hardware error detected on slot [UINT32].
参数解释	$1：单板所在的槽位号
日志等级	3
举例	DIAG/3/FMEA: Hardware error detected on slot 2.
日志说明	FMEA检测到接口板硬件故障，设备发送Syslog信息，不会修复故障
处理建议	请联系技术支持

28.11 DIAG_STORAGE_BELOW_THRESHOLD

日志内容	The usage of [STRING] ([UINT32]%) was below or equal to the threshold of [UINT32]%.
参数解释	$1：存储介质的名称 $2：存储介质磁盘空间使用率 $3：存储介质使用率阈值
日志等级	1
举例	DIAG/1/DIAG_STORAGE_BELOW_THRESHOLD: The usage of flash (90%) was below or equal to the threshold of 95%.
日志说明	存储介质磁盘空间使用率小于或等于阈值
处理建议	无

28.12 DIAG_STORAGE_EXCEED_THRESHOLD

日志内容	The usage of [STRING] ([UINT32]%) exceeded the threshold of [UINT32]%.
参数解释	$1：存储介质的名称 $2：存储介质磁盘空间使用率 $3：存储介质使用率的阈值
日志等级	1
举例	DIAG/1/DIAG_STORAGE_EXCEED_THRESHOLD: The usage of flash (96%) exceeded the threshold of 95%.
日志说明	存储介质磁盘空间使用率大于阈值
处理建议	对长期不使用的文件，例如日志文件和历史版本的软件包，使用**delete**命令直接删除或者备份到PC后再删除

28.13 MEM_ALERT

日志内容	system memory info: total used free shared buffers cached Mem: [ULONG] [ULONG] [ULONG] [ULONG] [ULONG] [ULONG] -/+ buffers/cache: [ULONG] [ULONG] Swap: [ULONG] [ULONG] [ULONG] Lowmem: [ULONG] [ULONG] [ULONG]

参数解释	• 整个系统中内存的统计信息：
	  ○ $1：系统可分配的物理内存的大小。设备总物理内存分为不可分配物理内存和可分配物理内存。其中，不可分配物理内存用于内核代码段存储、内核管理开销以及基本功能的运行等；可分配物理内存用于支撑业务模块的运行、文件存储等操作。不可分配内存的大小由设备根据系统运行需要自动计算划分，可分配物理内存的大小等于设备总物理内存减去不可分配内存的大小
	  ○ $2：整个系统已用的物理内存大小
	  ○ $3：整个系统可用的物理内存大小
	  ○ $4：多个进程共享的物理内存总额
	  ○ $5：已使用的文件缓冲区的大小
	  ○ $6：高速缓冲寄存器已使用的内存大小
	• 应用程序对内存的使用情况：
	  ○ $7：-/+ Buffers/Cache:used = Mem:Used – Mem:Buffers – Mem:Cached，表示应用程序已用的物理内存大小
	  ○ $8：-/+ Buffers/Cache:free = Mem:Free + Mem:Buffers + Mem:Cached，表示应用程序可用的物理内存大小
	• 交换分区的使用信息：
	  ○ $9：交换分区的总大小
	  ○ $10：已用的交换分区的大小
	  ○ $11：可用的交换分区的大小
	• Low memory 的使用情况：
	  ○ $12：Low memory 中内存的大小
	  ○ $13：Low memory 中已用内存的大小
	  ○ $14：Low memory 中可用内存的大小

日志等级	4
举例	DIAG/4/MEM_ALERT: system memory info: total used free shared buffers cached Mem: 1784424 920896 863528 0 0 35400 -/+ buffers/cache: 885496 898928 Swap: 0 0 0 Lowmem: 735848 637896 97952
日志说明	内存告警。当已使用的内存大于或等于一级、二级或三级内存告警门限时，系统会输出该信息，告知用户内存的具体使用情况
处理建议	1. 请使用 **display memory-threshold** 命令查看内存的一级、二级、三级告警门限。如果门限设置不合适，请使用 **memory-threshold** 命令修改

	2. 检查 ARP、路由表信息，排除设备受到非法攻击可能 3. 检查和优化组网，减少路由条目或者更换更高规格的设备

28.14 MEM_BELOW_THRESHOLD

日志内容	Memory usage has dropped below [STRING] threshold.
参数解释	$1：内存告警门限级别，包括： ○ minor：一级 ○ severe：二级 ○ critical：三级
日志等级	1
举例	DIAG/1/MEM_BELOW_THRESHOLD: Memory usage has dropped below critical threshold.
日志说明	内存告警解除。当系统剩余空闲内存大于内存恢复门限时，系统会输出该信息
处理建议	无

28.15 MEM_EXCEED_THRESHOLD

日志内容	Memory [STRING] threshold has been exceeded.
参数解释	$1：内存告警门限级别，包括： ○ minor：一级 ○ severe：二级 ○ critical：三级
日志等级	1
举例	DIAG/1/MEM_EXCEED_THRESHOLD: Memory minor threshold has been exceeded.
日志说明	内存告警。当已使用的内存大于或等于一级、二级或三级内存告警门限时，系统会输出该信息，并通知各业务模块进行自动修复：比如，不再申请新的内存或者释放部分内存
处理建议	1. 请使用 **display memory-threshold** 命令查看内存的一级、二级、三级告警门限。如果门限设置不合适，请使用 **memory-threshold** 命令修改 2. 检查 ARP、路由表信息，排除设备受到非法攻击可能 3. 检查和优化组网，减少路由条目或者更换更高规格的设备

29 DLDP

本节介绍 DLDP 模块输出的日志信息。

29.1 DLDP_AUTHENTICATION_FAILED

日志内容	The DLDP packet failed the authentication because of unmatched [STRING] field.
参数解释	$1：验证字段 ○ AUTHENTICATION PASSWORD：表示验证字不匹配 ○ AUTHENTICATION TYPE：表示验证类型不匹配 ○ INTERVAL：表示通告间隔不匹配
日志等级	5
举例	DLDP/5/DLDP_AUTHENTICATION_FAILED: The DLDP packet failed the authentication because of unmatched INTERVAL field.
日志说明	报文验证失败。可能的原因包括：验证类型不匹配、验证字不匹配、通告间隔不匹配
处理建议	检查DLDP验证类型、验证字和通告间隔是否与对端一致

29.2 DLDP_LINK_BIDIRECTIONAL

日志内容	DLDP detected a bidirectional link on interface [STRING].
参数解释	$1：接口名
日志等级	6
举例	DLDP/6/DLDP_LINK_BIDIRECTIONAL: DLDP detected a bidirectional link on interface Ethernet1/1.
日志说明	DLDP在接口上检测到双向链路
处理建议	无

29.3 DLDP_LINK_SHUTMODECHG

日志内容	DLDP automatically blocked the interface [STRING] because the port shutdown mode was changed to auto mode.
参数解释	$1：接口名
日志等级	5
举例	DLDP/5/DLDP_LINK_SHUTMODECHG: DLDP automatically blocked the interface Ethernet1/1 because the port shutdown mode was changed to auto mode.
日志说明	DLDP单通关闭模式由手动修改为自动，关闭端口
处理建议	无

29.4 DLDP_LINK_UNIDIRECTIONAL

日志内容	DLDP detected a unidirectional link on interface [STRING]. [STRING].
参数解释	$1：接口名 $2：接口关闭模式所指定的动作 ○ DLDP automatically blocked the interface：表示 DLDP 自动关闭了端口 ○ Please manually shut down the interface：表示需要用户手动关闭端口
日志等级	3
举例	DLDP/3/DLDP_LINK_UNIDIRECTIONAL: DLDP detected a unidirectional link on interface Ethernet1/1. DLDP automatically blocked the interface.
日志说明	DLDP在接口上检测到单向链路
处理建议	检查线缆是否错接、脱落或者出现其他故障

29.5 DLDP_NEIGHBOR_AGED

日志内容	A neighbor on interface [STRING] was deleted because the neighbor was aged. The neighbor's system MAC is [MAC], and the port index is [UINT16].
参数解释	$1：接口名 $2：MAC地址 $3：接口索引
日志等级	5
举例	DLDP/5/DLDP_NEIGHBOR_AGED: A neighbor on interface Ethernet1/1 was deleted because the neighbor was aged. The neighbor's system MAC is 000f-e269-5f21, and the port index is 1.
日志说明	接口删除了一个已老化的邻居
处理建议	无

29.6 DLDP_NEIGHBOR_CONFIRMED

日志内容	A neighbor was confirmed on interface [STRING]. The neighbor's system MAC is [MAC], and the port index is [UINT16].
参数解释	$1：接口名 $2：MAC地址 $3：接口索引
日志等级	6
举例	DLDP/6/DLDP_NEIGHBOR_CONFIRMED: A neighbor was confirmed on interface Ethernet1/1. The neighbor's system MAC is 000f-e269-5f21, and the port index is 1.
日志说明	接口检测到一个处于确定状态的邻居
处理建议	无

29.7 DLDP_NEIGHBOR_DELETED

日志内容	A neighbor on interface [STRING] was deleted because a [STRING] packet arrived. The neighbor's system MAC is [MAC], and the port index is [UINT16].
参数解释	$1：接口名 $2：报文类型 ○ DISABLE：表示收到了 Disable 报文 ○ LINKDOWN：表示收到了 LinkDown 报文 $3：MAC地址 $4：接口索引
日志等级	5
举例	DLDP/5/DLDP_NEIGHBOR_DELETED: A neighbor on interface Ethernet1/1 was deleted because a DISABLE packet arrived. The neighbor's system MAC is 000f-e269-5f21, and the port index is 1.
日志说明	由于收到了Disable报文或LinkDown报文，因此接口删除一个处于确定状态的邻居
处理建议	无

30 DOMAIN

本节介绍 DOMAIN 模块输出的日志信息。

30.1 DOMAIN_IP_LOWTHR_ALM

日志内容	-Domain=[STRING]-IPUsage=[STRING]-IPPoolLowerValue=[STRING]; IP resource usage reached or dropped below the lower threshold.
参数解释	$1：ISP域名称 $2：IP地址使用率 $3：IP地址使用率下限阈值
日志等级	4
举例	DOMAIN/4/DOMAIN_IP_LOWTHR_ALM: -Domain=abc-IPUsage=10%-IPPoolLowerValue=20%; IP resource usage reached or dropped below the lower threshold.
日志说明	当域下授权IP地址池/IP地址池组中的IP地址使用率达到或低于告警下限阈值，生成下限告警
处理建议	无

30.2 DOMAIN_IP_LOWTHR_ALM_REMOVE

日志内容	-Domain=[STRING]-IPUsage=[STRING]-IPPoolLowerValue=[STRING]; Low IP resource usage alarm condition cleared.
参数解释	$1：ISP域名称 $2：IP地址使用率 $3：IP地址使用率下限阈值
日志等级	4
举例	DOMAIN/4/DOMAIN_IP_LOWTHR_ALM_REMOVE: -Domain=dom1-IPUsage=50%-IPPoolLowerValue=20%; Low IP resource usage alarm condition cleared.
日志说明	当域下授权IP地址池/IP地址池组中的IP地址使用率>=（下限阈值+告警差值）时，生成使用率下限恢复告警 其中，告警差值=（上限阈值–下限阈值）*10%
处理建议	无

30.3 DOMAIN_IP_UPTHR_ALM

日志内容	-Domain=[STRING]-IPUsage=[STRING]-IPPoolUpperValue=[STRING]; IP resource usage reached or exceeded the upper threshold.
参数解释	$1：ISP域名称 $2：IP地址使用率 $3：IP地址使用率上限阈值
日志等级	4
举例	DOMAIN/4/DOMAIN_IP_UPTHR_ALM: -Domain=dom1-IPUsage=90%-IPPoolUpperValue=80%; IP resource usage reached or exceeded the upper threshold.
日志说明	当域下授权IP地址池中/IP地址池组的IP地址使用率达到或超过告警上限阈值，生成上限告警
处理建议	无

30.4 DOMAIN_IP_UPTHR_ALM_REMOVE

日志内容	-Domain=[STRING]-IPUsage=[STRING]-IPPoolUpperValue=[STRING]; High IP resource usage alarm condition cleared.
参数解释	$1：ISP域名称 $2：IP地址使用率 $3：IP地址使用率上限阈值
日志等级	4
举例	DOMAIN/4/DOMAIN_IP_UPTHR_ALM_REMOVE: -Domain=dom1-IPUsage=50%-IPPoolUpperValue=80%; High IP resource usage alarm condition cleared.
日志说明	当域下授权IP地址池/IP地址池组中的IP地址使用率<=（上限阈值–告警差值）时，生成使用率上限恢复告警 其中，告警差值=（上限阈值–下限阈值）*10%
处理建议	无

30.5 DOMAIN_IPV6_LOWTHR_ALM

日志内容	-Domain=[STRING]-IPv6Usage=[STRING]-IPv6PoolLowerValue=[STRING]; IPv6 address resource usage reached or dropped below the lower threshold.
参数解释	$1：ISP域名称 $2：IPv6地址使用率 $3：IPv6地址使用率下限阈值
日志等级	4
举例	DOMAIN/4/DOMAIN_IPV6_LOWTHR_ALM: -Domain=abc-IPv6Usage=10%-IPv6PoolLowerValue=20%; IPv6 address resource usage reached or dropped below the lower threshold.
日志说明	当域下授权IPv6地址池/IPv6地址池组中的IPv6地址使用率达到或低于告警下限阈值，生成下限告警
处理建议	无

30.6 DOMAIN_IPV6_LOWTHR_ALM_REMOVE

日志内容	-Domain=[STRING]-IPv6Usage=[STRING]-IPv6PoolLowerValue=[STRING]; Low IPv6 address resource usage alarm condition cleared.
参数解释	$1：ISP域名称 $2：IPv6地址使用率 $3：IPv6地址使用率下限阈值
日志等级	4
举例	DOMAIN/4/DOMAIN_IPV6_LOWTHR_ALM_REMOVE: -Domain=dom1-IPv6Usage=50%-IPv6PoolLowerValue=20%; Low IPv6 address resource usage alarm condition cleared.
日志说明	当域下授权IPv6地址池/IPv6地址池组中的IPv6地址使用率>=（下限阈值+告警差值）<=（上限阈值-告警差值）时，生成使用率恢复告警 其中，告警差值=（上限阈值–下限阈值）*10%
处理建议	无

30.7 DOMAIN_IPV6_UPTHR_ALM

日志内容	-Domain=[STRING]-IPv6Usage=[STRING]-IPv6PoolUpperValue=[STRING]; IPv6 address resource usage reached or exceeded the upper threshold.
参数解释	$1：ISP域名称 $2：IPv6地址使用率 $3：IPv6地址使用率上限阈值
日志等级	4
举例	DOMAIN/4/DOMAIN_IPV6_UPTHR_ALM: -Domain=abc-IPv6Usage=90%-IPv6PoolUpperValue=80%; IPv6 address resource usage reached or exceeded the upper threshold.
日志说明	当域下授权IPv6地址池/IPv6地址池组中的IPv6地址使用率达到或超过告警上限阈值，生成上限告警
处理建议	无

30.8 DOMAIN_IPV6_UPTHR_ALM_REMOVE

日志内容	-Domain=[STRING]-IPv6Usage=[STRING]-IPv6PoolUpperValue=[STRING]; High IPv6 address resource usage alarm condition cleared.
参数解释	$1：ISP域名称 $2：IPv6地址使用率 $3：IPv6地址使用率上限阈值
日志等级	4
举例	DOMAIN/4/DOMAIN_IPV6_UPTHR_ALM_REMOVE: -Domain=dom1-IPv6Usage=50%-IPv6PoolUpperValue=80%; High IPv6 address resource usage alarm condition cleared.
日志说明	当域下授权IPv6地址池/IPv6地址池组中的IPv6地址使用率<=（上限阈值-告警差值）时，生成使用率恢复告警 其中，告警差值=（上限阈值–下限阈值）*10%
处理建议	无

30.9 DOMAIN_ND_PREF_LOWTHR_ALM

日志内容	-Domain=[STRING]-NDPrefixUsage=[STRING]-IPv6PoolLowerValue=[STRING]; ND prefix resource usage reached or dropped below the lower threshold.
参数解释	$1：ISP域名称 $2：ND前缀使用率 $3：IPv6前缀使用率下限阈值
日志等级	4
举例	DOMAIN/4/DOMAIN_ND_PREF_LOWTHR_ALM: -Domain=abc-NDPrefixUsage=10%-IPv6PoolLowerValue=20%; ND prefix resource usage reached or dropped below the lower threshold.
日志说明	当域下授权ND前缀池/ND前缀地址池组中的ND前缀使用率达到或低于告警下限阈值，生成下限告警
处理建议	无

30.10 DOMAIN_ND_PREF_LOWTHR_ALM_REMOVE

日志内容	-Domain=[STRING]-NDPrefixUsage=[STRING]-IPv6PoolLowerValue=[STRING]; Low ND prefix resource usage alarm condition cleared.
参数解释	$1：ISP域名称 $2：ND前缀使用率 $3：IPv6前缀使用率下限阈值
日志等级	4
举例	DOMAIN/4/DOMAIN_ND_PREF_LOWTHR_ALM_REMOVE: -Domain=abc-NDPrefixUsage=50%-IPv6PoolLowerValue=20%; Low ND prefix resource usage alarm condition cleared.
日志说明	当域下授权ND前缀池/ND前缀地址池组中的ND前缀使用率>=（下限阈值+告警差值）<=（上限阈值-告警差值）时，生成使用率恢复告警 其中，告警差值=（上限阈值–下限阈值）*10%
处理建议	无

30.11 DOMAIN_ND_PREF_UPTHR_ALM

日志内容	-Domain=[STRING]-NDPrefixUsage=[STRING]-IPv6PoolUpperValue=[STRING]; ND prefix resource usage reached or exceeded the upper threshold.
参数解释	$1：ISP域名称 $2：ND前缀使用率 $3：IPv6前缀使用率上限阈值
日志等级	4
举例	DOMAIN/4/DOMAIN_ND_PREF_UPTHR_ALM: -Domain=abc-NDPrefixUsage=90%-IPv6PoolUpperValue=80%; ND prefix resource usage reached or exceeded the upper threshold.
日志说明	当域下授权ND前缀池/ND前缀地址池组中的ND前缀使用率达到或超过告警上限阈值，生成上限告警
处理建议	无

30.12 DOMAIN_ND_PREF_UPTHR_ALM_REMOVE

日志内容	-Domain=[STRING]-NDPrefixUsage=[STRING]-IPv6PoolUpperValue=[STRING]; High ND prefix resource usage alarm condition cleared.
参数解释	$1：ISP域名称 $2：ND前缀使用率 $3：IPv6前缀使用率上限阈值
日志等级	4
举例	DOMAIN/4/DOMAIN_ND_PREF_UPTHR_ALM_REMOVE: -Domain=abc-NDPrefixUsage=50%-IPv6PoolUpperValue=80%; High ND prefix resource usage alarm condition cleared.
日志说明	当域下授权ND前缀池/ND前缀地址池组中的ND前缀使用率<=（上限阈值-告警差值）时，生成使用率恢复告警 其中，告警差值=（上限阈值–下限阈值）*10%
处理建议	无

30.13 DOMAIN_PD_PREF_LOWTHR_ALM

日志内容	-Domain=[STRING]-PDPrefixUsage=[STRING]-IPv6PoolLowerValue=[STRING]; PD prefix resource usage reached or dropped below the lower threshold.
参数解释	$1：ISP域名称 $2：PD前缀地址使用率 $3：IPv6前缀使用率下限阈值
日志等级	4
举例	DOMAIN/4/DOMAIN_PD_PREF_LOWTHR_ALM: -Domain=abc-PDPrefixUsage=10%-IPv6PoolLowerValue=20%; PD prefix resource usage reached or dropped below the lower threshold.
日志说明	当域下授权IPv6地址池/IPv6地址池组中的PD前缀使用率达到或低于下限阈值，生成下限告警
处理建议	无

30.14 DOMAIN_PD_PREF_LOWTHR_ALM_REMOVE

日志内容	-Domain=[STRING]-PDPrefixUsage=[STRING]-IPv6PoolLowerValue=[STRING]; Low PD prefix resource usage alarm condition cleared.
参数解释	$1：ISP域名称 $2：PD前缀地址使用率 $3：IPv6前缀使用率下限阈值
日志等级	4
举例	DOMAIN/4/DOMAIN_PD_PREF_LOWTHR_ALM_REMOVE: -Domain=abc-PDPrefixUsage=50%-IPv6PoolLowerValue=20%; Low PD prefix resource usage alarm condition cleared.
日志说明	当域下授权IPv6地址池/IPv6地址池组中的PD前缀使用率>=（下限阈值+告警差值）<=（上限阈值-告警差值）时，生成使用率恢复告警 其中，告警差值=（上限阈值–下限阈值）*10%
处理建议	无

30.15 DOMAIN_PD_PREF_UPTHR_ALM

日志内容	-Domain=[STRING]-PDPrefixUsage=[STRING]-IPv6PoolUpperValue=[STRING]; PD prefix resource usage reached or exceeded the upper threshold.
参数解释	$1：ISP域名称 $2：PD前缀地址使用率 $3：IPv6前缀使用率上限阈值
日志等级	4
举例	DOMAIN/4/DOMAIN_PD_PREF_UPTHR_ALM: -Domain=abc-PDPrefixUsage=90%-IPv6PoolUpperValue=80%; PD prefix resource usage reached or exceeded the upper threshold.
日志说明	当域下授权IPv6地址池/IPv6地址池组中的PD前缀使用率达到或超过上限阈值，生成上限告警
处理建议	无

30.16 DOMAIN_PD_PREF_UPTHR_ALM_REMOVE

日志内容	-Domain=[STRING]-PDPrefixUsage=[STRING]-IPv6PoolUpperValue=[STRING]; High PD prefix resource usage alarm condition cleared.
参数解释	$1：ISP域名称 $2：PD前缀地址使用率 $3：IPv6前缀使用率上限阈值
日志等级	4
举例	DOMAIN/4/DOMAIN_PD_PREF_UPTHR_ALM_REMOVE: -Domain=abc-PDPrefixUsage=50%-IPv6PoolUpperValue=80%; High PD prefix resource usage alarm condition cleared.
日志说明	当域下授权IPv6地址池/IPv6地址池组中的PD前缀使用率<=（上限阈值-告警差值）时，生成使用率恢复告警 其中，告警差值=（上限阈值–下限阈值）*10%
处理建议	无

31 DOT1X

本节介绍 802.1X（DOT1X）模块输出的日志信息。

31.1 DOT1X_LOGIN_FAILURE

日志内容	-IfName=[STRING]-MACAddr=[STRING]-VLANID=[STRING]-Username=[STRING]; User failed 802.1X authentication.
参数解释	$1：接口名 $2：MAC地址 $3：VLAN ID $4：用户名
日志等级	6
举例	DOT1X/6/DOT1X_LOGIN_FAILURE:-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9-VLANID=444-Username=aaa; User failed 802.1X authentication.
日志说明	802.1X用户认证失败
处理建议	查看失败原因并修改相关配置

31.2 DOT1X_LOGIN_SUCC

日志内容	-IfName=[STRING]-MACAddr=[STRING]-VLANID=[STRING]-Username=[STRING]; User passed 802.1X authentication and came online.
参数解释	$1：接口名 $2：MAC地址 $3：VLAN ID $4：用户名
日志等级	6
举例	DOT1X/6/DOT1X_LOGIN_SUCC:-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9-VLANID=444-Username=aaa; User passed 802.1X authentication and came online.
日志说明	802.1X用户认证成功
处理建议	无

31.3 DOT1X_LOGOFF

日志内容	-IfName=[STRING]-MACAddr=[STRING]-VLANID=[STRING]-Username=[STRING]-ErrCode=[STRING]; 802.1X user was logged off.
参数解释	$1：接口名 $2：MAC地址 $3：VLAN ID $4：用户名 $5：错误码
日志等级	6
举例	DOT1X/6/DOT1X_LOGOFF:-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9-VLANID=444-Username=aaa-ErrCode=11; 802.1X user was logged off.
日志说明	802.1X用户下线
处理建议	查看下线原因或进行后续操作

31.4 DOT1X_NOTENOUGH_EADFREEIP_RES

日志内容	Failed to assign a rule for free IP [IPADDR] on interface [STRING] due to lack of ACL resources.
参数解释	$1：IP地址 $2：接口名
日志等级	3
举例	DOT1X/3/DOT1X_NOTENOUGH_EADFREEIP_RES: Failed to assign a rule for free IP 1.1.1.0 on interface Ethernet3/1/2 due to lack of ACL resources.
日志说明	当在接口上使能802.1X特性时，由于ACL资源不足，设备在接口上下发Free IP失败
处理建议	暂不使能802.1X，之后尝试重新使能802.1X

31.5 DOT1X_NOTENOUGH_EADFREERULE_RES

日志内容	Failed to assign a rule for permitting DHCP and DNS packets on interface [STRING] due to lack of ACL resources.
参数解释	$1：接口名
日志等级	3
举例	DOT1X/3/DOT1X_NOTENOUGH_EADFREERULE_RES: Failed to assign a rule for permitting DHCP and DNS packets on interface Ethernet3/1/2 due to lack of ACL resources.
日志说明	当在接口上使能802.1X特性时，由于ACL资源不足，设备不能下发允许该接口上DHCP协议和DNS协议报文通过的规则
处理建议	暂不使能802.1X，之后尝试重新使能802.1X

31.6 DOT1X_NOTENOUGH_EADMACREDIR_RES

日志内容	Failed to assign a rule for redirecting HTTP packets with source MAC address [MAC] on interface [STRING].
参数解释	$1：HTTP报文源MAC地址 $2：接口名
日志等级	3
举例	DOT1X/3/DOT1X_NOTENOUGH_EADMACREDIR_RES: Failed to assign a rule for redirecting HTTP packets with source MAC address 00e0-fc00-5915 on interface Ethernet3/1/2.
日志说明	当在接口上使能802.1X特性时，由于ACL资源不足，设备不能重定向在指定接口上收到的源MAC地址为特定地址的HTTP报文
处理建议	暂不使能802.1X，之后尝试重新使能802.1X

31.7 DOT1X_NOTENOUGH_EADPORTREDIR_RES

日志内容	Failed to assign a rule for redirecting HTTP packets on interface [STRING] due to lack of ACL resources.
参数解释	$1：接口名
日志等级	3
举例	DOT1X/3/DOT1X_NOTENOUGH_EADPORTREDIR_RES: Failed to assign a rule for redirecting HTTP packets on interface Ethernet3/1/2 due to lack of ACL resources.
日志说明	当在接口上使能802.1X特性时，由于ACL资源不足，设备不能指定规则允许该接口重定向HTTP报文
处理建议	暂不使能802.1X，之后尝试重新使能802.1X

31.8 DOT1X_NOTENOUGH_ENABLEDOT1X_RES

日志内容	Failed to enable 802.1X on interface [STRING] due to lack of ACL resources.
参数解释	$1：接口名
日志等级	3
举例	DOT1X/3/DOT1X_NOTENOUGH_ENABLEDOT1X_RES: Failed to enable 802.1X on interface Ethernet3/1/2 due to lack of ACL resources.
日志说明	因为ACL资源不足，不能配置接口的802.1X特性
处理建议	暂不使能802.1X，之后尝试重新使能802.1X

31.9 DOT1X_SMARTON_FAILURE

日志内容	-IfName=[STRING]-MACAddr=[STRING]; User failed SmartOn authentication because [STRING].
参数解释	$1：接口名 $2：MAC地址 $3：失败原因，包括如下取值： • the password was wrong.：密码错误 • the switch ID was wrong.：Switch ID 错误
日志等级	6
举例	DOT1X/6/DOT1X_SMARTON_FAILURE:-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9; User failed SmartOn authentication because the password is mismatched.
日志说明	SmartOn认证失败，及其原因
处理建议	根据失败原因修改相关配置

31.10 DOT1X_UNICAST_NOT_EFFECTIVE

日志内容	The unicast trigger feature is enabled but is not effective on interface [STRING].
参数解释	$1：接口名
日志等级	3
举例	DOT1X/3/DOT1X_UNICAST_NOT_EFFECTIVE: The unicast trigger feature is enabled but is not effective on interface Ethernet3/1/2.
日志说明	单播触发特性在接口上不生效，因为该接口不支持单播触发特性
处理建议	更换到支持单播触发功能的接口上对用户进行802.1X认证

32 DP

本节介绍 DP（DP 备份）模块输出的日志信息。

32.1 DP_SWITCH_SUCCESS

日志内容	Device with IP address [STRING] in DP backup group [UINT] switched to master.
参数解释	$1：备份组中主DP设备的IP地址 $2：DP备份组编号
日志等级	6
举例	DP/6/DP_SWITCH_SUCCESS: Device with IP address 1.1.1.1 in DP backup group 4 switched to master.
日志说明	指定的DP备份组中的主设备并启动主备切换成功
处理建议	无

33 DSTM

本节介绍 DSTM（Drive Stack Topology Management）模块输出的日志信息

33.1 DrvDebug

日志内容	Invalid member ID=[UINT]. The IRF member ID for this device model can only be 1 or 2.
参数解释	$1：设备在IRF中的成员编号
日志等级	4
举例	DRVPLAT/4/DrvDebug: Invalid member ID=4. The IRF member ID for this device model can only be 1 or 2.
日志说明	CR16018-F组建IRF时，IRF中的成员设备最多为2台，且成员设备框号只能配置1或2
处理建议	当CR16018-F组建IRF时，请将成员设备框号配置1或2

33.2 DrvDebug

日志内容	For the card in slot [UINT] on chassis [UINT] to start up, remove IRF port bindings for ports on the card and then reboot the card.
参数解释	$1：单板所在的槽位号 $2：设备在IRF中的成员编号
日志等级	4
举例	DRVPLAT/4/DrvDebug: For the card in slot 10 on chassis 4 to start up, remove IRF port bindings for ports on the card and then reboot the card.
日志说明	下面几种情况时出现此日志： • IRF 模式下，CSPEX 类单板（除 CSPEX-1204 之外）、CEPC 类单板上的接口作为 IRF 物理端口时，将该单板更换成 CSPC 类单板后，单板无法启动 • IRF 模式下，CSPEX 类单板（除 CSPEX-1204 之外）、CEPC 类单板上的接口作为 IRF 物理端口时，将该单板更换成 CSPEX-1204 单板和 CGN 单板后，单板无法启动 • IRF 模式下，CSPC 类单板上的接口作为 IRF 物理端口时，将该单板更换成 CSPEX 类单板、CEPC 类单板后，单板无法启动
处理建议	• 更换成 CSPC 类单板后，请取消该槽位上 IRF 物理端口与 IRF 端口绑定关系，并重启单板 • 更换成 CSPEX-1204 和 CGN 单板后，请取消该槽位上 IRF 物理端口与 IRF 端口绑定关系，并重启单板 • 更换成 CSPEX 类单板、CEPC 类单板后，请取消该槽位上 IRF 物理端口与 IRF 端口绑定关系，并重启单板

33.3 DrvDebug

日志内容	For the card in slot [UINT] on chassis [UINT] to start up, remove IRF port bindings for 100-GE ports on the card and then reboot the card.
参数解释	$1：单板所在的槽位号 $2：设备在IRF中的成员编号
日志等级	4
举例	DRVPLAT/4/DrvDebug: For the card in slot 3 on chassis 4 to start up, remove IRF port bindings for 100-GE ports on the card and then reboot the card.
日志说明	IRF模式下，如有100GE接口作为IRF物理端口时，将该单板更换成CSPC类单板后，单板无法启动
处理建议	更换成CSPC类单板后，请取消该槽位上100GE端口作为IRF物理端口与IRF端口的绑定关系，并重启单板

33.4 DrvDebug

日志内容	Please reboot the card in slot [UINT] on chassis [UINT] to clear the IRF port settings.
参数解释	$1：单板所在的槽位号 $2：设备在IRF中的成员编号
日志等级	4
举例	DRVPLAT/4/DrvDebug: Please reboot the card in slot 11 on chassis 4 to clear the IRF port settings.
日志说明	CSPEX类单板（除CSPEX-1204之外）、CEPC类单板上的接口作为IRF物理端口时，当取消该单板上所有IRF物理端口和IRF端口的绑定关系后，需要重启该单板
处理建议	请按照提示重启对应单板

33.5 DrvDebug

日志内容	Please reboot the card in slot [UINT] on chassis [UINT] to activate the IRF port settings.
参数解释	$1：单板所在的槽位号 $2：设备在IRF中的成员编号
日志等级	4
举例	DRVPLAT/4/DrvDebug: Please reboot the card in slot 11 on chassis 4 to activate the IRF port settings.
日志说明	CSPEX类单板（除CSPEX-1204之外）、CEPC类单板上首次有接口作为IRF物理端口，且与IRF端口绑定后，需要重启该单板
处理建议	请按照提示重启对应单板

33.6 DrvDebug

日志内容	To bind ports operating at another rate to IRF port [UINT] on member device [UINT], please remove the existing IRF port bindings first.
参数解释	$1：IRF端口号 $2：设备在IRF中的成员编号
日志等级	4
举例	DRVPLAT/4/DrvDebug: To bind ports operating at another rate to IRF port 1 on member device 4, please remove the existing IRF port bindings first.
日志说明	单板上有接口作为IRF物理端口时，如要更换单板，不支持将此接口更换成其他速率
处理建议	更换IRF物理端口所在单板时，请保证IRF链路两端的端口速率相同

33.7 UTL

日志内容	IRF physical port protection occurred. Please check the affected ports for VLAN configuration errors to restore the port state. IRF physical ports=[INT32].
参数解释	$1：IRF物理端口
日志等级	4
举例	STACK/4/UTL: IRF physical port protection occurred. Please check the affected ports for VLAN configuration errors to restore the port state. IRF physical ports=Ten1/3/0/24 Ten1/3/0/23.
日志说明	当IRF成员设备间采用非直连方式组网时，IRF物理链路上VLAN配置有误，导致链路存在环路，IRF物理端口启动保护措施
处理建议	(1) 执行**shutdown**命令关闭提示的IRF物理端口 (2) 请分别检查提示出错的IRF物理端口以及与其连接的中继设备端口的VLAN配置，查找配置错误的端口 (3) 修改错误的IRF物理端口的VLAN及中继设备对应端口VLAN的配置。由于每条IRF物理链路的IRF协议报文需要隔离传输，请为每条IRF物理链路划分不同的VLAN，且同一条IRF物理链路两端的端口配置的VLAN ID必须相同 (4) 执行**undo shutdown**命令开启上述IRF物理端口

34 E&M

本节介绍 E&M 模块输出的日志信息。

34.1 EM_CALLEDTALKING_IDLE

日志内容	[STRING] on the called party received an idle signal in talking state.
参数解释	$1：E&M语音接口名称
日志等级	6
举例	EM/6/EM_CALLEDTALKING_IDLE: E&M interface 2/3/1 on the called party received an idle signal in talking state.
日志说明	处于talking状态的被叫方E&M语音用户线收到了示闲信号，该接口将被释放
处理建议	无

34.2 EM_CALLEDTALKING_SEIZE

日志内容	[STRING] on the called party received a seizure signal in talking state.
参数解释	$1：E&M语音接口名称
日志等级	6
举例	EM/6/EM_CALLEDTALKING_SEIZE: E&M interface 2/3/1 on the called party received a seizure signal in talking state.
日志说明	处于talking状态的被叫方E&M语音用户线收到了占用信号
处理建议	无

34.3 EM_CALLERTALKING_IDLE

日志内容	[STRING] on the calling party received an idle signal in talking state.
参数解释	$1：E&M语音接口名称
日志等级	6
举例	EM/6/EM_CALLERTALKING_IDLE: E&M interface 2/3/1 on the calling party received an idle signal in talking state.
日志说明	处于talking状态的主叫方E&M语音用户线收到了示闲信号，即收到了拆除呼叫的消息，该接口将被释放
处理建议	无

34.4 EM_CALLERTALKING_SEIZE

日志内容	[STRING] on the calling party received a seizure signal in talking state.
参数解释	$1：E&M语音接口名称
日志等级	6
举例	EM/6/EM_CALLERTALKING_SEIZE: E&M interface 2/3/1 on the calling party received a seizure signal in talking state.
日志说明	处于talking状态的主叫方E&M语音用户线收到了占用信号
处理建议	无

34.5 EM_SEND_IDLE

日志内容	[STRING] sent out an idle signal.
参数解释	$1：E&M语音接口名称
日志等级	6
举例	EM/6/EM_SEND_IDLE: E&M interface 2/3/1 sent out an idle signal.
日志说明	E&M语音用户线发送了示闲信号，表明该接口已空闲
处理建议	无

34.6 EM_SEND_SEIZE

日志内容	[STRING] sent out a seizure signal.
参数解释	$1：E&M语音接口名称
日志等级	6
举例	EM/6/EM_SEND_SEIZE: E&M interface 2/3/1 sent out a seizure signal.
日志说明	E&M语音用户线发出了占用信号，表明该接口被占用
处理建议	无

35 EDEV

本节介绍扩展设备管理模块输出的日志信息。

35.1 EDEV_FAILOVER_GROUP_STATE_CHANGE

日志内容	Status of stateful failover group [STRING] with ID [UINT32] changed to [STRING].
参数解释	$1：备份组的名字 $2：备份组的ID $2：备份组的状态： ○ primary 表示备份组中 primary 节点处理业务 ○ secondary 表示备份组中 secondary 节点处理业务
日志等级	5
举例	EDEV/5/EDEV_FAILOVER_GROUP_STATE_CHANGE: -MDC=1; Status of stateful failover group 123 with ID 0 changed to primary.
日志说明	备份组的状态发生了变化
处理建议	无

36 EIGRP

本节介绍 EIGRP 模块输出的日志信息。

36.1 RID_CHANGE

日志内容	EIGRP [UINT32]: New elected router ID will take effect after EIGRP address family is reset.
参数解释	$1：EIGRP进程ID
日志等级	5
举例	EIGRP/5/RID_CHANGE: EIGRP 1: New elected router ID will take effect after EIGRP address family is reset.
日志说明	用户使用的接口IP发生变化导致EIGRP路由器ID变化。需要手动重启EIGRP地址族使新的路由器ID生效
处理建议	使用**reset eigrp process**命令使新的路由器ID生效

36.2 PEER_CHANGE

日志内容	EIGRP [UINT32]: Neighbor [STRING] ([STRING]) is [STRING]: [STRING].
参数解释	$1：EIGRP进程ID $2：邻居路由器的IP地址 $3：与邻居连接的接口 $4：邻居状态，取值包括： • Up：邻居状态变为 Up • Down：邻居状态变为 Down $5：EIGRP邻居状态变化的原因，取值请参见表36-1
日志等级	5
举例	EIGRP/5/PEER_CHANGE: EIGRP 2: Neighbor 100.100.10.2 (GigabitEthernet1/0/1) is Up: New neighbor.
日志说明	EIGRP邻居状态变化及变化原因
处理建议	检查EIGRP邻居状态改变的原因，参见表36-1进行处理

表36-1 EIGRP 邻居状态改变原因列表

EIGRP 邻居状态改变的原因	说明	处理建议
New neighbor	建立新的邻居	无需处理
Interface down	接口down	检查网络连接情况
Reset operation	执行**reset eigrp process**或**reset eigrp peer**命令	无需处理
Delete operation	删除进程或地址族	无需处理

EIGRP 邻居状态改变的原因	说明	处理建议
Hold timer expired	邻居保持定时器超时	检查网络状况或者配置的超时时间是否合理
Maximum retransmission times reached	报文重传次数超过限制	检查网络状况
Inconsistent K values	K值不匹配	检查两端K值是否一致
Neighbor restart	邻居重启	检查网络状况和确认邻居端是否有影响邻居关系的操作
Stuck in active	卡在激活状态	检查网络状况和邻居端的CPU占用情况
Peer termination	邻居主动结束邻接关系	确认邻居端是否有影响邻居关系的操作
Configuration changed	配置发生变化	检查配置是否正确
Process switchover	EIGRP进程倒换	无需处理
Insufficient memory	达到内存门限	检查系统内存，对占用内存较多的模块进行调整，尽量释放可用内存

37 EKDM

本节介绍 EKDM 模块输出的日志信息。

37.1 EKDM

日志内容	Global standby MPU in chassis [UINT32] slot [UINT32] rebooted abnormally [UINT32] times and was prevented from rebooting again.
参数解释	$1：设备在IRF中的成员编号 $2：单板所在的槽位号 $3：备用主控板异常掉电导致重启次数
日志等级	2
举例	DEVD/2/EKDM: -MDC=1; Global standby MPU in chassis 3 slot 1 rebooted abnormally 4 times and was prevented from rebooting again.
日志说明	指定槽位的全局备用主控板故障导致其异常掉电并重启，异常掉电并重启4次后系统将抑制备用主控板启动
处理建议	**1.** 请更换故障的全局备用主控板 **2.** 请联系技术支持

37.2 EKDM

日志内容	Standby MPU in slot [UINT32] rebooted abnormally [UINT32] times and was prevented from rebooting again.
参数解释	$1：单板所在的槽位号 $2：备用主控板异常重启次数
日志等级	2
举例	DEVD/2/EKDM: -MDC=1; Standby MPU in slot 1 rebooted abnormally 4 times and was prevented from rebooting again.
日志说明	指定槽位的备用主控板故障导致其异常掉电并重启，异常掉电并重启4次后系统将抑制备用主控板启动
处理建议	**1.** 请更换故障的备用主控板 **2.** 请联系技术支持

38 ERPS

本节介绍 ERPS 模块输出的日志信息。

38.1 ERPS_STATE_CHANGED

日志内容	Ethernet ring [UINT16] instance [UINT16] changed state to [STRING].
参数解释	$1：ERPS环号 $2：ERPS环实例编号 $3：ERPS实例状态
日志等级	6
举例	ERPS/4/ERPS_STATE_CHANGED: Ethernet ring 1 instance 1 changed state to Idle.
日志说明	ERPS环上实例状态发生改变
处理建议	无

39 ETH

本节介绍以太网模块输出的日志信息。

39.1 ETH_VLAN_DEFAULT_TERMINATION_FAILED

日志内容	The board in slot [STRING] doesn't support default termination.
参数解释	$1：单板槽位号
日志等级	3
举例	%Jul 3 15:13:56:232 2020 H3C LIF/3/IF: -MDC=1; The board in slot 3 doesn't support default termination.
日志说明	三层聚合接口中如果加入非CSPEX类单板（CSPEX-1204、CSPEX-1104-E除外）和CEPC类单板上的成员端口，该成员端口不支持Default终结功能，此时提示单板不支持Default终结功能
处理建议	如果需要使用该功能，建议使用CSPEX类单板（CSPEX-1204、CSPEX-1104-E除外）和CEPC类单板上的接口作为成员端口

39.2 ETH_VLAN_DEFAULT_TERMINATION_FAILED

日志内容	The board doesn't support default termination.
参数解释	无
日志等级	3
举例	%Jul 3 15:59:17:396 2020 H3C LIF/3/QINQ: -MDC=1-Slot=2; The board doesn't support default termination.
日志说明	CSPEX-1104-E和CSPEX-1204上的三层以太网子接口不支持Default终结功能，此时提示该单板不支持Default终结功能
处理建议	无

39.3 ETH_VLAN_TERMINATION_FAILED

日志内容	The vlan-type dot1q configuration on [STRING] failed.
参数解释	$1：接口名称
日志等级	4
举例	ETH/4/ETH_VLAN_TERMINATION_FAILED: -MDC=1; The vlan-type dot1q configuration on GigabitEthernet1/0/1.1 failed.
日志说明	接口下发**vlan-type dot1q**系列命令的配置时失败，可能由硬件资源不足引起
处理建议	联系H3C技术支持

39.4 ETH_VLAN_TERMINATION_NOT_SUPPORT

日志内容	The vlan-type dot1q configuration on [STRING] is not supported.
参数解释	$1：接口名称
日志等级	4
举例	ETH/4/ETH_VLAN_TERMINATION_NOT_SUPPORT: -MDC=1; The vlan-type dot1q configuration on GigabitEthernet1/0/1.1 is not supported.
日志说明	接口不支持**vlan-type dot1q**系列命令
处理建议	检查接口所在单板是否支持VLAN终结功能

39.5 ETH_VMAC_INEFFECTIVE

日志内容	Interface [STRING] failed to add a virtual MAC: [STRING].
参数解释	$1：接口名称 $2：接口添加虚拟MAC地址失败的原因
日志等级	3
举例	ETH/3/ETH_VMAC_INEFFECTIVE: Interface GigabitEthernet1/0/1 failed to add a virtual MAC: Insufficient hardware resources.
日志说明	添加虚拟MAC地址失败
处理建议	确定操作失败的根因并解决，例如接口上的VRRP的虚拟MAC地址数量达到上限，导致没有足够的硬件资源来添加新的虚拟MAC地址，此时可以删除空闲的VRRP备份组，释放部分硬件资源

40 ETHOAM

本节介绍 ETHOAM 模块输出的日志信息。

40.1 ETHOAM_CONNECTION_FAIL_DOWN

日志内容	The link is down on interface [string] because a remote failure occurred on peer interface.
参数解释	$1：接口名称
日志等级	5
举例	ETHOAM/5/ETHOAM_CONNECTION_FAIL_DOWN: The link is down on interface Ethernet1/0/1 because a remote failure occurred on peer interface.
日志说明	对端接口发生故障，链路down
处理建议	检查链路状态或对端的OAM状态

40.2 ETHOAM_CONNECTION_FAIL_TIMEOUT

日志内容	Interface [string] removed the OAM connection because it received no Information OAMPDU before the timer times out.
参数解释	$1：接口名称
日志等级	5
举例	ETHOAM/5/ETHOAM_CONNECTION_FAIL_TIMEOUT: Interface Ethernet1/0/1 removed the OAM connection because it received no Information OAMPDU before the timer times out.
日志说明	接口在超时时间内没有收到信息OAMPDU，所以删除OAM连接
处理建议	检查链路状态或对端的OAM状态

40.3 ETHOAM_CONNECTION_FAIL_UNSATISF

日志内容	Interface [string] failed to establish an OAM connection because the peer doesn’t match the capacity of the local interface.
参数解释	$1：接口名称
日志等级	3
举例	ETHOAM/3/ETHOAM_CONNECTION_FAIL_UNSATISF: Interface Ethernet1/0/1 failed to establish an OAM connection because the peer doesn’t match the capacity of the local interface.
日志说明	对端与本端接口的OAM协议状态不匹配，建立OAM连接失败
处理建议	分析两端发出的OAM报文中的协议状态字段

40.4 ETHOAM_CONNECTION_SUCCEED

日志内容	An OAM connection is established on interface [string].
参数解释	$1：接口名称
日志等级	6
举例	ETHOAM/6/ETHOAM_CONNECTION_SUCCEED: An OAM connection is established on interface Ethernet1/0/1.
日志说明	OAM连接建立成功
处理建议	无

40.5 ETHOAM_DISABLE

日志内容	Ethernet OAM is now disabled on interface [string].
参数解释	$1：接口名称
日志等级	6
举例	ETHOAM/6/ETHOAM_DISABLE: Ethernet OAM is now disabled on interface Ethernet1/0/1.
日志说明	以太网OAM功能已关闭
处理建议	无

40.6 ETHOAM_DISCOVERY_EXIT

日志内容	OAM interface [string] quit the OAM connection..
参数解释	$1：接口名称
日志等级	5
举例	ETHOAM/5/ ETHOAM_DISCOVERY_EXIT: OAM interface Ethernet1/0/1 quit the OAM connection.
日志说明	本端接口退出OAM连接
处理建议	无

40.7 ETHOAM_ENABLE

日志内容	Ethernet OAM is now enabled on interface [string].
参数解释	$1：接口名称
日志等级	6
举例	ETHOAM/6/ETHOAM_ENABLE: Ethernet OAM is now enabled on interface Ethernet1/0/1.
日志说明	以太网OAM功能已使能
处理建议	无

40.8 ETHOAM_ENTER_LOOPBACK_CTRLLED

日志内容	The local OAM entity enters remote loopback as controlled DTE on OAM interface [string].
参数解释	$1：接口名称
日志等级	6
举例	ETHOAM/6/ ETHOAM_ENTER_LOOPBACK_CTRLLED: The local OAM entity enters remote loopback as controlled DTE on OAM interface Ethernet1/0/1.
日志说明	对端使能OAM远端环回功能后，本端OAM实体作为被控制DTE进入远端环回
处理建议	无

40.9 ETHOAM_ENTER_LOOPBACK_CTRLLING

日志内容	The local OAM entity enters remote loopback as controlling DTE on OAM interface [string].
参数解释	$1：接口名称
日志等级	6
举例	ETHOAM/6/ ETHOAM_ENTER_LOOPBACK_CTRLLING: The local OAM entity enters remote loopback as controlling DTE on OAM interface Ethernet1/0/1.
日志说明	接口使能OAM远端环回功能后，本端OAM实体作为控制DTE进入远端环回
处理建议	无

40.10 ETHOAM_LOCAL_DYING_GASP

日志内容	A local Dying Gasp event occurred on interface [string].
参数解释	$1：接口名称
日志等级	4
举例	ETHOAM/4/ETHOAM_LOCAL_DYING_GASP: A local Dying Gasp event occurred on interface Ethernet1/0/1.
日志说明	重启设备或关闭接口导致本端产生致命故障（Dying Gasp）事件
处理建议	链路恢复之前不能使用

40.11 ETHOAM_LOCAL_ERROR_FRAME

日志内容	An errored frame event occurred on local interface [string].
参数解释	$1：接口名称
日志等级	6
举例	ETHOAM/6/ETHOAM_LOCAL_ERROR_FRAME: An errored frame event occurred on local interface Ethernet1/0/1.
日志说明	本地接口产生错误帧事件
处理建议	本端收到错误报文，检查一下本端和对端之间的链路是否正常

40.12 ETHOAM_LOCAL_ERROR_FRAME_PERIOD

日志内容	An errored frame period event occurred on local interface [string].
参数解释	$1：接口名称
日志等级	6
举例	ETHOAM/6/ETHOAM_LOCAL_ERROR_FRAME_PERIOD: An errored frame period event occurred on local interface Ethernet1/0/1.
日志说明	本地接口产生错误帧周期事件
处理建议	本端收到错误报文，检查一下本端和对端之间的链路是否正常

40.13 ETHOAM_LOCAL_ERROR_FRAME_SECOND

日志内容	An errored frame seconds event occurred on local interface [string].
参数解释	$1：接口名称
日志等级	6
举例	ETHOAM/6/ETHOAM_LOCAL_ERROR_FRAME_SECOND: An errored frame seconds event occurred on local port Ethernet1/0/1.
日志说明	本地接口产生错误帧秒事件
处理建议	本端收到错误报文，检查一下本端和对端之间的链路是否正常

40.14 ETHOAM_LOCAL_LINK_FAULT

日志内容	A local Link Fault event occurred on interface [string].
参数解释	$1：接口名称
日志等级	4
举例	ETHOAM/4/ETHOAM_LOCAL_LINK_FAULT: A local Link Fault event occurred on interface Ethernet1/0/1.
日志说明	本地链路down，产生链路故障事件
处理建议	重新连接本地接口的光纤接收端

40.15 ETHOAM_LOOPBACK_EXIT

日志内容	OAM interface [string] quit remote loopback.
参数解释	$1：接口名称
日志等级	4
举例	ETHOAM/4/ETHOAM_LOOPBACK_EXIT: OAM interface Ethernet1/0/1 quit remote loopback.
日志说明	远端环回连接建立未完成时，接口关闭远端环回或OAM连接断开后，OAM接口退出远端环回
处理建议	无

40.16 ETHOAM_LOOPBACK_EXIT_ERROR_STATU

日志内容	OAM interface [string] quit remote loopback due to incorrect multiplexer or parser status.
参数解释	$1：接口名称
日志等级	6
举例	ETHOAM/6/ETHOAM_LOOPBACK_EXIT_ERROR_STATU: OAM interface Ethernet1/0/1 quit remote loopback due to incorrect multiplexer or parser status.
日志说明	复用器或解析器状态错误，OAM接口Ethernet1/0/1退出远端环回
处理建议	在OAM实体上关闭并重新使能以太网OAM

40.17 ETHOAM_LOOPBACK_NO_RESOURCE

日志内容	OAM interface [string] can’t enter remote loopback due to insufficient resources.
参数解释	$1：接口名称
日志等级	4
举例	ETHOAM/4/ETHOAM_LOOPBACK_NO_RESOURCE: OAM interface Ethernet1/0/1 can’t enter remote loopback due to insufficient resources.
日志说明	当在本端或对端OAM实体上运行**oam remote-loopback start**命令时，OAM接口由于资源不足而无法进入远端环回
处理建议	端口上使能远端环回，需要设置端口的硬件转发资源，如果配置的端口过多，可能会导致资源不足，需要关闭一下其他端口的远端环回功能，再在本端口上重新运行**oam remote-loopback start**命令

40.18 ETHOAM_LOOPBACK_NOT_SUPPORT

日志内容	OAM interface [string] can’t enter remote loopback because the operation is not supported.
参数解释	$1：接口名称
日志等级	4
举例	ETHOAM/4/ETHOAM_LOOPBACK_NOT_SUPPORT: OAM interface Ethernet1/0/1 can’t enter remote loopback because the operation is not supported.
日志说明	由于设备不支持，OAM接口无法进入远端环回
处理建议	无

40.19 ETHOAM_NO_ENOUGH_RESOURCE

日志内容	The configuration failed on OAM interface [string] because of insufficient resources.
参数解释	$1：接口名称
日志等级	4
举例	ETHOAM/4/ ETHOAM_NO_ENOUGH_RESOURCE: The configuration failed on OAM interface Ethernet1/0/1 because of insufficient resources.
日志说明	系统内存资源不足导致OAM接口上的配置失败
处理建议	减少一下系统的无用配置，释放部分内存资源后，再重新配置

40.20 ETHOAM_NOT_CONNECTION_TIMEOUT

日志内容	Interface [string] quit Ethernet OAM because it received no Information OAMPDU before the timer times out.
参数解释	$1：接口名称
日志等级	5
举例	ETHOAM/5/ ETHOAM_NOT_CONNECTION_TIMEOUT: Interface Ethernet1/0/1 quit Ethernet OAM because it received no Information OAMPDU before the timer times out.
日志说明	本地端口在超时时间内没有收到信息OAMPDU，所以退出以太网OAM
处理建议	对端发送OAM报文不及时，检查本地和对端的链路状态是否正常，以及对端的OAM功能是否使能了

40.21 ETHOAM_QUIT_LOOPBACK_CTRLLED

日志内容	The local OAM entity quit remote loopback as controlled DTE on OAM interface [string].
参数解释	$1：接口名称
日志等级	6
举例	ETHOAM/6/ ETHOAM_QUIT_LOOPBACK_CTRLLED: The local OAM entity quit remote loopback as controlled DTE on OAM interface Ethernet1/0/1.
日志说明	当本端作为远端环回的被控端时，由于对端关闭了远端环回功能，本端也会退出远端环回
处理建议	无

40.22 ETHOAM_QUIT_LOOPBACK_CTRLLING

日志内容	The local OAM entity quit remote loopback as controlling DTE on OAM interface [string].
参数解释	$1：接口名称
日志等级	6
举例	ETHOAM/6/ETHOAM_QUIT_LOOPBACK_CONTROLLING: The local OAM entity quit remote loopback as controlling DTE on OAM interface Ethernet1/0/1.
日志说明	在接口上使能远端环回，当再将端口上的远端环回功能关闭后，本端会退出远端环回
处理建议	无

40.23 ETHOAM_REMOTE_CRITICAL

日志内容	A remote Critical event occurred on interface [string].
参数解释	$1：接口名称
日志等级	4
举例	ETHOAM/4/ETHOAM_REMOTE_CRITICAL: A remote Critical event occurred on interface Ethernet1/0/1.
日志说明	发生远端紧急事件
处理建议	链路恢复之前不能使用

40.24 ETHOAM_REMOTE_DYING_GASP

日志内容	A remote Dying Gasp event occurred on interface [string].
参数解释	$1：接口名称
日志等级	4
举例	ETHOAM/4/ETHOAM_REMOTE_DYING_GASP: A remote Dying Gasp event occurred on interface Ethernet1/0/1.
日志说明	重启远端设备或关闭接口导致远端产生致命故障（Dying Gasp）事件
处理建议	链路恢复之前不能使用

40.25 ETHOAM_REMOTE_ERROR_FRAME

日志内容	An errored frame event occurred on the peer interface [string].
参数解释	$1：接口名称
日志等级	6
举例	ETHOAM/6/ETHOAM_REMOTE_ERROR_FRAME: An errored frame event occurred on the peer interface Ethernet1/0/1.
日志说明	对端产生错误帧事件
处理建议	对端收到错误报文，检查一下本端和对端之间的链路是否正常

40.26 ETHOAM_REMOTE_ERROR_FRAME_PERIOD

日志内容	An errored frame period event occurred on the peer interface [string].
参数解释	$1：接口名称
日志等级	6
举例	ETHOAM/6/ETHOAM_REMOTE_ERROR_FRAME_PERIOD: An errored frame period event occurred on the peer interface Ethernet1/0/1.
日志说明	对端产生错误帧周期事件
处理建议	对端收到错误报文，检查一下本端和对端之间的链路是否正常

40.27 ETHOAM_REMOTE_ERROR_FRAME_SECOND

日志内容	An errored frame seconds event occurred on the peer interface [string].
参数解释	$1：接口名称
日志等级	6
举例	ETHOAM/6/ETHOAM_REMOTE_ERROR_FRAME_SECOND: An errored frame seconds event occurred on the peer interface Ethernet1/0/1.
日志说明	对端产生错误帧秒事件
处理建议	对端收到错误报文，检查一下本端和对端之间的链路是否正常

40.28 ETHOAM_REMOTE_ERROR_SYMBOL

日志内容	An errored symbol event occurred on the peer interface [string].
参数解释	$1：接口名称
日志等级	6
举例	ETHOAM/6/ETHOAM_REMOTE_ERROR_SYMBOL: An errored symbol event occurred on the peer interface Ethernet1/0/1.
日志说明	对端产生错误信号事件
处理建议	对端收到错误信号，检查一下本端和对端之间的链路是否正常

40.29 ETHOAM_REMOTE_EXIT

日志内容	OAM interface [string] quit OAM connection because Ethernet OAM is disabled on the peer interface.
参数解释	$1：接口名称
日志等级	5
举例	ETHOAM/5/ ETHOAM_REMOTE_EXIT: OAM interface Ethernet1/0/1 quit OAM connection because Ethernet OAM is disabled on the peer interface.
日志说明	对端接口关闭以太网OAM功能导致本端接口退出OAM连接
处理建议	无

40.30 ETHOAM_REMOTE_FAILURE_RECOVER

日志内容	Peer interface [string] recovered.
参数解释	$1：接口名称
日志等级	5
举例	ETHOAM/5/ ETHOAM_REMOTE_FAILURE_RECOVER: Peer interface Ethernet1/0/1 recovered.
日志说明	对端接口链路故障清除，OAM连接恢复
处理建议	无

40.31 ETHOAM_REMOTE_LINK_FAULT

日志内容	A remote Link Fault event occurred on interface [string].
参数解释	$1：接口名称
日志等级	4
举例	ETHOAM/4/ETHOAM_REMOTE_LINK_FAULT: A remote Link Fault event occurred on interface Ethernet1/0/1.
日志说明	远端链路down，产生远端链路故障事件
处理建议	重新连接远端接口的光纤接收端

41 EVB

本节介绍连接服务器的边缘交换机上 EVB 协议输出的日志信息。

41.1 EVB_AGG_FAILED

日志内容	Remove port [STRING] from aggregation group [STRING]. Otherwise, the EVB feature does not take effect.
参数解释	$1：物理接口名称 $2：聚合接口名称
日志等级	6
举例	EVB/6/EVB_AGG_FAILED: Remove port GigabitEthernet5/0/5 from aggregation group Bridge-Aggregation5. Otherwise, the EVB feature does not take effect.
日志说明	EVB交换机处理聚合组中物理接口失败
处理建议	将该物理接口从聚合组中删除

41.2 EVB_LICENSE_EXPIRE

日志内容	The EVB feature's license will expire in [UINT32] days.
参数解释	$1：天数
日志等级	6
举例	EVB/6/EVB_LICENSE_EXPIRE: The EVB feature's license will expire in 15 days.
日志说明	EVB的License将在指定天数后失效
处理建议	更新EVB的License

41.3 EVB_VSI_OFFLINE

日志内容	VSI [STRING] went offline.
参数解释	$1：VSI接口/VSI聚合接口名称
日志等级	6
举例	EVB/6/EVB_VSI_OFFLINE: VSI Schannel-Aggregation1:2.0 went offline.
日志说明	设备收到服务器发送的VDP报文，或者定时器已经超时，但设备还没收到服务器的VDP回复报文，VSI接口/VSI聚合接口被删除
处理建议	无

41.4 EVB_VSI_ONLINE

日志内容	VSI [STRING] came online, status is [STRING].
参数解释	$1：VSI接口/VSI聚合接口名称 $2：VSI状态
日志等级	6
举例	EVB/6/EVB_VSI_ONLINE: VSI Schannel-Aggregation1:2.0 came online, status is association.
日志说明	EVB交换机收到VDP报文并成功创建VSI接口/VSI聚合接口
处理建议	无

42 EVIISIS

本节介绍 EVI IS-IS 模块输出的日志信息。

42.1 EVIISIS_LICENSE

日志内容	The EVIISIS feature has [STRING] license.
参数解释	$1：License状态，包括： ○ available：表示 License 有效 ○ no available：表示 License 失效或没有 License
日志等级	5
举例	EVIISIS/5/EVIISIS_LICENSE: The EVIISIS feature has available license.
日志说明	EVI IS-IS的License状态改变（例如安装了License或License失效）时输出本信息
处理建议	若当前EVI IS-IS的License失效或没有License，安装有效的License

42.2 EVIISIS_NBR_CHG

日志内容	EVIISIS [UINT32], [STRING] adjacency [STRING] ([STRING]), state changed to [STRING].
参数解释	$1：EVI IS-IS进程ID $2：邻居级别 $3：邻居的System ID $4：接口名 $5：当前邻居状态 o up：表示邻居关系已建立，可以正常工作 o initializing：表示初始状态 o down：表示邻居关系结束
日志等级	5
举例	EVIISIS/5/EVIISIS_NBR_CHG: EVIISIS 1, Level-1 adjacency 0011.2200.1501 (Evi-Link0), state changed to down.
日志说明	接口EVI IS-IS邻居状态改变
处理建议	当某接口邻居状态变为down或initializing时，检查EVI IS-IS配置正确性和网络连通性

43 FCLINK

本节介绍 FCLINK 模块输出的日志信息。

43.1 FCLINK_FDISC_REJECT_NORESOURCE

日志内容	VSAN [UINT16], Interface [STRING]: An FDISC was rejected because the hardware resource is not enough.
参数解释	$1：VSAN ID $2：接口名称
日志等级	4
举例	FCLINK/4/FCLINK_FDISC_REJECT_NORESOURCE: VSAN 1, Interface FC2/0/1: An FDISC was rejected because the hardware resource is not enough.
日志说明	硬件资源不足时收到了FDISC报文
处理建议	减少节点的数量

43.2 FCLINK_FLOGI_REJECT_NORESOURCE

日志内容	VSAN [UINT16], Interface [STRING]: An FLOGI was rejected because the hardware resource is not enough.
参数解释	$1：VSAN ID $2：接口名称
日志等级	4
举例	FCLINK/4/FCLINK_FLOGI_REJECT_NORESOURCE: VSAN 1, Interface FC2/0/1: An FLOGI was rejected because the hardware resource is not enough.
日志说明	硬件资源不足时收到了FLOGI报文
处理建议	减少节点的数量

44 FCOE

本节介绍 FCOE 模块输出的日志信息。

44.1 FCOE_INTERFACE_NOTSUPPORT_FCOE

日志内容	Because the aggregate interface [STRING] has been bound to a VFC interface, assigning the interface [STRING] that does not support FCoE to the aggregate interface might cause incorrect processing.
参数解释	$1：聚合接口名称 $2：以太网接口名称
日志等级	4
举例	FCOE/4/FCOE_INTERFACE_NOTSUPPORT_FCOE: Because the aggregate interface Bridge-Aggregation 1 has been bound to a VFC interface, assigning the interface Ten-GigabitEthernet 2/0/1 that does not support FCoE to the aggregate interface might cause incorrect processing.
日志说明	当不支持FCoE功能的接口加入到已绑定到VFC接口的聚合接口时，打印本信息
处理建议	将支持FCoE功能的接口加入到聚合接口，或者解除聚合接口与VFC接口的绑定

44.2 FCOE_LAGG_BIND_ACTIVE

日志内容	The binding between aggregate interface [STRING] and the VFC interface takes effect again, because the member port is unbound from its bound VFC interface or removed from the aggregate interface.
参数解释	$1：聚合接口名称
日志等级	4
举例	FCOE/4/FCOE_LAGG_BIND_ACTIVE: The binding between aggregate interface Bridge-Aggregation1 and the VFC interface takes effect again, because the member port is unbound from its bound VFC interface or removed from the aggregate interface.
日志说明	因为聚合接口的成员接口解除VFC接口绑定或退出聚合组，所以聚合接口绑定的VFC接口生效
处理建议	无

44.3 FCOE_LAGG_BIND_DEACTIVE

日志内容	The binding between aggregate interface [STRING] and the VFC interface is no longer in effect, because the new member port has been bound to a VFC interface.
参数解释	$1：聚合接口名称
日志等级	4
举例	FCOE/4/FCOE_LAGG_BIND_DEACTIVE: The binding between aggregate interface Bridge-Aggregation1 and the VFC interface is no longer in effect, because the new member port has been bound to a VFC interface.
日志说明	因为聚合接口的成员口绑定了VFC接口，所以聚合接口绑定的VFC接口失效
处理建议	无

45 FCZONE

本节介绍 FCZONE 模块输出的日志信息。

45.1 FCZONE_DISTRIBUTE_FAILED

日志内容	-VSAN=[UINT16]; Zone distribution failed. The zoning configurations might consequently be inconsistent across the fabric.
参数解释	$1：VSAN ID
日志等级	4
举例	FCZONE/4/FCZONE_DISTRIBUTE_FAILED: -VSAN=2; Zone distribution failed. The zoning configurations might consequently be inconsistent across the fabric.
日志说明	扩散失败，Fabric中交换机的zone配置可能因此不一致
处理建议	不同情况下扩散失败的处理建议如下： • 如果是激活 Zone set 命令 **zoneset activate** 触发的扩散，需要分别在 Fabric 中各交换机上通过 **display current-configuration** 命令查看 VSAN 内的激活 Zone set 的配置，若配置不一致，则通过 **zoneset activate** 命令重新激活该 Zone set，以保证 Fabric 内所有交换机的激活 Zone set 的数据一致性 • 如果是完全扩散命令 **zoneset distribute** 触发的扩散，需要分别在 Fabric 中各交换机上通过 **display current-configuration** 命令查看 VSAN 内的激活 Zone set 和 Zone 数据库配置，若配置不一致，则通过 **zoneset distribute** 命令重新激发一次完全扩散，以保证 Fabric 内所有交换机的 Zone 配置的一致性 • 如果是 Zone 模式切换触发的扩散，需要分别在 Fabric 中各交换机上通过 **display zone status** 命令查看 VSAN 内的 Zone 模式，如果各交换机的 Zone 模式不一致，则通过 **zoneset distribute** 命令来主动激发一次完全扩散，以保证 Fabric 内所有交换机的 Zone 模式的一致性

45.2 FCZONE_HARDZONE_DISABLED

日志内容	-VSAN=[UINT16]; No enough hardware resource for zone rule, switched to soft zoning.
参数解释	$1：VSAN ID
日志等级	4
举例	FCZONE/4/FCZONE_HARDZONE_DISABLED: -VSAN=2; No enough hardware resource for zone rule, switched to soft zoning.
日志说明	硬件资源不足
处理建议	激活一个更小的zone set

45.3 FCZONE_HARDZONE_ENABLED

日志内容	-VSAN=[UINT16]; Hardware resource for zone rule is restored, switched to hard zoning.
参数解释	$1：VSAN ID
日志等级	6
举例	FCZONE/6/FCZONE_HARDZONE_ENABLED: -VSAN=2; Hardware resource for zone rule is restored, switched to hard zoning.
日志说明	硬件资源恢复时，切换到hard zoning
处理建议	无需处理

45.4 FCZONE_ISOLATE_ALLNEIGHBOR

日志内容	-VSAN=[UINT16]; The E ports connected to all neighbors were isolated, because the length of the locally generated MR packet exceeded the limit.
参数解释	$1：VSAN ID
日志等级	4
举例	FCZONE/4/FCZONE_ISOLATE_ALLNEIGHBOR: -VSAN=2; The E ports connected to all neighbors were isolated, because the length of the locally generated MR packet exceeded the limit.
日志说明	因本地生成的MR报文长度超限，隔离与所有邻居相连的E-Port
处理建议	通过**display current-configuration**命令查看本地交换机VSAN内的Zone配置，删除Zone set中不必要的配置，或重新激活一个较小的Zone set。然后，对因MR报文超大导致隔离的E-Port配置**shutdown**和**undo shutdown**命令，触发重新发起合并

45.5 FCZONE_ISOLATE_CLEAR_ALLVSAN

日志内容	-Interface=[STRING]; Isolation status was cleared in all supported VSANs.
参数解释	$1：接口名称
日志等级	6
举例	FCZONE/6/FCZONE_ISOLATE_CLEAR_ALLVSAN: -Interface=Fc1/0/1; Isolation status was cleared in all supported VSANs.
日志说明	接口在所有支持的VSAN内去隔离
处理建议	无需处理

45.6 FCZONE_ISOLATE_CLEAR_VSAN

日志内容	-Interface=[STRING]-VSAN=[UINT16]; Isolation status was cleared.
参数解释	$1：接口名称 $2：VSAN ID
日志等级	6
举例	FCZONE/6/FCZONE_ISOLATE_CLEAR_VSAN: -Interface=Fc1/0/1-VSAN=2; Isolation status was cleared.
日志说明	接口在指定VSAN内去隔离
处理建议	无需处理

45.7 FCZONE_ISOLATE_NEIGHBOR

日志内容	-VSAN=[UINT16]; All the E ports connected to a neighbor were isolated because of merge failure, and the neighbor's switch WWN is [STRING].
参数解释	$1：VSAN ID $2：交换机WWN
日志等级	4
举例	FCZONE/4/FCZONE_ISOLATE_NEIGHBOR: -VSAN=2; All the E ports connected to a neighbor were isolated because of merge failure, and the neighbor's switch WWN is 10:00:00:11:22:00:0d:01.
日志说明	因与邻居交换机合并失败，隔离与该邻居相连的所有E-Port
处理建议	分别在本地和邻居交换机上通过**display current-configuration**命令查看VSAN内的Zone配置，并修改配置使其符合合并规则。然后，对因合并失败导致隔离的E-Port配置**shutdown**和**undo shutdown**命令触发两台交换机重新发起合并

46 FDB

本节介绍 FDB 模块输出的日志信息。

46.1 LRN

日志内容	The number of MAC address received in interface [STRING] reaches the upper limit. The number of MAC address received in VLAN [INT32] reaches the upper limit.
参数解释	$1：接口名称 $2：VLAN ID
日志等级	3
举例	FDB/3/LRN: -MDC=1-Slot=3; The number of MAC address received in interface GigabitEthernet3/3/5 reaches the upper limit.
日志说明	接口或VLAN学习的MAC地址数目达到了上限
处理建议	无

47 FIB

本节包含 FIB 日志消息。

47.1 FIB_FILE

日志内容	Failed to save the IP forwarding table due to lack of storage resources.
参数解释	无
日志等级	4
举例	FIB/4/FIB_FILE: -MDC=1; Failed to save the IP forwarding table due to lack of storage resources.
日志说明	存储介质剩余空间不足，保存IP FIB信息失败
处理建议	删除其它无用文件，释放存储介质的存储空间

48 FILTER

本节介绍 FILTER 模块输出的日志信息。

48.1 FILTER_EXECUTION_ICMP

日志内容	RcvIfName(1023)=[STRING];Direction(1070)=[STRING];AclType(1067)=[STRING];Acl(1068)=[STRING];Protocol(1001)=[STRING];SrcIPAddr(1003)=[IPADDR];DstIPAddr(1007)=[IPADDR];IcmpType(1062)=[STRING]([UINT16]);IcmpCode(1063)=[UINT16];MatchAclCount(1069)=[UINT32];Event(1048)=[STRING];
参数解释	$1：接口名称 $2：方向 $3：ACL类型 $4：ACL编号或者名称 $5：四层协议名称 $6：源IP地址 $7：目的IP地址 $8：ICMP类型 $9：ICMP代码 $10：命中次数 $11：事件信息
日志等级	6
举例	FILTER/6/FILTER_EXECUTION_ICMP: RcvIfName(1023)=GigabitEthernet2/0/2;Direction(1067)=inbound;AclType(1064)=ACL;Acl(1065)=3000;Protocol(1001)=ICMP;SrcIPAddr(1003)=100.1.1.1;DstIPAddr(1007)=200.1.1.1;IcmpType(1059)=Echo(8);IcmpCode(1060)=0;MatchAclCount(1066)=1000;Event(1048)=Permit;
日志说明	首次命中包过滤时发送ICMP报文过滤日志，之后定时发送该日志
处理建议	无

48.2 FILTER_EXECUTION_ICMPV6

日志内容	RcvIfName(1023)=[STRING];Direction(1070)=[STRING];AclType(1067)=[STRING];Acl(1068)=[STRING];Protocol(1001)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];Icmpv6Type(1064)=[STRING]([UINT16]);Icmpv6Code(1065)=[UINT16];MatchAclCount(1069)=[UINT32];Event(1048)=[STRING];
参数解释	$1：接口名称 $2：方向 $3：ACL类型 $4：ACL编号或者名称 $5：四层协议名称 $6：源IPv6地址 $7：目的IPv6地址 $8：ICMPV6类型 $9：ICMPV6代码 $10：命中次数 $11：事件信息
日志等级	6
举例	FILTER/6/FILTER_EXECUTION_ICMPV6: RcvIfName(1023)=GigabitEthernet2/0/2;Direction(1067)=inbound;AclType(1064)=ACL;Acl(1065)=3000;Protocol(1001)=ICMPV6;SrcIPv6Addr(1036)=2001::1;DstIPv6Addr(1037)=3001::1;Icmpv6Type(1064)=Echo(128);Icmpv6Code(1065)=0;MatchAclCount(1066)=1000;Event(1048)=Permit;
日志说明	首次命中包过滤时发送ICMPV6报文过滤日志，之后定时发送该日志
处理建议	无

48.3 FILTER_IPV4_EXECUTION

日志内容	RcvIfName(1023)=[STRING];Direction(1070)=[STRING];AclType(1067)=[STRING];Acl(1068)=[STRING];Protocol(1001)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];MatchAclCount(1069)=[UINT32];Event(1048)=[STRING];
参数解释	$1：接口名称 $2：方向 $3：ACL类型 $4：ACL编号或者名称 $5：四层协议名称 $6：源IP地址 $7：源端口号 $8：目的IP地址 $9：目的端口号 $10：命中次数 $11：事件信息
日志等级	6
举例	FILTER/6/FILTER_IPV4_EXECUTION: RcvIfName(1023)=GigabitEthernet2/0/2;Direction(1070)=inbound;AclType(1067)=ACL;Acl(1068)=3000;Protocol(1001)=TCP;SrcIPAddr(1003)=100.1.1.1;SrcPort(1004)=1025;DstIPAddr(1007)=200.1.1.1;DstPort(1008)=1026;MatchAclCount(1069)=1000;Event(1048)=Permit;
日志说明	首次命中包过滤时发送报文过滤日志，之后定时发送该日志
处理建议	无

48.4 FILTER_IPV6_EXECUTION

日志内容	RcvIfName(1023)=[STRING];Direction(1070)=[STRING];AclType(1067)=[STRING];Acl(1068)=[STRING];Protocol(1001)=[STRING];SrcIPv6Addr(1036)=[IPADDR];SrcPort(1004)=[UINT16];DstIPv6Addr(1037)=[IPADDR];DstPort(1008)=[UINT16];MatchAclCount(1069)=[UINT32];Event(1048)=[STRING];
参数解释	$1：接口名称 $2：方向 $3：ACL类型 $4：ACL编号或者名称 $5：四层协议名称 $6：源IPv6地址 $7：源端口号 $8：目的IPv6地址 $9：目的端口号 $10：命中次数 $11：事件信息
日志等级	6
举例	FILTER/6/FILTER_IPV6_EXECUTION: RcvIfName(1023)=GigabitEthernet2/0/2;Direction(1070)=inbound;AclType(1067)=ACL;Acl(1068)=3000;Protocol(1001)=TCP;SrcIPv6Addr(1036)=2001::1;SrcPort(1004)=1025;DstIPv6Addr(1037)=3001::1;DstPort(1008)=1026;MatchAclCount(1069)=1000;Event(1048)=Permit;
日志说明	首次命中包过滤时发送报文过滤日志，之后定时发送该日志
处理建议	无

49 FIPSNG

本节介绍 FIP Snooping 模块输出的日志信息。

49.1 FIPSNG_HARD_RESOURCE_NOENOUGH

日志内容	No enough hardware resource for FIP snooping rule.
参数解释	N/A
日志等级	4
举例	FIPSNG/4/FIPSNG_HARD_RESOURCE_NOENOUGH: No enough hardware resource for FIP snooping rule.
日志说明	硬件资源不足
处理建议	无

49.2 FIPSNG_HARD_RESOURCE_RESTORE

日志内容	Hardware resource for FIP snooping rule is restored.
参数解释	N/A
日志等级	6
举例	FIPSNG/6/FIPSNG_HARD_RESOURCE_RESTORE: Hardware resource for FIP snooping is restored.
日志说明	硬件资源恢复
处理建议	无

50 FTPD

本节介绍 FTPD（File Transfer Protocol Daemon）模块输出的日志信息。

50.1 FTP_ACL_DENY

日志内容	The FTP Connection [IPADDR]([STRING]) request was denied according to ACL rules.
参数解释	$1：FTP客户端IP地址 $2：FTP客户端IP地址所在VPN
日志等级	5
举例	FTP/5/FTP_ACL_DENY: The FTP Connection 1.2.3.4(vpn1) request was denied according to ACL rules.
日志说明	FTP ACL规则限制登录IP地址。该日志在FTP服务端检测到非法客户端尝试登录时输出
处理建议	无

50.2 FTP_REACH_SESSION_LIMIT

日志内容	FTP client [STRING] failed to log in. The current number of FTP sessions is [NUMBER]. The maximum number allowed is ([NUMBER]).
参数解释	$1：FTP客户端IP地址 $2：当前的FTP会话数 $3：设备允许建立的FTP会话数
日志等级	6
举例	FTP/6/FTP_REACH_SESSION_LIMIT: FTP client 1.1.1.1 failed to log in. The current number of FTP sessions is 10. The maximum number allowed is (10).
日志说明	FTP登录用户达到上限。该日志在FTP服务端检测到登录客户端数达到上限时输出
处理建议	• 请使用 **display current-configuration | include sesion-limit** 命令查看设备当前允许的FTP最大登录用户数（如果执行该**display**命令后没有显示，则表示使用的是缺省配置） • 根据需要使用 **aaa session-limit** 命令配置允许的 FTP 最大登录用户数

51 gRPC

本节介绍 gRPC 模块输出的日志信息。

51.1 GRPC_LOGIN

日志内容	[STRING] logged in from [STRING], session id [INT32].
参数解释	$1：用户名 $2：客户端地址 $3：会话ID
日志等级	6
举例	GRPC/6/GRPC_LOGIN: user logged in from 127.0.0.1, session id 1.
日志说明	用户登录成功
处理建议	无

51.2 GRPC_LOGIN_FAILED

日志内容	[STRING] from [STRING] login failed. 或 [STRING] from [STRING] login failed. [STRING]
参数解释	$1：用户名 $2：客户端地址 $3：失败原因，取值为Number of the gRPC sessions reached the limit.
日志等级	4
举例	GRPC/4/GRPC_LOGIN_FAILED: user from 127.0.0.1 login failed. GRPC/4/GRPC_LOGIN_FAILED: user from 127.0.0.1 login failed. Number of the gRPC sessions reached the limit.
日志说明	用户登录失败
处理建议	**1.** 如果未显示失败原因，请检查是否已配置用户，以及用户名和密码是否正确 **2.** 如果显示 gRPC 会话到达数量上限，请减少 gRPC 客户端连接数

51.3 GRPC_LOGOUT

日志内容	[STRING] logged out, session id [INT32].
参数解释	$1：用户名 $2：会话ID
日志等级	6
举例	GRPC/6/GRPC_LOGOUT: user logged out, session id 1.
日志说明	用户正常登出
处理建议	无

51.4 GRPC_SERVER_FAILED

日志内容	Failed to enable gRPC server.
参数解释	无
日志等级	4
举例	GRPC/4/GRPC_SERVER_FAILED: Failed to enable gRPC server.
日志说明	因端口冲突，无法和gRPC服务器建立连接
处理建议	检查是否端口号被占用

51.5 GRPC_SUBSCRIBE_EVENT_FAILED

日志内容	Failed to subscribe event [STRING].
参数解释	$1：事件名
日志等级	4
举例	GRPC/4/GRPC_SUBSCRIBE_EVENT_FAILED: Failed to subscribe event syslog.
日志说明	订阅事件失败
处理建议	无

51.6 GRPC_RECEIVE_SUBSCRIPTION

日志内容	Received a subscription of module [STRING].
参数解释	$1：模块名
日志等级	6
举例	GRPC/6/GRPC_RECEIVE_SUBSCRIPTION: Received a subscription of module syslog.
日志说明	收到某个模块的一个订阅事件
处理建议	无

52 HA

本节介绍 HA 模块输出的日志信息。

52.1 HA_BATCHBACKUP_FINISHED

日志内容	Batch backup of standby board in [STRING] has finished.
参数解释	$1：当slot仅支持单CPU时，表示slot所在位置；当slot支持多CPU时，表示CPU所在位置
日志等级	5
举例	HA/5/HA_BATCHBACKUP_FINISHED: Batch backup of standby board in slot 1 CPU 0 has finished.
日志说明	指定slot/CPU的批量备份完成
处理建议	无

52.2 HA_BATCHBACKUP_STARTED

日志内容	Batch backup of standby board in [STRING] started.
参数解释	$1：当slot仅支持单CPU时，表示slot所在位置；当slot支持多CPU时，表示CPU所在位置
日志等级	5
举例	HA/5/HA_BATCHBACKUP_STARTED: Batch backup of standby board in slot 1 CPU 0 started.
日志说明	指定slot/CPU的批量备份开始
处理建议	无

52.3 HA_STANDBY_NOT_READY

日志内容	Standby board in [STRING] is not ready, reboot ...
参数解释	$1：当slot仅支持单CPU时，表示slot所在位置；当slot支持多CPU时，表示CPU所在位置
日志等级	4
举例	HA/4/HA_STANDBY_NOT_READY: Standby board in slot 1 CPU 0 is not ready, reboot ...
日志说明	主备倒换时，如果备用slot/CPU未准备好，则不会进行主备倒换，而是重启备用slot/CPU和主用slot/CPU，并在备用slot/CPU上打印该信息
处理建议	建议备用slot/CPU批量备份完成前不要进行主备倒换

52.4 HA_STANDBY_TO_MASTER

日志内容	Standby board in [STRING] changed to the master.
参数解释	$1：当slot仅支持单CPU时，表示slot所在位置；当slot支持多CPU时，表示CPU所在位置
日志等级	4
举例	HA/4/HA_STANDBY_TO_MASTER: Standby board in slot 1 CPU 0 changed to the master.
日志说明	发生主备倒换，备用slot/CPU成为主用slot/CPU
处理建议	无

53 HQOS

本节介绍 HQOS（Hierarchical QoS）模块输出的日志信息。

53.1 HQOS_DP_SET_FAIL

日志内容	Failed to set drop profile [STRING] globally.
参数解释	$1：丢弃策略的名称
日志等级	4
举例	HQOS/4/HQOS_DP_SET_FAIL: Failed to set drop profile b globally.
日志说明	首次应用全局丢弃策略或者修改全局丢弃策略时失败
处理建议	请检查丢弃策略配置，确保支持并且策略不冲突

53.2 HQOS_FP_SET_FAIL

日志内容	Failed to set [STRING] in forwarding profile [STRING] globally.
参数解释	$1：策略类型，可以为“gts”，“bandwidth”，“queue”或者“drop profile” $2：转发策略的名称
日志等级	4
举例	HQOS/4/HQOS_FP_SET_FAIL: Failed to set gts in forwarding profile b globally.
日志说明	首次应用全局转发策略或者修改全局转发策略时失败
处理建议	请检查转发策略，确保支持并且策略不冲突

53.3 HQOS_POLICY_APPLY_FAIL

日志内容	Failed to apply some forwarding classes or forwarding groups in scheduler policy [STRING] to the [STRING] direction of interface [STRING].
参数解释	$1：调度策略的名称 $2：策略方式，可以为“inbound”或者““outbound” $3：接口名称
日志等级	4
举例	HQOS/4/HQOS_POLICY_APPLY_FAIL: Failed to apply some forwarding classes or forwarding groups in scheduler policy b to the inbound direction of interface Ethernet3/1/2.
日志说明	接口上应用调度策略失败，或者修改接口上已应用的调度策略
处理建议	通过命令行**display qos scheduler-policy diagnosis interface**查看失败的转发节点以及失败原因，之后检查运行配置

53.4 HQOS_POLICY_RECOVER_FAIL

日志内容	Failed to recover scheduler policy [STRING] to the [STRING] direction of interface [STRING] due to [STRING].
参数解释	$1：调度策略的名称 $2：策略方式，可以为“inbound”或者“outbound” $3：接口名称 $4：失败原因
日志等级	4
举例	HQOS/4/HQOS_POLICY_RECOVER_FAIL: Failed to recover scheduler policy b to the outbound direction of interface Ethernet3/1/2 due to conflicting with QoS configuration.
日志说明	接口板重启或设备重启，恢复接口上应用的调度策略失败
处理建议	请根据失败原因检查配置

54 HTTPD

本节介绍 HTTPD（HTTP daemon）模块输出的日志信息。

54.1 HTTPD_CONNECT

日志内容	[STRING] client [STRING] connected to the server successfully.
参数解释	$1：连接类型，HTTP或HTTPS $2：客户端IP地址
日志等级	6
举例	HTTPD/6/HTTPD_CONNECT: HTTP client 192.168.30.117 connected to the server successfully.
日志说明	HTTP/HTTPS服务器接受了客户端的请求，HTTP/HTTPS连接成功建立
处理建议	无

54.2 HTTPD_CONNECT_TIMEOUT

日志内容	[STRING] client [STRING] connection idle timeout.
参数解释	$1：连接类型，HTTP或HTTPS $2：客户端IP地址
日志等级	6
举例	HTTPD/6/HTTPD_CONNECT_TIMEOUT: HTTP client 192.168.30.117 connection to server idle timeout.
日志说明	HTTP/HTTPS连接因空闲时间太长而断开
处理建议	无

54.3 HTTPD_DISCONNECT

日志内容	[STRING] client [STRING] disconnected from the server.
参数解释	$1：连接类型，HTTP或HTTPS $2：客户端IP地址
日志等级	6
举例	HTTPD/6/HTTPD_DISCONNECT: HTTP client 192.168.30.117 disconnected from the server.
日志说明	HTTP/HTTPS客户端断开了到服务器的连接
处理建议	无

54.4 HTTPD_FAIL_FOR_ACL

日志内容	[STRING] client [STRING] failed the ACL check and could not connect to the server.
参数解释	$1：连接类型，HTTP或HTTPS $2：客户端IP地址
日志等级	6
举例	HTTPD/6/HTTPD_FAIL_FOR_ACL: HTTP client 192.168.30.117 failed the ACL check and cannot connect to the server.
日志说明	HTTP/HTTPS客户端没有通过ACL检查，无法建立连接
处理建议	无

54.5 HTTPD_FAIL_FOR_ACP

日志内容	[STRING] client [STRING] was denied by the certificate access control policy and could not connect to the server.
参数解释	$1：连接类型，HTTP或HTTPS $2：客户端IP地址
日志等级	6
举例	HTTPD/6/HTTPD_FAIL_FOR_ACP: HTTP client 192.168.30.117 was denied by the certificate attribute access control policy and could not connect to the server.
日志说明	HTTP/HTTPS客户端没有通过证书接入控制策略检查，无法建立连接
处理建议	无

54.6 HTTPD_REACH_CONNECT_LIMIT

日志内容	[STRING] client [STRING] failed to connect to the server, because the number of connections reached the upper limit.
参数解释	$1：连接类型，HTTP或HTTPS $2：客户端IP地址
日志等级	6
举例	HTTPD/6/HTTPD_REACH_CONNECT_LIMIT: HTTP client 192.168.30.117 failed to connect to the server, because the number of connections reached the upper limit.
日志说明	已达到最大连接数，无法建立新的连接
处理建议	请根据需要使用命令**aaa session-limit**配置允许的Web最大登录用户数

55 IF

本节介绍接口管理模块输出的日志信息。

55.1 IF

日志内容	Interfaces of this board don’t support the bridge-forwarding enable command.
参数解释	• 无
日志等级	3
举例	LIF/3/IF: -MDC=1-Slot=3; Interfaces of this board don’t support the bridge-forwarding enable command.
日志说明	指定slot上的以太网接口由于其单板限制，不能配置**bridge-forwarding enable**命令
处理建议	仅CSPEX类单板（CSPEX-1204和CSPEX-1104-E除外）和CEPC类单板的以太网接口可以配置**bridge-forwarding enable**命令

55.2 IF

日志内容	Can’t assign [STRING] to [STRING] that was configured with the bridge-forwarding enable command.
参数解释	$1：以太网接口名称 • $2：三层聚合接口名称
日志等级	3
举例	LIF/3/IF: -MDC=1; Can’t assign GigabitEthernet3/1/1 to Route-Aggregation1 that was configured with the bridge-forwarding enable command.
日志说明	以太网接口由于其单板限制，不能加入已配置**bridge-forwarding enable**命令的三层聚合接口
处理建议	仅CSPEX类单板（CSPEX-1204和CSPEX-1104-E除外）和CEPC类单板的以太网接口可以加入已配置**bridge-forwarding enable**命令的三层聚合接口

55.3 IF

日志内容	Some member ports of [STRING] don't support the bridge-forwarding enable command.
参数解释	• $1：三层聚合接口名称
日志等级	3
举例	LIF/3/IF: -MDC=1-Slot=3; Some member ports of Route-Aggregation1 don't support the bridge-forwarding enable command.
日志说明	三层聚合接口由于其成员端口的单板限制，不支持配置**bridge-forwarding enable**命令
处理建议	三层聚合组的成员端口均属于CSPEX类单板（CSPEX-1204和CSPEX-1104-E除外）和CEPC类单板时，该聚合接口才支持配置**bridge-forwarding enable**命令

55.4 IF

日志内容	Cannot assign [STRING] to [STRING] when the route-aggregation different-mac-address enable command is configured.
参数解释	$1：接口名称 • $2：三层聚合接口名称
日志等级	3
举例	LIF/3/IF: -MDC=1-Slot=3; Cannot assign GigabitEthernet3/2/5 to Route-Aggregation100 when the route-aggregation different-mac-address enable command is configured.
日志说明	系统视图下已配置**route-aggregation different-mac-address enable**命令的情况下，某些单板的接口不支持加入三层聚合组
处理建议	系统视图下已配置**route-aggregation different-mac-address enable**命令的情况下，属于以下单板的成员端口不能加入三层聚合接口 • CSPC 类单板（CSPC-GE16XP4L-E、CSPC-GE24L-E 和 CSPC-GP24GE8XP2L-E 除外） • CMPE-1104 单板

55.5 IF

日志内容	Operation failed because of insufficient resources on Route-Aggregation [INT32].
参数解释	$1：聚合子接口编号
日志等级	2
举例	LIF/2/IF: -MDC=1-Slot=2; Operation failed because of insufficient resources on Route-Aggregation1.1.
日志说明	聚合子接口配置**traffic-statistic enable**时，因系统资源不足，统计功能不生效
处理建议	**1.** 用 undo traffic-statistic enable 命令关闭聚合子接口的报文统计功能 **2.** 联系技术支持

55.6 IF

日志内容	The operation is not supported because configuration conflicts on Route-Aggregation[INT32]
参数解释	$1：聚合子接口编号
日志等级	2
举例	LIF/2/IF: -MDC=1-Chassis=1-Slot=3; The operation is not supported because configuration conflicts on Route-Aggregation1.1.
日志说明	聚合子接口配置**traffic-statistic enable**时，与聚合子接口下的L2VPN专线配置冲突，统计功能不生效
处理建议	**1.** 用 **undo traffic-statistic enable** 命令关闭聚合子接口的报文统计功能 **2.** 在聚合子接口上 **undo** 掉 L2VPN 专线配置，再配置 **traffic-statistic enable** 命令 **3.** 如日志仍显示，请联系技术支持

55.7 IF

日志内容	Operation failed because of insufficient hardware resources.
参数解释	无
日志等级	3
举例	LIF/3/IF: -MDC=1-Slot=4; Operation failed because of insufficient hardware resources.
日志说明	因系统资源不足，创建的接口（例如VLAN接口）不可用
处理建议	**1.** 用 **undo** 命令删除该接口 **2.** 用 **display interface** *interface-type* **brief** 命令查看接口概要信息。删除不必要的接口以释放资源，再重新创建需要的接口 **3.** 若问题仍然存在，请联系技术支持

55.8 IF

日志内容	Operation failed on [STRING] because of insufficient hardware resources.
参数解释	$1：接口名称或VLAN编号
日志等级	3
举例	LIF/3/IF: -MDC=1-Slot=4; Operation failed on Route-Aggregation33.2999 because of insufficient hardware resources. LIF/3/IF: -MDC=1-Slot=4; Operation failed on VLAN222 because of insufficient hardware resources.
日志说明	因系统资源不足，创建的接口（例如三层聚合子接口）或Sub VLAN不可用
处理建议	1. 用 **undo** 命令删除该接口或 VLAN 2. 用 **display interface** *interface-type* **brief** 命令查看接口概要信息，或通过 **display supervlan** 命令查看 Super VLAN 及其关联的 Sub VLAN 信息。删除不必要的接口/Sub VLAN 以释放资源，再重新创建需要的接口或 VLAN 3. 若问题仍然存在，请联系技术支持

55.9 IF

日志内容	Not enough resources for [STRING].
参数解释	$1：接口名称
日志等级	6
举例	LIF/6/EPOLL: -MDC=1-Slot=5; Not enough resources for Route-Aggregation1.1.
日志说明	硬件资源不足，导致接口的QinQ终结功能（vlan-type dot1q vid second-dot1q命令）使能失败
处理建议	1. 通过 display current-configuration | include second-dot1q 命令查看当前 QinQ 终结配置，通过 undo vlan-type dot1q vid second-dot1q 命令删除暂不使用的配置来释放资源 2. 联系技术支持

56 IFNET

本节介绍接口管理模块输出的日志信息。

56.1 VLAN_MODE_CHANGE

日志内容	Dynamic VLAN [INT32] has changed to a static VLAN.
参数解释	$1：VLAN ID
日志等级	5
举例	IFNET/5/VLAN_MODE_CHANGE: -MDC=1; Dynamic VLAN 20 has changed to a static VLAN.
日志说明	创建VLAN接口导致对应的动态VLAN转换为静态VLAN
处理建议	无

56.2 IF_JUMBOFRAME_WARN

日志内容	The specified size of jumbo frames on the aggregate interface [STRING] is not supported on the member port [STRING].
参数解释	$1：聚合接口名称 $2：成员端口名称
日志等级	3
举例	IFNET/3/IF_JUMBOFRAME_WARN: -MDC=1-Slot=3; The specified size of jumbo frames on the aggregate interface Bridge-Aggregation1 is not supported on the member port GigabitEthernet1/0/1.
日志说明	聚合接口修改**`jumboframe enable`** [*`size`*]配置，部分成员端口不支持
处理建议	确认成员端口支持配置的*`size`*范围，将聚合接口的*`size`*配置在该范围内

56.3 INTERFACE_NOTSUPPRESSED

日志内容	Interface [STRING] is not suppressed.
参数解释	$1：接口名称
日志等级	6
举例	IFNET/6/INTERFACE_NOTSUPPRESSED: Interface GigabitEthernet1/0/1 is not suppressed.
日志说明	接口由抑制状态变为非抑制状态，此时上层业务可以感知接口UP/DOWN状态变化
处理建议	无

56.4 INTERFACE_SUPPRESSED

日志内容	Interface [STRING] was suppressed.
参数解释	$1：接口名称
日志等级	5
举例	IFNET/5/INTERFACE_SUPPRESSED: Interface GigabitEthernet1/0/1 was suppressed.
日志说明	当接口状态频繁变化时，接口被抑制。抑制期间，上层业务不能感知端口UP/DOWN状态变化
处理建议	**1.** 检查接口（本端或对端）连线是否被频繁插拔 **2.** 通过配置以太网接口物理连接状态抑制功能调整抑制参数

56.5 LINK_UPDOWN

日志内容	Line protocol state on the interface [STRING] changed to [STRING].
参数解释	$1：接口名称 $2：协议状态，up、down
日志等级	4
举例	IFNET/4/LINK_UPDOWN: Line protocol state on the interface GigabitEthernet1/0/1 changed to down.
日志说明	接口的链路层协议状态发生变化
处理建议	链路层状态为down时，请使用**display interface**命令查看链路层状态，进一步定位链路层状态为down的原因

56.6 PHY_UPDOWN

日志内容	Physical state on the interface [STRING] changed to [STRING].
参数解释	$1：接口名称 $2：链路状态，up、down
日志等级	3
举例	IFNET/3/PHY_UPDOWN: Physical state on the GigabitEthernet1/0/1 changed to down.
日志说明	接口的链路状态发生变化
处理建议	物理层状态为down时，请检查是否没有物理连线或者链路故障

56.7 PROTOCOL_UPDOWN

日志内容	Protocol [STRING] state on the interface [STRING] changed to [STRING].
参数解释	$1：协议名称 $2：接口名称 $3：协议状态，up、down
日志等级	5
举例	IFNET/5/PROTOCOL_UPDOWN: Protocol IPX state on the interface GigabitEthernet1/0/1 changed to up.
日志说明	接口上一个协议的状态发生变化
处理建议	网络层状态为down时，请检查网络层协议配置

56.8 VLAN_MODE_CHANGE

日志内容	Dynamic VLAN [INT32] has changed to a static VLAN.
参数解释	$1：VLANID
日志等级	5
举例	IFNET/5/VLAN_MODE_CHANGE: Dynamic VLAN 20 has changed to a static VLAN.
日志说明	创建VLAN虚接口导致动态VLAN转换成静态VLAN
处理建议	无

57 IKE

本节介绍 IKE 模块输出的日志信息。

57.1 IKE_P1_SA_ESTABLISH_FAIL

日志内容	Failed to establish phase 1 SA for the reason of [STRING]. The SA's source address is [STRING], and its destination address is [STRING].
参数解释	$1：失败原因，显示为no matching proposal、invalid ID information、unavailable certificate、unsupported DOI、unsupported situation、invalid proposal syntax、invalid SPI、invalid protocol ID、invalid certificate、authentication failure、invalid message header、invalid transform ID、malformed payload、retransmission timeout、或incorrect configuration $2：源地址 $3：目的地址
日志等级	6
举例	IKE/6/IKE_P1_SA_ESTABLISH_FAIL: Failed to establish phase 1 SA for the reason of no matching proposal. The SA's source address is 1.1.1.1 and its destination address is 2.2.2.2.
日志说明	IKE建立第一阶段SA失败以及失败原因
处理建议	检查本端和对端设备的IKE配置

57.2 IKE_P2_SA_ESTABLISH_FAIL

日志内容	Failed to establish phase 2 SA for the reason of [STRING]. The SA's source address is [STRING], and its destination address is [STRING].
参数解释	$1：失败原因，显示为invalid key information、invalid ID information、unavailable proposal、unsupported DOI、unsupported situation、invalid proposal syntax、invalid SPI、invalid protocol ID、invalid hash information、invalid message header、malformed payload、retransmission timeout、或incorrect configuration $2：源地址 $3：目的地址
日志等级	6
举例	IKE/6/IKE_P2_SA_ESTABLISH_FAIL: Failed to establish phase 2 SA for the reason of invalid key information. The SA's source address is 1.1.1.1, and its destination address is 2.2.2.2.
日志说明	IKE建立第二阶段SA失败以及失败原因
处理建议	检查本端和对端设备的IKE和IPsec配置

57.3 IKE_P2_SA_TERMINATE

日志内容	The IKE phase 2 SA was deleted for the reason of [STRING]. The SA's source address is [STRING], and its destination address is [STRING].
参数解释	$1：删除SA的原因，显示为SA expiration $2：源地址 $3：目的地址
日志等级	6
举例	IKE/6/IKE_P2_SA_TERMINATE: The IKE phase 2 SA was deleted for the reason of SA expiration. The SA's source address is 1.1.1.1, and its destination address is 2.2.2.2.
日志说明	第二阶段SA由于过期失效而删除
处理建议	无

58 INTRACE

本节介绍 INPCB（协议栈控制块）模块输出的日志信息。

58.1 WHITELIST

日志内容	-[STRING]; Failed to add ACL rule [STRING]:[UINT16] -> [STRING]:[UINT16] to the whitelist, VRF: [UINT16], error code: 0x[UINT32].
参数解释	$1：板号 $2：本地地址 $3：本地端口号 $4：远端地址 $5：远端端口号 $6：私网索引 $7：错误码，包括： • 0x22010002: ACL 规则已存在 • 0x22010008: 白名单规则已达上限 • 0x40010001: 其他异常，比如 MDC 控制块不存在 • 0x4001000B: 资源不足
日志等级	3
举例	INTRACE/3/WHITELIST: -Chassis=2-Slot=3; Failed to add ACL rule 1.1.1.1:36523 -> 1.1.1.2:179 to the whitelist, VRF: 0, error code: 0x22010002.
日志说明	TCP业务添加ACL白名单失败
处理建议	检查该TCP连接状态，查看该连接业务是否正常

日志内容	-[STRING]; Failed to delete ACL rule [STRING]:[UINT16] -> [STRING]:[UINT16] from the whitelist, VRF: [UINT16], error code: 0x[UINT32].
参数解释	$1：板号 $2：本地地址 $3：本地端口号 $4：远端地址 $5：远端端口号 $6：私网索引 $7：错误码，包括： • 0x40010001: 其他异常，比如 MDC 控制块不存在 • 0x40010008: 传入参数错误 • 0x4001000B: 资源不足
日志等级	3
举例	INTRACE/3/WHITELIST:-Chassis=2-Slot=3; Failed to delete ACL rule 1.1.1.1:36523 -> 1.1.1.2:179 from the whitelist, VRF: 0, error code: 0x22010001.
日志说明	TCP业务删除ACL白名单失败
处理建议	检查TCP和ACL白名单，查看是否出现内存残留或业务异常

59 IP ROUTING

本节介绍 IP ROUTING 模块输出的日志信息。

59.1 IPUC_ROUTE

日志内容	No enough resource
参数解释	无
日志等级	3
举例	L3/3/IPUC_ROUTE: -MDC=1-Slot=4; No enough resource
日志说明	硬件资源不足，无法完成当前操作。例如，统计报文的计数器资源不足，无法完成统计
处理建议	联系技术支持

59.2 IPUC_ROUTE

日志内容	Not enough ECMP-ID resource.
参数解释	无
日志等级	4
举例	L3/4/IPUC_ROUTE: -MDC=1-Slot=5; Not enough ECMP-ID resource.
日志说明	ECMP ID资源不足，单板不能学习新的等价路由
处理建议	联系技术支持

59.3 IPUC_ROUTE6

日志内容	Not enough ECMP-ID resource.
参数解释	无
日志等级	4
举例	L3/4/IPUC_ROUTE6: -MDC=1-Slot=5; Not enough ECMP-ID resource.
日志说明	ECMP ID资源不足，单板不能学习新的等价路由
处理建议	联系技术支持

59.4 IPUC_VN

日志内容	No enough VN index resource
参数解释	无
日志等级	4
举例	L3/4/IPUC_VN: -MDC=1-Slot=3; No enough VN index resource.
日志说明	虚拟下一跳索引资源不足，单板不能学习新的非主机路由
处理建议	联系技术支持

59.5 IPUC_VN

日志内容	Not enough ECMP-ID resource.
参数解释	无
日志等级	4
举例	L3/4/IPUC_VN: -MDC=1-Slot=3; Not enough ECMP-ID resource.
日志说明	ECMP ID资源不足，单板不能学习新的等价路由
处理建议	联系技术支持

60 IP6ADDR

本节介绍 IPv6 地址模块输出的日志信息。

60.1 IP6ADDR_CREATEADDRESS_ERROR

日志内容	Failed to create an address by the prefix. Reason: [STRING] on [STRING] and [STRING] on [STRING] overlap.
参数解释	$1：IPv6地址前缀 $2：接口名 $3：IPv6地址前缀 $4：接口名
日志等级	4
举例	IP6ADDR/4/IP6ADDR_CREATEADDRESS_ERROR: Failed to create an address by the prefix. Reason: 2001::/64 on GigabitEthernet1/0/2 and 2001::/64 on GigabitEthernet1/0/1 overlap.
日志说明	当配置接口通过引用前缀生成IPv6地址时，可能由于同一台设备的不同接口前缀覆盖，导致IPv6地址生成失败，此时输出本日志
处理建议	取消冲突接口上的通过前缀生成IPv6地址的配置，重新配置其他前缀的IPv6地址

60.2 IP6ADDR_CREATEADDRESS_INVALID

日志内容	Cann't configure the unspecified address or loopback address on [STRING] by using a prefix with all zeros.
参数解释	$1：接口名
日志等级	4
举例	IP6ADDR/4/IP6ADDR_CREATEADDRESS_INVALID: Cann't configure the unspecified address or loopback address on GigabitEthernet1/0/1 by using a prefix with all zeros.
日志说明	接口上的IPv6地址不能是未指定地址或者环回地址。如果使用**ipv6 prefix**命令配置了全零的IPv6地址前缀，并通过**ipv6 address** *prefix-number*命令引用全零的IPv6地址前缀为接口配置了未指定地址或者环回地址，则输出本日志
处理建议	取消无效配置，重新为接口配置新的IPv6地址

61 IP6FW

本节包含 IPv6 报文转发的日志消息。

61.1 IP6FW_ABNORMAL_HEADERS

日志内容	Received an IPv6 packet with repeated extension headers.
参数解释	N/A
日志等级	6
举例	IP6FW/6/IP6FW_ABNORMAL_HEADERS: Received an IPv6 packet with repeated extension headers.
日志说明	收到一个包含重复扩展头的IPv6报文
处理建议	检查报文源的合法性

62 IP6FW

本节包含 IP6FW（IPv6 Forwarding）日志信息。

62.1 IP6FW_ABNORMAL_HEADERS

日志内容	Received an IPv6 packet with repeated extension headers.
参数解释	无
日志等级	6
举例	IP6FW/6/IP6FW_ABNORMAL_HEADERS: Received an IPv6 packet with repeated extension headers.
日志说明	收到一个包含重复扩展头的IPv6报文
处理建议	检查报文源的合法性

62.2 IP6FW_FAILED_TO_SET_MTU

日志内容	Failed to set MTU [UINT32] on interface [STRING] for IPv6 packets.
参数解释	$1：MTU值 $2：接口名称
日志等级	5
举例	IP6FW/5/IP6FW_FAILED_TO_SET_MTU: Failed to set MTU 9600 on interface GigabitEthernet6/3/8 for IPv6 packets.
日志说明	在接口上配置MTU值失败
处理建议	修改接口下MTU值

63 IPADDR

本节介绍 IP 地址模块输出的日志信息。

63.1 IPADDR_HA_EVENT_ERROR

日志内容	A process failed HA upgrade because [STRING].
参数解释	$1：进程HA升级失败原因： • IPADDR failed the smooth upgrade：板间平滑失败 • IPADDR failed to reupgrade to the master process：重新升级为主失败 • IPADDR stopped to restart the timer：重启定时器停止 • IPADDR failed to upgrade to the master process：升级为主进程失败 • IPADDR failed to restart the upgrade：重新尝试升级失败 • IPADDR failed to add the unicast object to the master task epoll：将 sync 单播对象挂主任务 epoll 失败 • IPADDR failed to create an unicast object：创建单播失败 • IPADDR role switchover failed when the standby process switched to the master process：备升主时角色转换失败 • IPADDR switchover failed when the master process switched to the standby process：主变备时降级失败 • IPADDR HA upgrade failed：HA 升级失败 • IPADDR failed to set the interface filtering criteria：设置接口选择句柄失败 • IPADDR failed to register interface events：注册接口事件失败 • IPADDR failed to subscribe port events：订阅端口事件失败 • IPADDR failed to add a VPN port event to the master epoll：添加 VPN 的端口事件到主 Epoll 失败 • IRDP failed to open DBM：打开 DBM 数据库失败 • IRDP failed to initiate a connection to the device management module：向设备管理建立连接失败 • IRDP failed to add the master task epoll with the handle used to connect to the device management module ：与设备管理建立连接的句柄加 Epoll 失败 • IRDP failed to register device management events：注册设备管理事件失败 • IRDP failed to subscribe port events：订阅协议使能端口事件失败 • IRDP failed to add the master task epoll with the handle used to subscribe port events：订阅协议使能端口事件的句柄加 Epoll 失败 • IRDP failed to set the interface filtering criteria：设置接口选择句柄失败 • IRDP failed to register interface events：注册接口事件失败 • IRDP failed to register network events：注册网络事件失败 • IRDP failed to create the interface control block storage handle：创建接口控制块存储句柄失败 • IRDP failed to create the timer：创建定时器失败 • IRDP failed to add the master task epoll with the handle used to create the timer：创建定时器的句柄加 Epoll 失败 • IRDP failed to set the schedule time for the timer：设置定时器调度时间失败 • IRDP failed to set the timer to unblocked status：设置定制器为非阻塞失败 • IRDP failed to create a timer instance：创建定时器实例失败
日志等级	4

举例	IPADDR/4/IPADDR_HA_EVENT_ERROR: A process failed HA upgrade because IPADDR failed the smooth upgrade.
日志说明	进程HA升级失败，原因是板间平滑失败，重新升级为主失败等
处理建议	• 请联系技术支持

63.2 IPADDR_HA_STOP_EVENT

日志内容	The device received an HA stop event.
参数解释	无
日志等级	4
举例	IPADDR/4/IPADDR_HA_STOP_EVENT: The device received an HA stop event.
日志说明	设备收到HA STOP事件
处理建议	• 请联系技术支持

64 IPFW

本节包含 IPFW（IP Forwarding）日志信息。

64.1 IP_ADD_FLOW_ANTISYNFLD

日志内容	Add a flow-based entry: Packet type=[STRING]; SrcIP=[IPADDR]; DstPort=[UINT16]; VPN=[STRING].
参数解释	$1：报文类型，取值包括： • MPLS • IP $2：攻击报文的源IP地址 $3：被攻击的端口号 $4：VPN实例名称，公网取值为：N/A
日志等级	4
举例	IPFW/4/IP_ADD_FLOW_ANTISYNFLD: Add a flow-based entry: Packet type=IP; SrcIP=2000::1; DstPort=23; VPN=N/A.
日志说明	在公网中，添加一条基于流的TCP SYN Flood攻击防范表项，该表项的报文类型是IP，源IP地址是2000::1，目的端口号是23
处理建议	检查攻击来源

64.2 IP_ADD_INTERFACE_ANTISYNFLD

日志内容	Add an interface-based entry: Packet type=[STRING]; Interface=[STRING].
参数解释	$1：报文类型，取值包括： • MPLS • IP $2：接口名称
日志等级	4
举例	IPFW/4/IP_ADD_INTERFACE_ANTISYNFLD: Add an interface-based entry: Packets type=MPLS; Interface=GigabitEthernet1/0/1.
日志说明	添加一条基于接口的TCP SYN Flood攻击防范表项，该表项的报文类型是MPLS，接口名称是GigabitEthernet1/0/1
处理建议	检查攻击来源

64.3 IP_DEL_FLOW_ANTISYNFLD

日志内容	Delete a flow-based entry: Packet type=[STRING]; SrcIP=[IPADDR]; DstPort=[UINT16]; VPN=[STRING].
参数解释	$1：报文类型，取值包括： • MPLS • IP $2：攻击报文的源IP地址 $3：被攻击的端口号 $4：VPN实例名称，公网取值为：N/A
日志等级	4
举例	IPFW/4/IP_DEL_FLOW_ANTISYNFLD: Delete a flow-based entry: Packet type=MPLS; SrcIP=192.168.1.2; DstPort=80; VPN=vpn1.
日志说明	在私网中，删除一条基于流的TCP SYN Flood攻击防范表项，该表项的报文类型是MPLS，源IP地址是192.168.1.2，目的端口号是80，VPN实例名称是vpn1
处理建议	无需处理

64.4 IP_DEL_INTERFACE_ANTISYNFLD

日志内容	Delete an interface-based entry: Packet type=[STRING]; Interface=[STRING].
参数解释	$1：报文类型，取值包括： • MPLS • IP $2：接口名称
日志等级	4
举例	IPFW/4/IP_DEL_INTERFACE_ANTISYNFLD: Delete an interface-based entry: Packets type=IP, Interface=GigabitEthernet1/0/1.
日志说明	删除一条基于接口的TCP SYN Flood攻击防范表项，该表项的报文类型是IP，接口名称是GigabitEthernet1/0/1
处理建议	无需处理

64.5 IP_INSERT_FAILED_ANTISYNFLD

日志内容	Insert into AVL tree failed for flow-based entry: Family=[UINT32]; DstPort=[UINT16]; VRF=[UINT16].
参数解释	$1：协议簇编号 $2：目的端口号 $3：VRF索引
日志等级	5
举例	IPFW/5/IP_INSERT_FAILED_ANTISYNFLD: Insert into AVL tree failed for flow-based entry : Family=2; DstPort=80; VRF=2.
日志说明	基于流的TCP SYN Flood攻击防范的攻击表项插入AVL树失败，协议簇号是2，目的端口号是80，VRF索引是2
处理建议	无需处理

64.6 IP_NOTSUPPORT_ANTISYNFLD

日志内容	TCP SYN flood attack prevention is not supported.
参数解释	无
日志等级	6
举例	IPFW/6/IP_NOTSUPPORT_ANTISYNFLD: TCP SYN flood attack prevention is not supported.
日志说明	不支持TCP SYN Flood攻击防范功能
处理建议	无需处理

64.7 IP_SETTING_FAILED_ANTISYNFLD

日志内容	Setting entry to drive failed. Total failed count=[UINT32].
参数解释	$1：下驱动失败的攻击表项总个数
日志等级	5
举例	IPFW/5/IP_SETTING_FAILED_ANTISYNFLD: Setting entry to drive failed. Total failed count = 12345.
日志说明	表项下驱动失败，下驱动失败的攻击表项总个数为12345
处理建议	无需处理

64.8 IPFW_BPA_NORESOURCE

日志内容	Not enough resources are available on [STRING] to enable BGP policy accounting for interface [STRING].
参数解释	$1:chassis编号+slot编号或slot编号 $2: 接口名
日志等级	6
举例	IPFW/6/IPFW_BPA_NORESOURCE: -MDC=1-Slot=2; Not enough resources are available on slot2 to enable BGP policy accounting for interface Route-Aggregation1.
日志说明	配置**bgp-policy accounting**命令时，由于slot资源不足导致接口开启BGP策略计费功能失败
处理建议	无

64.9 IPFW_INFO

日志内容	The specified IP load sharing mode is not supported on this slot.
参数解释	无
日志等级	6
举例	IPFW/6/IPFW_INFO: -MDC=1-Slot=2; The specified IP load sharing mode is not supported on this slot.
日志说明	用户配置的IP负载均衡模式在此单板上不支持
处理建议	确认单板支持的模式，重新配置

日志内容	Failed to configure IP load sharing mode on this slot.
参数解释	无
日志等级	6
举例	IPFW/6/IPFW_INFO: -MDC=1-Slot=2; Failed to configure IP load sharing mode on this slot.
日志说明	用户配置的IP负载均衡模式在此单板上配置失败
处理建议	确认单板支持的模式，重新配置

64.10 IPFW_FAILED_TO_SET_MTU

日志内容	Failed to set MTU [UINT32] on interface [STRING] for IPv4 packets.
参数解释	$1：MTU值 $2：接口名称
日志等级	5
举例	IPFW/5/IPFW_FAILED_TO_SET_MTU: Failed to set MTU 9600 on interface GigabitEthernet6/3/8 for IPv4 packets.
日志说明	在接口上配置MTU值失败
处理建议	修改接口下MTU值

65 IPoE

本节介绍 IPoE 模块输出的 日志信息。

65.1 DIAG

日志内容	The [STRING] configuration conflicts with user-vlan configuration. To avoid conflicts, do not configure both features on interface [STRING].
参数解释	$1：配置名称，取值包括： • ip subscriber l2vpn-leased：IPoE L2VPN 专线用户配置 • ip subscriber routed enable：三层接入模式的 IPoE 配置 $2：子接口名称
日志等级	4
举例	DIPOE/4/DIAG: -MDC=1-Slot=4; The ip subscriber routed enable configuration conflicts with user-vlan configuration. To avoid conflicts, do not configure both features on interface Route-Aggregation1.2.
日志说明	子接口上同时配置了用户VLAN终结特性和以下特性，存在配置冲突 • IPoE L2VPN 专线用户（**ip subscriber l2vpn-leased**） • 三层接入模式的 IPoE 功能（**ip subscriber routed enable**）
处理建议	**1.** 子接口视图下使用 **display this** 命令查看是否同时存在用户 VLAN 终结配置和 IPoE L2VPN 专线用户配置（或三层接入模式的 IPoE 配置），然后使用 **undo** 命令删除其中一类配置命令 **2.** 如果问题仍然存在，联系技术支持

65.2 DIAG

日志内容	Insufficient BRAS statistics or BRAS rate-limiting profile resources for IPoE. The statistics or rate-limiting function of the session(UserID = [int32]) does not take effect.
参数解释	$1：用户ID值
日志等级	4
举例	DIPOE/4/DIAG:Insufficient BRAS statistics or BRAS rate-limiting profile resources for IPoE. The statistics or rate-limiting function of the session(UserID = 0x38200002) does not take effect.
日志说明	• 添加 IPoE 会话时，因系统资源不足，新增的 IPoE 会话部分功能（例如会话计费、限速等功能）不生效 • 端口加入已有处于在线状态的 IPoE 会话的聚合接口时，因系统资源不足，IPoE 会话部分功能（例如会话计费、限速等功能）对该端口上接入的用户不生效
处理建议	**1.** 执行 **display qos-acl resource** 命令显示当前单板上资源的使用情况 **2.** 删除一些没有必要多余的资源 **3.** 请联系技术支持

65.3 IPOE_ENABLE_ERROR

日志内容	Failed to [STRING] [STRING] [STRING] for the reason of [STRING] on [STRING].
参数解释	$1：操作类型，具体取值如下： ○ enable：开启 ○ disable：关闭 $2：协议栈类型，具体取值如下： ○ IPv4：IPv4 协议栈 ○ IPv6：IPv6 协议栈 $3：功能类型，具体取值如下： ○ IPOE：IPoE 功能或未知源 IP 报文上送 CPU ○ IPOE set web mode：Web 或 Web MAC 认证方式 ○ IPOE http fast reply：HTTP 报文的快速应答功能 $4：失败原因，具体原因请见表65-1 $5：接口名称
日志等级	3
举例	IPOE/3/IPOE_ENABLE_ERROR: Failed to enable IPv4 IPOE for the reason of not enough resources on Route-Aggregation1023.
日志说明	因资源不足、产品不支持或其它未知错误，导致在接口上开启或关闭IPoE功能失败
处理建议	具体处理建议请见表65-1

表65-1 失败原因列表

下发驱动失败原因	说明	处理建议
this operation is not supported	不支持	请确认接口是否支持IPoE功能
not enough resources	驱动资源不足	请联系技术支持
other unknown errors	其他未知错误	请联系技术支持
resource conflict	驱动资源冲突	请联系技术支持

65.4 IPOE_FREERULE_ERROR

日志内容	Failed to [STRING] [STRING] free rule for the reason of [STRING] on [STRING].
参数解释	$1：操作类型，具体取值如下： o add：添加 o delete：删除 $2：放行报文类型，具体取值如下： o DHCPv4：DHCPv4 报文 o DHCPv6：DHCPv6 报文 o IPv4 IGMP：IGMP 报文 o IPv4 VRRP：IPv4 VRRP 报文 o VRRP v6：IPv6 VRRP 报文 o ICMPv4：IPv4 ICMP 报文 o ICMPv6：IPv6 ICMP 报文 $3：失败原因，具体原因请见表65-1 $4：接口名称
日志等级	3
举例	IPOE/3/ IPOE_FREERULE_ERROR: Failed to add DHCPv4 free rule for the reason of not enough resources on Route-Aggregation1023.
日志说明	因资源不足、产品不支持或其它未知错误，导致在接口上添加或删除报文放行规则失败
处理建议	具体处理建议请见表65-1

65.5 IPOE_HTTP_DEFENSE

日志内容	An HTTP/HTTPS attack was detected, and the attacked destination IP was [IPADDR] in VPN [STRING].
参数解释	$1: HTTP/HTTPS攻击的目的IPv4或IPv6地址 $2: HTTP/HTTPS攻击发生所在VPN实例的名称（“N/A”表示攻击发生在公网）
日志等级	5
举例	IPOE/5/IPOE_HTTP_DEFENSE: An HTTP/HTTPS attack was detected, and the attacked destination IP was 1.1.1.1 in VPN vpn1.
日志说明	HTTP/HTTPS报文攻击达到阻断条件时输出攻击日志信息
处理建议	无

65.6 IPOE_IPV4_HTTP_ATTACK_EXCEED_ERROR

日志内容	The number of anti-HTTP attack IPv4 ACLs exceeded 30 percent of the total number of IPv4 ACLs. The percentage is [STRING].
参数解释	$1：HTTP防攻击IPv4 ACL表项数目占单板IPv4 ACL资源总数目的百分比
日志等级	4
举例	%Mar 15 01:18:25:071 2020 H3C DIPOE/4/DIAG: -MDC=1-Slot=4; The number of anti-HTTP attack IPv4 ACLs exceeded 30 percent of the total number of IPv4 ACLs. The percentage is 31%.
日志说明	HTTP防攻击IPv4 ACL表项数目超过单板IPv4 ACL资源总数目的30%，占比31%
处理建议	通过**display ip subscriber http-defense attack ip** [**slot** *slotnum*] 查看HTTP攻击统计表项

65.7 IPOE_IPV4_REMAIN_ACL_BELOW_ERROR

日志内容	The number of remaining IPv4 ACLs dropped below 20 percent of the total number of IPv4 ACLs. The percentage is [STRING].
参数解释	$1：剩余IPv4 ACL表项数目占单板IPv4 ACL资源总数目的百分比
日志等级	4
举例	%Mar 15 00:06:06:766 2020 H3C DIPOE/4/DIAG: -MDC=1-Slot=4; The number of remaining IPv4 ACLs dropped below 20 percent of the total number of IPv4 ACLs. The percentage is 18%.
日志说明	剩余IPv4 ACL表项数目占单板IPv4 ACL资源总数目的百分比小于20%，剩余IPv4 ACL表项数目为18%
处理建议	排查哪些业务占用了大量的IPv4 ACL资源

65.8 IPOE_IPV6_HTTP_ATTACK_EXCEED_ERROR

日志内容	The number of anti-HTTP attack IPv6 ACLs exceeded 30 percent of the total number of IPv6 ACLs. The percentage is [STRING].
参数解释	$1：HTTP防攻击IPv6 ACL表项数目占单板IPv6 ACL资源总数目的百分比
日志等级	4
举例	%Mar 15 01:18:25:071 2020 H3C DIPOE/4/DIAG: -MDC=1-Slot=4; The number of anti-HTTP attack IPv6 ACLs exceeded 30 percent of the total number of IPv6 ACLs. The percentage is 31%.
日志说明	HTTP 防攻击IPv6 ACL表项数目超过单板IPv6 ACL资源总数目的30%，占比31%
处理建议	通过**display ip subscriber http-defense attack ip** [**slot** *slotnum*] 查看HTTP攻击统计表项

65.9 IPOE_IPV6_REMAIN_ACL_BELOW_ERROR

日志内容	The number of remaining IPv6 ACLs dropped below 20 percent of the total number of IPv6 ACLs. The percentage is [STRING].
参数解释	$1：剩余IPv6 ACL表项数目占单板IPv6 ACL资源总数目的百分比
日志等级	4
举例	%Mar 15 00:06:06:766 2020 H3C DIPOE/4/DIAG: -MDC=1-Slot=4; The number of remaining IPv6 ACLs dropped below 20 percent of the total number of IPv6 ACLs. The percentage is 18%.
日志说明	剩余IPv6 ACL表项数目占单板IPv6 ACL资源总数目的百分比小于20%，剩余IPv6 ACL表项数目为18%
处理建议	排查哪些业务占用了大量的IPv6 ACL资源

65.10 IPOE_REDIRECTRULE_ERROR

日志内容	Failed to [STRING] [STRING] redirect rules for the reason of [STRING] on [STRING].
参数解释	$1：操作类型，具体取值如下： ○ add：添加 ○ delete：删除 $2：重定向报文类型，具体取值如下： ○ HTTP：HTTP 报文 ○ HTTPS：HTTPS 报文 $3：失败原因，具体原因请见表65-1 $4：接口名称
日志等级	3
举例	IPOE/3/IPOE_REDIRECTRULE_ERROR: Failed to add HTTP redirect rules for the reason of not enough resources on Route-Aggregation1023.
日志说明	因资源不足、产品不支持或其它未知错误，导致在接口上添加或删除重定向规则失败
处理建议	具体处理建议请见表65-1

表65-2 失败原因列表

下发驱动失败原因	说明	处理建议
this operation is not supported	不支持	请确认接口是否支持IPoE功能
not enough resources	驱动资源不足	请联系技术支持
other unknown errors	其他未知错误	请联系技术支持

65.11 IPOE_SESSION_ERROR

日志内容	Failed to [STRING] [STRING] for the reason of [STRING] on [STRING].
参数解释	$1：操作类型，具体取值如下： ○ add IPOE session：添加 IPoE 会话 ○ delete IPOE session：删除 IPoE 会话 ○ modify IPOE session：修改 IPoE 会话 ○ reload IPOE session：重新下发 IPoE 会话 $2：IP地址 $3：失败原因，具体原因请见表65-1 $4：接口名称
日志等级	3
举例	IPOE/3/ IPOE_SESSION_ERROR: Failed to add IPOE session 1.1.1.2 for the reason of not enough resources on Route-Aggregation1023.
日志说明	因资源不足、产品不支持或其它未知错误，导致在接口上添加、删除或修改IPoE会话信息失败
处理建议	具体处理建议请见表65-1

65.12 IPOE_USER_LOGON_SUCCESS

日志内容	-Username=[STRING]-IPAddr=[IPADDR]-IfName=[STRING]-OuterVLAN=[STRING]-InnerVLAN=[STRING]-MACAddr=[MAC]; The user came online successfully.
参数解释	$1：用户名 $2：IP地址 $3：接口名称 $4：外层VLAN ID $5：内层VLAN ID $6：MAC地址
日志等级	6
举例	IPOE/6/IPOE_USER_LOGON_SUCCESS:-Username=abc-IPAddr=1.1.1.2-IfName=Route-Aggregation1023.4000-OuterVLAN=1000-InnerVLAN=4000-MACAddr=0230-0103-5601; The user came online successfully.
日志说明	用户上线成功
处理建议	无

65.13 IPOE_USER_LOGON_FAILED

日志内容	-Username=[STRING]-IPAddr=[IPADDR]-IfName=[STRING]-OuterVLAN=[STRING]-InnerVLAN=[STRING]-MACAddr=[MAC]-Reason=[STRING]; The user failed to come online.
参数解释	$1：用户名 $2：IP地址 $3：接口名称 $4：外层VLAN ID $5：内层VLAN ID $6：MAC地址 $7：上线失败原因，具体原因请见表65-3
日志等级	5
举例	IPOE/5/IPOE_USER_LOGON_FAILED:-Username=abc-IPAddr=1.1.1.2-IfName=Route-Aggregation1023.4000-OuterVLAN=1000-InnerVLAN=4000-MACAddr=0230-0103-5601-Reason=Authentication failed; The user failed to come online.
日志说明	用户上线失败
处理建议	具体处理建议请见表65-3

表65-3 上线失败原因列表

上线失败原因	说明	处理建议
Authentication failed	认证失败	• 检查设备与认证服务器之间的通信是否正常 • 检查用户名是否合法 • 检查密码是否正确 • 检查设备上的认证域是否正确
Authorization failed	授权失败	• 检查设备与授权服务器之间的通信是否正常 • 检查授权服务器下发的授权属性在设备上是否存在并配置正确 • 检查设备是否支持授权服务器下发的授权属性
No authentication ACK from AAA	RADIUS服务器不能回应认证请求	• 请检查设备与 RADIUS 服务器之间的通信是否正常 • 检查 RADIUS 服务器的状态是否正常
TACACS authentication reject	TACACS服务器回应认证拒绝	• 请检查用户名是否合法 • 检查密码是否正确
Authentication request to AAA failed	设备向认证服务器发送认证请求失败	• 检查设备与认证服务器之间的通信是否正常 • 检查认证服务器状态是否正常
RADIUS authentication reject	RADIUS服务器回应认证拒绝	• 请检查用户名是否合法 • 检查密码是否正确
AAA authorization information error	添加用户授权信息失败	• 检查授权服务器下发的授权属性在设备上是否存在并正确配置

上线失败原因	说明	处理建议
Local authentication failed: wrong password	用户密码错误导致本地认证被拒绝	• 请检查用户名是否合法 • 检查密码是否正确
No AAA response during authentication	设备在认证超时时间内未收到认证服务器的回应	• 检查设备与认证服务器之间的通信是否正常 • 检查认证服务器状态是否正常 • 检查设备与认证服务器之间的共享密钥是否相同
The local user does not exist	设备上未配置该本地用户	• 检查拨号用户是否为合法用户 • 如果是合法用户接入，但设备上不存在对应本地用户，则需要在本地添加该用户
Exxxxxx（例如：E2531）	RADIUS服务器返回错误码	检查RADIUS服务器是否正常

Maximum number of IPoE sessions already reached	IPoE上线用户已达到系统或接口允许上线的最大数目，新用户无法上线	• 对于动态个人接入用户，请检查当前接口是否存在以下配置：
		  ◦ **ip subscriber dhcp max-session**
		  ◦ **ip subscriber dhcpv6 max-session**
		  ◦ **ip subscriber unclassified-ip max-session**
		  ◦ **ip subscriber unclassified-ipv6 max-session**
		  ◦ **ip subscriber ndrs max-session**
		• 如存在上述配置，请检查已上线用户是否已达到接口允许创建的 IPoE 会话的最大数目
		• 上线总用户已达到规格允许上线的最大数目，请联系 H3C 技术支持

65.14 IPOE_USER_LOGOFF

日志内容	-Username=[STRING]-IPAddr=[IPADDR]-IfName=[STRING]-OuterVLAN=[STRING]-InnerVLAN=[STRING]-MACAddr=[MAC]-Reason=[STRING]; The user logged off.
参数解释	$1：用户名 $2：IP地址 $3：接口名称 $4：外层VLAN ID $5：内层VLAN ID $6：MAC地址 $7：下线原因，具体取值请见表65-4
日志等级	6
举例	IPOE/6/IPOE_USER_LOGOFF:-Username=abc-IPAddr=1.1.1.2-IfName=Route-Aggregation1023.4000-OutVLAN=1000-InnerVLAN=4000-MACAddr=0230-0103-5601-Reason=DHCP user request; The user logged off.
日志说明	用户正常下线
处理建议	具体处理建议请见表65-4

表65-4 正常下线原因列表

下线原因	说明	处理建议
DHCP user request	用户主动请求下线	请检查该用户是否已经下线
DHCP decline	用户地址冲突下线	DHCP配置变化引起用户下线
PORTAL notify	Portal模块通知下线	请检查该用户是否已经下线
RedisDBM clear	通过Redis数据库完成用户迁移后，执行Clear操作清除用户在原设备上的会话信息	请检查用户是否在新设备成功上线

65.15 IPOE_USER_LOGOFF_ABNORMAL

日志内容	-Username=[STRING]-IPAddr=[IPADDR]-IfName=[STRING]-OuterVLAN=[STRING]-InnerVLAN=[STRING]-MACAddr=[MAC]-Reason=[STRING]; The user logged off abnormally.
参数解释	$1：用户名 $2：IP地址 $3：接口名称 $4：外层VLAN ID $5：内层VLAN ID $6：MAC地址 $7：下线原因，具体取值请见表65-4
日志等级	6
举例	IPOE/6/IPOE_USER_LOGOFF_ABNORMAL:-Username=abc-IPAddr=1.1.1.2-IfName=Route-Aggregation1023.4000-OutVLAN=1000-InnerVLAN=4000-MACAddr=0230-0103-5601-Reason=Admin reset; The user logged off abnormally.
日志说明	用户异常下线
处理建议	具体处理建议请见表65-5

表65-5 异常下线原因列表

下线原因	说明	处理建议
Admin reset	接入端口DOWN、清除动态IPoE会话或者删除静态IPoE会话的配置	• 检查接入端口状态是否为 DOWN • 检查是否执行命令 **reset ip subscriber session** 清除了动态 IPoE 会话 • 检查是否执行命令 **undo ip subscriber session static** 删除了静态 IPoE 会话的配置 • 检查是否有新增静态用户配置 • 检查是否执行命令 **undo ip subscriber { l2-connected | routed } enable** 清除了 IPoE 会话
Session timeout	用户上线时间达到了规定值或者用户的流量达到了规定值	通知用户上线超时或者去续费
Session idle cut	用户在规定时间内的流量没有达到设定阈值	请检查该用户是否已经下线
Traffic quota limit reached	用户的流量达到了规定值	通知用户流量耗尽或则去续费
Realtime accounting request to AAA failed	遍历所有计费服务器后，没有收到任何一个计费服务器的回应	• 检查设备与计费服务器之间的通信是否正常 • 检查计费服务器状态是否正常
No AAA response during realtime accounting	在实时计费阶段，设备在限制等待时间内，没有收到计费更新报文回应	• 检查设备与计费服务器之间的通信是否正常 • 检查计费服务器状态是否正常

下线原因	说明	处理建议
No AAA response for accounting start	在开始计费阶段，设备在限制等待时间内，没有收到计费开始报文的回应	• 检查设备与计费服务器之间的通信是否正常 • 检查计费服务器状态是否正常
No AAA response for accounting stop	在停止计费阶段，设备在限制等待时间内，没有收到计费停止报文的回应	• 检查设备与计费服务器之间的通信是否正常 • 检查计费服务器状态是否正常
Accounting request to AAA failed	设备向计费服务器发送计费请求失败	• 检查设备与计费服务器之间的通信是否正常 • 检查计费服务器状态是否正常
Accounting update failure	计费更新失败	• 检查设备与计费服务器之间的通信是否正常 • 检查计费服务器状态是否正常
Accounting failed	计费失败	• 检查设备与计费服务器之间的通信是否正常 • 检查认证计费服务器状态是否正常
AAA access limit reached	一个帐号允许接入的用户数超过了限制	• 检查一个帐号上线用户数 • 通过**access-limit**命令将使用当前本地用户名接入设备的最大用户数调整为更大的值
DHCP lease timeout	DHCP租约过期	通知用户地址租约到期
DHCP notify	DHCP模块通知下线	请检查该用户是否已经下线
No response from DHCP server	未收到DHCP服务器应答引起用户下线	检查DHCP服务器配置
DHCP configuration change	DHCP配置变化引起用户下线	检查DHCP服务器配置
DHCP IP address allocation failure	DHCP服务器分配IP地址失败引起用户下线	检查DHCP地址池中地址是否已经耗尽
IP conflict on DHCP server	DHCP server IP地址冲突	检查DHCP服务器分配地址是否与当前设备接口IP地址冲突
IPoE-DHCP data synchronization failed	与DHCP模块间数据同步导致下线	请将相关日志信息保存到本地，并联系H3C技术支持
User online detection failure	用户在线探测失败下线	请检查该用户是否已经下线
AAA request	RADIUS server要求用户下线	无
Insufficient hardware resources	硬件资源不足	请将相关日志信息保存到本地，并联系H3C技术支持
Interface down	接入接口Down	检查用户接入接口网线连接是否正常
Interface shutdown	接入接口SHUTDOWN	检查用户接入接口是否配置了命令**shutdown**
Interface deactivation	接口去激活引起用户下线	检查是否有接口板子卡插拔
VSRP status change	VSRP设备状态变化引起用户下线	请检查该用户是否已经下线
Standby device data deleted:	与VSRP Master设备平滑	请检查该用户是否已经下线

下线原因	说明	处理建议
master-standby device synchronization inconsistency	数据引起用户下线	
Failed to obtain IPv6 prefix	获取IPv6地址前缀失败	检查是否通过AAA授权IPv6地址前缀
Failed to recover AAA resources	恢复用户AAA相关资源失败	请检查是否有接口板插拔和VSRP模式下主备设备切换
Reauthorization during COA	COA重新授权引起用户下线	无
The static session already exists	新上线用户与已有的静态会话冲突引起下线	请检查当前上线用户与已有静态用户是否冲突
The DHCP session is updated	新上线用户与已有的DHCP会话冲突，导致已存在的DHCP会话下线	请检查当前上线用户与已有DHCP用户是否冲突
Inter-card data is synchronized	同步的会话与本地已经存在的会话冲突引起本地会话用户下线	请将相关日志信息保存到本地，并联系H3C技术支持
User aged out before coming online	老化未成功上线的用户	• 检查设备与 DHCP 服务器之前的通信是否正常 • 检查 DHCP 服务器地址池中地址是否已耗尽
MPU-LPU data synchronization failure	主控板与接口板之间数据平滑处理异常	请将相关日志信息保存到本地，并联系H3C技术支持
NAK from the DHCP server or tenant duration is 0	收到DHCP NAK报文或续租时长为0导致用户下线	请检查该用户是否已经下线
NAT failed	与NAT联动失败	请检查支持NAT联动功能的单板是否故障
The ND RS session is updated	新上线用户与已有的RS会话冲突，导致已存在的ND RS会话下线	请检查当前上线用户与已有ND RS用户是否冲突
BRAS errors	设备内部软件处理异常造成的用户下线	4. 请依次执行如下命令收集用户上线过程的调试信息 ○ **terminal monitor** ○ **terminal debugging** ○ **debugging ip subscriber** 5. 将相关日志信息和调试信息保存到本地，并联系H3C 技术支持
RedisDBM conflict	新设备上的原有用户与从Redis数据库迁移过来的其它设备上的用户冲突引起原有的冲突用户下线	无。新设备从Redis数据库恢复用户会话信息的过程中，如检测到用户冲突，则先删除设备上原有的冲突用户，然后再从Redis数据库恢复该用户的会话信息
RedisDBM block	在原设备上执行Block操作引起的用户下线	执行Block操作时，会清除设备上所有未处于Online状态的用户的会话，并强制用户下线，故在执行Block操作前，请确保所有用户的会话均处于Online状态

65.16 USER_TRACEINFO

日志内容	[objectID=[UINT16]][slotID=[UINT16]][STRING][user info: [STRING]][trace info:[STRING]]
参数解释	$1：业务跟踪对象的编号 $2：接入用户所属的槽位号 $3：业务跟踪阶段，目前有IPoE和AAA两个阶段 $4：用户信息。各用户信息含义请参见表65-6 $5：跟踪详细信息。IPoE和AAA阶段的详细跟踪信息请分别参见表65-7和表65-8
日志等级	7
举例	USER/7/USER_TRACEINFO:[objectID=1][slotID=1][IPoE][user info: MAC address: 4072-82a1-0206 IP address: 1.3.3.3 Access interface: GigabitEthernet1/0/1 Username: user1 Access mode: IPoE] [trace info: AAA processed accounting-stop request and returned processing]
日志说明	编号为1业务跟踪对象在IPoE阶段，主会话发送计费停止事件，AAA返回processing
处理建议	无

表65-6 被跟踪用户信息描述表

字段	描述
MAC address	接入用户的MAC地址
Access interface	接入用户接入接口
Service VLAN	接入用户的外层VLAN ID
Customer VLAN	接入用户的内层VLAN ID
Username	接入用户的用户名
IP address	接入用户的IP地址
Access mode	业务跟踪对象的接入模式

表65-7 被跟踪详细信息描述表（IPoE）

字段	描述

IPoE session received an event:event, Phase:phase, State=state, UserID=userid	IPoE会话收到了event事件，各字段含义如下：
	• event：事件名称
	  ○ Create and go：创建 IPoE 会话
	  ○ Init：报文触发用户上线
	  ○ Auth：进行认证的条件已经满足
	  ○ AuthPass：认证通过

字段	描述
	○ AuthFail：认证失败 ○ AssignIP：地址分配成功 ○ Age：动态会话老化 ○ RuleOK：规则下发成功 ○ RuleFail：规则下发失败 ○ Offline：用户下线 ○ Quiet：静默定时器超时 ○ Destroy：删除会话 ○ Change of Authorization：AAA 授权属性变更 ○ UserProfile OK：User Profile 下发驱动成功 ○ UserProfile Fail：User Profile 下发驱动失败 ○ WebAuth：收到 Portal 发送的 Web 用户认证消息 ○ PreAuth：收到 Portal 发送的 Web 用户从 Web 认证阶段退回到认证前域认证阶段的消息 ○ ModeAuth to AssignedIP：IPoE 会话从认证前域认证阶段迁移到 Web 认证阶段时，会话状态从 AuthPass 直接迁到 AssignedIP ○ Other：除上述事件之外的其他事件 • Phase：当前会话阶段 ○ Bind：绑定认证阶段 ○ Web：Web 认证阶段 • State：会话状态 ○ Invalid：无效状态 ○ Init：初始化 ○ Offline：正在下线 ○ Auth：认证中 ○ AuthFail：认证失败 ○ AuthPass：认证成功 ○ AssignedIP：用户已具备 IP 地址 ○ AssigningNewIP：Web 认证阶段正在重新分配 IP 状态 ○ AssignedNewIP：Web 认证阶段重新分配到 IP 状态 ○ Online：用户在线 ○ Backup：备份状态，表示该用户是由对端备份到本端的的表项 ○ Unknown：未知状态 • UserID：用户 ID
AAA processed type request and returned result	AAA处理*type*类型请求并返回结果为*result* *type*包括以下取值： • authentication：认证 • authorization：授权

字段	描述
	• accounting-start：计费开始 • accounting-update：实时计费 • accounting-stop：计费停止 *result*包括以下取值： • success： 成功 • processing：处理中 • fail(Errcode = code) ：失败（错误码为 code）
Received AAA type response and returned result	接收AAA type类型回复并返回结果为result type包括以下取值： • authentication：认证 • authorization： 授权 • accounting-start： 计费开始 • accounting-update：实时计费 • accounting-stop： 计费停止 result包括以下取值： • success：成功 • processing ： 处理中 • fail(Errcode = code)：失败（错误码为 code）
AAA processed type request and returned result, the traffic level is level	AAA处理type类型请求并返回结果为result，流量级别为level，其中： type包括以下取值： • authentication：认证 • authorization：授权 • accounting-start：计费开始 • accounting-update：实时计费 • accounting-stop：计费停止 result包括以下取值： • success： 成功 • processing： 处理中 • fail(Errcode = code) ：失败（错误码为 code）
Received AAA type response and returned result, the traffic level is level	接收AAA *type*类型回复并返回结果为*result*，流量级别为*level*，其中： *type*包括以下取值： • authentication：认证 • authorization： 授权 • accounting-start： 计费开始 • accounting-update：实时计费 • accounting-stop： 计费停止 result包括以下取值： • success：成功

字段	描述
	• processing ：处理中 • fail(Errcode = code)：失败（错误码为 code）

AAA processed type request and returned result, the service policy name is name	AAA处理*type*类型请求并返回结果为*result*，EDSG业务策略名称为*name*，*其中：*
	• *type* 包括以下取值：
	  ○ authentication：认证
	  ○ authorization：授权
	  ○ accounting-start：计费开始
	  ○ accounting-update：实时计费
	  ○ accounting-stop：计费停止
	• *result* 包括以下取值：
	  ○ success：成功
	  ○ processing：处理中
	  ○ fail(Errcode = code)：失败（错误码为 code）

Received AAA type response and returned result, the service policy name is name	接收AAA *type*类型回复并返回结果为*result*，EDSG业务策略名称为*name*，其中： *type*包括以下取值： • authentication：认证 • authorization： 授权 • accounting-start： 计费开始 • accounting-update：实时计费 • accounting-stop：计费停止 *result*包括以下取值： • success：成功 • processing：处理中 • fail(Errcode = code)：失败（错误码为 code）
DHCP user request	用户主动请求下线
DHCP lease timeout	DHCP租约过期
Session timeout	用户上线时间达到了规定值或者用户的流量达到了规定值
Authentication failure	认证失败
Authorization failure	授权失败
Admin reset	接入端口DOWN、清除动态IPoE会话或者删除静态IPoE会话的配置，主要包括包括： • 执行命令 **reset ip subscriber session** 清除了动态 IPoE 会话 • 执行命令 **undo ip subscriber session static** 删除了静态 IPoE 会话的配置 • 执行命令 **undo ip subscriber { l2-connected | routed } enable** 清除了 IPoE 会话

字段	描述
Session idle cut	用户在规定时间内的流量没有达到设定阈值
User online detection failure	用户在线探测失败下线
AAA request	RADIUS server要求用户下线
Insufficient hardware resources	硬件资源不足
Interface down	因故障导致接口DOWN（例如：网线断开）
Interface shutdown	由于管理的需要，管理员在用户接入接口配置**shutdown**命令，中断用户的连接
Interface deactivation	接口去激活引起用户下线。例如：接口所在单板被拔出导致接口去激活
BRAS errors	设备内部软件处理异常造成的用户下线
Failed to obtain IPv6 prefix	获取IPv6地址前缀失败
Failed to recover AAA resources	恢复用户AAA相关资源失败
DHCP decline	用户地址冲突下线
No response from DHCP server	未收到DHCP服务器应答引起用户下线
DHCP configuration change	DHCP配置变化引起用户下线
DHCP IP address allocation failure	DHCP服务器分配IP地址失败引起用户下线
Accounting update failure	实时计费更新失败
Accounting failed	计费失败
Reauthorization during COA	COA重新授权引起用户下线
The static session already exists	新上线用户与已有的静态会话冲突引起下线
The DHCP session already exists	新上线用户与已有的DHCP会话冲突，导致已存在的DHCP会话下线
Inter-card data is synchronized	同步的会话与本地已经存在的会话冲突引起本地会话用户下线
User aged out before coming online	老化未成功上线的用户
MPU-LPU data synchronization failure	主控板与接口板之间数据平滑处理异常
NAK from the DHCP server or tenant duration is 0	收到DHCP NAK报文或续租时长为0导致用户下线
AAA access limit reached	一个帐号允许接入的用户数超过了限制
The local user does not exist	设备上未配置该本地用户
Local authentication failed: wrong password	用户密码错误导致本地认证被拒绝
No AAA response during authentication	用户在认证超时时间内未收到认证服务器的回应
RADIUS authentication reject	RADIUS服务器回应认证拒绝
AAA authorization information error	添加用户授权信息失败
Realtime accounting request to AAA failed	遍历所有计费服务器后，没有收到任何一个计费服务器

字段	描述
	的回应
No AAA response during realtime accounting	在实时计费阶段，设备在限制等待时间内，没有收到计费更新报文回应
No AAA response for accounting start	在开始计费阶段，设备在限制等待时间内，没有收到计费开始报文的回应
No AAA response for accounting stop	在停止计费阶段，设备在限制等待时间内，没有收到计费停止报文的回应
Authentication request to AAA failed	设备向认证服务器发送认证请求失败
Accounting request to AAA failed	设备向计费服务器发送计费请求失败
No authentication ACK from AAA	RADIUS服务器不能回应认证请求
TACACS authentication reject	TACACS服务器回应认证拒绝
Traffic quota limit reached	用户的流量达到了规定值
IP conflict on DHCP server	DHCP server IP地址冲突
DHCP notify	DHCP模块通知下线
IPoE-DHCP data synchronization failed	与DHCP模块间数据同步导致下线
NAT failed	与NAT联动失败
PORTAL notify	PORTAL通知下线但是没有获取到下线原因的时候，填充的默认值
The ND RS session already exists	与已有的ND RS会话冲突

表65-8 被跟踪详细信息描述表（AAA）

字段	描述
LocalAuth: Authentication request initiated	本地认证：认证请求初始化
LocalAuth: Authentication succeeded	本地认证：认证成功
LocalAuth: Authorization request initiated	本地认证：授权请求初始化
LocalAuth: Authorization succeeded	本地认证：授权成功
LocalAuth: Accounting start request initiated	本地认证：计费开始请求初始化
LocalAuth: Accounting start succeeded	本地认证：计费开始成功
LocalAuth: Accounting stop request initiated	本地认证：计费停止请求初始化
LocalAuth: Accounting stop succeeded	本地认证：计费停止成功
LocalAuth: Authentication failed/Wrong password	本地认证：密码错误导致认证失败
LocalAuth: Authorization failed/Wrong password	本地认证：密码错误导致授权失败
LocalAuth: Accounting start failed/Wrong password	本地认证：密码错误导致计费开始失败
LocalAuth: Accounting stop failed/Wrong password	本地认证：密码错误导致计费停止失败

字段	描述
LocalAuth: Authentication failed/User blocked	本地认证：用户状态为block导致认证失败
LocalAuth: Authorization failed/User blocked	本地认证：用户状态为block导致授权失败
LocalAuth: Accounting start failed/User blocked	本地认证：用户状态为block导致计费开始失败
LocalAuth: Accounting stop failed/User blocked	本地认证：用户状态为block导致计费停止失败
LocalAuth: Authentication failed/Service type mismatch	本地认证：用户接入类型不匹配，导致认证失败
LocalAuth: Authorization failed/Service type mismatch	本地认证：用户接入类型不匹配导致授权失败
LocalAuth: Accounting start failed/Service type mismatch	本地认证：用户接入类型不匹配导致计费开始失败
LocalAuth: Accounting stop failed/Service type mismatch	本地认证：用户接入类型不匹配导致计费停止失败
LocalAuth: Authentication failed/Binding attribute mismatch	本地认证：用户绑定属性与实际属性不符，导致认证失败
LocalAuth: Authorization failed/Binding attribute mismatch	本地认证：用户绑定属性与实际属性不符导致授权失败
LocalAuth: Accounting start failed/Binding attribute mismatch	本地认证：用户绑定属性与实际属性不符导致计费开始失败
LocalAuth: Accounting stop failed/Binding attribute mismatch	本地认证：用户绑定属性与实际属性不符导致计费停止失败
LocalAuth: Accounting start failed/Access limit reached	本地认证：用户接入数达到上限导致计费开始失败
LocalAuth: Authentication failed/User doesn’t exist	本地认证：用户不存在导致认证失败
LocalAuth: Authorization failed/User doesn’t exist	本地认证：用户不存在导致授权失败
LocalAuth: Accounting start failed/User doesn’t exist	本地认证：用户不存在导致计费开始失败
LocalAuth: Accounting stop failed/User doesn’t exist	本地认证：用户不存在导致计费停止失败
RADIUS: Authentication request initiated	RADIUS：认证请求初始化
RADIUS: Authentication succeeded	RADIUS：认证成功
RADIUS: Accounting start request initiated	RADIUS：计费开始请求初始化
RADIUS: Accounting start succeeded	RADIUS：计费开始成功
RADIUS: Accounting stop request initiated	RADIUS：计费停止请求初始化
RADIUS: Accounting stop succeeded	RADIUS：计费停止成功
RADIUS: Authentication failed/Server reject	RADIUS：因用户密码错误等原因RADIUS服务器返回拒绝
RADIUS: Authentication failed/System error	RADIUS：因指定的RADIUS方案不存在等原因的系统错误，导致认证失败
RADIUS: Accounting start failed/System error	RADIUS：因指定的RADIUS方案不存在等原因的系统错误导致计费开始失败

字段	描述
RADIUS: Accounting update failed/System error	RADIUS：因指定的RADIUS方案不存在等原因的系统错误导致计费更新失败
RADIUS: Accounting stop failed/System error	RADIUS：因指定的RADIUS方案不存在等原因的系统错误导致计费停止失败
RADIUS: Authentication failed/Response timeout	RADIUS：因请求回应超时导致认证失败
RADIUS: Accounting start failed/Response timeout	RADIUS：因请求回应超时导致计费开始失败
RADIUS: Accounting update failed/Response timeout	RADIUS：因请求回应超时导致计费更新失败
RADIUS: Accounting stop failed/Response timeout	RADIUS：因请求回应超时导致计费停止失败
RADIUS: Accounting update request initiated	RADIUS：计费更新请求初始化
RADIUS：Authentication failed/Server blocked	RADIUS：因指定RADIUS方案下配置的所有认证服务器均无回应导致认证失败
RADIUS: Accounting start failed/Server blocked	RADIUS：因指定RADIUS方案下配置的所有计费服务器均无回应导致计费开始失败
RADIUS: Accounting update failed/Server blocked	RADIUS：因指定RADIUS方案下配置的所有计费服务器均无回应导致计费更新失败
RADIUS: Accounting stop failed/Server blocked	RADIUS：因指定RADIUS方案下配置的所有计费服务器均无回应导致计费停止失败

66 IPSEC

本节介绍 IPsec 模块输出的日志信息。

66.1 IPSEC_FAILED_ADD_FLOW_TABLE

日志内容	Failed to add flow-table due to [STRING].
参数解释	$1：失败原因
日志等级	4
举例	IPSEC/4/IPSEC_FAILED_ADD_FLOW_TABLE: Failed to add flow-table due to no enough resource.
日志说明	添加流表失败，可能原因包括硬件资源不足等
处理建议	对于硬件资源不足情况，请联系技术支持

66.2 IPSEC_PACKET_DISCARDED

日志内容	IPsec packet discarded, Src IP:[STRING], Dst IP:[STRING], SPI:[UINT32], SN:[UINT32], Cause:[STRING].
参数解释	$1：报文的源IP地址 $2：报文的目的IP地址 $3：SPI（Security Parameter Index，安全参数索引） $4：报文的序列号 $5：报文丢弃的原因： • 抗重放检测失败，显示为：Anti-replay checking failed. • AH 认证失败，显示为：AH authentication failed. • ESP 认证失败，显示为：ESP authentication failed. • SA 无效，显示为：Invalid SA. • ESP 解密失败，显示为：ESP decryption failed. • 报文的源地址匹配不上 SA，显示为：Source address of packet does not match the SA. • 没有匹配的 ACL 规则，显示为：No ACL rule matched.
日志等级	6
举例	IPSEC/6/IPSEC_PACKET_DISCARDED: IPsec packet discarded, Src IP:1.1.1.2, Dest IP:1.1.1.4, SPI:1002, SN:0, Cause:ah authentication failed
日志说明	IPsec报文被丢弃
处理建议	无

66.3 IPSEC_SA_ESTABLISH

日志内容	Established IPsec SA. The SA’s source address is [STRING], destination address is [STRING], protocol is [STRING], and SPI is [UINT32].
参数解释	$1：IPsec SA的源IP地址 $2：IPsec SA的目的IP地址 $3：IPsec SA使用的安全协议 $4：IPsec SA的SPI
日志等级	6
举例	IPSEC/6/IPSEC_SA_ESTABLISH: Established IPsec SA. The SA’s source address is 1.1.1.1, destination address is 2.2.2.2, protocol is AH, and SPI is 2435.
日志说明	IPsec SA创建成功
处理建议	无

66.4 IPSEC_SA_ESTABLISH_FAIL

日志内容	Failed to establish IPsec SA for the reason of [STRING]. The SA's source address is [STRING], and its destination address is [STRING].
参数解释	$1：IPsec SA创建失败的原因： • 隧道创建失败，显示为：Tunnel establishment failure. • 配置不完整，显示为：Incomplete configuration. • 配置的安全提议无效，显示为：Unavailable transform set. $2：源IP地址 $3：目的IP地址
日志等级	6
举例	IPSEC/6/IPSEC_SA_ESTABLISH_FAIL: Failed to establish IPsec SA for the reason of creating tunnel failure. The SA's source address is 1.1.1.1, and its destination address is 2.2.2.2.
日志说明	IPsec SA创建失败。触发该日志的原因可能有：隧道创建失败、配置不完整、或者配置的安全提议无效
处理建议	检查本端和对端设备上的IPsec配置

66.5 IPSEC_SA_INITINATION

日志内容	Began to establish IPsec SA. The SA's source address is [STRING], and its destination address is [STRING].
参数解释	$1：IPsec SA的源IP地址 $2：IPsec SA的目的IP地址
日志等级	6
举例	IPSEC/6/IPSEC_SA_INITINATION: Began to establish IPsec SA. The SA's source address is 1.1.1.1, and its destination address is 2.2.2.2.
日志说明	开始创建IPsec SA
处理建议	无

66.6 IPSEC_SA_TERMINATE

日志内容	The IPsec SA was deleted for the reason of [STRING]. The SA's source address is [STRING], destination address is [STRING], protocol is [STRING], and SPI is [UINT32].
参数解释	$1：IPsec SA被删除的原因： • SA 空闲超时，显示为：SA idle timeout. • 执行了 reset 命令，显示为：**reset** command executed. $2：源IP地址 $3：目的IP地址 $4：使用的安全协议 $5：SPI
日志等级	6
举例	IPSEC/6/IPSEC_SA_TERMINATE: The IPsec SA was deleted for the reason of SA idle timeout. The SA's source address is 1.1.1.1, destination address is 2.2.2.2, protocol is ESP, and SPI is 34563.
日志说明	IPsec SA被删除。触发该日志的原因可能有：SA空闲超时或者执行了reset命令
处理建议	无

67 IPSG

本节介绍 IPSG（IP Source Guard）模块输出的日志信息。

67.1 IPSG_ADDENTRY_ERROR

日志内容	Failed to add an IP source guard binding (IP [STRING], MAC [STRING], and VLAN [STRING]) on interface [STRING]. [STRING].
参数解释	$1：IP地址（如果没有指定，则显示N/A） $2：MAC地址（如果没有指定，则显示为N/A） $3：VLAN ID（如果没有指定，则显示为N/A） $4：接口名（如果没有指定，则显示为N/A） $5：失败原因： • Feature not supported：特性不支持 • Not enough resources：资源不足 • Unknown error：未知错误
日志等级	6
举例	IPSG/6/IPSG_ADDENTRY_ERROR: Failed to add an IP source guard binding (IP 1.1.1.1, MAC 0001-0001-0001, and VLAN 1) on interface Vlan-interface1. Not enough resources.
日志说明	下发静态或动态IP Source Guard绑定表项失败，可能的原因有：特性不支持、资源不足或未知错误
处理建议	• 当提示硬件资源不足时，可清理设备内存以释放资源 • 当下发是静态 IP Source Guard 绑定表项时，可重新执行命令下发该表项 • 当下发静态或动态 IP Source Guard 绑定表项失败原因为未知错误时，请联系技术支持

67.2 IPSG_DELENTRY_ERROR

日志内容	Failed to delete an IP source guard binding (IP [STRING], MAC [STRING], and VLAN [STRING]) on interface [STRING]. [STRING].
参数解释	$1：IP地址（如果没有指定，则显示N/A） $2：MAC地址（如果没有指定，则显示为N/A） $3：VLAN ID（如果没有指定，则显示为N/A） $4：接口名（如果没有指定，则显示为N/A） $5：失败原因： • Feature not supported： 特性不支持 • Unknown error：未知错误
日志等级	6
举例	IPSG/6/IPSG_DELENTRY_ERROR: Failed to delete an IP source guard binding (IP 1.1.1.1, MAC 0001-0001-0001, and VLAN 1) on interface Vlan-interface1. Unknown error.
日志说明	删除全局静态IP Source Guard绑定表项失败，可能的原因有：特性不支持或者未知错误
处理建议	• 重新执行命令删除该表项 • 当删除全局静态 IP Source Guard 绑定表项失败原因为未知错误时，请联系技术支持

68 IRDP

本节介绍 IRDP 模块输出的日志信息。

68.1 IRDP_EXCEED_ADVADDR_LIMIT

日志内容	The number of advertisement addresses on interface［STRING］exceeded the limit 255.
参数解释	$1：接口名称
日志等级	6
举例	IRDP/6/IRDP_EXCEED_ADVADDR_LIMIT: The number of advertisement addresses on interface GigabitEthernet1/0/1 exceeded the limit 255.
日志说明	接口上待通告的地址数超过了上限值
处理建议	删除接口上不需要的地址

69 IRF

本节介绍 IRF（Intelligent Resilient Framework）模块输出的日志信息。

69.1 IRF

日志内容	Packet for IRF link detection timed out on interface [INT32].
参数解释	$1：IRF物理端口
日志等级	4
举例	PORT/4/IRF: -MDC=1-Chassis=1-Slot=0; Packet for IRF link detection timed out on interface Ten-GigabitEthernet1/0/2/1.
日志说明	当IRF链路上的设备对应的端口配置不正确或物理链路故障时，会产生IRF物理链路检测超时，导致该IRF物理端口关闭或协议状态处于down状态
处理建议	1. 请确保该端口所在 IRF 链路上所有设备端口的物理状态处于 up 2. 请确保该端口所在 IRF 链路上所有设备对应端口的生成树协议处于关闭状态 3. 请确保该该端口所在 IRF 物理链路两端的端口配置的 VLAN ID 相同，且中继设备的对应端口的配置需要满足以下条件： • 中继设备不能使用 Access 端口 • 使用 Trunk 时，请确保 IRF 报文的 VLAN ID 在端口允许通过的列表中，但是不能与 PVID 相同 • 使用 Hybrid 端口时，请确保发送 IRF 报文携带 VLAN Tag

69.2 IRF

日志内容	IRF link detection recovered on interface [INT32].
参数解释	$1：IRF物理端口
日志等级	4
举例	PORT/4/IRF: -MDC=1-Chassis=1-Slot=0; IRF link detection recovered on interface Ten-GigabitEthernet1/0/2/1.
日志说明	IRF链路已从故障中恢复
处理建议	无

69.3 IRF_LINK_BLOCK

日志内容	IRF port went blocked.
参数解释	无
日志等级	2
举例	IRF/2/IRF_LINK_BLOCK: IRF port went blocked.
日志说明	IRF端口链路状态变为blocked。处于该状态的IRF端口不能转发数据报文，只能收发IRF协议报文。例如，检测到成员编号冲突时，优先级低的设备上会打印该日志信息
处理建议	请确认组网中是否存在成员编号冲突的设备。如果存在，请将成员编号修改为不同的值

69.4 IRF_LINK_DOWN

日志内容	IRF port went down.
参数解释	无
日志等级	3
举例	IRF/3/IRF_LINK_DOWN: IRF port went down.
日志说明	IRF端口链路状态变为down
处理建议	请确认： • IRF 端口下是否绑定了物理接口 • 绑定的物理接口是否和对端正确连接

69.5 IRF_LINK_UP

日志内容	IRF port came up.
参数解释	无
日志等级	6
举例	IRF/6/IRF_LINK_UP: IRF port came up.
日志说明	IRF端口链路状态变为up
处理建议	无

69.6 IRF_MEMBERID_CONFLICT

日志内容	IRF member ID conflict occurred. The ID [UINT32] has been used for another device with CPU-Mac: [STRING].
参数解释	$1：设备的成员编号 $2：设备的CPU MAC
日志等级	4
举例	IRF/4/IRF_MEMBERID_CONFLICT:-slot = 5; IRF member ID conflict occurred, The ID 5 has been used for another device with CPU-Mac: 000c-29d7-c1ae.
日志说明	在同一广播域中发现跟自己成员编号相同的设备时，打印该日志，提示成员冲突
处理建议	根据提示信息，检查IRF中的成员编号，重新设置新加入设备的成员编号

69.7 IRF_MERGE

日志内容	IRF merge occurred.
参数解释	无
日志等级	4
举例	IRF/4/IRF_MERGE: IRF merge occurred.
日志说明	IRF发生合并时，打印该日志信息
处理建议	无

69.8 IRF_MERGE_NEED_REBOOT

日志内容	IRF merge occurred. This IRF system needs a reboot.
参数解释	无
日志等级	4
举例	IRF/4/IRF_MERGE_NEED_REBOOT: IRF merge occurred. This IRF system needs a reboot.
日志说明	IRF发生合并时，主设备优先级低的IRF需要重启，打印该日志
处理建议	重启主设备优先级低的IRF完成合并

69.9 IRF_MERGE_NOT_NEED_REBOOT

日志内容	IRF merge occurred. This IRF system does not need to reboot.
参数解释	无
日志等级	5
举例	IRF/5/IRF_MERGE_NOT_NEED_REBOOT: IRF merge occurred. This IRF system does not need to reboot.
日志说明	IRF发生合并时，主设备优先级高的IRF不需要重启，打印该日志
处理建议	无

70 ISIS

本节介绍 IS-IS 模块输出的日志信息。

70.1 ISIS_LSP_CONFLICT

日志内容	IS-IS [UINT16], [STRING] LSP, LSPID=[STRING], SeqNum=[HEX], system ID conflict might exist.
参数解释	$1：进程ID $2：IS类型，值为Level-1或Level-2 $3：LSP ID $4：LSP序列号
日志等级	4
举例	ISIS/4/ISIS_LSP_CONFLICT: -MDC=1; IS-IS 1, Level-1 LSP, LSPID=1111.1111.1111.00-00, SeqNum=0x000045bf, system ID conflict might exist.
日志说明	网络中可能存在System ID冲突
处理建议	检查产生该LSP的设备的System ID是否和其他设备的System ID冲突

70.2 ISIS_MEM_ALERT

日志内容	ISIS Process received system memory alert [STRING] event.
参数解释	$1：内存告警类型
日志等级	5
举例	ISIS/5/ISIS_MEM_ALERT: ISIS Process received system memory alert start event.
日志说明	IS-IS模块收到内存告警信息
处理建议	当超过各级内存门限时，检查系统内存占用情况，对占用内存较多的模块进行调整，尽量释放可用内存

70.3 ISIS_NBR_CHG

日志内容	IS-IS [UINT16], [STRING] adjacency [STRING] ([STRING]), state changed to [STRING], Reason: [STRING].
参数解释	$1：IS-IS进程ID $2：IS-IS邻居等级 $3：邻居ID $4：接口名称 $5：邻居状态 $6：邻居状态变化原因
日志等级	3
举例	ISIS/3/ISIS_NBR_CHG: IS-IS 1, Level-1 adjacency 0000.0000.0001 (GigabitEthernet1/0/1), state changed to DOWN, Reason: circuit data clean.
日志说明	邻居状态发生变化
处理建议	需要关注邻居状态变化原因。当邻居状态变为down时，检查IS-IS配置正确性和网络连通性

71 ISSU

本节介绍 ISSU 模块输出的日志信息。

71.1 ISSU_PROCESSWITCHOVER

日志内容	Switchover completed. The standby process became the active process.
参数解释	无
日志等级	5
举例	ISSU/5/ISSU_PROCESSWITCHOVER: Switchover completed. The standby process became the active process.
日志说明	用户执行**issu run switchover**进行主备倒换完成，备进程已升级为主进程
处理建议	无

71.2 ISSU_ROLLBACKCHECKNORMAL

日志内容	The rollback might not be able to restore the previous version for [STRING] because the status is not normal.
参数解释	$1：chassis编号+slot编号或slot编号
日志等级	4
举例	ISSU/4/ISSU_ROLLBACKCHECKNORMAL: The rollback might not be able to restore the previous version for chassis 1 slot 2 because the state is not normal.
日志说明	ISSU升级，ISSU状态处理Switching，用户执行**issu rollback**回滚或ISSU回滚定时器超时自动回滚，如果有升级过的板状态不为Normal，会输出该日志
处理建议	无

72 KHTTP

本节介绍 KHTTP 模块输出的日志信息。

72.1 KHTTP_BIND_PORT_ALLOCETED

日志内容	Failed to bind TCP connection [STRING]/[UINT32] to VPN instance [UINT32] because the port was already allocated.
参数解释	$1：绑定的IP地址 $2：绑定的端口号 $3：VPN实例的索引号
日志等级	3
举例	KHTTP/3/KHTTP_BIND_PORT_ALLOCETED: Failed to bind TCP connection 192.168.30.117/10000 to VPN instance 0 because the port was already allocated.
日志说明	由于绑定的端口号已被分配，该IP地址和端口号与VPN实例绑定失败
处理建议	通过**display tcp-proxy port-info**和**display ipv6 tcp-proxy port-info命令查看可用端口信息，**重新进行绑定

72.2 KHTTP_BIND_ADDRESS_INUSED

日志内容	Failed to bind TCP connection [STRING]/[UINT32] to VPN instance [UINT32] because the address was already used.
参数解释	$1：绑定的IP地址 $2：绑定的端口号 $3：VPN实例的索引号
日志等级	3
举例	KHTTP/3/KHTTP_BIND_ADDRESS_INUSED: Failed to bind TCP connection 192.168.30.117/10000 to VPN instance 0 because the address was already used.
日志说明	由于绑定的IP地址已被使用，且不可重用，该IP地址和端口号与VPN实例绑定失败
处理建议	通过**display tcp-proxy**命令检查绑定的IP地址的占用情况，并使用未被使用或可重用的IP地址重新进行绑定

73 L2MC

本节介绍二层组播模块输出的日志信息。

73.1 L2MC_INIT

日志内容	No enough resource!
参数解释	无
日志等级	3
举例	L2MC/3/L2MC_INIT_N: -MDC=1-Slot=4; No enough resource!
日志说明	硬件资源不足，无法完成当前操作。例如，当组播表项添加出接口时，出现硬件资源不足，出接口无法添加成功
处理建议	**1.** 在 Probe 视图下执行 display hardware internal l2mc slot global 命令查看当前单板上资源的使用情况 **2.** 联系技术支持

74 L2PT

本节介绍 L2PT 模块输出的日志信息。

74.1 L2PT_ADD_GROUPMEMBER_FAILED

日志内容	Failed to add [STRING] as a member to the VLAN tunnel group for [STRING].
参数解释	$1：接口名称 $2：协议类型
日志等级	4
举例	L2PT/4/L2PT_ADD_GROUPMEMBER_FAILED: Failed to add GigabitEthernet2/0/1 as a member to the VLAN tunnel group for STP.
日志说明	接口加入协议的VLAN Tunnel组播组失败
处理建议	无

74.2 L2PT_CREATE_TUNNELGROUP_FAILED

日志内容	Failed to create a VLAN tunnel group for [STRING].
参数解释	$1：协议类型
日志等级	4
举例	L2PT/4/L2PT_CREATE_TUNNELGROUP_FAILED: Failed to create a VLAN tunnel group for STP.
日志说明	创建协议的VLAN Tunnel组播组失败
处理建议	无

74.3 L2PT_ENABLE_DROP_FAILED

日志内容	Failed to enable [STRING] packet drop on [STRING].
参数解释	$1：协议类型 $2：接口名称
日志等级	4
举例	L2PT/4/L2PT_ENABLE_DROP_FAILED: Failed to enable STP packet drop on GigabitEthernet2/0/1.
日志说明	接口上使能L2PT Drop功能失败
处理建议	无

74.4 L2PT_SET_MULTIMAC_FAILED

日志内容	Failed to set a tunnel destination MAC address to [MAC].
参数解释	$1：MAC地址
日志等级	4
举例	L2PT/4/L2PT_SET_MULTIMAC_FAILED: Failed to set a tunnel destination MAC address to 010f-e200-0003.
日志说明	配置BPDU Tunnel报文的目的MAC地址失败
处理建议	无

75 L2TPV2

本节介绍 L2TPV2 模块输出的日志信息。

75.1 L2TPV2_TUNNEL_EXCEED_LIMIT

日志内容	Number of L2TP tunnels exceeded the limit.
参数解释	无
日志等级	4
举例	L2TPV2/4/L2TPV2_TUNNEL_EXCEED_LIMIT: Number of L2TP tunnels exceeded the limit.
日志说明	设备上建立的L2TP隧道数目已经达到最大值
处理建议	要想建立新的L2TP隧道，可以通过**reset l2tp tunnel**命令立即断开空闲的L2TP隧道，或等待Hello定时器超时后设备自动断开空闲的L2TP隧道

75.2 L2TPV2_SESSION_EXCEED_LIMIT

日志内容	Number of L2TP sessions exceeded the limit.
参数解释	无
日志等级	4
举例	L2TPV2/4/L2TPV2_SESSION_EXCEED_LIMIT: Number of L2TP sessions exceeded the limit.
日志说明	设备上建立的L2TP会话数目已经达到最大值
处理建议	无

75.3 L2TPV2_SESSIONS_LOWER_THRESHOLD

日志内容	The L2TP session number is below the lower warning threshold (LowerThreshold=[INT32]).
参数解释	$1：在线L2TP会话数目的下限告警阈值
日志等级	4
举例	L2TPV2/4/L2TPV2_SESSIONS_LOWER_THRESHOLD: The L2TP session number is below the lower warning threshold (LowerThreshold=20).
日志说明	在线L2TP会话数目已低于配置的下限告警阈值
处理建议	1. 确认 L2TP 用户是否非正常大量下线 2. 执行 **display l2tp session statistic** 命令查看 L2TP 会话的统计信息

75.4 L2TPV2_SESSIONS_RECOVER_NORMAL

日志内容	The L2TP session number has recovered to normal state.
参数解释	无
日志等级	4
举例	L2TPV2/4/L2TPV2_SESSIONS_RECOVER_NORMAL: The L2TP session number has recovered to normal state.
日志说明	在线L2TP会话数目重新恢复到设定的正常范围内
处理建议	无

75.5 L2TPV2_SESSIONS_UPPER_THRESHOLD

日志内容	The L2TP session number is above the upper warning threshold (UpperThreshold=[INT32]).
参数解释	$1：在线L2TP会话数目的上限告警阈值
日志等级	4
举例	L2TPV2/4/L2TPV2_SESSIONS_UPPER_THRESHOLD: The L2TP session number is above the upper warning threshold (UpperThreshold=80).
日志说明	在线L2TP会话数目已高于配置的上限告警阈值
处理建议	1. 确认是否存在大量非法 L2TP 用户上线 2. 执行 **display l2tp session statistic** 命令查看 L2TP 会话的统计信息

76 L2VPN

本节介绍 L2VPN 模块输出的日志信息。

76.1 L2VPN_BGPVC_CONFLICT_LOCAL

日志内容	Remote site ID [INT32] (From [STRING], route distinguisher [STRING]) conflicts with local site.
参数解释	$1：冲突的远端Site ID $2：引发冲突的远端Site的IP地址 $3：引发冲突的远端Site的Route Distinguisher
日志等级	4
举例	L2VPN/4/L2VPN_BGPVC_CONFLICT_LOCAL: Remote site ID 1 (From 1.1.1.1, route distinguisher 1:1) conflicts with local site.
日志说明	本端Site ID和另一个远端Site ID冲突。触发该日志的原因可能有： • 新接收到一个远端 Site ID 和本端 Site ID 相同 • 新配置本端 Site ID 和已接收到的一个远端 Site ID 相同
处理建议	更改远端或本端Site ID，或者修改配置使得远端Site不引入到本端Site所在实例

76.2 L2VPN_BGPVC_CONFLICT_REMOTE

日志内容	Remote site ID [INT32] (From [STRING], route distinguisher [STRING]) conflicts with another remote site.
参数解释	$1：冲突的远端Site ID $2：引发冲突的远端Site的IP地址 $3：引发冲突的远端Site的Route Distinguisher
日志等级	4
举例	L2VPN/4/L2VPN_BGPVC_CONFLICT_REMOTE: Remote site ID 1 (From 1.1.1.1, route distinguisher 1:1) conflicts with another remote site.
日志说明	两个远端的Site ID冲突。触发该日志的原因可能为：在已经接收一个远端Site的情况下，接收到另一个远端Site，两者的Site ID相同
处理建议	更改其中一个远端Site ID，或者修改配置使得两个远端不引入到同一个实例中

76.3 L2VPN_HARD_RESOURCE_NOENOUGH

日志内容	No enough hardware resource for L2VPN.
参数解释	无
日志等级	4
举例	L2VPN/4/L2VPN_HARD_RESOURCE_NOENOUGH: No enough hardware resource for L2VPN.
日志说明	L2VPN硬件资源不足
处理建议	请检查是否生成了当前业务不需要的VSI、PW或AC，是则删除对应配置

76.4 L2VPN_HARD_RESOURCE_RESTORE

日志内容	Hardware resources for L2VPN are restored.
参数解释	无
日志等级	2
举例	L2VPN/2/L2VPN_HARD_RESOURCE_RESTORE: Hardware resources for L2VPN are restored.
日志说明	L2VPN硬件资源恢复
处理建议	无

76.5 L2VPN_LABEL_DUPLICATE

日志内容	Incoming label [INT32] for a static PW in [STRING] [STRING] is duplicate.
参数解释	$1：入标签值 $2：L2VPN类型，交叉连接组或者VSI $3：交叉连接组或者VSI的名称
日志等级	4
举例	L2VPN/4/L2VPN_LABEL_DUPLICATE: Incoming label 1024 for a static PW in Xconnect-group aaa is duplicate.
日志说明	交叉连接组或者VSI的静态PW的入标签被静态LSP或者静态CRLSP占用。触发该日志的原因可能有： • 在 MPLS 已使能的情况下，配置了一条入标签被静态 LSP 或者静态 CRLSP 占用的静态 PW • 在入标签被静态 LSP 或静态 CRLSP 占用的静态 PW 存在的情况下，使能 MPLS
处理建议	删除该静态PW，重新配置一条静态PW，并指定新的入标签值

76.6 L2VPN_MACLIMIT_FALL_AC

日志内容	The number of MAC address entries on the AC fell below the upper limit. (VSI name=[STRING], link ID=[UINT32], max-mac-entries=[UINT32], current-mac-entries=[UINT32])
参数解释	$1：AC关联的VSI的名称 $2：AC的Link ID $3：AC的最大MAC地址学习数，取值为unlimited时，表示不对学习的最大MAC地址数进行限制 $4：AC当前学习到的MAC地址数
日志等级	4
举例	L2VPN/4/L2VPN_MACLIMIT_FALL_AC: -MDC=1-Slot=5; The number of MAC address entries on the AC fell below the upper limit. (VSI name=aaa, link ID=1, max-mac-entries=100, current-mac-entries=80)
日志说明	AC上学习到的MAC地址数量回落到上限值的90%以下
处理建议	无

76.7 L2VPN_MACLIMIT_FALL_PW

日志内容	The number of MAC address entries on the PW fell below the upper limit. (VSI name=[STRING], link ID=[UINT32], max-mac-entries=[UINT32], current-mac-entries=[UINT32])
参数解释	$1：PW所在的VSI的名称 $2：PW的Link ID $3：PW的最大MAC地址学习数，取值为unlimited时，表示不对学习的最大MAC地址数进行限制 $4：PW当前学习到的MAC地址数
日志等级	4
举例	L2VPN/4/L2VPN_MACLIMIT_FALL_PW: -MDC=1-Slot=5; The number of MAC address entries on the PW fell below the upper limit. (VSI name=aaa, link ID=100, max-mac-entries=50, current-mac-entries=30)
日志说明	PW上学习到的MAC地址数量回落到上限值的90%以下
处理建议	无

76.8 L2VPN_MACLIMIT_FALL_VSI

日志内容	The number of MAC address entries on the VSI fell below the upper limit. (VSI name=[STRING], max-mac-entries=[UINT32], current-mac-entries=[UINT32])
参数解释	$1：VSI的名称 $2：VSI的最大MAC地址学习数 $3：VSI当前学习到的MAC地址数，取值为unlimited时，表示不对学习的最大MAC地址数进行限制
日志等级	4
举例	L2VPN/4/L2VPN_MACLIMIT_FALL_VSI: -MDC=1-Slot=5; The number of MAC address entries on the VSI fell below the upper limit. (VSI name=aaa, max-mac-entries=200, current-mac-entries=150)
日志说明	VSI内学习到的MAC地址数量回落到上限值的90%以下
处理建议	无

76.9 L2VPN_MACLIMIT_MAX_AC

日志内容	The number of MAC address entries on the AC reached the upper limit. (VSI name=[STRING], link ID=[UINT32], max-mac-entries=[UINT32])
参数解释	$1：AC关联的VSI的名称 $2：AC的Link ID $3：AC的最大MAC地址学习数
日志等级	4
举例	L2VPN/4/L2VPN_MACLIMIT_MAX_AC: -MDC=1-Slot=5; The number of MAC address entries on the AC reached the upper limit. (VSI name=aaa, link ID=1, max-mac-entries=100)
日志说明	AC上学习到的MAC地址数量达到上限
处理建议	无

76.10 L2VPN_MACLIMIT_MAX_PW

日志内容	The number of MAC address entries on the PW reached the upper limit. (VSI name=[STRING], link ID=[UINT32], max-mac-entries=[UINT32])
参数解释	$1：PW所在的VSI的名称 $2：PW的Link ID $3：PW的最大MAC地址学习数
日志等级	4
举例	L2VPN/4/L2VPN_MACLIMIT_MAX_PW: -MDC=1-Slot=5; The number of MAC address entries on the PW reached the upper limit. (VSI name=aaa, link ID=100, max-mac-entries=50)
日志说明	PW上学习到的MAC地址数量达到上限
处理建议	无

76.11 L2VPN_MACLIMIT_MAX_VSI

日志内容	The number of MAC address entries on the VSI reached the upper limit. (VSI name=[STRING], max-mac-entries=[UINT32])
参数解释	$1：VSI的名称 $2：VSI的最大MAC地址学习数
日志等级	4
举例	L2VPN/4/L2VPN_MACLIMIT_MAX_VSI: -MDC=1-Slot=5; The number of MAC address entries on the VSI reached the upper limit. (VSI name=aaa, max-mac-entries=200)
日志说明	VSI内学习到的MAC地址数量达到上限
处理建议	无

77 L3

本节介绍 L3 模块输出的日志信息。

77.1 COMMON

日志内容	This board does not support the statistics l3-packet enable command on this interface.
参数解释	无
日志等级	2
举例	L3/2/L3_COMMON: -MDC=1-Slot=4; This board does not support the statistics l3-packet enable command on this interface.
日志说明	CSPC类单板（CSPC-GE16XP4L-E、CSPC-GE24L-E和CSPC-GP24GE8XP2L-E除外）、CMPE-1104单板路由口和路由子接口不支持IPV4和IPV6报文统计，在此类接口下使能该统计会打印该单板不支持统计
处理建议	无

77.2 COMMON

日志内容	This board does not support the statistics l3-packet enable command on this interface.
参数解释	无
日志等级	2
举例	L3/2/L3_COMMON: -MDC=1-Slot=4; This board does not support the statistics l3-packet enable command on this interface.
日志说明	CSPEX-1204单板路由口和路由子接口不支持IPV4和IPV6报文统计，在此类接口下使能该统计会打印该单板不支持统计
处理建议	无

77.3 COMMON

日志内容	This board does not support the statistics l3-packet enable command on this interface.
参数解释	无
日志等级	2
举例	L3/2/L3_COMMON: -MDC=1-Slot=4; This board does not support the statistics l3-packet enable command on this interface.
日志说明	对于聚合口或者聚合子接口，如果该聚合口或者聚合子接口的成员口内存在CSPC类单板（CSPC-GE16XP4L-E、CSPC-GE24L-E和CSPC-GP24GE8XP2L-E除外）、CMPE-1104单板和CSPEX-1204单板的接口，CSPC类单板（CSPC-GE16XP4L-E、CSPC-GE24L-E和CSPC-GP24GE8XP2L-E除外）、CMPE-1104单板和CSPEX-1204单板不支持子接口报文统计和IPV4和IPV6报文统计
处理建议	无

77.4 COMMON

日志内容	Operation failed on [string] because of insufficient resources.
参数解释	$1：根据接口索引获取的具体端口号
日志等级	2
举例	L3/2/L3_COMMON: -MDC=1-Slot=2; Operation failed on GigabitEthernet3/1/1.1 because of insufficient resources.
日志说明	使能IPV4和IPV6统计失败，入方向和出方向接口令牌桶资源不足
处理建议	查看出入方向接口统计类型令牌桶计数器资源是否已经占满

77.5 COMMON

日志内容	Operation failed on [string] because of insufficient resources.
参数解释	$1：接口索引
日志等级	2
举例	L3/2/L3_COMMON: -MDC=1-Slot=2; Operation failed on 9728 because of insufficient resources.
日志说明	使能IPV4和IPV6统计失败，入方向和出方向接口令牌桶资源不足
处理建议	查看出入方向接口统计类型令牌桶计数器资源是否已经占满

77.6 COMMON

日志内容	The operation is not supported because configuration conflicts on [string].
参数解释	$1：根据接口索引获取的具体端口号
日志等级	2
举例	L3/2/L3_COMMON: -MDC=1-Slot=2; The operation is not supported because configuration conflicts on GigabitEthernet3/1/1.1.
日志说明	使能IPV4和IPV6统计失败，存在配置冲突
处理建议	查看是否配置了IPOE L2VPN专线用户或VLAN AC口统计

77.7 COMMON

日志内容	The operation is not supported because configuration conflicts on [string].
参数解释	$1：接口索引
日志等级	2
举例	L3/2/L3_COMMON: -MDC=1-Slot=2; The operation is not supported because configuration conflicts on 9728.
日志说明	如果使能IPV4和IPV6统计失败，存在配置冲突
处理建议	查看是否配置了IPOE L2VPN专线用户或VLAN AC口统计

77.8 L3_ARP

日志内容	Not enough ARP index resource.
参数解释	无
日志等级	4
举例	L3/4/L3_ARP: -MDC=1; Not enough ARP index resource.
日志说明	ARP索引资源不足，设备不能学习新的ARP或ND
处理建议	联系技术支持

77.9 L3_ARP

日志内容	Not enough NextHop resource.
参数解释	无
日志等级	4
举例	L3/4/L3_ARP: -MDC=1-Slot=5; Not enough NextHop resource.
日志说明	下一跳表项资源不足，单板不能学习新的ARP/ND及非等价的路由，可能会有流量转发不通的问题
处理建议	联系技术支持

77.10 L3_PAD

日志内容	Not enough IPv4 prefix resource.
参数解释	无
日志等级	4
举例	L3/4/L3_PAD: -MDC=1-Slot=3; Not enough IPv4 prefix resource.
日志说明	IPv4前缀资源不足，单板不能学习新的IPv4路由
处理建议	联系技术支持

77.11 L3_PAD

日志内容	Not enough IPv6 prefix resource.
参数解释	无
日志等级	4
举例	L3/4/L3_PAD: -MDC=1-Slot=3; Not enough IPv6 prefix resource.
日志说明	IPv6前缀资源不足，单板不能学习新的IPv6路由
处理建议	联系技术支持

77.12 L3_PAD

日志内容	Arp Attack!!!
参数解释	无
日志等级	4
举例	L3/4/L3_PAD: -MDC=1-Slot=3; Arp Attack!!!
日志说明	设备受到ARP报文攻击，请联系技术支持处理
处理建议	联系技术支持

77.13 L3_PAD

日志内容	ICMP Attack!
参数解释	无
日志等级	4
举例	L3/4/L3_PAD: -MDC=1-Slot=3; ICMP Attack!
日志说明	设备受到ICMP报文攻击，请联系技术支持处理
处理建议	联系技术支持

77.14 L3_ARP

日志内容	The Board on slot [INT32] doesn't support the ARP safe guard function.
参数解释	$1：接口板所在槽号，提示该槽的单板不支持ARP双向分离功能
日志等级	4
举例	L3/4/L3_ARP: -MDC=1-Slot=5; The Board on slot 5 doesn't support the ARP safe guard function.
日志说明	仅CSPEX类单板（除CSPEX-1204之外）、CEPC类单板支持ARP双向分离功能。当三层以太网接口/三层聚合组的某个成员端口/VLAN接口所属VLAN的某个端口在这些类型之外的其他单板上时，该三层以太网口及子接口/三层聚合接口及子接口/VLAN接口不支持ARP双向分离功能
处理建议	使用支持ARP双向分离功能的单板的接口

77.15 L3_COMMON

日志内容	The Board on slot [INT32] doesn't support the ARP safe guard function.
参数解释	$1：接口板所在槽号，提示该槽的单板不支持ARP双向分离功能
日志等级	4
举例	L3/4/L3_COMMON: -MDC=1-Slot=5; The Board on slot 5 doesn't support the ARP safe guard function.
日志说明	仅CSPEX类单板（除CSPEX-1204之外）、CEPC类单板支持ARP双向分离功能。当三层以太网接口/三层聚合组的某个成员端口/VLAN接口所属VLAN的某个端口在这些类型之外的其他单板上时，该三层以太网口及子接口/三层聚合接口及子接口/VLAN接口不支持ARP双向分离功能
处理建议	使用支持ARP双向分离功能的单板的接口

77.16 L3_P2C

日志内容	The resources are insufficient.
参数解释	无
日志等级	4
举例	L3/4/L3_P2C: -MDC=1-Slot=4; The resources are insufficient.
日志说明	在VT口配置协议（例如：MLD协议）时，该协议会遍历下发到所有绑定该VT的物理接口上，因TCAM资源不足导致遍历到某物理接口时协议下发失败
处理建议	建议用户避免使用所配的协议的功能。如果需要使用所配的协议，建议通过关闭所绑定VT口下的无用协议，或减少某些无用接口与VT口的绑定的方式，释放出足够的TCAM资源，然后在VT口下先关闭下发失败的协议，再重新开启该协议

77.17 L3_P2C

日志内容	The resources are insufficient.
参数解释	无
日志等级	4
举例	L3/4/L3_P2C: -MDC=1-Slot=4; The resources are insufficient.
日志说明	在将某物理接口与一个VT口绑定时，系统会遍历下发该VT口下配置的所有协议到绑定该VT口的物理接口上，因TCAM资源不足导致某协议下发到物理接口失败
处理建议	建议用户避免使用协议下发失败的物理接口。如果需要使用协议下发失败的物理接口，建议通过关闭所绑定VT口下的无用协议，或减少某些无用接口与VT口的绑定的方式，释放出足够的TCAM资源，然后先在该物理接口下取消绑定VT口，再重新绑定VT口

77.18 L3_P2C

日志内容	The IPv4 ACL resource usage exceeds 80%.
参数解释	无
日志等级	4
举例	L3/4/L3_P2C: -MDC=1-Slot=4; The IPv4 ACL resource usage exceeds 80%.
日志说明	IPV4 ACL资源使用超过80%，此时不在下发DHCP Flood防攻击表项
处理建议	在系统视图下执行display qos-acl resource 命令查看当前单板上ACL资源的使用情况，释放部分IPV4 ACL资源

77.19 L3_P2C

日志内容	The IPv6 ACL resource usage exceeds 80%.
参数解释	无
日志等级	4
举例	L3/4/L3_P2C: -MDC=1-Slot=4; The IPv6 ACL resource usage exceeds 80%.
日志说明	IPV6 ACL资源使用超过80%，此时不在下发DHCPv6 Flood防攻击表项
处理建议	在系统视图下执行display qos-acl resource 命令查看当前单板上ACL资源的使用情况，释放部分IPV6 ACL资源

77.20 L3_MTU

日志内容	Insufficient system resources!
参数解释	无
日志等级	3
举例	L3/3/L3_MTU: -MDC=1-Slot=3; Insufficient system resources!
日志说明	MTU索引资源不足，将MTU设置为默认值
处理建议	联系技术支持

78 L3MC

本节介绍三层组播模块输出的日志信息。

78.1 L3MC_IPv4

日志内容	No enough resource!
参数解释	无
日志等级	3
举例	L3MC/3/L3MC_IPv4_N: -MDC=1-Slot=4; No enough resource!
日志说明	硬件资源不足，无法完成当前操作。例如，当添加组播转发表项时，出现硬件资源不足，无法配置硬件表项
处理建议	1. 在 Probe 视图下执行 display hardware internal l3mc slot global 命令查看当前单板上资源的使用情况 2. 联系技术支持

78.2 L3MC_IPv4

日志内容	Not enough ACL resource
参数解释	无
日志等级	4
举例	L3MC/4/L3MC_IPV4_N: -MDC=1-Slot=4; Not enough ACL resource
日志说明	使能基于接口的IGMP攻击抑制功能或基于源MAC地址的IGMP攻击抑制功能的设备，检测到IGMP攻击流，出现硬件资源不足ACL下发失败，导致IGMP防攻击无法生效
处理建议	**1.** 在系统视图下执行 display qos-acl resource slot 4 命令查看当前单板上 ACL 资源的使用情况 **2.** 收集当前 ACL 资源使用情况并联系 H3C 技术支持

78.3 L3MC_BRAS

日志内容	No enough resource!
参数解释	无
日志等级	3
举例	L3MC/3/L3MC_BRASE_N: -MDC=1; Slot=4; No enough resource!
日志说明	IPoE用户接入接口上开启IGMP攻击防范功能时，出现硬件资源不足ACL下发失败，导致IGMP防攻击无法生效
处理建议	**1.** 在系统视图下执行 display qos-acl resource slot 4 命令查看当前单板上 ACL 资源的使用情况 **2.** 收集当前 ACL 资源使用情况并联系 H3C 技术支持

78.4 L3MC_IPv6

日志内容	No enough resource!
参数解释	无
日志等级	3
举例	L3MC/3/L3MC_IPv6_N: -MDC=1-Slot=4; No enough resource!
日志说明	硬件资源不足，无法完成当前操作。例如，当添加组播转发表项时，出现硬件资源不足，无法配置硬件表项
处理建议	**1.** 在 Probe 视图下执行 display hardware internal l3mc slot global 命令查看当前单板上资源的使用情况 **2.** 联系技术支持

78.5 L3MC_IPv6

日志内容	Not enough ACL resource
参数解释	无
日志等级	4
举例	L3MC/4/L3MC_IPV6_N: -MDC=1-Slot=4; Not enough ACL resource
日志说明	使能基于接口的MLD攻击抑制或基于源MAC地址的MLD攻击抑制功能时，存在MLD攻击流，出现硬件资源不足ACL下发失败，导致MLD防攻击无法生效
处理建议	1. 在系统视图下执行 display qos-acl resource slot 4 命令查看当前单板上 ACL 资源的使用情况 2. 收集当前 ACL 资源使用情况并联系 H3C 技术支持

78.6 L3MC_MVPN

日志内容	MtunnelCreate No enough resource!
参数解释	无
日志等级	3
举例	L3MC/3/L3MC_MVPN_M: -MDC=1; MtunnelCreate No enough resource!
日志说明	组播VPN配置已达到产品规格限制，无法创建当前Mtunnel接口
处理建议	无

79 LAGG

本节介绍 LAGG 模块输出的日志信息。

79.1 LAGG_ACTIVE

日志内容	Member port [STRING] of aggregation group [STRING] changed to the active state.
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6
举例	LAGG/6/LAGG_ACTIVE: Member port GE1/0/1 of aggregation group BAGG1 changed to the active state.
日志说明	聚合组内某成员端口成为激活端口
处理建议	无

79.2 LAGG_INACTIVE_AICFG

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the member port and the aggregate interface have different attribute configurations.
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6
举例	LAGG/6/LAGG_INACTIVE_AICFG: Member port GE1/0/1 of aggregation group BAGG1 changed to the inactive state, because the member port and the aggregate interface have different attribute configurations.
日志说明	由于聚合组内某成员端口的属性类配置与聚合接口属性类配置不同，该成员端口成为去激活端口
处理建议	修改该成员端口的属性类配置，使其与聚合接口属性类配置一致

79.3 LAGG_INACTIVE_BFD

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the BFD session state of the port was down.
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6
举例	LAGG/6/LAGG_INACTIVE_BFD: Member port GE1/0/1 of aggregation group BAGG1 changed to the inactive state, because the BFD session state of the port is down.
日志说明	聚合成员端口上的BFD会话down时，该成员端口变为去激活状态
处理建议	排查链路故障、检查该非选中状态的成员端口的操作key和属性类配置是否与参考端口一致

79.4 LAGG_INACTIVE_CONFIGURATION

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the aggregation configuration of the port is incorrect.
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6
举例	LAGG/6/LAGG_INACTIVE_CONFIGURATION: Member port GE1/0/1 of aggregation group BAGG1 changed to the inactive state, because the aggregation configuration of the port is incorrect.
日志说明	由于聚合组内某成员端口配置限制，该成员端口变为去激活状态
处理建议	无

79.5 LAGG_INACTIVE_DUPLEX

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the duplex mode is different between the member port and the reference port.
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6
举例	LAGG/6/LAGG_INACTIVE_DUPLEX: Member port GE1/0/1 of aggregation group BAGG1 changed to the inactive state, because the duplex mode is different between the member port and the reference port.
日志说明	由于聚合组内某成员端口的双工模式与参考端口不一致，该成员端口变为去激活状态
处理建议	修改该端口双工模式，使其与参考端口一致

79.6 LAGG_INACTIVE_HARDWAREVALUE

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because of the port's hardware restirction.
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6
举例	LAGG/6/LAGG_INACTIVE_HARDWAREVALUE: Member port GE1/0/1 of aggregation group BAGG1 changed to the inactive state, because of the port's hardware restirction.
日志说明	聚合组内某成员端口因硬件限制与参考端口不一致，该成员端口变为去激活状态
处理建议	无

79.7 LAGG_INACTIVE_LINKQUALITY_LOW

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the member port has low link quality.
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6
举例	LAGG/6/LAGG_INACTIVE_LINKQUALITY_LOW: Member port FGE1/0/50 of aggregation group BAGG1 changed to the inactive state, because the member port has low link quality.
日志说明	聚合组内成员端口因为链路质量低，无法满足正常的业务转发需求，端口变为去激活状态
处理建议	检查网线是否老化，接口模块是否故障等

79.8 LAGG_INACTIVE_IRFSELECTMODE

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the port does not meet the Selected port requirements of the IRF member device it belongs to.
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6
举例	LAGG/6/LAGG_INACTIVE_IRFSELECTMODE: Member port GE1/0/1 of aggregation group BAGG1 changed to the inactive state, because the port does not meet the Selected port requirements of the IRF member device it belongs to.
日志说明	由于聚合组配置了**lacp irf-select**命令，IRF成员设备上动态聚合组选中端口的选择方式发生变化，IRF中该成员设备上的成员端口变为非选中状态
处理建议	无

79.9 LAGG_INACTIVE_LOWER_LIMIT

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the number of active ports is below the lower limit.
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6
举例	LAGG/6/LAGG_INACTIVE_LOWER_LIMIT: Member port GE1/0/1 of aggregation group BAGG1 changed to the inactive state, because the number of active ports is below the lower limit.
日志说明	因聚合组内激活端口数量未达到配置的最小激活端口数，聚合组内某成员端口变为去激活状态
处理建议	增加激活端口数量，使其达到最小激活端口数

79.10 LAGG_INACTIVE_PARTNER

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the aggregation configuration of its peer port is incorrect.
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6
举例	LAGG/6/LAGG_INACTIVE_PARTNER: Member port GE1/0/1 of aggregation group BAGG1 changed to the inactive state, because the aggregation configuration of its peer port is incorrect.
日志说明	动态聚合组内，由于对端端口聚合配置不正确变为去激活状态，本端端口变为去激活状态
处理建议	无

79.11 LAGG_INACTIVE_PHYSTATE

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the physical state of the port is down.
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6
举例	LAGG/6/LAGG_INACTIVE_PHYSTATE: Member port GE1/0/1 of aggregation group BAGG1 changed to the inactive state, because the physical state of the port is down.
日志说明	聚合组内某成员端口处于down状态，该成员端口变为去激活状态
处理建议	使该端口处于UP状态

79.12 LAGG_INACTIVE_RESOURCE_INSUFICIE

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because all aggregate resources are occupied.
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	3
举例	LAGG/3/LAGG_INACTIVE_RESOURCE_INSUFICIE: Member port GE1/0/1 of aggregation group BAGG1 changed to the inactive state, because all aggregate resources are occupied.
日志说明	聚合资源不足导致聚合组内成员端口变为去激活端口
处理建议	无

79.13 LAGG_INACTIVE_SPEED

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the speed configuration of the port is incorrect.
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6
举例	LAGG/6/LAGG_INACTIVE_SPEED: Member port GE1/0/1 of aggregation group BAGG1 changed to the inactive state, because the speed configuration of the port is incorrect.
日志说明	聚合组内某成员端口速率与参考端口不一致，该端口变为去激活状态
处理建议	修改该端口速率，使其与参考端口一致

79.14 LAGG_INACTIVE_UPPER_LIMIT

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the number of active ports has reached the upper limit.
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	3
举例	LAGG/3/LAGG_INACTIVE_UPPER_LIMIT: Member port GE1/0/1 of aggregation group BAGG1 changed to the inactive state, because the number of active ports has reached the upper limit.
日志说明	动态聚合组内激活端口数量已达到上限。后加入的成员端口成为激活端口，致使某成员端口变为去激活状态
处理建议	无

80 LB

本节介绍 LB（Load Balancing）模块输出的日志信息。

80.1 LB_SLB_LICENSE_INSTALLED

日志内容	The license for SLB has been installed. Server load balancing is available.
参数解释	无
日志等级	5
举例	LB/5/LB_SLB_LICENSE_INSTALLED: The license for SLB has been installed. Server load balancing is available.
日志说明	SLB License已安装，服务器负载均衡功能可用
处理建议	无需处理

80.2 LB_SLB_LICENSE_UNINSTALLED

日志内容	The license for SLB has been uninstalled. Server load balancing is not available.
参数解释	无
日志等级	5
举例	LB/5/LB_SLB_LICENSE_UNINSTALLED: The license for SLB has been uninstalled. Server load balancing is not available.
日志说明	SLB License已卸载，服务器负载均衡功能不可用
处理建议	安装SLB License

81 LDP

本节介绍 LDP 模块输出的日志信息。

81.1 LDP_SESSION_CHG

日志内容	Session ([STRING], [STRING]) is [STRING].
参数解释	$1：对等体的LDP ID。如果无法获得对等体的LDP ID，显示为0.0.0.0:0 $2：VPN实例名。如果该会话属于公网，显示为public instance $3：会话状态，up或者down。如果会话状态是down，则会在括号内显示会话失败的原因
日志等级	4
举例	LDP/4/LDP_SESSION_CHG: Session (22.22.22.2:0, public instance) is up. LDP/4/LDP_SESSION_CHG: Session (22.22.22.2:0, VPN instance: vpn1) is down (hello hold timer expired).
日志说明	会话状态改变了
处理建议	当会话状态是up时，无 当会话状态是down时，根据会话失败原因检查接口状态，链路状态和其他相关配置 会话失败原因包括： • interface not operational：接口不可用 • MPLS disabled on interface：接口已取消使能 MPLS • LDP disabled on interface：接口已取消使能 LDP • LDP auto-configure disabled on interface：接口已取消使能 LDP 自动配置功能 • VPN instance changed on interface：接口所属的 VPN 实例已更改 • LDP instance deleted：LDP 实例已删除 • targeted peer deleted：LDP 对等体已删除。其中，targeted peer 可以有 4 种方式产生：手动配置、L2VPN 自动注册、TE 隧道自动注册（LDP over TE 功能）、会话保护自动注册 • L2VPN disabled targeted peer：L2VPN 注销 targeted peer • TE tunnel disabled targeted peer：TE 隧道注销 targeted peer • session protection disabled targeted peer：会话保护注销 targeted peer • process deactivated：LDP 进程降级 • failed to receive the initialization message：未收到初始化信息 • graceful restart reconnect timer expired：平滑重启重连时间超时 • failed to recover adjacency by NSR：NSR 恢复邻接关系失败 • failed to upgrade session by NSR：NSR 升级会话失败 • closed the GR session：GR 会话关闭 • keepalive hold timer expired：keepalive 保持时间超时 • adjacency hold timer expired：邻接关系保持时间超时 • session reset：重启会话 • TCP connection down：TCP 连接断开 • received a fatal notification message ：收到致命的通知信息 • internal error：内部错误 • memory in critical state：内存达到 critical 状态 • transport address changed on interface：接口上的传输地址更改

81.2 LDP_SESSION_GR

日志内容	Session ([STRING], [STRING]): ([STRING]).
参数解释	$1：对等体的LDP ID。如果无法获得对等体的LDP ID，显示为0.0.0.0:0 $2：VPN实例名。如果该会话属于公网，显示为public instance $3：会话平滑重启的状态，取值包括： • Start reconnection：启动会话重连 • Reconnection failed：会话重连失败 • Start recovery：会话重连成功，进入标签通告恢复过程 • Recovery completed：会话恢复全过程完成
日志等级	5
举例	LDP/5/LDP_SESSION_GR: Session (22.22.22.2:0, VPN instance: vpn1): Start reconnection.
日志说明	当已协商支持对端设备LDP平滑重启的LDP会话down时，触发该日志。日志显示会话平滑重启过程的状态变化
处理建议	从LDP_SESSION_CHG 日志消息可以查看会话平滑重启的原因 当会话平滑重启状态显示为Reconnection failed时，根据会话失败原因检查接口状态，链路状态和其他相关配置，其他情况无需处理

81.3 LDP_SESSION_SP

日志内容	Session ([STRING], [STRING]): ([STRING]).
参数解释	$1：对等体的LDP ID。如果无法获得对等体的LDP ID，显示为0.0.0.0:0 $2：VPN实例名。如果该会话属于公网，显示为public instance $3：会话保护状态，取值包括： • Hold up the session：保持会话，等待 Link hello 邻接关系恢复 • Session recovered successfully：Link hello 邻接关系恢复成功 • Session recovery failed：Link hello 邻接关系恢复失败
日志等级	5
举例	LDP/5/LDP_SESSION_SP: Session (22.22.22.2:0, VPN instance: vpn1): Hold up the session.
日志说明	当会话的最后一个Link hello邻接关系丢失时，触发该日志。日志显示会话保护过程的状态变化
处理建议	检查接口状态和链路状态

82 LIF

本节介绍 LIF 模块输出的日志信息。

82.1 API

日志内容	This board does not support the statistics l3-packet enable command on the VLAN interface.
参数解释	无
日志等级	2
举例	LIF/2/API: -MDC=1-Slot=4; This board does not support the statistics l3-packet enable command on the VLAN interface.
日志说明	对于Vlan虚接口，如果该Vlan的成员口内存在CSPC类单板（CSPC-GE16XP4L-E、CSPC-GE24L-E和CSPC-GP24GE8XP2L-E除外）、CMPE-1104单板和CSPEX-1204单板的接口，CSPC类单板（CSPC-GE16XP4L-E、CSPC-GE24L-E和CSPC-GP24GE8XP2L-E除外）、CMPE-1104单板和CSPEX-1204单板不支持IPV4和IPV6报文统计
处理建议	无

82.2 API

日志内容	This board does not support the statistics l3-packet enable and traffic-statistic enable commands on the VLAN interface.
参数解释	无
日志等级	2
举例	LIF/2/API: -MDC=1-Slot=4; This board does not support the statistics l3-packet enable and traffic-statistic enable commands on the VLAN interface.
日志说明	对于Vlan虚接口，如果该Vlan的成员口内存在CSPC类单板（CSPC-GE16XP4L-E、CSPC-GE24L-E和CSPC-GP24GE8XP2L-E除外）、CMPE-1104单板和CSPEX-1204单板的接口，CSPC类单板（CSPC-GE16XP4L-E、CSPC-GE24L-E和CSPC-GP24GE8XP2L-E除外）、CMPE-1104单板和CSPEX-1204单板不支持子接口报文统计和IPV4和IPV6报文统计
处理建议	无

82.3 DATA

日志内容	Not enough OutlifID resource.
参数解释	无
日志等级	4
举例	LIF/4/DATA: -MDC=1-Slot=3; Not enough OutlifID resource.
日志说明	Outlif ID资源不足，单板不能学习新的ARP/ND和非主机的路由，可能会有流量转发不通的问题
处理建议	联系技术支持

82.4 EPOLL

日志内容	Not enough resources for [STRING].
参数解释	$1：接口名称
日志等级	6
举例	LIF/6/EPOLL: -MDC=1-Slot=5; Not enough resources for Route-Aggregation1.1.
日志说明	硬件资源不足，导致接口的QinQ终结功能（vlan-type dot1q vid second-dot1q命令）使能失败
处理建议	1. 通过 display current-configuration | include second-dot1q 命令查看当前 QinQ 终结配置，通过 undo vlan-type dot1q vid second-dot1q 命令删除暂不使用的配置来释放资源 2. 联系技术支持

82.5 IF

日志内容	Some member ports of [STRING] don't support the mac-address command.
参数解释	$1：三层聚合接口名称。如果名称获取失败，则不显示接口编号
日志等级	3
举例	LIF/3/IF: -MDC=1-Slot=3; Some member ports of Route-Aggregation100 don't support the mac-address command. LIF/3/IF: -MDC=1-Slot=3; Some member ports of Route-Aggregation don't support the mac-address command.
日志说明	由于三层聚合接口的成员端口属于某些不支持配置MAC地址的单板，导致该聚合接口不支持配置**mac-address**命令
处理建议	请确保聚合接口的成员端口属于CSPEX类单板（除CSPEX-1204之外）或CEPC类单板，再配置**mac-address**命令

82.6 IF

日志内容	Member port of Route-Aggregation doesn't support the mac-address command.
参数解释	• 无
日志等级	3
举例	LIF/3/IF: -MDC=1-Slot=3; Member port of Route-Aggregation doesn't support the mac-address command.
日志说明	已加入聚合组的三层以太网接口不能配置**mac-address**命令
处理建议	可以在三层聚合接口上配置**mac-address**命令

82.7 IF

日志内容	[STRING] has been configured with a MAC address and can't be assigned to [STRING].
参数解释	$1：接口名称。如果名称获取失败，显示为The interface $2：三层聚合接口名称。如果名称获取失败，则不显示接口编号
日志等级	3
举例	LIF/3/IF: -MDC=1-Slot=3; GigabitEthernet3/2/5 has been configured with a MAC address and can't be assigned to Route-Aggregation100. LIF/3/IF: -MDC=1-Slot=3; The interface has been configured with a MAC address and can't be assigned to Route-Aggregation.
日志说明	已配置**mac-address**命令的三层以太网接口不能加入聚合组
处理建议	三层以太网接口通过**undo mac-address**命令删除配置的MAC地址后，才能加入聚合组

82.8 IF

日志内容	[STRING] can't be assigned to [STRING] configured with a MAC address.
参数解释	$1：接口名称。如果名称获取失败，显示为The interface • $2：三层聚合接口名称。如果名称获取失败，则不显示接口编号
日志等级	3
举例	LIF/3/IF: -MDC=1-Slot=3; GigabitEthernet3/2/5 can't be assigned to Route-Aggregation100 configured with a MAC address. LIF/3/IF: -MDC=1-Slot=3; The interface can't be assigned to Route-Aggregation configured with a MAC address.
日志说明	三层聚合接口已配置**mac-address**命令的情况下，某些单板的接口不支持加入该聚合组
处理建议	三层聚合接口已配置**mac-address**命令的情况下，仅CSPEX类单板（除CSPEX-1204之外）或CEPC类单板的以太网接口可以加入该聚合组

82.9 IF

日志内容	This board doesn't support VE-L3VPN interfaces configured with the mac-address command.
参数解释	• 无
日志等级	3
举例	LIF/3/IF: -MDC=1-Slot=3; This board doesn't support VE-L3VPN interfaces configured with the mac-address command.
日志说明	该单板不支持配置**mac-address**命令的VE-L3VPN接口
处理建议	在VE-L3VPN接口上配置**mac-address**命令后，仅保证CSPEX类单板（除CSPEX-1204之外）或CEPC类单板使用该接口时功能正常，其他单板使用该接口时可能功能异常

82.10 IF

日志内容	Subinterface [STRING] only supports VLAN termination by commands starting with vlan-type dot1q vid [INT32].
参数解释	$1：子接口名称 $2：VLAN ID
日志等级	5
举例	LIF/5/IF: -MDC=1-Slot=1; Subinterface Ten-GigabitEthernet1/0/1.2048 only supports VLAN termination by commands starting with vlan-type dot1q vid 2048.
日志说明	指定的子接口仅支持终结第一层VLAN ID等于子接口编号的报文
处理建议	在指定的子接口上配置Dot1q终结或QinQ终结时，确保终结的第一层VLAN ID等于子接口编号

82.11 IF

日志内容	This board does not support traffic statistics on the VLAN interface.
参数解释	无
日志等级	2
举例	LIF/2/IF: -MDC=1-Slot=3; This board does not support traffic statistics on the VLAN interface.
日志说明	单板上的端口不支持其所属 VLAN 的 VLAN 接口的流量统计
处理建议	无

82.12 IF

日志内容	The second-tier VLAN IDs will not include 4094. The board in slot [UINT32] doesn't support VLAN 4094. 或 Operation failed: The board in slot [UINT32] doesn't support VLAN 4094.
参数解释	$1：单板所在的槽位号
日志等级	5
举例	LIF/5/IF: -MDC=1-Slot=3; The second-tier VLAN IDs will not include 4094. The board in slot 3 doesn't support VLAN 4094. 或 LIF/5/IF: -MDC=1-Slot=3; Operation failed: The board in slot 3 doesn't support VLAN 4094.
日志说明	CSPC 类单板（CSPC-GE16XP4L-E、CSPC-GE24L-E 和 CSPC-GP24GE8XP2L-E 除外）和 CMPE-1104 单板不支持子接口配置内层为 4094 的 VLAN
处理建议	无

82.13 IF

日志内容	[STRING] that doesn't support the mac-address command can't be assigned to [STRING] configured with this command. 或 The port that doesn't support the mac-address command can't be assigned to Route-Aggregation configured with this command.
参数解释	$1：接口名称 $2：聚合口名称
日志等级	3
举例	LIF/3/IF: -MDC=1-Slot=3; Ten-GigabitEthernet3/1/1 that doesn't support the mac-address command can't be assigned to Route-Aggregation 1 configured with this command. 或 LIF/3/IF: -MDC=1-Slot=3; The port that doesn't support the mac-address command can't be assigned to Route-Aggregation configured with this command.
日志说明	如果聚合口上配置了**mac-address**命令，则不支持CSPC类单板和CMPE-1104、CSPEX-1104-E、CSPEX-1204单板上的接口加入该聚合口
处理建议	无

82.14 IF

日志内容	Some member ports of [STRING] don't support the mac-address command. 或 Some member ports of Route-Aggregation don't support the mac-address command.
参数解释	$1：聚合口名称
日志等级	3
举例	LIF/3/IF: -MDC=1-Slot=3; Some member ports of Route-Aggregation 1 don't support the mac-address command. 或 LIF/3/IF: -MDC=1-Slot=3; Some member ports of Route-Aggregation don't support the mac-address command.
日志说明	CSPC类单板（CSPC-GE16XP4L-E、CSPC-GE24L-E和CSPC-GP24GE8XP2L-E除外）和CMPE-1104单板上的接口不支持配置**mac-address**命令
处理建议	无

82.15 QINQ

日志内容	Subinterface [STRING] only supports VLAN termination by commands starting with vlan-type dot1q vid [INT32].
参数解释	$1：子接口名称 $2：VLAN ID
日志等级	5
举例	LIF/5/QINQ: -MDC=1-Slot=1; Subinterface Ten-GigabitEthernet1/0/1.2048 only supports VLAN termination by commands starting with vlan-type dot1q vid 2048.
日志说明	指定的子接口仅支持终结第一层VLAN ID等于子接口编号的报文
处理建议	在指定的子接口上配置Dot1q终结或QinQ终结时，确保终结的第一层VLAN ID等于子接口编号

82.16 QINQ

日志内容	Subinterface [STRING] only supports VLAN termination by the vlan-type dot1q vid [INT32] command.
参数解释	$1：子接口名称 $2：VLAN ID
日志等级	5
举例	LIF/5/QINQ: -MDC=1; Subinterface VE-L3VPN1.1 only supports VLAN termination by the vlan-type dot1q vid 1 command.
日志说明	L3VE子接口仅支持Dot1q终结，且第一层VLAN ID必须等于子接口编号
处理建议	在指定的子接口上配置Dot1q终结时，确保终结的第一层VLAN ID等于子接口编号

82.17 QINQ

日志内容	Not enough resources for user-vlan QINQ termination on [STRING]. 或 Not enough resources for user-vlan QINQ termination on [INT32].
参数解释	$1：子接口名称 $2：接口索引
日志等级	4
举例	LIF/4/QINQ: -MDC=1-Slot=5; Not enough resources for user-vlan QINQ termination on Route-Aggregation1.1.
日志说明	硬件资源不足，导致接口的QinQ终结功能（**user-vlan dot1q vid second-dot1q**命令）使能失败
处理建议	**1.** 子接口下配置 user-vlan 终结时出现资源不足，通过 **display current-configuration | include second-dot1q** 命令查看当前 user-vlan QinQ 终结配置，通过 **undo user-vlan dot1q vid second-dot1q** 命令回退当前配置，然后删除暂不使用的配置来释放资源 **2.** 端口加入聚合时出现硬件资源不足，通过 **display link-aggregation verbose** 命令查看当前聚合口的配置，通过 **undo port link-aggregation group** 命令回退当前配置，然后将暂不使用的成员口退出聚合来释放资源。还可以通过步骤 1 的方式，查看并删除子接口下暂不使用的配置来释放资源 **3.** 联系技术支持

82.18 QINQ

日志内容	Not enough resources for QinQ termination.
参数解释	无
日志等级	2
举例	LIF/2/QINQ: -MDC=1-Slot=3; Not enough resources for QinQ termination.
日志说明	指定单板上用于用户VLAN QinQ终结的硬件资源不足 通常由上线的IPoE或PPPoE用户数量过多，或者QinQ终结所用的接口过于集中在某块单板导致
处理建议	1. 如果使用三层聚合子接口来进行用户 VLAN QinQ 终结，可通过减少单板加入相关聚合组的成员端口的数量，来减轻该单板的负载 2. 联系 H3C 技术支持

82.19 QINQ

日志内容	The user-vlan configuration conflicts with [STRING] configuration. To avoid conflicts, do not configure both features on interface [STRING].
参数解释	$1：配置名称，取值包括： • ip subscriber l2vpn-leased：IPoE L2VPN 专线用户配置 • ip subscriber routed enable：三层接入模式的 IPoE 配置 • portal：Portal 认证配置 $2：子接口名称
日志等级	4
举例	LIF/4/QINQ: -MDC=1-Slot=4; The user-vlan configuration conflicts with portal configuration. To avoid conflicts, do not configure both features on interface Route-Aggregation1.2.
日志说明	子接口上同时配置了用户VLAN终结特性和以下特性，存在配置冲突 • Portal 认证（**portal [ipv6] enable**） • IPoE L2VPN 专线用户（**ip subscriber l2vpn-leased**） • 三层接入模式的 IPoE 功能（**ip subscriber routed enable**）
处理建议	1. 子接口视图下使用 **display this** 命令查看是否同时存在用户 VLAN 终结配置和 IPoE L2VPN 专线用户配置（或三层接入模式的 IPoE 配置、Portal 认证配置），然后使用 **undo** 命令删除其中一类配置命令 2. 如果问题仍然存在，联系技术支持

83 LLDP

本节介绍 LLDP 模块输出的日志信息。

83.1 LLDP_CREATE_NEIGHBOR

日志内容	[STRING] agent neighbor created on port [STRING] (IfIndex [UINT32]), neighbor's chassis ID is [STRING], port ID is [STRING].
参数解释	$1：代理类型 $2：接口名称 $3：接口索引 $4：邻居的设备号 $5：邻居的端口号
日志等级	6
举例	LLDP/6/LLDP_CREATE_NEIGHBOR: Nearest bridge agent neighbor created on port GigabitEthernet1/0/1 (IfIndex 599), neighbor's chassis ID is 3822-d666-ba00, port ID is GigabitEthernet1/0/2.
日志说明	端口收到新邻居发来的LLDP报文
处理建议	无

83.2 LLDP_DELETE_NEIGHBOR

日志内容	[STRING] agent neighbor deleted on port [STRING] (IfIndex [UINT32]), neighbor's chassis ID is [STRING], port ID is [STRING].
参数解释	$1：代理类型 $2：接口名称 $3：接口索引 $4：邻居的设备号 $5：邻居的接口号
日志等级	6
举例	LLDP/6/LLDP_DELETE_NEIGHBOR: Nearest bridge agent neighbor deleted on port GigabitEthernet1/0/1 (IfIndex 599), neighbor's chassis ID is 3822-d666-ba00, port ID is GigabitEthernet1/0/2.
日志说明	当邻居被删除时，接口收到删除消息
处理建议	无

83.3 LLDP_LESS_THAN_NEIGHBOR_LIMIT

日志内容	The number of [STRING] agent neighbors maintained by port [STRING] (IfIndex [UINT32]) is less than [UINT32], and new neighbors can be added.
参数解释	$1：代理类型 $2：接口名称 $3：接口索引 $4：接口可以维护的最大邻居数
日志等级	6
举例	LLDP/6/LLDP_LESS_THAN_NEIGHBOR_LIMIT: The number of nearest bridge agent neighbors maintained by port GigabitEthernet1/0/1 (IfIndex 599) is less than 5, and new neighbors can be added.
日志说明	接口邻居数未达到最大值，还可以为接口增加新邻居
处理建议	无

83.4 LLDP_NEIGHBOR_AGE_OUT

日志内容	[STRING] agent neighbor aged out on port [STRING] (IfIndex [UINT32]), neighbor's chassis ID is [STRING], port ID is [STRING].
参数解释	$1：代理类型 $2：接口名称 $3：接口索引 $4：邻居的设备号 $5：邻居的接口号
日志等级	4
举例	LLDP/4/LLDP_NEIGHBOR_AGE_OUT: Nearest bridge agent neighbor aged out on port GigabitEthernet1/0/1 (IfIndex599), neighbor's chassis ID is 3822-d666-ba00, port ID is GigabitEthernet1/0/2.
日志说明	当接口在一段时间内没有收到邻居发来的LLDP报文时，打印本信息
处理建议	检查链路状态，或者检查对端LLDP的接收和发送状态

83.5 LLDP_PVID_INCONSISTENT

日志内容	PVID mismatch discovered on [STRING] (PVID [UINT32]), with [STRING] [STRING] (PVID [STRING]).
参数解释	$1：接口名称 $2：VLAN ID $3：系统名称 $4：接口名称 $5：VLAN ID
日志等级	5
举例	LLDP/5/LLDP_PVID_INCONSISTENT: MDC=1; PVID mismatch discovered on GigabitEthernet1/0/1 (PVID 1), with Ten-GigabitEthernet0/2/7 (PVID 500).
日志说明	当邻居的PVID信息与接口本地的PVID不同时，打印本信息
处理建议	修改邻居两端的PVID，使其一致

83.6 LLDP_REACH_NEIGHBOR_LIMIT

日志内容	The number of [STRING] agent neighbors maintained by the port [STRING] (IfIndex [UINT32]) has reached [UINT32], and no more neighbors can be added.
参数解释	$1：代理类型 $2：接口名称 $3：接口索引 $4：接口可以维护的最大邻居数
日志等级	3
举例	LLDP/3/LLDP_REACH_NEIGHBOR_LIMIT: The number of nearest bridge agent neighbors maintained by the port GigabitEthernet1/0/1 (IfIndex 599) has reached 5, and no more neighbors can be added.
日志说明	当邻居数达到最大值的接口收到LLDP报文时，打印本信息
处理建议	无

84 LOAD

本节介绍 LOAD 模块输出的日志信息。

84.1 BOARD_LOADING

日志内容	Board in chassis [INT32] slot [INT32] is loading software images.
参数解释	$1：chassis编号 $2：slot编号
日志等级	4
举例	LOAD/4/BOARD_LOADING: Board in chassis 1 slot 5 is loading software images.
日志说明	单板启动过程中，加载启动软件包
处理建议	无

84.2 LOAD_FAILED

日志内容	Board in chassis [INT32] slot [INT32] failed to load software images.
参数解释	$1：chassis编号 $2：slot编号
日志等级	3
举例	LOAD/3/LOAD_FAILED: Board in chassis 1 slot 5 failed to load software images.
日志说明	单板在启动过程中，加载启动软件包失败
处理建议	1. 使用 **display boot-loader** 命令查看单板使用的下次启动软件包 2. 使用 **dir** 命令查看启动软件包是否存在。如果不存在或者损坏，请重新获取启动软件包或者设置其它软件包作为该单板的下次启动软件包 3. 如果仍不能解决，请联系工程师

84.3 LOAD_FINISHED

日志内容	Board in chassis [INT32] slot [INT32] has finished loading software images.
参数解释	$1：chassis编号 $2：slot编号
日志等级	5
举例	LOAD/5/LOAD_FINISHED: Board in chassis 1 slot 5 has finished loading software images.
日志说明	单板完成文件加载
处理建议	无

85 LOCAL

本节介绍 LOCAL 模块输出的日志信息。

85.1 LOCAL_CMDDENY

日志内容	-Line=[STRING]-IPAddr=[STRING]-User=[STRING]; Permission denied for visiting user [STRING].
参数解释	$1：用户线名称（如果不涉及该参数，则显示为**） $2：操作者的IP地址（如果不涉及该参数，则显示为**） $3：操作者的用户名（如果不涉及该参数，则显示为**） $4：本地用户名
日志等级	5
举例	LOCAL/5/LOCAL_CMDDENY: -Line=vty0-IPAddr=111.8.10.111-User=opt; Permission denied for visiting user admin.
日志说明	因操作者访问权限不足，执行进入本地用户视图的命令失败
处理建议	无

日志内容	-Line=[STRING]-IPAddr=[STRING]-User=[STRING]; Permission denied for adding user [STRING].
参数解释	$1：用户线名称（如果不涉及该参数，则显示为**） $2：操作者的IP地址（如果不涉及该参数，则显示为**） $3：操作者的用户名（如果不涉及该参数，则显示为**） $4：本地用户名
日志等级	5
举例	LOCAL/5/LOCAL_CMDDENY: -Line=vty0-IPAddr=111.8.10.111-User=opt; Permission denied for adding user admin.
日志说明	因操作者访问权限不足，执行添加本地用户的命令失败
处理建议	无

日志内容	-Line=[STRING]-IPAddr=[STRING]-User=[STRING]; Permission denied for deleting user [STRING].
参数解释	$1：用户线名称（如果不涉及该参数，则显示为**） $2：操作者的IP地址（如果不涉及该参数，则显示为**） $3：操作者的用户名（如果不涉及该参数，则显示为**） $4：本地用户名
日志等级	5
举例	LOCAL/5/LOCAL_CMDDENY: -Line=vty0-IPAddr=111.8.10.111-User=opt; Permission denied for deleting user admin.
日志说明	因操作者访问权限不足，执行删除本地用户的命令失败
处理建议	无

日志内容	-Line=[STRING]-IPAddr=[STRING]-User=[STRING]; Permission denied for configuring user [STRING]'s [STRING].
参数解释	$1：用户线名称（如果不涉及该参数，则显示为**） $2：操作者的IP地址（如果不涉及该参数，则显示为**） $3：操作者的用户名（如果不涉及该参数，则显示为**） $4：本地用户名 $5：配置的用户属性项，包括以下取值： • password：密码 • state：用户状态 • service-type：服务类型 • authorization-attribute：授权属性 • bind-attribute：绑定属性 • group：用户组 • access-limit：最大用户数
日志等级	5
举例	LOCAL/5/LOCAL_CMDDENY: -Line=vty0-IPAddr=111.8.10.111-User=opt; Permission denied for configuring user admin's access-limit.
日志说明	因操作者访问权限不足，执行配置本地用户属性的命令失败
处理建议	无

日志内容	-Line=[STRING]-IPAddr=[STRING]-User=[STRING]; Permission denied for visiting group [STRING].
参数解释	$1：用户线名称（如果不涉及该参数，则显示为**） $2：操作者的IP地址（如果不涉及该参数，则显示为**） $3：操作者的用户名（如果不涉及该参数，则显示为**） $4：用户组名称
日志等级	5
举例	LOCAL/5/LOCAL_CMDDENY: -Line=vty0-IPAddr=111.8.10.111-User=opt; Permission denied for visiting group system.
日志说明	因操作者访问权限不足，执行进入用户组的命令失败
处理建议	无

日志内容	-Line=[STRING]-IPAddr=[STRING]-User=[STRING]; Permission denied for adding group [STRING].
参数解释	$1：用户线名称（如果不涉及该参数，则显示为**） $2：操作者的IP地址（如果不涉及该参数，则显示为**） $3：操作者的用户名（如果不涉及该参数，则显示为**） $4：用户组名称
日志等级	5
举例	LOCAL/5/LOCAL_CMDDENY: -Line=vty0-IPAddr=111.8.10.111-User=opt; Permission denied for adding group system.
日志说明	因操作者访问权限不足，执行添加用户组的命令失败
处理建议	无

日志内容	-Line=[STRING]-IPAddr=[STRING]-User=[STRING]; Permission denied for deleting group [STRING].
参数解释	$1：用户线名称（如果不涉及该参数，则显示为**） $2：操作者的IP地址（如果不涉及该参数，则显示为**） $3：操作者的用户名（如果不涉及该参数，则显示为**） $4：用户组名称
日志等级	5
举例	LOCAL/5/LOCAL_CMDDENY: -Line=vty0-IPAddr=111.8.10.111-User=opt; Permission denied for deleting group system.
日志说明	因操作者访问权限不足，执行删除用户组的命令失败
处理建议	无

86 LOGIN

本节介绍 LOGIN（登录管理）模块输出的日志信息。

86.1 LOGIN_AUTHENTICATION_FAILED

日志内容	Authentication failed for [STRING] from [STRING] because of [STRING].
参数解释	$1：用户名 $2：用户线名或IP地址 $3：失败原因： ○ no AAA response from any server during the authentication：AAA 服务器无响应 ○ invalid username or password or service type mismatch：用户名、密码错误或服务类型不匹配 ○ configuration error or other errors：配置错误或其它错误
日志等级	5
举例	LOGIN/5/LOGIN_AUTHENTICATION_FAILED: Authentication failed for Usera from console0 because of no AAA response from any server during the authentication.
日志说明	用户登录时认证失败
处理建议	请根据错误原因进行相应的处理

86.2 LOGIN_FAILED

日志内容	[STRING] failed to log in from [STRING].
参数解释	$1：用户名 $2：用户线名和IP地址
日志等级	5
举例	LOGIN/5/LOGIN_FAILED: TTY failed to log in from console0. LOGIN/5/LOGIN_FAILED: usera failed to log in from 192.168.11.22.
日志说明	用户登录失败
处理建议	无

86.3 LOGIN_INVALID_USERNAME_PWD

日志内容	Invalid username or password from [STRING].
参数解释	$1：用户线名和IP地址
日志等级	5
举例	LOGIN/5/LOGIN_INVALID_USERNAME_PWD: Invalid username or password from console0. LOGIN/5/LOGIN_INVALID_USERNAME_PWD: Invalid username or password from 192.168.11.22.
日志说明	用户输入无效的用户名或密码
处理建议	无

87 LPDT

本节介绍 LPDT 模块输出的日志信息。

87.1 LPDT_LOOPED

日志内容	A loop was detected on [STRING].
参数解释	$1：接口名
日志等级	4
举例	LPDT/4/LPDT_LOOPED: A loop was detected on Ethernet6/4/2.
日志说明	接口首次检测到有VLAN发生环路时，环路检测模块会生成该信息
处理建议	检查网络环路

87.2 LPDT_QINQ_LOOPED

日志内容	A loop was detected on [STRING] in SVLAN [UINT16] and CVLAN [UINT16].
参数解释	$1：接口名 $2：外层VLAN ID $3：内层VLAN ID
日志等级	4
举例	LPDT/4/LPDT_QINQ_LOOPED: A loop was detected on Ethernet6/4/1 in SVLAN 1 and CVLAN 1.
日志说明	接口检测到一个双层VLAN Tag的网络发生环路时，环路检测模块会生成该信息
处理建议	检查该双层VLAN Tag网络的环路

87.3 LPDT_QINQ_RECOVERED

日志内容	A loop was removed on [STRING] in SVLAN [UINT16] and CVLAN [UINT16].
参数解释	$1：接口名 $2：外层VLAN ID $3：内层VLAN ID
日志等级	5
举例	LPDT/5/LPDT_QINQ_RECOVERED: A loop was removed on Ethernet6/4/1 in SVLAN 1 and CVLAN 1.
日志说明	接口检测到一个双层VLAN Tag网络的环路消除时，环路检测模块会生成该信息
处理建议	无需处理

87.4 LPDT_RECOVERED

日志内容	All loops were removed on [STRING].
参数解释	$1：接口名
日志等级	5
举例	LPDT/5/LPDT_RECOVERED: All loops were removed on Ethernet6/4/1.
日志说明	接口检测到所有VLAN的环路都消除时，环路检测模块会生成该信息
处理建议	无需处理

87.5 LPDT_VLAN_LOOPED

日志内容	A loop was detected on [STRING] in VLAN [UINT16].
参数解释	$1：接口名 $2：VLAN ID
日志等级	4
举例	LPDT/4/LPDT_VLAN_LOOPED: A loop was detected on Ethernet6/4/1 in VLAN 1.
日志说明	接口检测到一个VLAN发生环路时，环路检测模块会生成该信息
处理建议	检查该VLAN的网络环路

87.6 LPDT_VLAN_RECOVERED

日志内容	A loop was removed on [STRING] in VLAN [UINT16].
参数解释	$1：接口名 $2：VLAN ID
日志等级	5
举例	LPDT/5/LPDT_VLAN_RECOVERED: A loop was removed on Ethernet6/4/1 in VLAN 1.
日志说明	接口检测到一个VLAN的环路消除时，环路检测模块会生成该信息
处理建议	无需处理

88 LS

本节包含本地服务器日志信息。

88.1 LS_ADD_USER_TO_GROUP

日志内容	Admin [STRING] added user [STRING] to group [STRING].
参数解释	$1：管理员名 $2：用户名 $3：用户组名
日志等级	4
举例	LS/4/LS_ADD_USER_TO_GROUP: Admin admin added user user1 to group group1.
日志说明	管理员添加一个用户到一个用户组
处理建议	无

88.2 LS_AUTHEN_FAILURE

日志内容	User [STRING] from [STRING] failed authentication. [STRING]
参数解释	$1：用户名 $2：IP地址 $3：失败原因 • 用户没有找到 • 密码认证失败 • 用户未上线 • 接入类型不匹配 • 绑定属性失败 • 用户在黑名单
日志等级	5
举例	LS/5/LS_AUTHEN_FAILURE: User cwf@system from 192.168.0.22 failed authentication. “User not found.”
日志说明	本地服务器拒绝了一个用户的认证请求
处理建议	无

88.3 LS_AUTHEN_SUCCESS

日志内容	User [STRING] from [STRING] was authenticated successfully.
参数解释	$1：用户名 $2：IP地址
日志等级	6
举例	LS/6/LS_AUTHEN_SUCCESS: User cwf@system from 192.168.0.22 was authenticated successfully.
日志说明	本地服务器接受了一个用户的认证请求
处理建议	无

88.4 LS_DEL_USER_FROM_GROUP

日志内容	Admin [STRING] delete user [STRING] from group [STRING].
参数解释	$1：管理员名 $2：用户名 $3：用户组名
日志等级	4
举例	LS/4/LS_DEL_USER_FROM_GROUP: Admin admin delete user user1 from group group1.
日志说明	管理员将用户从用户组里删除
处理建议	无

88.5 LS_DELETE_PASSWORD_FAIL

日志内容	Failed to delete the password for user [STRING].
参数解释	$1：用户名
日志等级	4
举例	LS/4/LS_DELETE_PASSWORD_FAIL: Failed to delete the password for user abcd.
日志说明	删除用户密码失败
处理建议	检查文件系统

88.6 LS_PWD_ADDBLACKLIST

日志内容	User [STRING] was added to the blacklist due to multiple login failures, [STRING].
参数解释	$1：用户名 $2：结果 • 但是可以做其他的尝试 • 被永久阻塞 • 被临时阻塞指定时间（单位：分钟）
日志等级	4
举例	LS/4/LS_PWD_ADDBLACKLIST: user1 was added to the blacklist due to multiple login failures, but could make other attempts.
日志说明	用户多次登录失败后被加入了黑名单
处理建议	检查用户的密码

88.7 LS_PWD_CHGPWD_FOR_AGEDOUT

日志内容	User [STRING] changed the password because it was expired.
参数解释	$1：用户名
日志等级	4
举例	LS/4/LS_PWD_CHGPWD_FOR_AGEDOUT: aaa changed the password because it was expired.
日志说明	用户由于密码已过期而修改了密码
处理建议	无

88.8 LS_PWD_CHGPWD_FOR_AGEOUT

日志内容	User [STRING] changed the password because it was about to expire.
参数解释	$1：用户名 $2：老化时间
日志等级	4
举例	LS/4/LS_PWD_CHGPWD_FOR_AGEOUT: aaa changed the password because it was about to expire.
日志说明	用户由于密码即将过期而修改了密码
处理建议	无

88.9 LS_PWD_CHGPWD_FOR_COMPOSITION

日志内容	User [STRING] changed the password because it had an invalid composition.
参数解释	$1：用户名
日志等级	4
举例	LS/4/LS_PWD_CHGPWD_FOR_COMPOSITION: aaa changed the password because it had an invalid composition.
日志说明	用户由于密码组合错误而修改了密码
处理建议	无

88.10 LS_PWD_CHGPWD_FOR_FIRSTLOGIN

日志内容	User [STRING] changed the password at the first login.
参数解释	$1：用户名
日志等级	4
举例	LS/4/LS_PWD_CHGPWD_FOR_FIRSTLOGIN: aaa changed the password at the first login.
日志说明	用户首次登录修改了密码
处理建议	无

88.11 LS_PWD_CHGPWD_FOR_LENGTH

日志内容	User [STRING] changed the password because it was too short.
参数解释	$1：用户名
日志等级	4
举例	LS/4/LS_PWD_CHGPWD_FOR_LENGTH: aaa changed the password because it was too short.
日志说明	用户因为密码太短而修改了密码
处理建议	无

88.12 LS_PWD_FAILED2WRITEPASS2FILE

日志内容	Failed to write the password records to file.
参数解释	无
日志等级	4
举例	LS/4/LS_PWD_FAILED2WRITEPASS2FILE: Failed to write the password records to file.
日志说明	把密码记录写到文件失败
处理建议	无

88.13 LS_PWD_MODIFY_FAIL

日志内容	Admin [STRING] from [STRING] could not modify the password for user [STRING], because [STRING].
参数解释	$1：管理员名 $2：IP地址 $3：用户名 $4：原因： • 密码不匹配 • 不能写密码历史 • 密码无法验证
日志等级	4
举例	LS/4/LS_PWD_MODIFY_FAIL: Admin admin from 1.1.1.1 could not modify the password for user user1, because passwords do not match.
日志说明	修改用户密码失败
处理建议	无

88.14 LS_PWD_MODIFY_SUCCESS

日志内容	Admin [STRING] from [STRING] modify the password for user [STRING] successfully.
参数解释	$1：管理员名 $2：IP地址 $3：用户名
日志等级	6
举例	LS/6/LS_PWD_MODIFY_SUCCESS: Admin admin from 1.1.1.1 modify the password for user abc successfully.
日志说明	管理员成功修改了用户密码
处理建议	无

88.15 LS_REAUTHEN_FAILURE

日志内容	User [STRING] from [STRING] failed reauthentication.
参数解释	$1：用户名 $2：IP地址
日志等级	5
举例	LS/5/LS_REAUTHEN_FAILURE: User abcd from 1.1.1.1 failed reauthentication.
日志说明	用户再次认证失败
处理建议	检查旧密码

88.16 LS_UPDATE_PASSWORD_FAIL

日志内容	Failed to update the password for user [STRING].
参数解释	$1：用户名
日志等级	4
举例	LS/4/LS_UPDATE_PASSWORD_FAIL: Failed to update the password for user abc.
日志说明	为用户更新密码失败
处理建议	检查文件系统

88.17 LS_USER_CANCEL

日志内容	User [STRING] from [STRING] cancelled inputting the password.
参数解释	$1：用户名 $2：IP地址
日志等级	5
举例	LS/5/LS_USER_CANCEL: User 1 from 1.1.1.1 cancelled inputting the password.
日志说明	用户取消输入密码或者没有在90秒内输入密码
处理建议	无

88.18 LS_USER_PASSWORD_EXPIRE

日志内容	User [STRING]'s login idle timer timed out.
参数解释	$1：用户名
日志等级	5
举例	LS/5/LS_USER_PASSWORD_EXPIRE: User 1's login idle timer timed out.
日志说明	用户登录空闲时间超时
处理建议	无

88.19 LS_USER_ROLE_CHANGE

日志内容	Admin [STRING] [STRING] the user role [STRING] for [STRING].
参数解释	$1：管理员名 $2：添加/删除 $3：用户角色 $4：用户名
日志等级	4
举例	LS/4/LS_USER_ROLE_CHANGE: Admin admin add user role network-admin for user abcd.
日志说明	管理员修改了用户的用户角色
处理建议	无

88.20 LOCALSVR_PROMPTED_CHANGE_PWD

日志内容	Please change the password of [STRING] [STRING], because [STRING].
参数解释	$1：密码类型 o device management user：设备管理用户 o user line：用户线 o user line class：用户线类 $2：用户名/用户线名 $3：提醒修改密码原因 o the current password is a weak-password：密码是弱密码 o the current password is the default password：密码是缺省密码 o it is the first login of the current user or the password had been reset：首次登录或者密码已被重置 o the password had expired：密码已经老化
日志等级	6
举例	LOCALSVR/6/LOCALSVR_PROMPTED_CHANGE_PWD: Please change the password of device management user hhh, because the current password is a weak password.
日志说明	如果用户使用不符合密码策略的密码登录设备，系统会在该用户登录后每隔24小时输出一条日志信息提醒该用户修改当前密码
处理建议	根据用户登录时采用的认证方式不同，处理建议如下： • 认证方式为 scheme 时，请修改用户的本地密码 • 认证方式为 password 时，请修改用户所在用户线/用户线类的认证密码

89 LSM

本节介绍 LSM 模块输出的日志信息。

89.1 LSM_SR_LABEL_CONFLICT

日志内容	Protocol [STRING] assigned label ([STRING]) for prefix ([STRING]), which already has label ([STRING]) assigned by protocol [STRING].
参数解释	$1：路由协议1 $2：标签值1 $3：前缀地址及掩码 $4：标签值2 $3：路由协议2
日志等级	4
举例	LSM/4/LSM_SR_LABEL_CONFLICT: Protocol ISIS assigned label (16000) to prefix (5.5.5.5/32), which already has label (17000) assigned by protocol OSPF.
日志说明	在同一SR节点上不同路由协议为同一前缀地址分配不同的标签
处理建议	• 不同路由协议为同一前缀地址分配相同标签 • 在 SR 节点上删除未被使用的路由协议进程，保证仅一个路由协议为前缀地址分配标签

89.2 LSM_SR_PREFIX_CONFLICT

日志内容	Label ([STRING]) for prefix ([STRING]) has been used by prefix ([STRING]).
参数解释	$1：标签值 $2：前缀地址1及掩码 $3：前缀地址2及掩码
日志等级	4
举例	LSM/4/LSM_SR_PREFIX_CONFLICT: The label(16700) for prefix(8.8.8.8/32) has been used by prefix(5.5.5.5/32).
日志说明	前缀地址标签分配冲突，同一个标签被分配给两个不同的前缀地址
处理建议	给新前缀地址分配不同标签

90 LSPV

本节介绍 LSP 验证模块输出的日志信息。

90.1 LSPV_PING_STATIS_INFO

日志内容	Ping statistics for [STRING]: [UINT32] packets transmitted, [UINT32] packets received, [DOUBLE]% packets loss, round-trip min/avg/max = [UINT32]/[UINT32]/[UINT32] ms.
参数解释	$1：FEC $2：发出的请求数 $3：收到的应答数 $4：未收到应答的次数占发送请求总数的比例 $5：最小往返延迟时间 $6：平均往返延迟时间 $7：最大往返延迟时间
日志等级	6
举例	LSPV/6/LSPV_PING_STATIS_INFO: Ping statistics for FEC 192.168.1.1/32: 5 packets transmitted, 5 packets received, 0.0% packets loss, round-trip min/avg/max = 1/2/5 ms.
日志说明	执行**ping mpls**命令，触发该日志。日志显示ping的统计信息
处理建议	如果没有收到应答报文，检测到LSP隧道或者PW的连通性

91 MAC

本节介绍 MAC 模块输出的日志消息。

91.1 MAC_TABLE_FULL_GLOBAL

日志内容	The number of MAC address entries exceeded the maximum number [UNIT32].
参数解释	$1：单板的MAC地址表项最大数量。对CSPC类单板和CMPE-1104单板，该值为65536；对其他单板，该值为1048576
日志等级	5
举例	MAC/5/MAC_TABLE_FULL_GLOBAL: -MDC=1-Chassis=1-Slot=3; The number of MAC address entries exceeded the maximum number 1048576.
日志说明	单板的MAC地址表项超过了允许的最大数量
处理建议	无

91.2 MAC_TABLE_FULL_GLOBAL

日志内容	The number of MAC address entries exceeded the maximum number [UINT32].
参数解释	$1：最大MAC地址数量
日志等级	4
举例	MAC/4/MAC_TABLE_FULL_GLOBAL: The number of MAC address entries exceeded the maximum number 1024.
日志说明	全局MAC地址表中的表项数量超过了允许的最大数量
处理建议	无

91.3 MAC_TABLE_FULL_PORT

日志内容	The number of MAC address entries exceeded the maximum number [UINT32] for interface [STRING].
参数解释	$1：最大MAC地址数量 $2：接口名称
日志等级	4
举例	MAC/4/MAC_TABLE_FULL_PORT: The number of MAC address entries exceeded the maximum number 1024 for interface GigabitEthernet2/0/32.
日志说明	接口对应的MAC地址表中的表项数量超过了允许的最大数量
处理建议	无

91.4 MAC_TABLE_FULL_VLAN

日志内容	The number of MAC address entries exceeded the maximum number [UINT32] in VLAN [UINT32].
参数解释	$1：最大MAC地址数量 $2：VLAN ID
日志等级	4
举例	MAC/4/MAC_TABLE_FULL_VLAN: The number of MAC address entries exceeded the maximum number 1024 in VLAN 2.
日志说明	VLAN对应的MAC地址表中的表项数量超过了允许的最大数量
处理建议	无

92 MACA

本节介绍 MAC 地址认证模块输出的日志信息。

92.1 MACA_ENABLE_NOT_EFFECTIVE

日志内容	MAC authentication is enabled but is not effective on interface [STRING].
参数解释	$1：接口名
日志等级	3
举例	MACA/3/MACA_ENABLE_NOT_EFFECTIVE: MAC authentication is enabled but is not effective on interface Ethernet3/1/2.
日志说明	MAC地址认证配置在接口上不生效，因为该接口不支持MAC地址认证
处理建议	关闭接口上的MAC地址认证

92.2 MACA_LOGIN_FAILURE

日志内容	-IfName=[STRING]-MACAddr=[STRING]-VLANID=[STRING]-Username=[STRING]-UsernameFormat=[STRING]; User failed MAC authentication.
参数解释	$1：接口名 $2：MAC地址 $3：VLAN ID $4：用户名 $5：用户名格式
日志等级	6
举例	MACA/6/MACA_LOGIN_FAILURE:-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9-VLANID=444-Username=00-10-84-00-22-b9-UsernameFormat=MAC address; User failed MAC authentication.
日志说明	用户MAC地址认证失败
处理建议	查看失败原因并修改相关配置

92.3 MACA_LOGIN_SUCC

日志内容	-IfName=[STRING]-MACAddr=[STRING]-VLANID=[STRING]-Username=[STRING]-UsernameFormat=[STRING]; User passed MAC authentication and came online.
参数解释	$1：接口名 $2：MAC地址 $3：VLAN ID $4：用户名 $5：用户名格式
日志等级	6
举例	MACA/6/MACA_LOGIN_SUCC:-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9-VLANID=444-Username=00-10-84-00-22-b9-UsernameFormat=MAC address; User passed MAC authentication and came online.
日志说明	MAC地址认证成功
处理建议	无

92.4 MACA_LOGOFF

日志内容	-IfName=[STRING]-MACAddr=[STRING]-VLANID=[STRING]-Username=[STRING]-UsernameFormat=[STRING]; MAC authentication user was logged off.
参数解释	$1：接口名 $2：MAC地址 $3：VLAN ID $4：用户名 $5：用户名格式
日志等级	6
举例	MACA/6/MACA_LOGOFF:-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9-VLANID=444-Username=00-10-84-00-22-b9-UsernameFormat=MAC address; MAC authentication user was logged off.
日志说明	MAC地址认证用户下线
处理建议	查看下线原因或进行后续操作

93 MACSEC

本节介绍 MAC Security 模块输出的日志信息。

93.1 MACSEC_MKA_KEEPALIVE_TIMEOUT

日志内容	The live peer with SCI [STRING] and CKN [STRING] aged out on interface [STRING].
参数解释	$1：SCI $2：CKN $3：接口名
日志等级	4
举例	MACSEC/4/MACSEC_MKA_KEEPALIVE_TIMEOUT: The live peer with SCI 00E00100000A0006 and CKN 80A0EA0CB03D aged out on interface GigabitEthernet1/0/1.
日志说明	本端参与者和对端参与者相互学习到后，本端参与者为对端参与者启动一个保活定时器。如果本端参与者在保活定时器超时的时间内没有收到对端参与者的MKA报文，则将对端参与者的信息从本端删除掉，并触发该日志
处理建议	检查本端参与者和对端参与者所在链路是否故障，如果链路故障，则请恢复链路

93.2 MACSEC_MKA_PRINCIPAL_ACTOR

日志内容	The actor with CKN [STRING] became principal actor on interface [STRING].
参数解释	$1：CKN $2：接口名
日志等级	6
举例	MACSEC/6/MACSEC_MKA_PRINCIPAL_ACTOR: The actor with CKN 80A0EA0CB03D became principal actor on interface GigabitEthernet1/0/1.
日志说明	接口上可能存在多个行动者，具有最高优先级的Key Server的行动者被选举为主要行动者，触发该日志
处理建议	无

93.3 MACSEC_MKA_SAK_REFRESH

日志内容	The SAK has been refreshed on interface [STRING].
参数解释	$1：接口名
日志等级	6
举例	MACSEC/6/MACSEC_MKA_SAK_REFRESH: The SAK has been refreshed on interface GigabitEthernet1/0/1.
日志说明	接口上的参与者派生出或接收到新的SAK时，触发该日志
处理建议	无

93.4 MACSEC_MKA_SESSION_REAUTH

日志内容	The MKA session with CKN [STRING] was re-authenticated on interface [STRING].
参数解释	$1：CKN $2：接口名
日志等级	6
举例	MACSEC/6/MACSEC_MKA_SESSION_REAUTH: The MKA session with CKN 80A0EA0CB03D was re-authenticated on interface GigabitEthernet1/0/1.
日志说明	接口进行802.1X重认证时，触发该日志。重认证过程中，参与者接收到新的CAK，并使用它重建会话
处理建议	无

93.5 MACSEC_MKA_SESSION_SECURED

日志内容	The MKA session with CKN [STRING] was secured on interface [STRING].
参数解释	$1：CKN $2：接口名
日志等级	6
举例	MACSEC/6/MACSEC_MKA_SESSION_SECURED: The MKA session with CKN 80A020EA0CB03D was secured on interface GigabitEthernet1/0/1.
日志说明	接口上的MKA会话采用密文通信方式。触发该日志的原因可能包括： • MKA 会话由明文通信切换为密文通信 • Key Server 和它对端的接口都支持 MACsec 功能，且两端至少有一个期望 MACsec 保护的情况下，两端协商出新的会话
处理建议	无

93.6 MACSEC_MKA_SESSION_START

日志内容	The MKA session with CKN [STRING] started on interface [STRING].
参数解释	$1：CKN $2：接口名
日志等级	6
举例	MACSEC/6/MACSEC_MKA_SESSION_START: The MKA session with CKN 80A020EA0CB03D started on interface GigabitEthernet1/0/1.
日志说明	MKA会话协商开始。触发该日志的原因可能包括： • 使能 MKA 功能后，有新的可用 CAK • 用户重建 MKA 会话 • 协商会话失败的接口收到新的 MKA 报文
处理建议	无

93.7 MACSEC_MKA_SESSION_STOP

日志内容	The MKA session with CKN [STRING] stopped on interface [STRING].
参数解释	$1：CKN $2：接口名
日志等级	5
举例	MACSEC/5/MACSEC_MKA_SESSION_STOP: The MKA session with CKN 80A020EA0CB03D stopped on interface GigabitEthernet1/0/1.
日志说明	MKA会话终止。触发该日志的原因可能包括： • 用户删除或重建了接口的 MKA 会话 • MKA 会话所在链路故障
处理建议	使用**display mka session**命令查看会话是否存在。如果会话不存在且不是用户删除的，则需要检查会话所在链路是否故障。如果链路故障，则请恢复链路

93.8 MACSEC_MKA_SESSION_UNSECURED

日志内容	The MKA session with CKN [STRING] was not secured on interface [STRING].
参数解释	$1：CKN $2：接口名
日志等级	5
举例	MACSEC/5/MACSEC_MKA_SESSION_UNSECURED: The MKA session with CKN 80A020EA0CB03D was not secured on interface GigabitEthernet1/0/1.
日志说明	接口上的MKA会话采用明文通信方式。输出该日志的触发条件可能包括： • MKA 会话由密文通信切换为明文通信 • Key Server 和它对端的接口未能都支持 MACsec 功能，或两端均未期望 MACsec 保护的情况下，两端协商出新的会话
处理建议	如果用户希望会话采用密文通信方式，则请先确认Key Server和它对端的接口都支持MACsec功能，再确认两个接口中至少有一个期望MACsec保护，只有两个条件都成立，会话才能采用密文通信方式

94 MBFD

本节介绍 MPLS BFD 模块输出的日志信息。

94.1 MBFD_TRACEROUTE_FAILURE

日志内容	[STRING] is failed. ([STRING].)
参数解释	$1：LSP信息 $2：LSP失败原因
日志等级	4
举例	MBFD/4/MBFD_TRACEROUTE_FAILURE: LSP (LDP IPv4: 22.22.2.2/32, nexthop: 20.20.20.2) is failed. (Replying router has no mapping for the FEC.) MBFD/4/MBFD_TRACEROUTE_FAILURE: TE tunnel (RSVP IPv4: Tunnel1) is failed. (No label entry.)
日志说明	通过周期性Traceroute功能检测LSP或MPLS TE隧道时，如果收到带有不合法返回代码的应答，则打印本日志信息，说明LSP或者MPLS TE隧道出现了故障
处理建议	检查LSP或者MPLS TE隧道的配置情况

95 MBUF

本节介绍 MBUF 模块输出的日志信息。

95.1 MBUF_DATA_BLOCK_CREATE_FAIL

日志内容	Failed to create an MBUF data block because of insufficient memory. Failure count: [UINT32].
参数解释	$1：失败次数
日志等级	2
举例	MBUF/2/MBUF_DATA_BLOCK_CREATE_FAIL: Failed to create an MBUF data block because of insufficient memory. Failure count: 128.
日志说明	当申请MBUF数据块失败时，输出该日志。为避免该日志输出过于频繁，本次申请MBUF数据块失败距上次申请MBUF数据块失败间隔大于等于一分钟时，才会输出该日志
处理建议	1. 在 Probe 视图下执行 **display system internal kernel memory pool | include mbuf** 命令查询已申请的 MBUF 数据块的数量 2. 在系统视图下执行 **display memory** 命令查询系统内存总量 3. 将“已申请的 MBUF 数据块的数量”和“系统内存总量”比较，判断是否已申请的 MBUF 数据块过多导致申请失败 • 如果不是，则通过其他内存管理命令查询出占用内存较多的模块 • 如果是，则继续通过 Probe 视图下的 **display system internal mbuf socket statistics** 命令查询 Socket 申请的 MBUF 数据块的数量，对比已申请的 MBUF 数据块的数量，判断是否某个进程缓存在 Socket 缓冲区中的 MBUF 数据块过多 ○ 如果是，则进一步分析进程不能及时释放 Socket 缓冲区中的 MBUF 数据块的原因 ○ 如果不是，则需要通过其他手段找出申请大量 MBUF 数据块的真正原因

96 MDC

本节介绍 MDC（Multitenant Device Context，多租户设备环境）模块输出的日志信息。

96.1 MDC_CREATE

日志内容	MDC [UINT16] was created.
参数解释	$1：MDC的编号
日志等级	5
举例	MDC/5/MDC_CREATE: MDC 2 was created.
日志说明	MDC成功创建
处理建议	无

96.2 MDC_CREATE_ERR

日志内容	Failed to create MDC [UINT16] for insufficient resources.
参数解释	$1：MDC的编号
日志等级	5
举例	MDC/5/MDC_CREATE_ERR: -Slot=1; Failed to create MDC 2 for insufficient resources.
日志说明	备用主控板启动时会从主用主控板获取所有已创建的MDC的信息，并在备用主控板创建同样的MDC。如果备用主控板因为资源限制无法创建该MDC，则输出此日志信息。MDC进驻备用主控板失败，无法在该备用主控板上提供服务
处理建议	1. 使用 **display mdc resource** 命令查询新插入的备用主控板的 CPU、内存空间和磁盘空间 2. 增加备用主控板的内存或减少磁盘使用，以保证新 MDC 可创建 3. 使用 **undo mdc** 命令删除该 MDC，或者换一块资源足够的主控板作为备用主控板

96.3 MDC_DELETE

日志内容	MDC [UINT16] was deleted.
参数解释	$1：MDC的编号
日志等级	5
举例	MDC/5/MDC_DELETE: MDC 2 was deleted.
日志说明	MDC成功删除
处理建议	无

96.4 MDC_EVENT_ERROR

日志内容	Function [STRING] returned [STRING] when handling event [UINT32] on virtual OS [UINT32]. Reason: [STRING].
参数解释	$1：函数的地址 $2：函数的处理结果 $3：事件的编号 $4：MDC的编号 $5：函数处理结果出现的原因，取值为： ○ Not enough resources available for this MDC：资源不足导致处理失败 ○ Not enough memory space to complete the operation：内存不足导致处理失败 ○ Other reason：其他原因导致的处理失败
日志等级	4
举例	MDC/4/MDC_EVENT_ERROR: -MDC=1; Function 0xfacd26b1 returned 0x40010001 when handling event 1 on virtual OS 2. Reason: Other reason.
日志说明	MDC相关事件处理失败
处理建议	联系工程师分析解决

96.5 MDC_KERNEL_EVENT_TOOLONG

日志内容	[STRING] [UINT32] kernel event in sequence [STRING] function [STRING] failed to finish within [UINT32] minutes.
参数解释	$1：取值为MDC或Context $2：MDC或Context的编号 $3：内核事件的阶段 $4：内核事件阶段对应的函数的地址 $5：所用时间
日志等级	4
举例	MDC/4/MDC_KERNEL_EVENT_TOOLONG: -slot=1; MDC 2 kernel event in sequence 0x4fe5 function 0xff245e failed to finish within 15 minutes.
日志说明	某内核事件在长时间内未完成
处理建议	**1.** 重启单板，尝试恢复 **2.** 联系工程师分析解决

96.6 MDC_LICENSE_EXPIRE

日志内容	The MDC feature's license will expire in [UINT32] days.
参数解释	$1：天数，取值范围为1到30天
日志等级	5
举例	MDC/5/MDC_LICENSE_EXPIRE: The MDC feature’s license will expire in 5 days.
日志说明	MDC License将在指定天数后失效
处理建议	安装新的License

96.7 MDC_NO_FORMAL_LICENSE

日志内容	The feature MDC has no formal license.
参数解释	无
日志等级	5
举例	MDC/5/MDC_NO_FORMAL_LICENSE: The feature MDC has no formal license.
日志说明	备用主控板变为主用主控板了，但是新主用主控板没有安装MDC License。系统会给新主用主控板一个MDC试用期。试用期过期，如果用户还没有给新主用主控板安装License，则不能继续使用MDC特性
处理建议	安装正式MDC License

96.8 MDC_NO_LICENSE_EXIT

日志内容	The MDC feature is being disabled, because it has no license.
参数解释	无
日志等级	5
举例	MDC/5/MDC_NO_LICENSE_EXIT: The MDC feature is being disabled, because it has no license.
日志说明	MDC特性被禁用，因为MDC License过期或者被卸载了
处理建议	安装MDC License

96.9 MDC_OFFLINE

日志内容	MDC [UINT16] is offline now.
参数解释	$1：MDC的编号
日志等级	5
举例	MDC/5/MDC_OFFLINE: MDC 2 is offline now.
日志说明	MDC停用了
处理建议	无

96.10 MDC_ONLINE

日志内容	MDC [UINT16] is online now.
参数解释	$1：MDC的编号
日志等级	5
举例	MDC/5/MDC_ONLINE: MDC 2 is online now.
日志说明	MDC启用了
处理建议	无

96.11 MDC_STATE_CHANGE

日志内容	MDC [UINT16] status changed to [STRING].
参数解释	$1：MDC的编号 $2：MDC的状态： ○ updating 表示正在给 MDC 分配接口板，即对 MDC 执行 **location** 命令 ○ stopping 表示 MDC 正在停止，即 MDC 正在执行 **undo mdc start** 命令 ○ inactive 表示 MDC 处于未启动状态 ○ starting 表示 MDC 正在启动中，即对 MDC 正在执行 **mdc start** 命令 ○ active 表示 MDC 正常运行
日志等级	5
举例	MDC/5/MDC_STATE_CHANGE: MDC 2 state changed to active.
日志说明	MDC状态发生了变化
处理建议	无

97 MFIB

本节介绍组播转发模块输出的日志信息。

97.1 MFIB_CFG_NOT_SUPPORT

日志内容	Failed to apply [STRING] configuration because the operation is not supported.
参数解释	$1：组播模块的命令行
日志等级	4
举例	MFIB/4/MFIB_OIF_NOT_SUPPORT: Failed to apply multicast rpf-fail-pkt flooding configuration because the operation is not supported.
日志说明	因硬件不支持对应配置而导致配置失败
处理建议	无

97.2 MFIB_MTI_NO_ENOUGH_RESOURCE

日志内容	Failed to create [STRING] because of insufficient resources.
参数解释	$1：MTunnel隧道的名称
日志等级	4
举例	MFIB/4/MFIB_MTI_NO_ENOUGH_RESOURCE: Failed to create MTunnel1 because of insufficient resources.
日志说明	因硬件资源不足而导致MTunnel隧道创建失败
处理建议	使用**undo group** *group-address* **source** *source-address*命令删除暂时不用的组播隧道，释放组播隧道资源

97.3 MFIB_OIF_NOT_SUPPORT

日志内容	Failed to add oif to entry ([[STRING], [STRING]) because some oifs are not supported.
参数解释	$1：组播表项源地址 $2：组播表项组地址
日志等级	4
举例	MFIB/4/MFIB_OIF_NOT_SUPPORT: Failed to add oif to entry (1.1.1.1, 225.0.0.1) because some oifs are not supported.
日志说明	硬件不支持向组播表项添加某些出接口
处理建议	检查生成该日志的板卡上各接口是否配置了如下命令： • **igmp static-group** *group-address* [**source** *source-address*] { **dot1q vid** *vlan-list* | **dot1q vid** *vlan-id* **second-dot1q** *vlan-list* } • **igmp user-vlan-aggregation dot1q vid** *vlan-id* [**second-dot1q** *vlan-id*] • **mld static-group** *ipv6-group-address* [**source** *ipv6-source-address*] { **dot1q vid** *vlan-list* | **dot1q vid** *vlan-id* **second-dot1q** *vlan-list* } • **mld user-vlan-aggregation dot1q vid** *vlan-id* [**second-dot1q** *vlan-id*] 如果配置了上述命令，则删除相关配置

98 MGROUP

本节主要介绍与镜像组相关的日志消息。

98.1 MGROUP_APPLY_SAMPLER_FAIL

日志内容	Failed to apply the sampler for mirroring group [UINT16], because the sampler resources are insufficient.
参数解释	$1：镜像组编号
日志等级	3
举例	MGROUP/3/MGROUP_APPLY_SAMPLER_FAIL: Failed to apply the sampler for mirroring group 1, because the sampler resources are insufficient.
日志说明	采样器资源不足时，新镜像组引用采样器失败
处理建议	无

98.2 MGROUP_RESTORE_CPUCFG_FAIL

日志内容	Failed to restore configuration for mirroring CPU of [STRING] in mirroring group [UINT16], because [STRING]
参数解释	$1：单板所在的槽位号 $2：镜像组编号 $3：恢复源CPU配置失败的原因
日志等级	3
举例	MGROUP/3/MGROUP_RESTORE_CPUCFG_FAIL: Failed to restore configuration for mirroring CPU of chassis 1 slot 2 in mirroring group 1, because the type of the monitor port in the mirroring group is not supported.
日志说明	当单板上的CPU用作镜像组的源CPU时，在单板拔出阶段，配置发生变化，单板再插入时，可能会引起镜像组源CPU的配置恢复失败
处理建议	排查配置恢复失败的原因，如果是由于系统不支持变化的配置，删除不支持的配置，重新配置镜像组的源CPU

98.3 MGROUP_RESTORE_IFCFG_FAIL

日志内容	Failed to restore configuration for interface [STRING] in mirroring group [UINT16], because [STRING]
参数解释	$1：接口名称 $2：镜像组编号 $3：恢复源端口配置失败的原因
日志等级	3
举例	MGROUP/3/MGROUP_RESTORE_IFCFG_FAIL: Failed to restore configuration for interface Ethernet3/1/2 in mirroring group 1, because the type of the monitor port in the mirroring group is not supported.
日志说明	当单板上的接口用作镜像组的源端口时，在单板拔出阶段，配置发生变化，单板再插入时，可能会引起镜像组源端口的配置恢复失败
处理建议	排查配置恢复失败的原因，如果是由于系统不支持变化的配置，删除不支持的配置，重新配置镜像组的源端口

98.4 MGROUP_SYNC_CFG_FAIL

日志内容	Failed to restore configuration for mirroring group [UINT16] in [STRING], because [STRING]
参数解释	$1：镜像组编号 $2：单板所在的槽位号 $3：恢复镜像组配置失败的原因
日志等级	3
举例	MGROUP/3/MGROUP_SYNC_CFG_FAIL: Failed to restore configuration for mirroring group 1 in chassis 1 slot 2, because monitor resources are insufficient.
日志说明	当向单板同步完整的镜像组配置时，由于单板资源不足，引起配置恢复失败
处理建议	删除配置恢复失败的镜像组

99 MPLS

本节介绍 MPLS 模块输出的日志信息。

99.1 MPLS_ILM

日志内容	No enough resource
参数解释	无
日志等级	3
举例	MPLS/3/ MPLS_ILM: -MDC=1-Slot=4; No enough resource
日志说明	单板上硬件资源不足，无法完成该操作。例如：当单板上的隧道资源耗尽后，该单板上无法创建MPLS隧道
处理建议	请联系技术支持

99.2 MPLS_NHLFE

日志内容	No enough resource
参数解释	无
日志等级	3
举例	MPLS/3/ MPLS_ NHLFE: -MDC=1-Slot=2; No enough resource
日志说明	单板上硬件资源不足，无法完成该操作。例如：当单板上的隧道资源耗尽后，该单板上无法创建MPLS隧道
处理建议	请联系技术支持

99.3 MPLS_RSC

日志内容	No enough resource
参数解释	无
日志等级	3
举例	MPLS/3/MPLS_RSC: -MDC=1-Slot=4; No enough resource
日志说明	单板上硬件资源不足，无法完成该操作。例如：当单板上的隧道资源耗尽后，该单板上无法创建MPLS隧道
处理建议	请联系技术支持

99.4 MPLS_VN

日志内容	Not enough hardware resources for P2MP-TE tunnel.
参数解释	无
日志等级	2
举例	MPLS/2/MPLS_VN: -MDC=1; Not enough hardware resources for P2MP-TE tunnel.
日志说明	单板上硬件资源不足，无法完成该操作。例如：当单板上的隧道资源耗尽后，该单板上无法创建MPLS隧道
处理建议	请联系技术支持

99.5 TE

日志内容	Hardware resources not enough. Can't deploy [STRING]'s MPLS TE bandwidth configuration to [STRING] when [STRING] is added to [STRING]
参数解释	$1：MPLS TE隧道接口名称 $2：MPLS TE隧道关联的物理接口名称 $3：MPLS TE隧道关联的物理接口名称 $4：MPLS TE隧道接口名称
日志等级	4
举例	DRVPLAT/4/DrvDebug: -MDC=1; Hardware resources not enough. Can't deploy Tunnel 1's MPLS TE bandwidth configuration to GigabitEthernet4/1/2 when GigabitEthernet4/1/2 is added to Tunnel 1
日志说明	在配置MPLS TE带宽预留时，由于硬件资源不足，配置失败
处理建议	请联系技术支持

99.6 VPLS_AC

日志内容	The device supports only one HUB.
参数解释	无
日志等级	4
举例	DRVPLAT/4/DrvDebug: -MDC=1; The device supports only one HUB.
日志说明	在Hub-Spoke组网方式中，每个VPLS实例只支持配置一个HUB站点
处理建议	请确保每个实例中只有一个HUB站点

99.7 VPLS_AC

日志内容	No enough resource.
参数解释	无
日志等级	3
举例	MPLS/3/ MPLS_ NHLFE: -MDC=1-Slot=2; No enough resource.
日志说明	开启AC的报文统计功能时，硬件资源不足。此时报文仍然可以正常转发，但是报文统计功能无效
处理建议	请联系技术支持

99.8 VPLS_AC

日志内容	Operation conflicts with the configuration on this interface.
参数解释	无
日志等级	3
举例	VPLS/3/VPLS_AC: -MDC=1-Slot=3; Operation conflicts with the configuration on this interface.
日志说明	VXLAN AC口配置统计命令时，若AC所在口配置了子接口统计或IPoE L2VPN专线，就会提示配置冲突
处理建议	删除不需要的配置

99.9 VPLS_AC

日志内容	The number of ACs or PWs in the VSI has reached the limit.
参数解释	无
日志等级	4
举例	VPLS/4/VPLS_AC: -MDC=1; The number of ACs or PWs in the VSI has reached the limit.
日志说明	VSI实例内配置的AC或PW数量超过允许配置的范围
处理建议	请联系技术支持

99.10 VPLS_PW

日志内容	The number of ACs or PWs in the VSI has reached the limit.
参数解释	无
日志等级	4
举例	VPLS/4/VPLS_PW: -MDC=1; The number of ACs or PWs in the VSI has reached the limit.
日志说明	VSI实例内配置的AC或PW数量超过允许配置的范围
处理建议	请联系技术支持

99.11 VLL_FWD

日志内容	AC Ethernet access and vBRAS AC Ethernet access are both configured. Only vBRAS AC Ethernet access takes effect.
参数解释	无
日志等级	3
举例	VLL/3/VLL_FWD: -MDC=1; AC Ethernet access and vBRAS AC Ethernet access are both configured. Only vBRAS AC Ethernet access takes effect.
日志说明	同一主接口下，存在不同的子接口，部分子接口作为VLL的AC口且配置了以太接入，部分子接口作为VXLAN的AC口且配置了以太接入，那么仅vBRAS以太接入生效
处理建议	1. 如果不需要普通以太接入功能（VLL AC 口以太接入），不需要处理 2. 如果需要普通以太接入功能，需要去除其他所有配置 vBRAS 以太接入的子接口配置

99.12 VLL_FWD

日志内容	AC Ethernet access takes effect.
参数解释	无
日志等级	3
举例	VLL/3/VLL_FWD: -MDC=1; AC Ethernet access takes effect.
日志说明	去除某个主接口下所有配置vBRAS的子接口后，若还有其它子接口配置了普通以太接入（VLL AC口以太接入），就会提示普通AC口以太接入生效
处理建议	无

99.13 VPLS_CFG

日志内容	A VSI interface configured with BRAS can be mapped to only a VSI configured with one AC.
参数解释	无
日志等级	3
举例	VPLS/3/VPLS_CFG: -MDC=1; A VSI interface configured with BRAS can be mapped to only a VSI configured with one AC.
日志说明	• 当 VSI 实例关联的 VSI 虚接口上配置了 BRAS 业务时，该 VSI 实例只允许关联一个 AC • 当某一 VSI 虚接口与配置了多个 AC 的 VSI 实例关联后，不允许在该 VSI 虚接口上配置 BRAS 业务
处理建议	无

99.14 VPLS_CFG

日志内容	A VSI interface configured with BRAS cannot be mapped to a VSI configured with multiple ACs. Please delete all ACs, and add your AC.
参数解释	无
日志等级	3
举例	VPLS/3/VPLS_CFG: -MDC=1; A VSI interface configured with BRAS cannot be mapped to a VSI configured with multiple ACs. Please delete all ACs, and add your AC.
日志说明	配置了多个AC的VSI实例不允许与配置了BRAS业务的VSI虚接口进行关联
处理建议	无

99.15 VPLS_CFG

日志内容	vBRAS cannot be configured on a VSI interface mapped to multiple VSIs.
参数解释	无
日志等级	3
举例	VPLS/3/VPLS_CFG: -MDC=1; vBRAS cannot be configured on a VSI interface mapped to multiple VSIs.
日志说明	不允许在关联了多个VSI实例的VSI虚接口上配置vBRAS业务
处理建议	无

99.16 VPLS_CFG

日志内容	vBRAS vsiif([INT32]) only supports one VSI. Please delete the relationship with all VSIs([INT32]), and then map the VSI interface to your VSI.
参数解释	$1：VSI虚接口的接口索引号 $2：VSI虚接口关联的VSI实例的个数
日志等级	3
举例	VPLS/3/VPLS_CFG: -MDC=1;vBRAS vsiif([8971]) only support one VSI. Please delete the relationship with all VSIs(2), and then map the VSI interface to your VSI.
日志说明	配置了vBRAS业务的VSI虚接口最多只允许关联一个VSI实例
处理建议	无

99.17 VPLS_CFG

日志内容	AC Ethernet access and vBRAS AC Ethernet access are both configured. Only vBRAS AC Ethernet access takes effect.
参数解释	无
日志等级	3
举例	VPLS/3/VPLS_CFG: -MDC=1; AC Ethernet access and vBRAS AC Ethernet access are both configured. Only vBRAS AC Ethernet access takes effect.
日志说明	同一主接口下，存在不同的子接口，部分子接口作为VPLS的AC口且配置了以太接入，部分子接口作为VXLAN的AC口且配置了以太接入，那么仅vBRAS以太接入生效
处理建议	1. 如果不需要普通以太接入功能（VPLS AC 口以太接入），不需要处理 2. 如果需要普通以太接入功能，需要去除其它所有配置 vBRAS 以太接入的子接口配置

99.18 VPLS_CFG

日志内容	AC Ethernet access takes effect.
参数解释	无
日志等级	3
举例	VPLS/3/VPLS_CFG: -MDC=1; AC Ethernet access takes effect.
日志说明	去除某个主接口下所有配置vBRAS的子接口，若还有其它子接口配置了普通以太接入（VPLS AC口以太接入），就会提示普通AC口以太接入生效
处理建议	无

99.19 MPLS_HARD_RESOURCE_NOENOUGH

日志内容	No enough hardware resource for MPLS.
参数解释	无
日志等级	2
举例	MPLS/2/MPLS_HARD_RESOURCE_NOENOUGH: No enough hardware resource for MPLS.
日志说明	MPLS硬件资源不足
处理建议	请检查是否生成了当前业务不需要的大量LSP，是则配置获调整标签分发协议的LSP触发策略、标签通告策略、标签接受策略，以过滤掉不需要的LSP

99.20 MPLS_HARD_RESOURCE_RESTORE

日志内容	Hardware resources for MPLS are restored.
参数解释	无
日志等级	2
举例	MPLS/2/MPLS_HARD_RESOURCE_RESTORE: Hardware resources for MPLS are restored.
日志说明	MPLS硬件资源恢复
处理建议	无

100 MSC

本节介绍 MSC 模块输出的日志信息。

100.1 MSC_NO_RTP_IN2SECS

日志内容	No RTP or RTCP packets received in [UINT32] seconds.
参数解释	$1：RTP流检查时间间隔
日志等级	6
举例	MSC/6/MSC_NO_RTP_IN2SECS: No RTP or RTCP packets received in 2 seconds.
日志说明	呼叫建立后，在指定时间内没有检测到RTP或RTCP流
处理建议	请确认呼叫双方是否都没有说话

100.2 MSC_NO_RTP_IN2XNSECS

日志内容	No RTP or RTCP packets received in [UINT32] seconds ([UINT32] probes).
参数解释	$1：RTP流检查间隔时间 $2：检测总次数
日志等级	4
举例	MSC/4/MSC_NO_RTP_IN2XNSECS: No RTP or RTCP packets received in 2 seconds (30 probes).
日志说明	呼叫建立后，在指定时间内没有检测到RTP或RTCP流，且达到一定次数
处理建议	请检查呼叫线路、网络是否出现了短暂的故障

100.3 MSC_NO_RTP_IN120SECS

日志内容	No RTP or RTCP packets received in [UINT32] seconds. A release message was sent.
参数解释	$1：呼叫拆除前，检测RTP流所占用的时长
日志等级	4
举例	MSC/4/MSC_NO_RTP_IN120SECS: No RTP or RTCP packets received in 120 seconds. A release message was sent.
日志说明	呼叫建立后，在指定时间内没有检测到RTP或RTCP接收流，发送呼叫拆除消息
处理建议	请检查呼叫线路网络是否已经故障

101 MTLK

本节介绍 Monitor Link 模块输出的日志信息。

101.1 MTLK_UPLINK_STATUS_CHANGE

日志内容	The uplink of monitor link group [UINT32] is [STRING].
参数解释	$1：Monitor Link组ID $2：Monitor Link组状态 ○ down：故障 ○ up：正常
日志等级	6
举例	MTLK/6/MTLK_UPLINK_STATUS_CHANGE: The uplink of monitor link group 1 is up.
日志说明	Monitor Link组上行链路up或down
处理建议	检查故障链路

102 NAT

本节介绍 NAT 模块输出的日志信息。

102.1 DSLITE_SYSLOG

日志内容	All port block resources ran out in address group [UINT 16].
参数解释	$1：地址组名称
日志等级	6
举例	NAT/6/DSLITE_SYSLOG: All port block resources ran out in address group 1.
日志说明	DS-Lite B4端口块资源耗尽导致端口块分配失败时会发送该日志
处理建议	无

102.2 EIM_MODE_PORT_USAGE_ALARM

日志内容	[STRING] Port usage reaches [STRING]%; SrcIPAddr=[IPADDR]; VPNInstance=[STRING]; NATIPAddr=[IPADDR]; ConnectCount=[UINT16].
参数解释	$1：协议类型 $2：百分比 $3：源IP地址 $4：源VPN名称 $5：转换后的源IP地址 $6：分配端口数
日志等级	4
举例	NAT/4/EIM_MODE_PORT_USAGE_ALARM: UDP Port usage reaches 40%; SrcIPAddr=1.1.1.211; VPNInstance=-; NATIPAddr=198.1.1.16; ConnectCount=40.
日志说明	当NAT端口块中端口的使用率大于或等于通过命令**nat log port-block port-usage threshold**配置的告警阈值，且PAT方式出方向动态地址转换模式为Endpoint-Independent Mapping时，才会发送该日志
处理建议	无

102.3 NAT_ADDR_BIND_CONFLICT

日志内容	Failed to activate NAT configuration on interface [STRING], because global IP addresses already bound to another service card.
参数解释	$1：接口名称
日志等级	4
举例	NAT/4/NAT_ADDR_BIND_CONFLICT: Failed to activate NAT configuration on interface GigabitEthernet1/0/1, because global IP addresses already bound to another service card.
日志说明	配置中的外网地址绑定指定业务板时发现其已经绑定到其他业务板上，则触发该日志
处理建议	如果有多个接口引用了相同的外网地址，则这些接口必须指定同一块业务板进行NAT处理。请使用**display nat all**命令检查配置，并修改配置使引用相同外网地址的接口绑定相同的业务板。另外，由于该绑定冲突，失效配置需要先删除，再重新进行配置

102.4 NAT_EIM

日志内容	Protocol(1001)=[STRING];LocalIPAddr(1003)=[IPADDR];LocalPort(1004)=[UINT16];GlobalIPAddr(1005)=[IPADDR];GlobalPort(1006)=[UINT16];RcvVPNInstance(1042)=[STRING];SndVPNInstance(1043)=[STRING];RcvDSLiteTunnelPeer(1040)=[STRING];BeginTime_e(1013)=[STRING];EndTime_e(1014)=[STRING];Event(1048)=[STRING];
参数解释	$1：协议类型 $2：源IP地址 $3：源端口号 $4：转换后的源IP地址 $5：转换后的源端口号 $6：源VPN名称 $7：目的VPN名称 $8：源DS-Lite Tunnel $9：创建EIM表项的时间 $10：EIM表项删除时间 $11：日志类型描述信息，包括： • NAT EIM entry created：NAT EIM 表项创建日志 • NAT EIM entry deleted：NAT EIM 表项删除日志
日志等级	6
举例	NAT/6/NAT_EIM: -Protocol(1001)=UDP;LocalIPAddr(1003)=1.1.1.2;LocalPort(1004)=1024;GlobalIPAddr(1005)=30.3.1.231;GlobalPort(1006)=1026;RcvVPNInstance(1042)=;SndVPNInstance(1043)=;RcvDSLiteTunnelPeer(1040)=;BeginTime_e(1013)=10261971001739;EndTime_e(1014)=;Event(1048)=Nat eim created;
日志说明	创建、删除NAT EIM表项时会发送该日志
处理建议	无

102.5 NAT_FAILED_ADD_FLOW_RULE

日志内容	Failed to add flow-table due to: [STRING].
参数解释	$1：失败原因
日志等级	4
举例	NAT/4/NAT_FAILED_ADD_FLOW_RULE: Failed to add flow-table due to: Not enough resources are available to complete the operation.
日志说明	添加流表失败，可能原因包括硬件资源不足、内存不足等
处理建议	请联系技术支持

102.6 NAT_FAILED_ADD_FLOW_TABLE

日志内容	Failed to add flow-table due to [STRING].
参数解释	$1：失败原因
日志等级	4
举例	NAT/4/NAT_FAILED_ADD_FLOW_TABLE: Failed to add flow-table due to no enough resource.
日志说明	添加流表失败，可能原因包括硬件资源不足、NAT配置地址存在重叠等
处理建议	对于硬件资源不足情况，请联系技术支持 对于NAT配置地址存在重叠情况，请尽量避免出现部分地址重叠，如果不可避免，请将重叠部分地址和不重叠地址分开，单独配置

102.7 NAT_FLOW

日志内容	Protocol(1001)=[STRING];Application(1002)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];NATSrcIPAddr(1005)=[IPADDR];NATSrcPort(1006)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];NATDstIPAddr(1009)=[IPADDR];NATDstPort(1010)=[UINT16];InitPktCount(1044)=[UINT32];InitByteCount(1046)=[UINT32];RplyPktCount(1045)=[UINT32];RplyByteCount(1047)=[UINT32];RcvVPNInstance(1042)=[STRING];SndVPNInstance(1043)=[STRING];RcvDSLiteTunnelPeer(1040)=[STRING];SndDSLiteTunnelPeer(1041)=[STRING];BeginTime_e(1013)=[STRING];EndTime_e(1014)=[STRING];Event(1048)=([UNIT16])[STRING];
参数解释	$1：协议类型 $2：应用层协议 $3：源IP地址 $4：源端口号 $5：转换后的源IP地址 $6：转换后的源端口号 $7：目的IP地址 $8：目的端口号 $9：转换后的目的IP地址 $10：转换后的目的端口号 $11：入方向的报文总数 $12：入方向的字节总数 $13：出方向的报文总数 $14：出方向的字节总数 $15：源VPN名称 $16：目的VPN名称 $17：源DS-Lite Tunnel $18：目的DS-Lite Tunnel $19：创建会话的时间 $20：会话删除时间 $22：日志类型 $22：日志类型描述信息，包括： • Session created：NAT 会话创建日志 • Active data flow timeout：流量或时间阈值日志 • Normal over：正常流结束，会话删除日志 • Aged for timeout：会话老化删除日志 • Aged for reset or config-change：通过配置删除会话日志 • Other：其他原因删除会话日志，如由其他模块删除
日志等级	6
举例	NAT/6/NAT_FLOW: Protocol(1001)=UDP;Application(1002)=other;SrcIPAddr(1003)=1.1.1.2;SrcPort(1004)=1024;NatSrcIPAddr(1005)=30.3.1.231;NatSrcPort(1006)=1026;DstIPAddr(1007)=2.1.1.2;DstPort(1008)=1024;NatDstIPAddr(1009)=2.1.1.2;NatDstPort(1010)=1024;InitPktCount(1044)=1;InitByteCount(1046)=110;RplyPktCount(1045)=0;RplyByteCount(1047)=0;RcvVPNInstance(1042)=;SndVPNInstance(1043)=;RcvDSLiteTunnelPeer(1040)=;SndDSLiteTunnelPeer(1041)=;BeginTime_e(1013)=03232017091640;EndTime_e(1014)=;Event(1048)=(8)Session created;

日志说明	创建、删除NAT会话时会发送该日志 NAT会话过程中会定时发送该日志 NAT会话的流量或时间达到指定的阈值时会发送该日志
处理建议	无

102.8 NAT_INSTANCE_SERVER_INVALID

日志内容	The NAT server with Easy IP is invalid because its global settings conflict with that of another NAT server in the same instance.
参数解释	无
日志等级	4
举例	NAT/4/NAT_INSTANCE_SERVER_INVALID: The NAT server with Easy IP is invalid because its global settings conflict with that of another NAT server in the same instance.
日志说明	Easy IP方式的NAT服务器配置生效时，当同一个实例下存在其他NAT服务器配置也包含相同的外网信息，则触发该日志
处理建议	同一个实例下配置的NAT服务器，其协议类型、外网地址和外网端口号的组合必须是唯一的。请修改相应实例的NAT服务器配置

102.9 NAT_SERVER_INVALID

日志内容	The NAT server with Easy IP is invalid because its global settings conflict with that of another NAT server on this interface.
参数解释	无
日志等级	4
举例	NAT/4/NAT_SERVER_INVALID: The NAT server with Easy IP is invalid because its global settings conflict with that of another NAT server on this interface.
日志说明	Easy IP方式的NAT服务器配置生效时发现同一个接口下存在其他NAT服务器配置也包含相同的外网信息，则触发该日志
处理建议	同一个接口下配置的NAT服务器，其协议类型、外网地址和外网端口号的组合必须是唯一的。请修改相应接口的NAT服务器配置

102.10 NAT_SERVICE_CARD_RECOVER_FAILURE

日志内容	形式一： Failed to recover the configuration of binding the service card on slot [UINT16] to interface [STRING], because [STRING]. 形式二： Failed to recover the configuration of binding the service card on chassis [UINT16] slot [UINT16] to interface [STRING], because [STRING].
参数解释	形式一： $1：slot编号 $2：接口名称 $3：指定接口绑定业务板配置恢复失败的原因 • NAT addresses already bound to another service card：NAT 地址已经绑定到其他业务板 • NAT service is not supported on this service card：指定业务板不支持 NAT 业务 • the hardware resources are not enough：硬件资源不足 • unknown error：未知错误 形式二： $1：chassis编号 $2：slot编号 $3：接口名称 $4：指定接口绑定业务板配置恢复失败的原因 • NAT addresses already bound to another service card：NAT 地址已经绑定到其他业务板 • NAT service is not supported on this service card：指定业务板不支持 NAT 业务 • the hardware resources are not enough：硬件资源不足 • unknown error：未知错误
日志等级	4
举例	NAT/4/NAT_SERVICE_CARD_RECOVER_FAILURE: Failed to recover the configuration of binding the service card on slot 3 to interface GigabitEthernet0/0/2, because NAT service is not supported on this service card.
日志说明	恢复接口绑定业务板配置失败时触发该日志
处理建议	• 如果提示 NAT 地址已经绑定到其他业务板，则使用 **display nat all** 检查配置，并修改配置使引用相同外网地址的接口绑定相同的业务板 • 如果提示业务板不支持 NAT 业务、硬件资源不足或者未知错误，请排查业务板的硬件问题

102.11 NAT444_SYSLOG

日志内容	All port block resources ran out in address group [UINT 16].
参数解释	$1：地址组名称
日志等级	3
举例	NAT/3/NAT444_SYSLOG: All port block resources ran out in address group 1.
日志说明	NAT444端口块资源耗尽导致端口块分配失败时会发送该日志
处理建议	无

102.12 PORT_USAGE_ALARM

日志内容	[STRING] Port usage reaches [STRING]%; SrcIPAddr=[IPADDR]; VPNInstance=[STRING]; NATIPAddr=[IPADDR]; ConnectCount=[UINT16].
参数解释	$1：协议类型 $2：百分比 $3：源IP地址 $4：源VPN名称 $5：转换后的源IP地址 $6：分配端口数
日志等级	4
举例	NAT/4/PORT_USAGE_ALARM: UDP Port usage reaches 40%; SrcIPAddr=1.1.1.211; VPNInstance=-; NATIPAddr=16.1.1.198; ConnectCount=40.
日志说明	当NAT端口块中端口的使用率大于或等于通过命令**nat log port-block port-usage threshold**配置的告警阈值，且PAT方式出方向动态地址转换模式为Connection-Dependent Mapping时，才会发送该日志
处理建议	无

102.13 PORTBLOCK_ALARM

日志内容	Address group [UINT16]; total port blocks [UINT16]; active port blocks [UINT16]; usage [STRING] [UINT16]%.
参数解释	$1：地址组名称 $2：端口块总数 $3：分配了的端口块数 $4：端口块使用率超过或低于设定的阈值 $5：端口块使用率
日志等级	4
举例	NAT/4/PORTBLOCK_ALARM: Address group 3; total port blocks 16575; active port blocks 6630; usage reaches 40%. NAT/6/PORTBLOCK_ALARM: Address group 3; total port blocks 16575; active port blocks 5800; usage below 35%.
日志说明	NAT端口块的使用率大于或等于通过命令**nat log port-block usage threshold**配置的告警阈值时会发送资源告警日志 NAT端口块的使用率小于通过命令**nat log port-block usage threshold**配置的告警阈值的87.5%时会发送资源恢复日志，恢复日志在再次到达告警阈值前只会输出一次
处理建议	无

102.14 PORTBLOCKGRP_MEMORY_WARNING

日志内容	Insufficient memory caused by excessive public addresses in port block group [UINT16]. Please reconfigure the public address space.
参数解释	$1：NAT端口块组的编号
日志等级	4
举例	NAT/4/PORTBLOCKGRP_MEMORY_WARNING: Insufficient memory caused by excessive public addresses in port block group 1. Please reconfigure the public address space.
日志说明	端口块组内配置的公网地址成员的地址范围太大，导致内存不足，会发送该日志
处理建议	用户需要重新配置公网地址成员的地址范围

103 ND

本节介绍 ND 模块输出的日志信息。

103.1 ND_CONFLICT

日志内容	[STRING] is inconsistent.
参数解释	$1：配置类型 • M_FLAG：被管理地址配置标志位 • O_FLAG：其他信息配置标志位 • CUR_HOP_LIMIT：跳数限制 • REACHABLE TIME：保持邻居可达状态的时间 • NS INTERVAL：邻居请求消息间隔 • MTU：发布链路的 MTU • PREFIX VALID TIME：前缀的有效存活时间 • PREFIX PREFERRED TIME：前缀用于无状态地址配置的优选项的存活时间
日志等级	6
举例	ND/6/ND_CONFLICT：PREFIX VALID TIME is inconsistent.
日志说明	设备收到一个路由通告消息，导致与邻居路由器上的配置不一致
处理建议	检查并保证设备与邻居路由器上的配置一致

103.2 ND_DUPADDR

日志内容	Duplicate address: [STRING] on the interface [STRING].
参数解释	$1：将要分配的IPv6地址 $2：接口名称
日志等级	6
举例	ND/6/ND_DUPADDR: Duplicate address: 33::8 on interface Vlan-interface9.
日志说明	分配给该接口的地址已经被其他设备使用
处理建议	分配一个新的IPv6地址

103.3 ND_HOST_IP_CONFLICT

日志内容	The host [STRING] connected to interface [STRING] cannot communicate correctly, because it uses the same IPv6 address as the host connected to interface [STRING].
参数解释	$1：IPv6地址 $2：接口名 $3：接口名
日志等级	4
举例	ND/4/ND_HOST_IP_CONFLICT: The host 2::2 connected to interface GigabitEthernet1/0/1 cannot communicate correctly, because it uses the same IPv6 address as the host connected to interface GigabitEthernet1/0/1.
日志说明	分配给该接口的地址已经被其他设备使用
处理建议	分配一个新的IPv6地址。如果非法，需要断开该主机网络

103.4 ND_MAC_CHECK

日志内容	Packet received on interface [STRING] was dropped because source MAC [STRING] was inconsistent with link-layer address [STRING].
参数解释	$1：接收ND报文的接口名 $2：ND报文中的的源MAC地址 $3：ND报文的链路层源MAC地址
日志等级	6
举例	ND/6/ND_MAC_CHECK: Packet received on interface Ethernet2/0/2 was dropped because source MAC 0002-0002-0001 was inconsistent with link-layer address 0002-0002-0002.
日志说明	**ipv6 nd mac-check enable**命令用来在网关设备上开启ND协议报文源MAC地址一致性检查功能。在网关开启此功能后，会对接收的ND协议报文进行检查，如果ND协议报文中的源MAC地址和源链路层选项地址中的MAC地址不同，则丢弃该报文。若使用**ipv6 nd check log enable**命令来开启ND日志信息功能，会有相关的log信息输出
处理建议	检查链路层源MAC对应主机的合法性

103.5 ND_MAXNUM_DEV

日志内容	The number of dynamic neighbor entries for the device has reached the maximum.
参数解释	无
日志等级	6
举例	The number of dynamic neighbor entries for the device has reached the maximum.
日志说明	设备学到的动态邻居表项总数到达最大值，打印该提示日志
处理建议	无

103.6 ND_MAXNUM_IF

日志内容	The number of dynamic neighbor entries on interface [STRING] has reached the maximum.
参数解释	$1：接口名
日志等级	3
举例	The number of dynamic neighbor entries on interface GigabitEthernet3/0/1 has reached the maximum.
日志说明	接口学到的动态邻居表项总数到达最大值，打印该提示日志
处理建议	无

103.7 ND_RAGUARD_DROP

日志内容	Dropped RA messages with the source IPv6 address [STRING] on interface [STRING]. [STRING] messages dropped in total on the interface.
参数解释	$1：被丢弃报文的源IPv6地址 $2：丢弃报文的端口名 $3：该端口已丢弃的报文总数
日志等级	4
举例	ND/6/ND_RAGUARD_DROP: Dropped RA messages with the source IPv6 address FE80::20 on interface GigabitEthernet1/0/1. 20 RA messages dropped in total on the interface.
日志说明	RA Guard检测到攻击，丢弃相应的报文并提示日志信息
处理建议	检查发送报文的设备是否合法

103.8 ND_SET_PORT_TRUST_NORESOURCE

日志内容	Not enough resources to complete the operation.
参数解释	无
日志等级	2
举例	ND/2/ND_SET_PORT_TRUST_NORESOURCE: Not enough resources to complete the operation.
日志说明	下发端口规则失败，原因是驱动资源不足
处理建议	释放设备驱动资源，重新下发

103.9 ND_SET_VLAN_REDIRECT_NORESOURCE

日志内容	Not enough resources to complete the operation.
参数解释	无
日志等级	6
举例	ND/6/ND_VLAN_REDIRECT_NORESOURCE: Not enough resources to complete the operation.
日志说明	下发VLAN规则失败，原因是驱动资源不足
处理建议	释放设备驱动资源，重新下发

104 NETCONF

本节介绍 NETCONF 模块输出的日志信息。

104.1 CLI

日志内容	User ([STRING], [STRING][STRING]) performed an CLI operation: [STRING] operation result=[STRING][STRING]
参数解释	$1：用户名或用户线类型 • 如果用户使用 Scheme 方式登录设备，该值为用户名 • 如果用户使用无认证或 Password 方式登录设备，该值为用户线的类型，例如 VTY $2：用户IP地址或用户线类型及相对编号 • 用户通过 Telnet 或 SSH 登录设备时，该字段取值为用户的 IP 地址 • 用户通过 Console 或 AUX 登录设备时，该字段取值为用户线的类型及相对编号，例如 CON0 $3：NETCONF会话的编号（Web和RESTful类型会话无此字段） $4：NETCONF请求中的message-id（Web和RESTful类型会话无此字段） $5：CLI的执行成功，取值为Succeeded；CLI的执行失败，取值为Failed $6：CLI执行失败的原因（仅已知失败原因的情况显示该信息）
日志等级	6
举例	XMLSOAP/6/CLI: -MDC=1; User (test, 169.254.5.222, session ID=1) performed an CLI operation:message ID=101, operation result=Succeeded.
日志说明	CLI配置执行完毕后，输出CLI的执行结果
处理建议	无

104.2 EDIT-CONFIG

日志内容	User ([STRING], [STRING][STRING])[STRING] operation=[STRING] [STRING] [STRING], result=[STRING]. No attributes. 或 User ([STRING], [STRING],[STRING]),[STRING] operation=[STRING] [STRING] [STRING], result=[STRING]. Attributes: [STRING].
参数解释	$1：用户名或用户线类型 • 如果用户使用 Scheme 方式登录设备，该值为用户名 • 如果用户使用无认证或 Password 方式登录设备，该值为用户线的类型，例如 VTY $2：用户IP地址或用户线类型及相对编号 • 用户通过 Telnet 或 SSH 登录设备时，该字段取值为用户的 IP 地址 • 用户通过 Console 或 AUX 登录设备时，该字段取值为用户线的类型及相对编号，例如 console0 $3：NETCONF会话的编号，没有则不显示 $4：NETCONF请求中的message-id，没有则不显示 $5：NETCONF行操作名称 $6：模块和表名称 $7：索引信息。仅下发索引时显示，用括号包围；如果日志中包含多个索引，则索引之间用逗号分隔 $8：NETCONF行操作的处理结果，NETCONF行操作执行成功时，取值为Succeeded；执行失败时，取值为Failed $9：属性列信息。仅配置属性列时显示该信息
日志等级	6
举例	XMLSOAP/6/EDIT-CONFIG: -MDC=1; User (test, 192.168.200.220, session ID 1), message ID=101, operation=merge DHCP/DHCPServerPoolStatic (PoolIndex=1, Ipv4Address=1.1.1.1), result=Failed. Attributes: CID="aaaaa", HType=1.
日志说明	按NETCONF行操作输出日志，用户下发一次NETCONF操作，设备输出该操作中每个请求行操作的日志 仅action和set操作支持输入该日志
处理建议	无

104.3 NETCONF_MSG_DEL

日志内容	A NETCONF message was dropped. Reason: Packet size exceeded the upper limit.
参数解释	无
日志等级	7
举例	NETCONF/7/NETCONF_MSG_DEL: A NETCONF message was dropped. Reason: Packet size exceeded the upper limit.
日志说明	来自NETCONF over SSH客户端或XML视图的NETCONF报文由于其大小超过设备支持的上限而被删除
处理建议	减小发往设备的单个NETCONF报文的大小，例如删除报文中的空格等无效字符

104.4 REPLY

日志内容	Sent a NETCONF reply to the client: Session ID=[UINT16], Content=[STRING]. 或 Sent a NETCONF reply to the client: Session ID=[UINT16], Content (partial)=[STRING].
参数解释	$1：NETCONF会话ID，建立会话前，该字段显示为“-” $2：设备发送到客户端的NETCONF报文
日志等级	7
举例	XMLSOAP/7/REPLY: -MDC=1; Sent a NETCONF reply to the client: Session ID=1, Content=</env:Body></env:Envelope>.
日志说明	设备发送到客户端的NETCONF报文，用于调试NETCONF工作是否正常 如果一条日志中的NETCONF报文内容太多，则分多条日志输出，每条日志添加“partial”标识
处理建议	无

104.5 THREAD

日志内容	Maximum number of NETCONF threads already reached.
参数解释	无
日志等级	3
举例	XMLCFG/3/THREAD: -MDC=1; Maximum number of NETCONF threads already reached.
日志说明	NETCONF线程数达到上限
处理建议	NETCONF线程数达到上限，请稍后重试

105 NP

本节介绍 NP 模块输出的日志信息

105.1 NP

日志内容	The link of [STRING] flaps frequently. Please check the hardware link!
参数解释	$1：接口名称
日志等级	4
举例	PORT/4/NP: The link of Ten-GigabitEthernet5/0/1 flaps frequently. Please check the hardware link!
日志说明	CSPEX类单板上的接口（除MIC-GP20L、MIC-GT20L、MIC-GP10L-V2子卡上的接口）频繁UP/DOWN导致链路震荡
处理建议	**1.** 请检查并确保链路正常 **2.** 请检查并确保对端接口正常 **3.** 如故障仍然存在，请重启链路对端接口所在的单板 **4.** 请联系技术支持

106 NPD

本节介绍 NPD 模块输出的日志信息。

106.1 MONT

日志内容	MAC TX FIFO error detected on chassis [INT32] slot [INT32].
参数解释	$1：设备在IRF中的成员编号 $2：单板所在的槽位号
日志等级	4
举例	NPD/4/MONT: MAC TX FIFO error detected on chassis 1 slot 3.
日志说明	检测到接口MAC先进先出发送队列(MAC TX FIFO)故障，一定次数尝试后没有效果，打印此日志
处理建议	请联系技术支持

106.2 MONT

日志内容	MAC TX FIFO error detected on slot [INT32].
参数解释	$1：单板所在的槽位号
日志等级	4
举例	NPD/4/MONT: MAC TX FIFO error detected on slot 3.
日志说明	检测到接口MAC先进先出发送队列（MAC TX FIFO）故障，一定次数尝试后没有效果，打印此日志
处理建议	请联系技术支持

106.3 MONT

日志内容	MAC TX FIFO error detected on interface [STRING].
参数解释	$1：接口编号
日志等级	3
举例	NPD/3/MONT: MAC TX FIFO error detected on interface 1/2/0/1.
日志说明	检测到接口MAC先进先出发送队列（MAC TX FIFO）故障，一定次数尝试后没有效果，打印此日志
处理建议	请联系技术支持

106.4 ECC_ERROR

日志内容	ECC reset-level error occurred on chassis [UINT32] slot [UINT32]. Error not corrected after three fast reset actions.
参数解释	$1：设备在IRF中的成员编号 $2：单板所在的槽位号
日志等级	2
举例	NPD/2/ECC_ERROR: -MDC=1-Chassis=2-Slot=5; ECC reset-level error occurred on chassis 2 slot 5. Error not corrected after three fast reset actions.
日志说明	CSPEX类单板（CSPEX-1204、CSPEX-1104-E和CSPEX-1802X除外）和CEPC类单板上故障检测控制功能检测到reset级别的故障，已执行三次快速复位修复，故障仍存在
处理建议	请更换该单板

106.5 ECC_ERROR

日志内容	ECC reset-level error occurred on slot [UINT32]. Error not corrected after three fast reset actions.
参数解释	$1：单板所在的槽位号
日志等级	2
举例	NPD/2/ECC_ERROR: -MDC=1-Slot=5; ECC reset-level error occurred on slot 5. Error not corrected after three fast reset actions.
日志说明	CSPEX类单板（CSPEX-1204、CSPEX-1104-E和CSPEX-1802X除外）和CEPC类单板上故障检测控制功能检测到reset级别的故障，已执行三次快速复位修复，故障仍存在
处理建议	请更换该单板

107 NQA

本节介绍 NQA 模块输出的日志信息。

107.1 NQA_LOG_UNREACHABLE

日志内容	Server [STRING] unreachable.
参数解释	$1：NQA服务器的IP地址
日志等级	6
举例	NQA/6/NQA_LOG_UNREACHABLE: Server 192.168.30.117 unreachable.
日志说明	NQA客户端检测到NQA服务器不可达
处理建议	检查网络环境

107.2 NQA_PACKET_OVERSIZE

日志内容	NQA entry ([STRING]-[STRING]): The payload size exceeds 65503 bytes, and all IPv6 UDP probe packets will be dropped by the NQA server.
参数解释	$1：NQA测试组的管理员名称 $2：测试操作的标签
日志等级	6
举例	NQA/6/NQA_PACKET_OVERSIZE: NQA entry (1-1): The payload size exceeds 65503 bytes, and all IPv6 UDP probe packets will be dropped by the NQA server.
日志说明	NQA客户端发送了使用UDP协议、目的地址为IPv6地址、且数据段长度超过65503字节的探测报文，这样的探测报文将在服务器端被丢弃
处理建议	检查设备配置，修改NQA测试的**data-size**数据字段大小

107.3 NQA_SCHEDULE_FAILURE

日志内容	NQA entry ([STRING]- [STRING]): Failed to start the scheduled NQA operation because port [STRING] used by the operation is not available.
参数解释	$1：NQA测试组的管理员名称 $2：测试操作的标签 $3：端口号
日志等级	4
举例	NQA/4/NQA_SCHEDULE_FAILURE: NQA entry (admin-tag): Failed to start the scheduled NQA operation because port 10000 used by the operation is not available.
日志说明	由于端口被其他服务占用，导致NQA客户端的测试调度失败
处理建议	调度失败的情况下，用户需要修改NQA测试中被占用的端口或是关闭已占用端口的服务

107.4 NQA_SEVER_FAILURE

日志内容	Failed to enable the NQA server because listening port [STRING] is not available.
参数解释	$1：端口号
日志等级	4
举例	NQA/4/NQA_SEVER_FAILURE: Failed to enable the NQA server because listening port 10000 is not available.
日志说明	由于端口被其他服务占用，导致NQA服务器功能开启失败
处理建议	服务器功能开启失败的情况下，用户需要修改被占用的端口或是关闭已占用端口的服务

108 NTP

本节介绍 NTP 模块输出的日志信息。

108.1 NTP_CLOCK_CHANGE

日志内容	System clock changed from [STRING] to [STRING], the NTP server's IP address is [STRING].
参数解释	$1：起始时间 $2：同步后时间 $3：IP地址
日志等级	5
举例	NTP/5/NTP_CLOCK_CHANGE: System clock changed from 02:12:58:345 12/28/2012 to 02:29:12:879 12/28/2012, the NTP server's IP address is 192.168.30.116.
日志说明	NTP客户端的时间已经和NTP服务器同步
处理建议	无

108.2 NTP_LEAP_CHANGE

日志内容	System Leap Indicator changed from [UINT32] to [UINT32] after clock update.
参数解释	$1：起始闰秒标识 $2：当前闰秒标识
日志等级	5
举例	NTP/5/NTP_LEAP_CHANGE: System Leap Indicator changed from 00 to 01 after clock update.
日志说明	• NTP 闰秒标识是一个二位码，预报当天最近的分钟里要被插入的闰秒秒数 • 比特值在闰秒秒数插入当天 23:59 前或次日 00:00 后设置。因此秒数会比插入当天的时间提前或推后 1 秒 • 系统的闰秒标识会发生变化。例如，NTP 状态会从未同步状态变为已同步状态
处理建议	无

108.3 NTP_SOURCE_CHANGE

日志内容	NTP server's IP address changed from [STRING] to [STRING].
参数解释	$1：起始时钟源的IP地址 $2：新时钟源的IP地址
日志等级	5
举例	NTP/5/NTP_SOURCE_CHANGE: NTP server's IP address changed from 1.1.1.1 to 1.1.1.2.
日志说明	系统改变了时钟源
处理建议	无

108.4 NTP_SOURCE_LOST

日志内容	Lost synchronization with NTP server with IP address [STRING].
参数解释	$1：IP 地址
日志等级	4
举例	NTP/4/NTP_SOURCE_LOST: Lost synchronization with NTP server with IP address 1.1.1.1.
日志说明	NTP交互中的时钟源处于未同步状态或不可达
处理建议	检查NTP服务器及网络连接，若NTP服务器故障，请在客户端配置新的服务器作为时钟源

108.5 NTP_STRATUM_CHANGE

日志内容	System stratum changed from [UINT32] to [UINT32] after clock update.
参数解释	$1：起始层 $2：当前层
日志等级	5
举例	NTP/5/NTP_STRATUM_CHANGE: System stratum changed from 6 to 5 after clock update.
日志说明	系统的层数已发生变化
处理建议	无

109 OBJP

本节介绍 OBJP（对象策略）模块输出的日志信息。

109.1 OBJP_ACCELERATE_NO_RES

日志内容	Failed to accelerate [STRING] object-policy [STRING]. The resources are insufficient.
参数解释	$1：对象策略版本 $2：对象策略名称
日志等级	4
举例	OBJP/4/OBJP_ACCELERATE_NO_RES: Failed to accelerate IPv6 object-policy a. The resources are insufficient.
日志说明	因硬件资源不足，系统加速对象策略失败
处理建议	删除一些规则或者关闭其他对象策略的加速功能，释放硬件资源

109.2 OBJP_ACCELERATE_NOT_SUPPORT

日志内容	Failed to accelerate [STRING] object-policy [STRING]. Object-policy acceleration is not supported.
参数解释	$1：对象策略版本 $2：对象策略名称
日志等级	4
举例	OBJP/4/OBJP_ACCELERATE_NOT_SUPPORT: Failed to accelerate IPv6 object-policy a. The operation is not supported.
日志说明	因系统不支持对象策略加速而导致对象策略加速失败
处理建议	无

109.3 OBJP_ACCELERATE_UNK_ERR

日志内容	Failed to accelerate [STRING] object-policy [STRING].
参数解释	$1：对象策略版本 $2：对象策略名称
日志等级	4
举例	OBJP/4/OBJP_ACCELERATE_UNK_ERR: Failed to accelerate IPv6 object-policy a.
日志说明	因系统故障导致对象策略加速失败
处理建议	无

110 OFP

本节介绍 OpenFlow 模块输出的日志信息。

110.1 OFC_DATAPATH_CHANNEL_CONNECT

日志内容	OpenFlow Controller datapath [STRING], channel with IP address [STRING] connected
参数解释	$1：OpenFlow实例的Datapath ID $2：和控制器连接的OpenFlow交换机的IP地址
日志等级	5
举例	OFC/5/OFC_DATAPATH_CHANNEL_CONNECT: OpenFlow Controller datapath 0x174258ae43182, channel with IP address 169.28.25.123 connected
日志说明	控制器建立了一个新的连接
处理建议	无

110.2 OFC_DATAPATH_CHANNEL_DISCONNECT

日志内容	OpenFlow Controller datapath [STRING], channel with IP address [STRING] disconnected
参数解释	$1：OpenFlow实例的Datapath ID $2：和控制器连接的OpenFlow交换机的IP地址
日志等级	5
举例	OFC/6/OFC_DATAPATH_CHANNEL_DISCONNECT:OpenFlow Controller datapath 0x174258ae43182, channel with IP address 169.28.25.123 disconnected
日志说明	OpenFlow交换机与控制器的安全通道连接断开
处理建议	无

110.3 OFC_FLOW_ADD

日志内容	App [CHAR] added flow entry: [STRING].
参数解释	$1：App ID $2：流表项内容，其中match的内容为匹配域，action的内容为动作集
日志等级	5
举例	OFC/5/OFC_FLOW_ADD：App 1 added flow entry: match(context 0x12a56, ipaddr 1.1.1.1, vxlan id 1), action(set svlan 2, set cvlan 3, modify destination mac 0-0-5, output 11).
日志说明	控制器上的App向OpenFlow交换机下发增加流表项的信息
处理建议	无

110.4 OFC_FLOW_DEL

日志内容	App [CHAR] deleted flow entry: [STRING].
参数解释	$1：App ID $2：流表项内容，其中match的内容为匹配域，action的内容为动作集
日志等级	5
举例	OFC/5/OFC_FLOW_DEL：App 1 deleted flow entry: match(context 0x12a56, ipaddr 1.1.1.1, vxlan id 1), action(set svlan 2, set cvlan 3, modify destination mac 0-0-5, output 11).
日志说明	控制器上的App向OpenFlow交换机下发删除流表项的信息
处理建议	无

110.5 OFC_FLOW_MOD

日志内容	App [CHAR] modified flow entry: [STRING].
参数解释	$1：App ID $2：流表项内容，其中match的内容为匹配域，action的内容为动作集
日志等级	5
举例	OFC/5/OFC_FLOW_MOD：App 1 modified flow entry: match(context 0x12a56, ipaddr 1.1.1.1, vxlan id 1), action(set svlan 2, set cvlan 3, modify destination mac 0-0-5, output 11).
日志说明	控制器上的App向OpenFlow交换机下发修改流表项的信息
处理建议	无

110.6 OFP_ACTIVE

日志内容	Activate openflow instance [UINT16]
参数解释	$1：实例ID
日志等级	5
举例	OFP/5/OFP_ACTIVE: Activate openflow instance 1.
日志说明	收到激活OpenFlow实例的命令
处理建议	无

110.7 OFP_ACTIVE_FAILED

日志内容	Failed to activate instance [UINT16].
参数解释	$1：实例ID
日志等级	4
举例	OFP/4/OFP_ACTIVE_FAILED: Failed to activate instance 1.
日志说明	激活OpenFlow实例失败
处理建议	无

110.8 OFP_CONNECT

日志内容	Openflow instance [UINT16], controller [CHAR] is [STRING].
参数解释	$1：实例ID $2：控制器ID $3：连接状态，显示为connected或disconnected
日志等级	5
举例	OFP/5/OFP_CONNECT: Openflow instance 1, controller 0 is connected.
日志说明	控制器连接状态变化
处理建议	无

110.9 OFP_FAIL_OPEN

日志内容	Openflow instance [UINT16] is in fail [STRING] mode.
参数解释	$1：实例ID $2：连接中断模式，显示为secure或standalone
日志等级	5
举例	OFP/5/OFP_FAIL_OPEN: Openflow instance 1 is in fail secure mode.
日志说明	实例激活后无法连接控制器或者从所有控制器断开，显示连接中断模式
处理建议	无

110.10 OFP_FLOW_ADD

日志内容	Openflow instance [UINT16] controller [CHAR]: add flow entry [UINT32], xid 0x[HEX], cookie 0x[HEX], table id [CHAR].
参数解释	$1：实例ID $2：控制器ID $3：规则ID $4：XID $5：流表项cookie $6：流表ID
日志等级	5
举例	OFP/5/OFP_FLOW_ADD: Openflow instance 1 controller 0: add flow entry 1, xid 0x1, cookie 0x0, table id 0.
日志说明	收到修改流表信息（增加操作）并通过报文检查。即将添加流表项
处理建议	无

110.11 OFP_FLOW_ADD_DUP

日志内容	Openflow instance [UINT16] controller [CHAR]: add duplicate flow entry [UINT32], xid 0x[HEX], cookie 0x[HEX], table id [CHAR].
参数解释	$1：实例ID $2：控制器ID $3：规则ID $4：XID $5：Cookie $6：流表ID
日志等级	5
举例	OFP/5/OFP_FLOW_ADD_DUP: Openflow instance 1 controller 0: add duplicate flow entry 1, xid 0x1, cookie 0x1, table id 0.
日志说明	表项重复添加
处理建议	无

110.12 OFP_FLOW_ADD_FAILED

日志内容	Openflow instance [UINT16] controller [CHAR]: failed to add flow entry [UINT32], table id [CHAR].
参数解释	$1：实例ID $2：控制器ID $3：规则ID $4：流表ID
日志等级	4
举例	OFP/4/OFP_FLOW_ADD_FAILED: Openflow instance 1 controller 0: failed to add flow entry 1, table id 0.
日志说明	添加流表项失败
处理建议	无

110.13 OFP_FLOW_ADD_TABLE_MISS

日志内容	Openflow instance [UINT16] controller [CHAR]: add table miss flow entry, xid 0x[HEX], cookie 0x[HEX], table id [CHAR].
参数解释	$1：实例ID $2：控制器ID $3：XID $4：流表项cookie $5：流表ID
日志等级	5
举例	OFP/5/OFP_FLOW_ADD_TABLE_MISS: Openflow instance 1 controller 0: add table miss flow entry, xid 0x1, cookie 0x0, table id 0.
日志说明	收到修改流表信息（增加操作）并通过报文检查。即将添加miss规则
处理建议	无

110.14 OFP_FLOW_ADD_TABLE_MISS_FAILED

日志内容	Openflow instance [UINT16] controller [CHAR]: failed to add table miss flow entry, table id [CHAR].
参数解释	$1：实例ID $2：控制器ID $3：流表ID
日志等级	4
举例	OFP/4/OFP_FLOW_ADD_TABLE_MISS_FAILED: Openflow instance 1 controller 0: failed to add table miss flow entry, table id 0.
日志说明	添加miss规则失败
处理建议	无

110.15 OFP_FLOW_DEL

日志内容	Openflow instance [UINT16] controller [CHAR]: delete flow entry, xid 0x[HEX], cookie 0x[HEX], table id [STRING].
参数解释	$1：实例ID $2：控制器ID $3：XID $4：流表项cookie $5：流表ID
日志等级	5
举例	OFP/5/OFP_FLOW_DEL: Openflow instance 1 controller 0: delete flow entry, xid 0x1, cookie 0x0, table id 0.
日志说明	收到修改流表信息（删除操作）并通过报文检查。即将删除对应的流表项
处理建议	无

110.16 OFP_FLOW_DEL_TABLE_MISS

日志内容	Openflow instance [UINT16] controller [CHAR]: delete table miss flow entry, xid 0x[HEX], cookie 0x[HEX], table id [STRING].
参数解释	$1：实例ID $2：控制器ID $3：XID $4：流表项cookie $5：流表ID
日志等级	5
举例	OFP/5/OFP_FLOW_DEL_TABLE_MISS: Openflow instance 1 controller 0: delete table miss flow entry, xid 0x1, cookie 0x0, table id 0.
日志说明	收到修改流表信息（删除操作）并通过报文检查。即将删除对应的miss规则
处理建议	无

110.17 OFP_FLOW_DEL_TABLE_MISS_FAILED

日志内容	Openflow instance [UINT16] controller [CHAR]: failed to delete table miss flow entry, table id [STRING].
参数解释	$1：实例ID $2：控制器ID $3：流表ID
日志等级	4
举例	OFP/4/OFP_FLOW_DEL_TABLE_MISS_FAILED: Openflow instance 1 controller 0: failed to delete table miss flow entry, table id 0.
日志说明	删除miss规则失败
处理建议	无

110.18 OFP_FLOW_MOD

日志内容	Openflow instance [UINT16] controller [CHAR]: modify flow entry, xid 0x[HEX], cookie 0x[HEX], table id [CHAR].
参数解释	$1：实例ID $2：控制器ID $3：XID $4：流表项cookie $5：流表ID
日志等级	5
举例	OFP/5/OFP_FLOW_MOD: Openflow instance 1 controller 0: modify flow entry, xid 0x1, cookie 0x0, table id 0.
日志说明	收到修改流表信息（修改操作）并通过报文检查。即将修改对应的流表项
处理建议	无

110.19 OFP_FLOW_MOD_FAILED

日志内容	Openflow instance [UINT16] controller [CHAR]: failed to modify flow entry, table id [CHAR].
参数解释	$1：实例ID $2：控制器ID $3：流表ID
日志等级	4
举例	OFP/4/OFP_FLOW_MOD_FAILED: Openflow instance 1 controller 0: failed to modify flow entry, table id 0.
日志说明	修改流表项失败
处理建议	控制器重试修改操作或直接删除流表项

110.20 OFP_FLOW_MOD_TABLE_MISS

日志内容	Openflow instance [UINT16] controller [CHAR]: modify table miss flow entry, xid 0x[HEX], cookie 0x[HEX], table id [CHAR].
参数解释	$1：实例ID $2：控制器ID $3：XID $4：流表项cookie $5：流表ID
日志等级	5
举例	OFP/5/OFP_FLOW_MOD_TABLE_MISS: Openflow instance 1 controller 0: modify table miss flow entry, xid 0x1, cookie 0x0, table id 0.
日志说明	收到修改流表信息（修改操作）并通过报文检查。即将修改对应的miss规则
处理建议	无

110.21 OFP_FLOW_MOD_TABLE_MISS_FAILED

日志内容	Openflow instance [UINT16] controller [CHAR]: failed to modify table miss flow entry, table id [CHAR].
参数解释	$1：实例ID $2：控制器ID $3：流表ID
日志等级	4
举例	OFP/4/OFP_FLOW_MOD_TABLE_MISS_FAILED: Openflow instance 1 controller 0: failed to modify table miss flow entry, table id 0.
日志说明	修改miss规则失败
处理建议	控制器重试修改操作或直接删除miss规则

110.22 OFP_FLOW_RMV_GROUP

日志内容	The flow entry [UINT32] in table [CHAR] of instance [UINT16] was deleted with a group_mod message.
参数解释	$1：规则ID $2：流表ID $3：实例ID
日志等级	5
举例	OFP/5/OFP_FLOW_RMV_GROUP: The flow entry 1 in table 0 of instance 1 was deleted with a group_mod message.
日志说明	Group删除导致的表项删除
处理建议	无

110.23 OFP_FLOW_RMV_HARDTIME

日志内容	The flow entry [UINT32] in table [CHAR] of instance [UINT16] was deleted because of an hard-time expiration.
参数解释	$1：规则ID $2：流表ID $3：实例ID
日志等级	5
举例	OFP/5/OFP_FLOW_RMV_HARDTIME: The flow entry 1 in table 0 of instance 1 was deleted because of an hard-time expiration.
日志说明	Hard-time超时导致的表项删除
处理建议	无

110.24 OFP_FLOW_RMV_IDLETIME

日志内容	The flow entry [UINT32] in table [CHAR] of instance [UINT16] was deleted because of an idle-time expiration.
参数解释	$1：规则ID $2：流表ID $3：实例ID
日志等级	5
举例	OFP/5/OFP_FLOW_RMV_IDLETIME: The flow entry 1 in table 0 of instance 1 was deleted because of an idle-time expiration.
日志说明	Idle-time超时导致的表项删除
处理建议	无

110.25 OFP_FLOW_RMV_METER

日志内容	The flow entry [UINT32] in table [CHAR] of instance [UINT16] was deleted with a meter_mod message.
参数解释	$1：规则ID $2：流表ID $3：实例ID
日志等级	5
举例	OFP/5/OFP_FLOW_RMV_GROUP: The flow entry 1 in table 0 of instance1 was deleted with a meter_mod message.
日志说明	Meter删除导致的表项删除
处理建议	无

110.26 OFP_FLOW_UPDATE_FAILED

日志内容	OpenFlow instance [UINT16] table [CHAR]: failed to update or synchronize flow entry [UINT32].
参数解释	$1：实例ID $2：流表ID $3：流表项ID
日志等级	4
举例	OFP/4/OFP_FLOW_UPDATE_FAILED: OpenFlow instance 1 table 0: failed to update or synchronize flow entry 10000.
日志说明	主备倒换时，新主用主控板更新流表项失败 设备插入新接口板时，接口板同步主控板的流表项失败 IRF中主从设备倒换时，新主设备更新流表项失败 IRF中加入新成员设备时，成员设备同步主设备的流表项失败
处理建议	删除下发失败的流表项

110.27 OFP_GROUP_ADD

日志内容	Openflow instance [UINT16] controller [CHAR]: add group [STRING], xid 0x[HEX].
参数解释	$1：实例ID $2：控制器ID $3：Group表项ID $4：XID
日志等级	5
举例	OFP/5/OFP_GROUP_ADD: Openflow instance 1 controller 0: add group 1, xid 0x1.
日志说明	收到修改group表信息（增加操作）并通过报文检查。即将添加group表项
处理建议	无

110.28 OFP_GROUP_ADD_FAILED

日志内容	Openflow instance [UINT16] controller [CHAR]: failed to add group [STRING].
参数解释	$1：实例ID $2：控制器ID $3：Group表项ID
日志等级	4
举例	OFP/4/OFP_GROUP_ADD_FAILED: Openflow Instance 1 controller 0: failed to add group 1.
日志说明	添加group表项失败
处理建议	无

110.29 OFP_GROUP_DEL

日志内容	Openflow instance [UINT16] controller [CHAR]: delete group [STRING], xid [HEX].
参数解释	$1：实例ID $2：控制器ID $3：Group表项ID $4：XID
日志等级	5
举例	OFP/5/OFP_GROUP_DEL: Openflow instance 1 controller 0: delete group 1, xid 0x1.
日志说明	收到修改group表信息（删除操作）并通过报文检查。即将删除对应group表项
处理建议	无

110.30 OFP_GROUP_MOD

日志内容	Openflow instance [UINT16] controller [CHAR]: modify group [STRING], xid 0x[HEX].
参数解释	$1：实例ID $2：控制器ID $3：Group表项ID $4：XID
日志等级	5
举例	OFP/5/OFP_GROUP_MOD: Openflow instance 1 controller 0: modify group 1, xid 0x1.
日志说明	收到修改group表信息（修改操作）并通过报文检查。即将修改对应group表项
处理建议	无

110.31 OFP_GROUP_MOD_FAILED

日志内容	Openflow instance [UINT16] controller [CHAR]: failed to modify group [STRING].
参数解释	$1：实例ID $2：控制器ID $3：Group表项ID
日志等级	4
举例	OFP/4/OFP_GROUP_MOD_FAILED: Openflow instance 1 controller 0: failed to modify group 1.
日志说明	修改group表项失败
处理建议	控制器重试修改操作或直接删除group表项

110.32 OFP_METER_ADD

日志内容	Openflow instance [UINT16] controller [CHAR]: add meter [STRING], xid 0x[HEX].
参数解释	$1：实例ID $2：控制器ID $3：Meter表项ID $4：XID
日志等级	5
举例	OFP/5/OFP_METER_ADD: Openflow instance 1 controller 0: add meter 1, xid 0x1.
日志说明	收到修改meter表信息（增加操作）并通过报文检查。即将添加meter表项
处理建议	无

110.33 OFP_METER_ADD_FAILED

日志内容	Openflow instance [UINT16] controller [CHAR]: failed to add meter [STRING].
参数解释	$1：实例ID $2：控制器ID $3：Meter表项ID
日志等级	4
举例	OFP/4/OFP_METER_ADD_FAILED: Openflow Instance 1 controller 0: failed to add meter 1.
日志说明	添加meter表项失败
处理建议	无

110.34 OFP_METER_DEL

日志内容	Openflow instance [UINT16] controller [CHAR]: delete meter [STRING], xid 0x[HEX].
参数解释	$1：实例ID $2：控制器ID $3：Meter表项ID $4：XID
日志等级	5
举例	OFP/5/OFP_METER_DEL: Openflow instance 1 controller 0: delete meter 1, xid 0x1.
日志说明	收到修改meter表信息（删除操作）并通过报文检查。即将删除指定的meter表项
处理建议	无

110.35 OFP_METER_MOD

日志内容	Openflow instance [UINT16] controller [CHAR]: modify meter [STRING], xid 0x[HEX].
参数解释	$1：实例ID $2：控制器ID $3：Meter表项ID $4：XID
日志等级	5
举例	OFP/5/OFP_METER_MOD: Openflow Instance 1 controller 0: modify meter 1, xid 0x1.
日志说明	收到修改meter表信息（修改操作）并通过报文检查。即将修改指定的meter表项
处理建议	无

110.36 OFP_METER_MOD_FAILED

日志内容	Openflow instance [UINT16] controller [CHAR]: failed to modify meter [STRING].
参数解释	$1：实例ID $2：控制器ID $3：Meter表项ID
日志等级	4
举例	OFP/4/OFP_METER_MOD_FAILED: Openflow instance 1 controller 0: failed to modify meter 1.
日志说明	修改meter表项失败
处理建议	控制器重试修改操作或直接删除meter表项

110.37 OFP_MISS_RMV_GROUP

日志内容	The table-miss flow entry in table [CHAR] of instance [UINT16] was deleted with a group_mod message.
参数解释	$1：流表ID $2：实例ID
日志等级	5
举例	OFP/5/OFP_MISS_RMV_GROUP: The table-miss flow entry in table 0 of instance 1 was deleted with a group_mod message.
日志说明	Group删除导致的table-miss表项删除
处理建议	无

110.38 OFP_MISS_RMV_HARDTIME

日志内容	The table-miss flow entry in table [CHAR] of instance [UINT16] was deleted because of an hard-time expiration.
参数解释	$1：流表ID $2：实例ID
日志等级	5
举例	OFP/5/OFP_MISS_RMV_HARDTIME: The table-miss flow entry in table 0 of instance 1 was deleted because of an hard-time expiration.
日志说明	Hard-time超时导致的table-miss表项删除
处理建议	无

110.39 OFP_MISS_RMV_IDLETIME

日志内容	The table-miss flow entry in table [CHAR] of instance [UINT16] was deleted because of an idle-time expiration.
参数解释	$1：流表ID $2：实例ID
日志等级	5
举例	OFP/5/OFP_MISS_RMV_IDLETIME: The table-miss flow entry in table 0 of instance 1 was deleted because of an idle-time expiration.
日志说明	Idle-time超时导致的table-miss表项删除
处理建议	无

110.40 OFP_MISS_RMV_METER

日志内容	The table-miss flow entry in table [CHAR] of instance [UINT16] was deleted with a meter_mod message.
参数解释	$1：流表ID $2：实例ID
日志等级	5
举例	OFP/5/OFP_MISS_RMV_METER: The table-miss flow entry in table 0 of instance 1 was deleted with a meter_mod message.
日志说明	Meter删除导致的table-miss表项删除
处理建议	无

111 OPENSRC（RSYNC）

本节介绍 OPENSRC 模块输出的开源软件 RSYNC 日志信息。

111.1 同步成功

日志内容	Rsync transfer statistics(sn=[STRING]):Src files([STRING]::[STRING]) sync transfer successfully.
参数解释	$1：设备的序列号 $2：服务器的IPv4地址 $3：服务器上需要同步的文件或文件夹
日志等级	5
举例	OPENSRC/5/SYSLOG: -MDC=1; Rsync transfer statistics(sn=2013AYU0711103):Src files(1.1.1.13::test/dir1) sync transfer successfully.
日志说明	同步成功
处理建议	无

111.2 同步失败

日志内容	Rsync error(sn=[STRING]):Src files([STRING]::[STRING]) [NUMBER] files transfer failed.
参数解释	$1：设备的序列号 $2：服务器的IPv4地址 $3：服务器上需要同步的文件或文件夹 $4：传输失败的文件个数
日志等级	5
举例	OPENSRC/5/SYSLOG: -MDC=1; Rsync transfer statistics(sn=2013AYU0711103):Src files(1.1.1.13::test/dir1) 2 files transfer failed.
日志说明	从服务器同步文件失败，并记录失败的文件个数
处理建议	请根据同步错误日志信息，采取相应的措施

111.3 同步错误

日志内容	Rsync error(sn=[STRING]): [STRING].
参数解释	$1：设备的序列号 $2：出错的原因，取值为： • error starting client-server protocol：设备上的 RSYNC 进程不能正常工作，无法提供同步服务 • error in socket IO：用于同步的 Socket 出现错误 • error in file IO：读取文件系统时出现错误 • some files/attrs were not transferred (see previous errors)：部分文件/文件属性传输失败 • error allocating core memory buffers：内存申请错误 • timeout waiting for daemon connection：服务器连接超时
日志等级	5
举例	OPENSRC/5/SYSLOG: -MDC=1; Rsync error(sn=2013AYU0711103): error starting client-server protocol .
日志说明	同步失败时，提示失败的原因，方便用户定位问题
处理建议	检查各命令参数是否正确、服务器是否可达、本地磁盘是否已满、执行同步操作的用户是否具有文件的操作权限等

112 OPTMOD

本节介绍 OPTMOD 模块输出的日志信息。

112.1 BIAS_HIGH

日志内容	[STRING]: Bias current is high.
参数解释	$1：端口类型和编号
日志等级	2
举例	OPTMOD/2/BIAS_HIGH: GigabitEthernet1/0/1: Bias current is high.
日志说明	光模块的偏置电流超过上限
处理建议	1. **display transceive diagnosis interface** 命令查看当前偏置电流值是否已经超过高告警门限 2. **display transceive alarm interface** 命令查看当前是否确实有偏置电流值高的告警 3. 如果确实超过门限了，模块有问题，更换模块。

112.2 BIAS_LOW

日志内容	[STRING]: Bias current is low.
参数解释	$1：端口类型和编号
日志等级	3
举例	OPTMOD/3/BIAS_LOW: GigabitEthernet1/0/1: Bias current is low.
日志说明	光模块的偏置电流低于下限
处理建议	1. **display transceive diagnosis interface** 命令查看当前偏置电流值是否已经超过低告警门限 2. **display transceive alarm interface** 命令查看当前是否确实有偏置电流高的告警 3. 如果低于低告警门限，模块有问题，更换模块

112.3 BIAS_NORMAL

日志内容	[STRING]: Bias current is normal.
参数解释	$1：端口类型和编号
日志等级	3
举例	OPTMOD/3/BIAS_NORMAL: GigabitEthernet1/0/1: Bias current is normal.
日志说明	光模块的偏置电流恢复至正常范围
处理建议	无

112.4 CFG_ERR

日志内容	[STRING]: Transceiver type and port configuration mismatched.
参数解释	$1：端口类型和编号
日志等级	3
举例	OPTMOD/3/CFG_ERR: GigabitEthernet1/0/1: Transceiver type and port configuration mismatched.
日志说明	光模块类型与端口配置不匹配
处理建议	检查端口当前配置与光模块类型，如果确实不匹配，则更换匹配模块，或更新配置

112.5 CHKSUM_ERR

日志内容	[STRING]: Transceiver information checksum error.
参数解释	$1：端口类型和编号
日志等级	3
举例	OPTMOD/3/CHKSUM_ERR: GigabitEthernet1/0/1: Transceiver information checksum error .
日志说明	光模块寄存器信息校验失败
处理建议	更换光模块，或联系工程师解决

112.6 FIBER_SFP MODULE_INVALID

日志内容	[STRING]: This transceiver module is not compatible with the interface card. HP does not guarantee the correct operation of the transceiver module. The transceiver module will be invalidated in [UINT32] days. Please replace it with a compatible one as soon as possible.
参数解释	$1：端口类型和编号 $2：光模块失效天数
日志等级	4
举例	OPTMOD/4/FIBER_SFPMODULE_INVALID: GigabitEthernet1/0/1: This transceiver module is not compatible with the interface card. HP does not guarantee the correct operation of the transceiver module. The transceiver module will be invalidated in 3 days. Please replace it with a compatible one as soon as possible.
日志说明	光模块与接口卡不匹配
处理建议	更换光模块

112.7 FIBER_SFPMODULE_NOWINVALID

日志内容	[STRING]: This is not a supported transceiver for this platform. HP does not guarantee the normal operation or maintenance of unsupported transceivers. Please review the platform datasheet on the HP web site or contact your HP sales rep for a list of supported transceivers.
参数解释	$1：端口类型和编号
日志等级	4
举例	OPTMOD/4/FIBER_SFPMODULE_NOWINVALID: GigabitEthernet1/0/1: This is not a supported transceiver for this platform. HP does not guarantee the normal operation or maintenance of unsupported transceivers. Please review the platform datasheet on the HP web site or contact your HP sales rep for a list of supported transceivers.
日志说明	不支持该光模块
处理建议	更换光模块

112.8 IO_ERR

日志内容	[STRING]: The transceiver information I/O failed.
参数解释	$1：端口类型和编号
日志等级	3
举例	OPTMOD/3/IO_ERR: GigabitEthernet1/0/1: The transceiver information I/O failed.
日志说明	设备读取光模块寄存器信息失败
处理建议	执行**display transceive diagnosis interface**或者**display transceive alarm interface**命令，如果都显示fail，则表示光模块故障，请更换

112.9 MOD_ALM_OFF

日志内容	[STRING]: [STRING] was removed.
参数解释	$1：端口类型和编号 $2：故障类型
日志等级	3
举例	OPTMOD/3/MOD_ALM_OFF: GigabitEthernet1/0/1: Module_not_ready was removed.
日志说明	光模块的某故障被清除
处理建议	无

112.10 MOD_ALM_ON

日志内容	[STRING]: [STRING] was detected.
参数解释	$1：端口类型和编号 $2：故障类型
日志等级	3
举例	OPTMOD/3/MOD_ALM_ON: GigabitEthernet1/0/1: Module_not_ready wasdetected.
日志说明	检测到光模块一故障
处理建议	执行**display transceive alarm interface**命令，如果仍然显示Module not ready，则表示光模块有问题，请更换

112.11 MODULE_IN

日志内容	[STRING]: The transceiver is [STRING].
参数解释	$1：端口类型和编号 $2：光模块类型
日志等级	4
举例	OPTMOD/4/MODULE_IN: GigabitEthernet1/0/1: The transceiver is 1000_BASE_T_AN_SFP.
日志说明	光模块类型。当一光模块插入某端口时，设备生成此日志信息
处理建议	无

112.12 MODULE_OUT

日志内容	[STRING]: Transceiver absent.
参数解释	$1：端口类型和编号
日志等级	4
举例	OPTMOD/4/MODULE_OUT: GigabitEthernet1/0/1: The transceiver is absent.
日志说明	光模块被拔出
处理建议	无

112.13 PHONY_MODULE

日志内容	[STRING]: This transceiver is not sold by H3C. H3C does not guarantee the correct operation of the module or assume maintenance responsibility.
参数解释	$1：端口类型和编号
日志等级	4
举例	OPTMOD/4/PHONY_MODULE: GigabitEthernet1/0/1: This transceiver is not sold by H3C. H3C does not guarantee the correct operation of the module or assume maintenance responsibility.
日志说明	光模块非H3C生产
处理建议	更换光模块

112.14 RX_ALM_OFF

日志内容	[STRING]: [STRING] was removed.
参数解释	$1：端口类型和编号 $2：RX故障类型
日志等级	3
举例	OPTMOD/3/RX_ALM_OFF: GigabitEthernet1/0/1: RX_not_ready was removed.
日志说明	光模块RX故障被清除
处理建议	无

112.15 RX_ALM_ON

日志内容	[STRING]: [STRING] was detected.
参数解释	$1：端口类型和编号 $2：RX故障类型
日志等级	3
举例	OPTMOD/3/RX_ALM_ON: GigabitEthernet1/0/1: RX_not_ready was detected.
日志说明	检测到光模块RX故障
处理建议	使用**display transceive alarm interface**命令可查看到这个故障，确认是模块问题，更换模块

112.16 RX_POW_HIGH

日志内容	[STRING]: RX power is high.
参数解释	$1：端口类型和编号
日志等级	3
举例	OPTMOD/3/RX_POW_HIGH: GigabitEthernet1/0/1: RX power is high.
日志说明	光模块RX功率超过上限
处理建议	1. **display transceive diagnosis interface** 命令查看功率是否已经超过高告警门限 2. **display transceive alarm interface** 命令查看当前是否确实有功率高的告警 3. 如果确实超过门限了，模块有问题，更换模块

112.17 RX_POW_LOW

日志内容	[STRING]: RX power is low.
参数解释	$1：端口类型和编号
日志等级	3
举例	OPTMOD/3/RX_POW_LOW: GigabitEthernet1/0/1: RX power is low.
日志说明	光模块RX功率低于下限
处理建议	1. **display transceive diagnosis interface** 命令查看功率是否已经低于低告警门限 2. **display transceive alarm interface** 命令查看当前是否确实有功率低告警 3. 如果确实低于门限了，模块有问题，更换模块

112.18 RX_POW_NORMAL

日志内容	[STRING]: RX power is normal.
参数解释	$1：端口类型和编号
日志等级	3
举例	OPTMOD/3/RX_POW_NORMAL: GigabitEthernet1/0/1: RX power is normal.
日志说明	光模块RX功率恢复至正常范围
处理建议	无

112.19 TEMP_HIGH

日志内容	[STRING]: Temperature is high.
参数解释	$1：端口类型和编号
日志等级	3
举例	OPTMOD/3/TEMP_HIGH: GigabitEthernet1/0/1: Temperature is high.
日志说明	光模块温度超过上限
处理建议	检查设备风扇是否工作正常，安装风扇或更换故障风扇 检查环境温度，如果温度确实过高就调节温度 如果设备风扇正常，且环境温度正常，则模块故障，更换模块

112.20 TEMP_LOW

日志内容	[STRING]: Temperature is low.
参数解释	$1：端口类型和编号
日志等级	3
举例	OPTMOD/3/TEMP_LOW: GigabitEthernet1/0/1: Temperature is low.
日志说明	光模块温度低于下限
处理建议	检查环境温度，如果温度确实过低高就调节温度，如果环境温度正常，就是模块故障，更换模块

112.21 TEMP_NORMAL

日志内容	[STRING]: Temperature is normal.
参数解释	$1：端口类型和编号
日志等级	3
举例	OPTMOD/3/TEMP_NORMAL: GigabitEthernet1/0/1: Temperature is normal.
日志说明	光模块温度恢复至正常范围
处理建议	无

112.22 TX_ALM_OFF

日志内容	[STRING]: [STRING] was removed.
参数解释	$1：端口类型和编号 $2：TX故障类型
日志等级	3
举例	OPTMOD/3/TX_ALM_OFF: GigabitEthernet1/0/1: TX_fault was removed.
日志说明	光模块TX故障被清除
处理建议	无

112.23 TX_ALM_ON

日志内容	[STRING]: [STRING] was detected.
参数解释	$1：端口类型和编号 $2：TX故障类型
日志等级	3
举例	OPTMOD/3/TX_ALM_ON: GigabitEthernet1/0/1: TX_fault was detected.
日志说明	检测到光模块TX故障
处理建议	使用**display transceive alarm interface**命令可查看到这个故障，确认是模块问题，更换模块

112.24 TX_POW_HIGH

日志内容	[STRING]: TX power is high.
参数解释	$1：端口类型和编号
日志等级	2
举例	OPTMOD/2/TX_POW_HIGH: GigabitEthernet1/0/1: TX power is high.
日志说明	光模块TX功率超过上限
处理建议	1. **display transceive diagnosis interface** 命令查看功率是否已经超过高告警门限 2. **display transceive alarm interface** 命令查看当前是否确实有功率高告警 3. 如果确实超过门限了，模块有问题，更换模块

112.25 TX_POW_LOW

日志内容	[STRING]: TX power is low.
参数解释	$1：端口类型和编号
日志等级	3
举例	OPTMOD/3/TX_POW_LOW: GigabitEthernet1/0/1: TX power is low.
日志说明	光模块TX功率低于下限
处理建议	1. **display transceive diagnosis interface** 命令查看功率是否已经低于低告警门限 2. **display transceive alarm interface** 命令查看当前是否确实有功率低告警 3. 如果确实低于门限了，模块有问题，更换模块

112.26 TX_POW_NORMAL

日志内容	[STRING]: TX power is normal.
参数解释	$1：端口类型和编号
日志等级	3
举例	OPTMOD/3/TX_POW_NORMAL: GigabitEthernet1/0/1: TX power is normal.
日志说明	光模块TX功率恢复至正常范围
处理建议	无

112.27 TYPE_ERR

日志内容	[STRING]: The transceiver type is not supported by port hardware.
参数解释	$1：端口类型和编号
日志等级	3
举例	OPTMOD/3/TYPE_ERR: GigabitEthernet1/0/1: The transceiver type is not supported by port hardware.
日志说明	端口硬件不支持光模块类型
处理建议	更换光模块

112.28 VOLT_HIGH

日志内容	[STRING]: Voltage is high.
参数解释	$1：端口类型和编号
日志等级	3
举例	OPTMOD/3/VOLT_HIGH: GigabitEthernet1/0/1: Voltage is high.
日志说明	光模块电压超过上限
处理建议	1. **display transceive diagnosis interface** 命令查看电压是否已经超过高告警门限 2. **display transceive alarm interface** 命令查看当前是否确实有电压高告警 3. 如果确实超过门限了，模块有问题，更换模块

112.29 VOLT_LOW

日志内容	[STRING]: Voltage is low.
参数解释	$1：端口类型和编号
日志等级	3
举例	OPTMOD/3/VOLT_LOW: GigabitEthernet1/0/1: Voltage is low.
日志说明	光模块电压低于下限
处理建议	1. **display transceive diagnosis interface** 命令查看电压是否已经超过低告警门限 2. **display transceive alarm interface** 命令查看当前是否确实有电压低告警 3. 如果确实超过门限了，模块有问题，更换模块

112.30 VOLT_NORMAL

日志内容	[STRING]: Voltage is normal.
参数解释	$1：端口类型和编号
日志等级	3
举例	OPTMOD/3/VOLT_NORMAL: GigabitEthernet1/0/1: Voltage is normal!
日志说明	光模块电压恢复至正常范围
处理建议	无

113 OSPF

本节介绍 OSPF 模块输出的日志信息。

113.1 OSPF_DUP_RTRID_NBR

日志内容	OSPF [UINT16] Duplicate router ID [STRING] on interface [STRING], sourced from IP address [IPADDR].
参数解释	$1：OSPF进程ID $2：路由器ID $3：接口名称 $4：IP地址
日志等级	4
举例	OSPF/4/OSPF_DUP_RTRID_NBR: OSPF 1 Duplicate router ID 11.11.11.11 on interface GigabitEthernet0/0/3, sourced from IP address 11.2.2.2.
日志说明	检测到两台直连设备配置了相同的路由器ID
处理建议	修改其中一台设备的路由器ID，并使用**reset ospf process**命令使新的路由器ID生效

113.2 OSPF_IP_CONFLICT_INTRA

日志内容	OSPF [UINT16] Received newer self-originated network-LSAs. Possible conflict of IP address [IPADDR] in area [STRING] on interface [STRING].
参数解释	$1：OSPF进程ID $2：IP地址 $3：OSPF区域ID $4：接口名称
日志等级	6
举例	OSPF/6/OSPF_IP_CONFLICT_INTRA: OSPF 1 Received newer self-originated network-LSAs. Possible conflict of IP address 11.1.1.1 in area 0.0.0.1 on interface GigabitEthernet0/0/3.
日志说明	同一OSPF区域内两台设备的接口上可能配置了相同的主IP地址，其中至少一台设备是DR
处理建议	在确保同一OSPF区域内不存在Router ID冲突的情况下，修改IP地址配置

113.3 OSPF_LAST_NBR_DOWN

日志内容	OSPF [UINT32] Last neighbor down event: Router ID: [STRING] Local address: [STRING] Remote address: [STRING] Reason: [STRING]
参数解释	$1：OSPF进程ID $2：路由器ID $3：本地IP地址 $4：邻居IP地址 $5：原因
日志等级	6
举例	OSPF/6/OSPF_LAST_NBR_DOWN: OSPF 1 Last neighbor down event: Router ID: 2.2.2.2 Local address: 10.1.1.1 Remote address: 10.1.1.2 Reason: Dead Interval timer expired.
日志说明	最近一次OSPF邻居down事件
处理建议	检查OSPF邻居down事件的原因，根据具体原因进行处理： • 如果是配置相关命令导致邻居 down，如接口参数变化等，请检查配置是否正确 • 如果是超时邻居 down，检查网络状况或者配置的超时时间是否合理 • 如果是 BFD 检测导致的邻居 down，检查网络状况或者 BFD 检测时间配置是否合理 • 如果是接口状态变化导致的邻居 down，检查网络连接情况

113.4 OSPF_MEM_ALERT

日志内容	OSPF Process received system memory alert [STRING] event.
参数解释	$1：内存告警类型
日志等级	5
举例	OSPF/5/OSPF_MEM_ALERT: OSPF Process received system memory alert start event.
日志说明	OSPF模块收到内存告警信息
处理建议	当超过各级内存门限时，检查系统内存，对占用内存较多的模块进行调整，尽量释放可用内存

113.5 OSPF_NBR_CHG

日志内容	OSPF [UINT32] Neighbor [STRING] ([STRING]) changed from [STRING] to [STRING]
参数解释	$1：OSPF进程ID $2：邻居路由器ID $3：接口名称 $4：旧邻接状态 $5：新邻接状态
日志等级	3
举例	OSPF/3/OSPF_NBR_CHG: OSPF 1 Neighbor 2.2.2.2 (Vlan-interface100) changed from Full to Down.
日志说明	接口OSPF邻接状态改变
处理建议	当某接口与邻居邻接状态从Full变为其他状态时，检查OSPF配置正确性和网络连通性

113.6 OSPF_RT_LMT

日志内容	OSPF [UINT32] route limit reached.
参数解释	$1：OSPF进程ID
日志等级	4
举例	OSPF/4/OSPF_RT_LMT: OSPF 1 route limit reached.
日志说明	OSPF进程的路由数达到了上限值
处理建议	检查是否受到攻击或者减少网络路由数

113.7 OSPF_RTRID_CHG

日志内容	OSPF [UINT32] New router ID elected, please restart OSPF if you want to make the new router ID take effect.
参数解释	$1：OSPF进程ID
日志等级	5
举例	OSPF/5/OSPF_RTRID_CHG: OSPF 1 New router ID elected, please restart OSPF if you want to make the new router ID take effect.
日志说明	用户更改了router ID或者是使用的接口IP发生变化而改变了OSPF路由器ID。需要手动重启OSPF使新的路由器ID生效
处理建议	使用**reset ospf process**命令使新的路由器ID生效

113.8 OSPF_RTRID_CONFLICT_INTER

日志内容	OSPF [UINT16] Received newer self-originated ase-LSAs. Possible conflict of router ID [STRING].
参数解释	$1：OSPF进程ID $2：路由器ID
日志等级	6
举例	OSPF/6/OSPF_RTRID_CONFILICT_INTER: OSPF 1 Received newer self-originated ase-LSAs. Possible conflict of router ID 11.11.11.11.
日志说明	同一OSPF域内非直连的两台设备可能配置了相同的路由器ID，其中一台设备为ASBR
处理建议	修改其中一台设备的路由器ID，并使用**reset ospf process**命令使新的路由器ID生效

113.9 OSPF_RTRID_CONFLICT_INTRA

日志内容	OSPF [UINT16] Received newer self-originated router-LSAs. Possible conflict of router ID [STRING] in area [STRING].
参数解释	$1：OSPF进程ID $2：路由器ID $3：OSPF区域ID
日志等级	4
举例	OSPF/4/OSPF_RTRID_CONFLICT_INTRA: OSPF 1 Received newer self-originated router-LSAs. Possible conflict of router ID 11.11.11.11 in area 0.0.0.1.
日志说明	同一OSPF区域内非直连的两台设备可能配置了相同的路由器ID
处理建议	修改其中一台设备的路由器ID，并使用**reset ospf process**命令使新的路由器ID生效

113.10 OSPF_VLINKID_CHG

日志内容	OSPF [UINT32] Router ID changed, reconfigure Vlink on peer
参数解释	$1：OSPF进程ID
日志等级	5
举例	OSPF/5/OSPF_VLINKID_CHG:OSPF 1 Router ID changed, reconfigure Vlink on peer
日志说明	新的OSPF路由器ID生效。需要根据新的路由器ID检查并修改对端路由器的虚连接配置
处理建议	根据新的路由器ID检查并修改对端路由器的虚连接配置

114 OSPFV3

本节介绍 OSPFv3 模块输出的日志信息。

114.1 OSPFV3_LAST_NBR_DOWN

日志内容	OSPFv3 [UINT32] Last neighbor down event: Router ID: [STRING] Local interface ID: [UINT32] Remote interface ID: [UINT32] Reason: [STRING].
参数解释	$1：OSPFv3进程ID $2：路由器ID $3：本地接口ID $4：对端接口ID $5：原因
日志等级	6
举例	OSPFV3/6/OSPFV3_LAST_NBR_DOWN: OSPFv3 1 Last neighbor down event: Router ID: 2.2.2.2 Local interface ID: 1111 Remote interface ID: 2222 Reason: Dead Interval timer expired.
日志说明	最近一次OSPFv3邻居down事件
处理建议	检查OSPFV3邻居down事件的原因，根据具体原因进行处理： • 如果是配置相关命令导致邻居 down，如接口参数变化等，请检查配置是否正确 • 如果是超时邻居 down，检查网络状况或者配置的超时时间是否合理 • 如果是 BFD 检测导致的邻居 down，检查网络状况或者 BFD 检测时间配置是否合理 • 如果是接口状态变化导致的邻居 down，检查网络连接情况

114.2 OSPFV3_MEM_ALERT

日志内容	OSPFV3 Process received system memory alert [STRING] event.
参数解释	$1：内存告警类型
日志等级	5
举例	OSPFV3/5/OSPFV3_MEM_ALERT: OSPFV3 Process received system memory alert start event.
日志说明	OSPFv3模块收到内存告警信息
处理建议	当超过各级内存门限时，检查系统内存占用情况，对占用内存较多的模块进行调整，尽量释放可用内存

114.3 OSPFV3_NBR_CHG

日志内容	OSPFv3 [UINT32] Neighbor [STRING] ([STRING]) received [STRING] and its state changed from [STRING] to [STRING].
参数解释	$1：OSPFv3进程ID $2：邻居路由器ID $3：接口名称 $4：邻居事件 $5：旧邻接状态 $6：新邻接状态
日志等级	3
举例	OSPFV3/3/OSPFV3_NBR_CHG: OSPFv3 1 Neighbor 2.2.2.2 (Vlan100) received 1-Way and its state changed from Full to Init.
日志说明	接口OSPFv3邻接状态改变
处理建议	当某接口与邻居邻接状态从Full变为其他状态时，检查OSPFv3配置正确性和网络连通性

114.4 OSPFV3_RT_LMT

日志内容	OSPFv3 [UINT32] route limit reached.
参数解释	$1：OSPFv3进程ID
日志等级	3
举例	OSPFV3/3/OSPFV3_RT_LMT:OSPFv3 1 route limit reached.
日志说明	OSPFv3进程的路由数达到了上限值
处理建议	检查是否受到攻击或者减少网络路由数

115 PBB

本节介绍 PBB 模块输出的日志信息。

115.1 PBB_JOINAGG_WARNING

日志内容	Because the aggregate interface [STRING] has been configured with PBB, assigning the interface [STRING] that does not support PBB to the aggregation group will cause incorrect processing.
参数解释	$1：聚合组名称 $2：接口名称
日志等级	4
举例	PBB/4/PBB_JOINAGG_WARNING: Because the aggregate interface Bridge-Aggregation1 has been configured with PBB, assigning the interface Ten-GigabitEthernet9/0/30 that does not support PBB to the aggregation group will cause incorrect processing.
日志说明	将不支持PBB的接口加入已经配置了PBB的聚合组会引发处理错误，配置为PBB实例上行口的聚合组的成员端口都需支持PBB
处理建议	将该接口从聚合组中删除

116 PBR

本节介绍 PBR 模块输出的日志信息。

116.1 PBR_HARDWARE_BIND_ERROR

日志内容	Failed to apply the policy [STRING] to interface [STRING] because of [STRING]..
参数解释	$1：策略名 $2：接口名 $3：硬件处理失败的原因，包括以下三种类型： • insufficient hardware resources：资源不足 • unsupported operations：系统不支持该操作 • insufficient hardware resources and unsupported operations：硬件资源不足且系统不支硬件持
日志等级	4
举例	PBR/4/PBR_HARDWARE_BIND_ERROR: Failed to apply the policy abc to interface GigabitEthernet1/0/1 because of unsupported operations.
日志说明	接口配置单播策略路由发生错误
处理建议	根据错误原因修改策略中的配置

116.2 PBR_HARDWARE_ERROR

日志内容	Failed to update policy [STRING] due to [STRING].
参数解释	$1：策略名 $2：硬件处理失败的原因，包括以下三种类型： • insufficient hardware resources：资源不足 • unsupported operations：系统不支持该操作 • insufficient hardware resources and unsupported operations：硬件资源不足且系统不支硬件持
日志等级	4
举例	PBR/4/PBR_HARDWARE_ERROR: Failed to update policy aaa due to insufficient hardware resources and not supported operations.
日志说明	更新单播策略路由配置失败
处理建议	根据失败原因修改策略中的配置

116.3 PBR_NEXTHOP_CHANGE

日志内容	The link to next hop [IPADDR] of policy [STRING] (node ID: [STRING], VPN instance: [STRING]) changed due to [STRING].
参数解释	$1：下一跳地址 $2：策略名称 $3：节点名称 $4：VPN名称，如果是公网，则取值为Public network $5：下一跳发生变化的原因，包括以下五种类型： • FIB change ：FIB 信息发生变化 • reachable status ：下一跳地址从不可达到可达 • unreachable status ：下一跳地址从可达到不可达 • direct change ：配置下一跳动作带不带 **direct** 参数时直连下一跳路由发生变化 • track change ：track 项状态发生变化
日志等级	4
举例	PBR/4/PBR_NEXTHOP_CHANGE: The link to next hop 1.1.1.1 of policy a (node ID: 0, VPN instance: Public network) changed due to FIB change..
日志说明	公网中的节点编号为0的策略路由a，由于FIB表发生改变下一跳链路发生变化
处理建议	提示用户具体的下一跳链路发生改变，方便用户定位问题并解决问题

117 PCE

本节介绍 PCE 模块输出的日志信息

117.1 PCE_PCEP_SESSION_CHG

日志内容	Session ([STRING], [STRING]) is [STRING].
参数解释	$1：会话对端IP地址 $2：会话所在VPN实例名称，如果无法获取则显示为unknown $3：会话的状态变更，up或者down，如果状态变更为down，则一并显示会话down的原因
日志等级	3
举例	PCE/3/PCE_PCEP_SESSION_CHG: Session (22.22.22.2, public instance) is up. PCE/3/PCE_PCEP_SESSION_CHG: Session (22.22.22.2, public instance) is down (dead timer expired).

日志说明	显示会话的状态变化以及会话down的原因
	down 的原因可能包括：
	• TCP connection down：TCP 连接断开
	• received a close message：在如下五种情况下会收到对端的关闭消息
	  ○ No explanation provided：未提供详细原因（当会话空闲超过 3 分钟，会以此种形式关闭会话）
	  ○ DeadTimer expired：deadtimer 定时器超时
	  ○ Reception of a malformed PCEP message：消息格式错误或者收到畸形消息
	  ○ Reception of an unacceptable number of unknown requests/replies：收到超过限制的未知计算请求/计算应答
	  ○ Reception of an unacceptable number of unrecognized PCEP messages：收到超过限制的未知消息
	• reception of a malformed PCEP message：收到非法消息
	• internal error：内部错误
	• memory in critical state：内存不足
	• dead timer expired：会话超时
	• process deactivated：PCE 进程去激活
	• remote peer unavailable/untriggered：对等体失效
	• reception of an unacceptable number of unrecognized PCEP messages：收到超过限制的未知消息
	• reception of an unacceptable number of unknown requests/replies：收到超过限制的未知计算请求/计算应答
	• PCE address changed：PCE 地址变化
	• initialization failed：初始化失败

处理建议	如果会话的状态变更为up，不需要进行其它操作 如果会话的状态变更为down，请根据提示原因检查网络环境或者配置

118 PEX（IRF3.1）

本节介绍 IRF3.1 PEX（Port Extender）模块输出的日志信息。

118.1 PEX_AUTOCONFIG_BAGG_ASSIGNMEMBER

日志内容	[STRING] was assigned to [STRING].
参数解释	$1：物理接口名称 $2：聚合接口名称
日志等级	5
举例	PEX/5/PEX_AUTOCONFIG_BAGG_ASSIGNMEMBER: GigabitEthernet 1/2/0/1 was assigned to Bridge-Aggregation10.
日志说明	父设备运行IRF3.1系统自动配置功能时，自动将连接PEX的物理接口添加到作为级联接口的聚合组中
处理建议	不需要处理

118.2 PEX_AUTOCONFIG_BAGG_CREATE

日志内容	[STRING] was created by the PEX auto-config feature.
参数解释	$1：聚合接口名称
日志等级	5
举例	PEX/5/PEX_AUTOCONFIG_BAGG_CREATE: Bridge-Aggregation10 was created by the PEX auto-config feature.
日志说明	父设备运行IRF3.1系统自动配置功能时，自动创建聚合接口用来作级联接口
处理建议	不需要处理

118.3 PEX_AUTOCONFIG_BAGG_NORESOURCE

日志内容	Not enough resources to create a Layer 2 aggregate interface.
参数解释	无
日志等级	5
举例	PEX/5/PEX_AUTOCONFIG_BAGG_NORESOURCE: Not enough resources to create a Layer 2 aggregate interface.
日志说明	父设备运行IRF3.1系统自动配置功能时，没有空闲资源创建二层聚合接口
处理建议	删除设备上不需要使用的聚合接口，释放资源

118.4 PEX_AUTOCONFIG_BAGG_REMOVEMEMBER

日志内容	[STRING] was removed from [STRING].
参数解释	$1：物理接口名称 $2：聚合接口名称
日志等级	5
举例	PEX/5/PEX_AUTOCONFIG_BAGG_REMOVEMEMBER: GigabitEthernet 1/2/0/1 was removed from Bridge-Aggregation10.
日志说明	父设备运行IRF3.1系统自动配置功能时，会自动将连接PEX的物理接口添加到作为级联接口的聚合组中。添加端口时，如果检查到该物理接口已经被添加到其他级联接口的聚合组中，则先将该物理接口从其他级联接口的聚合组中删除
处理建议	不需要处理

118.5 PEX_AUTOCONFIG_CAPABILITY_ENABLE

日志内容	PEX connection capability was enabled on [STRING] and the interface was assigned to PEX group [UINT32].
参数解释	$1：聚合接口名称 $2：PEX组编号
日志等级	5
举例	PEX/5/PEX_AUTOCONFIG_CAPABILITY_ENABLE: PEX connection capability was enabled on Bridge-Aggregation 10 and the interface was assigned to PEX group 1.
日志说明	父设备运行IRF3.1系统自动配置功能时，自动开启连接PEX的聚合接口的PEX连接能力，并将该接口加入PEX组中
处理建议	不需要处理

118.6 PEX_AUTOCONFIG_CASCADELIMIT

日志内容	Failed to assign cascade port [STRING] to PEX group [UINT32]. Reason: Maximum number of cascade ports already reached in the PEX group.
参数解释	$1：聚合接口名称 $2：PEX组编号
日志等级	5
举例	PEX/5/PEX_AUTOCONFIG_CASCADELIMIT: Failed to assign cascade port Bridge-Aggregation10 to PEX group1. Reason: Maximum number of cascade ports already reached in the PEX group.
日志说明	父设备运行IRF3.1系统自动配置功能时，检测到PEX组中级联接口的数目已达到上限，无法再将聚合接口加入该PEX组中
处理建议	删除该组中空闲的级联接口，释放资源

118.7 PEX_AUTOCONFIG_CONNECTION_ERROR

日志内容	A PEX connected to more than one upper-tier PEXs.
参数解释	无
日志等级	5
举例	PEX/5/PEX_AUTOCONFIG_CONNECTION_ERROR: A PEX connected to more than one upper-tier PEXs.
日志说明	父设备运行IRF3.1系统自动配置功能时，检测到PEX和两台或两台以上上级PEX之间存在物理连接
处理建议	PEX上行链路只能连接到同一台上级PEX，否则可能导致PEX无法上线或上线后功能运行异常。请检查并修改组网连接

118.8 PEX_AUTOCONFIG_DIFFGROUPNUMBER

日志内容	[STRING] failed to join in PEX group [UINT32]. Reason: Its upper-tier PEX was in PEX group [UINT32]. Please make sure they are in the same PEX group.
参数解释	$1：聚合接口名称 $2：PEX组编号 $3：PEX组编号
日志等级	5
举例	PEX/5/PEX_AUTOCONFIG_DIFFGROUPNUMBER: Bridge-Aggregation10 failed to join in PEX group 1. Reason: Its upper-tier PEX was in PEX group 2. Please make sure they are in the same PEX group.
日志说明	父设备运行IRF3.1系统自动配置功能，开启PEX二层聚合接口或PEX三层聚合接口连接PEX的能力并将接口加入PEX组时，所指定的PEX组编号与上级PEX所在PEX组编号不同。
处理建议	下级PEX只能与上级PEX加入同一PEX组，请修改配置

118.9 PEX_AUTOCONFIG_DYNAMICBAGG_STP

日志内容	[STRING] was automatically set to dynamic aggregation mode and configured as an STP edge port.
参数解释	$1：二层聚合接口名称
日志等级	5
举例	PEX/5/PEX_AUTOCONFIG_DYNAMICBAGG_STP: Bridge-Aggregation10 was automatically set to dynamic aggregation mode and configured as an STP edge port.
日志说明	父设备运行IRF3.1系统自动配置功能时，将级联接口自动配置为动态聚合模式并且配置为STP边缘端口。
处理建议	不需要处理

118.10 PEX_AUTOCONFIG_GROUP_CREATE

日志内容	PEX group [UINT32] was created.
参数解释	$1：PEX组编号
日志等级	5
举例	PEX/5/PEX_AUTOCONFIG_GROUP_CREATE: PEX group 1 was created.
日志说明	父设备运行IRF3.1系统自动配置功能时，自动创建PEX组
处理建议	不需要处理

118.11 PEX_AUTOCONFIG_NONUMBERRESOURCE

日志内容	形式一： No virtual slot numbers are available. 形式二： No virtual chassis numbers are available.
参数解释	无
日志等级	5
举例	PEX/5/PEX_AUTOCONFIG_NONUMBERRESOURCE: No virtual slot numbers are available.
日志说明	父设备运行IRF3.1系统自动配置功能时，没有虚拟槽位号/虚拟框号资源用来分配
处理建议	删除空闲级联接口或在空闲级联接口上取消分配虚拟槽位号/虚拟框号的配置，释放资源

118.12 PEX_AUTOCONFIG_NOT_CASCADEPORT

日志内容	[STRING] was already assigned to [STRING], which is an aggregate interface not enabled with PEX connection capability. Please remove [STRING] from [STRING] or use another physical interface to connect the PEX.
参数解释	$1：物理接口名称 $2：聚合接口名称 $3：物理接口名称 $4：聚合接口名称
日志等级	5
举例	PEX/5/PEX_AUTOCONFIG_NOT_CASCADEPORT: GigabitEthernet 1/2/0/1 was already assigned to Bridge-Aggregation10, which is an aggregate interface not enabled with PEX connection capability. Please remove GigabitEthernet 1/2/0/1 from Bridge-Aggregation10 or use another physical interface to connect the PEX.
日志说明	父设备运行IRF3.1系统自动配置功能时，检测到连接PEX的物理接口已经加入到聚合组中，但对应聚合接口没有开启连接PEX的能力
处理建议	将物理接口从聚合组中退出或更换其他物理接口

118.13 PEX_AUTOCONFIG_NUMBER_ASSIGN

日志内容	形式一： Virtual slot number [UINT32] was assigned on [STRING]. 形式二： Virtual chassis number [UINT32] was assigned on [STRING].
参数解释	形式一： $1：虚拟槽位号 $2：聚合接口名称 形式二： $1：虚拟框号 $2：聚合接口名称
日志等级	5
举例	PEX/5/PEX_AUTOCONFIG_NUMBER_ASSIGN: Virtual slot number 100 was assigned on Bridge-Aggregation 10.
日志说明	父设备运行IRF3.1系统自动配置功能时，在连接PEX的聚合接口上，自动为PEX分配虚拟槽位号/虚拟框号
处理建议	不需要处理

118.14 PEX_LLDP_DISCOVER

日志内容	Discover peer device on interface [STRING]: MAC=STRING, priority=UINT32.
参数解释	$1：接口名称 $2：对端MAC地址 $3：PEX设备上行口的优先级
日志等级	5
举例	PEX/5/PEX_LLDP_DISCOVER: Discover peer device on interface Ten-GigabitEthernet1/0/1: MAC=20f4-9cb6-0100, priority=0.
日志说明	父设备或PEX设备通过LLDP协议发现对端
处理建议	正常状态，无需任何处理

118.15 PEX_MEMBERID_EXCEED

日志内容	To use the IRF fabric connected to interface [STRING] as a PEX, the IRF member ID must be in the range of 1 to 4.
参数解释	$1：接口名称
日志等级	4
举例	PEX/4/PEX_MEMBERID_EXCEED: To use the IRF fabric connected to interface Bridge-Aggregation1 as a PEX, the IRF member ID must be in the range of 1 to 4.
日志说明	设备作为PEX加入IRF3.1系统时，PEX设备的IRF成员编号必须在1~4范围以内
处理建议	请检查PEX设备的IRF成员编号是否在1～4范围之内。如果不是，用户可登录PEX设备，用**irf member renumber**命令修改PEX设备的成员编号

118.16 PEX_PECSP_OPEN_RCVD

日志内容	Received a CSP Open message on interface [STRING].
参数解释	$1：接口名称
日志等级	5
举例	PEX/5/PEX_PECSP_OPEN_RCVD: Received a CSP Open message on interface Bridge-Aggregation1.
日志说明	接口收到PE CSP协议的OPEN报文，表示对端请求建立连接。如果双方均能在发送请求后60秒内接收到对端回复的OPEN报文，则父设备和PEX之间的连接建立成功
处理建议	正常状态，无需任何处理

118.17 PEX_PECSP_OPEN_SEND

日志内容	Sent a CSP Open message on interface [STRING].
参数解释	$1：接口名称
日志等级	5
举例	PEX/5/PEX_PECSP_OPEN_SEND: Sent a CSP Open message on interface Bridge-Aggregation1.
日志说明	父设备级联口或PEX设备上行口发送PE CSP协议的OPEN报文，表示请求与对方建立连接。如果双方均能在发送请求后60秒内接收到对端回复的OPEN报文，则父设备和PEX之间的连接建立成功
处理建议	正常状态，无需任何处理

118.18 PEX_PECSP_TIMEOUT

日志内容	PE CSP timed out on interface [STRING].
参数解释	$1：接口名称
日志等级	4
举例	PEX/4/PEX_PECSP_TIMEOUT: PE CSP timed out on interface Bridge-Aggregation1.
日志说明	PE CSP协议超时，PEX设备和父设备无法建立连接
处理建议	请检查父设备和PEX之间链路和IRF3.1相关配置

119 PEX（IRF3）

本节介绍 PEX（Port Extender）模块输出的日志信息。

119.1 PEX_ASSOCIATEID_MISMATCHING

日志内容	The associated ID of PEX port [UNIT32] is [UNIT32] on the parent fabric, but the PEX connected to the port has obtained ID [UNIT32].
参数解释	$1：PEX端口编号 $2：父设备侧配置的虚拟槽位号或虚拟框号 $3：实际连接的邻居PEX设备虚拟槽位号或虚拟框号
日志等级	5
举例	PEX/5/PEX_ASSOCIATEID_MISMATCHING: The associated ID of PEX port 1 is 100 on the parent fabric, but the PEX connected to the port has obtained ID 101.
日志说明	用户配置的虚拟槽位号/虚拟框号与实际连接的PEX设备虚拟槽位号/虚拟框号不一致
处理建议	请检查组网连接

119.2 PEX_CONFIG_ERROR

日志内容	PEX port [UINT32] discarded a REGISTER request received from [STRING] through interface [STRING]. Reason: The PEX was not assigned an ID, or the PEX was assigned an ID equal to or greater than the maximum value ([UINT32]).
参数解释	$1：PEX端口ID $2：PEX产品型号 $3：PEX物理端口名称 $4：指定PEX类型的设备允许配置的最大虚拟槽位号或虚拟框号
日志等级	4
举例	PEX/4/PEX_CONFIG_ERROR: PEX port 1 discarded a REGISTER request received from PEX-S5120HI-S5500HI through interface Ten-GigabitEthernet10/0/31. Reason: The PEX was not assigned an ID, or the PEX was assigned an ID equal to or greater than the maximum value 130.
日志说明	PEX设备启动前必须通过**associate**命令配置虚拟槽位号/虚拟框号 PEX不同型号的产品允许分配的虚拟槽位号/虚拟框号有最大值限制 XX型号的连接到XX端口的PEX没有配置虚拟槽位号/虚拟框号或者配置的虚拟槽位号/虚拟框号超过了产品允许的最大范围
处理建议	通过**associate**命令将分配给PEX的虚拟槽位号/虚拟框号修改到正确的虚拟槽位号/虚拟框号范围内

119.3 PEX_CONNECTION_ERROR

日志内容	PEX port [UINT32] discarded a REGISTER request received from [STRING] through interface [STRING]. Reason: Another PEX has been registered on the PEX port.
参数解释	$1：PEX端口ID $2：PEX产品型号 $3：PEX物理端口名称
日志等级	4
举例	PEX/4/PEX_CONNECTION_ERROR: PEX port 1 discarded a REGISTER request received from PEX-S5120HI-S5500HI through interface Ten-GigabitEthernet10/0/31. Reason: Another PEX has been registered on the PEX port.
日志说明	每个PEX端口只允许加入一个PEX设备，如果有一个PEX已经启动，其他的PEX连接到该端口上属于配置错误，丢弃请求
处理建议	检查连线是否错误，请确认同一个PEX端口下只连接了一个PEX设备

119.4 PEX_FORBID_STACK

日志内容	Can't connect PEXs [UNIT32] and [UNIT32]: The PEX ports to which the PEXs belong are in different PEX port groups.
参数解释	$1：PEX设备的虚拟槽位号或虚拟框号 $2：PEX设备的虚拟槽位号或虚拟框号
日志等级	5
举例	PEX/5/PEX_FORBID_STACK: Can't connect PEXs 100 and 102: The PEX ports to which the PEXs belong are in different PEX port groups.
日志说明	属于不同PEX端口组的PEX设备连接在一起
处理建议	请检查组网连接

119.5 PEX_LINK_BLOCK

日志内容	Status of [STRING] changed from [STRING] to blocked.
参数解释	$1：端口名称 $2：端口的链路状态
日志等级	4
举例	PEX/4/PEX_LINK_BLOCK: Status of Ten-GigabitEthernet2/0/1 changed from forwarding to blocked.
日志说明	处于blocked状态的链路可以转发协议包，但是不能转发数据包。Blocked是一种介于down与forwarding之间的过渡状态 下面的事件可以触发PEX链路状态进入blocked状态： • 物理连接错误，即同一 PEX 设备上的 PEX 物理接口连接到了父设备上不同 PEX 端口下绑定的 PEX 物理接口或者父设备上同一 PEX 端口下绑定的 PEX 物理接口连接到了不同的 PEX 设备 • 被设备强制限制成 Blocked 状态。在 PEX 设备启动阶段，PEX 设备会将未被用于加载启动软件包的、物理状态为 UP 的 PEX 物理端口状态设置为 Blocked • 接口的物理状态为 UP，但是父设备和 PEX 设备的 PEX 连接中断
处理建议	从down到blocked，说明接口up了，属于正常状态。但是如果长期停在blocked状态，请确认连线是否正确或者线路是否正常 从forwarding到blocked，并且长期停在blocked，请检查是否存在IRF分裂，导致PEX存在两个IRF组中

119.6 PEX_LINK_DOWN

日志内容	Status of [STRING] changed from [STRING] to down.
参数解释	$1：端口名称 $2：端口的链路状态
日志等级	4
举例	PEX/4/PEX_LINK_DOWN: Status of Ten-GigabitEthernet2/0/1 changed from forwarding to down.
日志说明	处于down状态的链路无法转发任何报文 许多事件，例如：物理链路故障、管理员执行**shutdown**命令、系统重启等等，都可以使链路进入down状态
处理建议	请确认是否有管理员输入**shutdown**命令或者系统重启操作导致，如果是以上操作导致，则属于正常状态。如果不是，请检查物理接口的连线是否进行过插拔操作或松动

119.7 PEX_LINK_FORWARD

日志内容	Status of [STRING] changed from [STRING] to forwarding.
参数解释	$1：端口名称 $2：端口的链路状态
日志等级	5
举例	PEX/5/PEX_LINK_FORWARD: Status of Ten-GigabitEthernet2/0/1 changed from blocked to forwarding.

日志说明	• 链路进入 forwarding 状态，可以开始转发数据报文
	• 下面的事件可以触发 PEX 链路进入 forwarding 状态：
	  ○ 链路进入 blocked 状态后，重新检测成功
	  ○ PEX 完成软件加载，使 PEX 端口状态变成 forwarding

处理建议	正常状态，无需任何处理

119.8 PEX_REG_JOININ

日志内容	PEX ([STRING]) registered successfully on PEX port [UINT32].
参数解释	$1：虚拟槽位号或虚拟框号 $2：PEX端口ID
日志等级	5
举例	PEX/5/PEX_REG_JOININ: PEX (slot 101) registered successfully on PEX port 1.
日志说明	PEX端口完成注册，可以开始管理及配置PEX设备。在父设备上可以将PEX设备视为一块接口板进行操作
处理建议	正常事件，无需任何处理

119.9 PEX_REG_LEAVE

日志内容	PEX ([STRING]) unregistered on PEX port [UINT32].
参数解释	$1：虚拟槽位号或虚拟框号 $2：PEX端口ID
日志等级	4
举例	PEX/4/PEX_REG_LEAVE: PEX (slot 101) unregistered on PEX port 1.
日志说明	PEX端口取消注册，此后从父设备上无法操作PEX设备 下面的事件可以导致PEX端口取消注册： • PEX 设备在 30 分钟内启动失败 • PEX 端口内的所有物理接口 down。例如将所有和父设备连接的接口都 shutdown 或者将物理连接全部断开 • PEX 端口内的所有物理端口的链路检测均失败 • PEX 设备重启
处理建议	1. 如果是 PEX 设备重启或者用户将 PEX 和父设备之间的相连的所有端口都手工关闭了导致 PEX 设备取消注册，属于正常事件，无需任何处理 2. 否则，请使用命令行 **display device** 查看 PEX 的设备的虚拟槽位号/虚拟框号是否存在，State 是否正常，如果没有显示 PEX 设备的虚拟槽位号/虚拟框号或 PEX 设备的 State 不是 Normal，请前往 3 3. 使用命令行 **display pex-port** 检查 PEX 端口是否存在虚拟槽位号/虚拟框号配置，如果不存在请重新配置；如果存在请检查 PEX 物理端口状态是否全部为 down 或者全部 blocked，如果 PEX 物理端口状态全部为 down 或者全部 blocked 请前往 4 4. 使用命令行 **display interface** 检查 PEX 端口内的所有物理接口对应的 Current state 字段是否为 down。如果 Current state 字段显示为 down，请检查接口连接线缆是否被拔出或故障

119.10 PEX_REG_REQUEST

日志内容	Received a REGISTER request on PEX port [UINT32] from PEX ([STRING]).
参数解释	$1：PEX端口ID $2：虚拟槽位号或虚拟框号
日志等级	5
举例	PEX/5/PEX_REG_REQUEST: Received a REGISTER request on PEX port 1 from PEX (slot 101).
日志说明	PEX相关配置已经成功，PEX设备和父设备连线正确，PEX设备启动时候，PEX端口收到注册请求后准备启动加载版本
处理建议	正常事件，无需任何处理

119.11 PEX_STACKCONNECTION_ERROR

日志内容	A device was connected to a PEX that already had two neighboring devices.
参数解释	无
日志等级	5
举例	PEX/5/PEX_STACKCONNECTION_ERROR: A device was connected to a PEX that already had two neighboring devices.
日志说明	系统中存在连接错误，有一条链路连接到了一个PEX，这个PEX已经存在两个邻居设备
处理建议	请检查组网连接

120 PFILTER

本节介绍报文过滤模块输出的日志信息。

120.1 PFILTER_GLB_RES_CONFLICT

日志内容	Failed to apply or refresh [STRING] ACL [UINT] to the [STRING] direction globally. [STRING] ACL [UINT] has already been applied globally.
参数解释	$1：ACL版本 $2：ACL编号 $3：流量方向 $4：ACL类型 $5：ACL编号
日志等级	3
举例	PFILTER/3/PFILTER_GLB_RES_CONFLICT: Failed to apply or refresh IPv6 ACL 2000 to the inbound direction globally. IPv6 ACL 3000 has already been applied globally.
日志说明	IPv4、IPv6、MAC类型的ACL在某方向上全局应用了，系统无法在此方向上全局应用或更新相同类型的ACL规则
处理建议	删除相同类型的ACL

120.2 PFILTER_GLB_IPV4_DACT_NO_RES

日志内容	Failed to apply or refresh the IPv4 default action to the [STRING] direction globally. The resources are insufficient.
参数解释	$1：流量方向
日志等级	3
举例	PFILTER/3/PFILTER_GLB_IPV4_DACT_NO_RES: Failed to apply or refresh the IPv4 default action to the inbound direction globally. The resources are insufficient.
日志说明	因硬件资源不足，系统无法在某个方向上全局应用或更新IPv4缺省动作
处理建议	使用**display qos-acl resource**命令检查硬件资源使用情况

120.3 PFILTER_GLB_IPV4_DACT_UNK_ERR

日志内容	Failed to apply or refresh the IPv4 default action to the [STRING] direction globally.
参数解释	$1：流量方向
日志等级	3
举例	PFILTER/3/PFILTER_GLB_IPV4_DACT_UNK_ERR: Failed to apply or refresh the IPv4 default action to the inbound direction globally.
日志说明	因故障导致系统无法在某个方向上全局应用或更新IPv4缺省动作
处理建议	无

120.4 PFILTER_GLB_IPV6_DACT_NO_RES

日志内容	Failed to apply or refresh the IPv6 default action to the [STRING] direction globally. The resources are insufficient.
参数解释	$1：流量方向
日志等级	3
举例	PFILTER/3/PFILTER_GLB_IPV6_DACT_NO_RES: Failed to apply or refresh the IPv6 default action to the inbound direction globally. The resources are insufficient.
日志说明	因硬件资源不足，系统无法在某个方向上全局应用或更新IPv6缺省动作
处理建议	使用**display qos-acl resource**命令检查硬件资源使用情况

120.5 PFILTER_GLB_IPV6_DACT_UNK_ERR

日志内容	Failed to apply or refresh the IPv6 default action to the [STRING] direction globally.
参数解释	$1：流量方向
日志等级	3
举例	PFILTER/3/PFILTER_GLB_IPV6_DACT_UNK_ERR: Failed to apply or refresh the IPv6 default action to the inbound direction globally.
日志说明	因故障导致系统无法在某个方向上全局应用或更新IPv6缺省动作
处理建议	无

120.6 PFILTER_GLB_MAC_DACT_NO_RES

日志内容	Failed to apply or refresh the MAC default action to the [STRING] direction globally. The resources are insufficient.
参数解释	$1：流量方向
日志等级	3
举例	PFILTER/3/PFILTER_GLB_MAC_DACT_NO_RES: Failed to apply or refresh the MAC default action to the inbound direction globally. The resources are insufficient.
日志说明	因硬件资源不足，系统无法在某个方向上全局应用或更新MAC缺省动作
处理建议	使用**display qos-acl resource**命令检查硬件资源使用情况

120.7 PFILTER_GLB_MAC_DACT_UNK_ERR

日志内容	Failed to apply or refresh the MAC default action to the [STRING] direction globally.
参数解释	$1：流量方向
日志等级	3
举例	PFILTER/3/PFILTER_GLB_MAC_DACT_UNK_ERR: Failed to apply or refresh the MAC default action to the inbound direction globally.
日志说明	因故障导致系统无法在某个方向上全局应用或更新MAC缺省动作
处理建议	无

120.8 PFILTER_GLB_NO_RES

日志内容	Failed to apply or refresh [STRING] ACL [UINT] [STRING] to the [STRING] direction globally. The resources are insufficient.
参数解释	$1：ACL版本 $2：ACL编号 $3：规则的ID及内容 $4：流量方向
日志等级	3
举例	PFILTER/3/PFILTER_GLB_NO_RES: Failed to apply or refresh IPv6 ACL 2000 rule 1 to the inbound direction globally. The resources are insufficient.
日志说明	因硬件资源不足，系统无法在某个方向上全局应用或更新ACL规则
处理建议	使用**display qos-acl resource**命令检查硬件资源使用情况

120.9 PFILTER_GLB_NOT_SUPPORT

日志内容	Failed to apply or refresh [STRING] ACL [UINT] [STRING] to the [STRING] direction globally. The ACL is not supported.
参数解释	$1：ACL版本 $2：ACL编号 $3：规则的ID及内容 $4：流量方向
日志等级	3
举例	PFILTER/3/PFILTER_GLB_NOT_SUPPORT: Failed to apply or refresh IPv6 ACL 2000 rule 1 to the inbound direction globally. The ACL is not supported.
日志说明	因系统不支持ACL规则而导致无法在某个方向上全局应用或更新ACL规则
处理建议	检查ACL规则并删除不支持的配置

120.10 PFILTER_GLB_UNK_ERR

日志内容	Failed to apply or refresh [STRING] ACL [UINT] [STRING] to the [STRING] direction globally.
参数解释	$1：ACL版本 $2：ACL编号 $3：ACL规则的ID及内容 $4：流量方向
日志等级	3
举例	PFILTER/3/PFILTER_GLB_UNK_ERR: Failed to apply or refresh IPv6 ACL 2000 rule 1 to the inbound direction globally.
日志说明	因故障导致系统无法在某个方向上全局应用或更新ACL
处理建议	无

120.11 PFILTER_IF_IPV4_DACT_NO_RES

日志内容	Failed to apply or refresh the IPv4 default action to the [STRING] direction of interface [STRING]. The resources are insufficient.
参数解释	$1：流量方向 $2：接口名称
日志等级	3
举例	PFILTER/3/PFILTER_IF_IPV4_DACT_NO_RES: Failed to apply or refresh the IPv4 default action to the inbound direction of interface Ethernet 3/1/2. The resources are insufficient.
日志说明	因硬件资源不足，系统无法在接口的某个方向上应用或更新IPv4缺省动作
处理建议	使用**display qos-acl resource**命令检查硬件资源使用情况

120.12 PFILTER_IF_IPV4_DACT_UNK_ERR

日志内容	Failed to apply or refresh the IPv4 default action to the [STRING] direction of interface [STRING].
参数解释	$1：流量方向 $2：接口名称
日志等级	3
举例	PFILTER/3/PFILTER_IF_IPV4_DACT_UNK_ERR: Failed to apply or refresh the IPv4 default action to the inbound direction of interface Ethernet 3/1/2.
日志说明	因故障系统无法在接口的某个方向上应用或更新IPv4缺省动作
处理建议	无

120.13 PFILTER_IF_IPV6_DACT_NO_RES

日志内容	Failed to apply or refresh the IPv6 default action to the [STRING] direction of interface [STRING]. The resources are insufficient.
参数解释	$1：流量方向 $2：接口名称
日志等级	3
举例	PFILTER/3/PFILTER_IF_IPV6_DACT_NO_RES: Failed to apply or refresh the IPv6 default action to the inbound direction of interface Ethernet 3/1/2. The resources are insufficient.
日志说明	因硬件资源不足，系统无法在接口的某个方向上应用或更新IPv6缺省动作
处理建议	使用**display qos-acl resource**命令检查硬件资源使用情况

120.14 PFILTER_IF_IPV6_DACT_UNK_ERR

日志内容	Failed to apply or refresh the IPv6 default action to the [STRING] direction of interface [STRING].
参数解释	$1：流量方向 $2：接口名称
日志等级	3
举例	PFILTER/3/PFILTER_IF_IPV6_DACT_UNK_ERR: Failed to apply or refresh the IPv6 default action to the inbound direction of interface Ethernet 3/1/2.
日志说明	因故障系统无法在接口的某个方向上应用或更新IPv6缺省动作
处理建议	无

120.15 PFILTER_IF_MAC_DACT_NO_RES

日志内容	Failed to apply or refresh the MAC default action to the [STRING] direction of interface [STRING]. The resources are insufficient.
参数解释	$1：流量方向 $2：接口名称
日志等级	3
举例	PFILTER/3/PFILTER_IF_MAC_DACT_NO_RES: Failed to apply or refresh the MAC default action to the inbound direction of interface Ethernet 3/1/2. The resources are insufficient.
日志说明	因硬件资源不足，系统无法在接口的某个方向上应用或更新MAC缺省动作
处理建议	使用**display qos-acl resource**命令检查硬件资源使用情况

120.16 PFILTER_IF_MAC_DACT_UNK_ERR

日志内容	Failed to apply or refresh the MAC default action to the [STRING] direction of interface [STRING].
参数解释	$1：流量方向 $2：接口名称
日志等级	3
举例	PFILTER/3/PFILTER_IF_MAC_DACT_UNK_ERR: Failed to apply or refresh the MAC default action to the inbound direction of interface Ethernet 3/1/2.
日志说明	因故障系统无法在接口的某个方向上应用或更新MAC缺省动作
处理建议	无

120.17 PFILTER_IF_NO_RES

日志内容	Failed to apply or refresh [STRING] ACL [UINT] [STRING] to the [STRING] direction of interface [STRING]. The resources are insufficient.
参数解释	$1：ACL版本 $2：ACL编号 $3：ACL规则的ID及内容 $4：流量方向 $5：接口名称
日志等级	3
举例	PFILTER/3/PFILTER_IF_NO_RES: Failed to apply or refresh IPv6 ACL 2000 rule 1 to the inbound direction of interface Ethernet 3/1/2. The resources are insufficient.
日志说明	因硬件资源不足，系统无法在接口的某个方向上应用或更新ACL规则
处理建议	使用**display qos-acl resource**命令检查硬件资源使用情况

120.18 PFILTER_IF_NOT_SUPPORT

日志内容	Failed to apply or refresh [STRING] ACL [UINT] [STRING] to the [STRING] direction of interface [STRING]. The ACL is not supported.
参数解释	$1：ACL版本 $2：ACL编号 $3：ACL规则的ID及内容 $4：流量方向 $5：接口名称
日志等级	3
举例	PFILTER/3/PFILTER_IF_NOT_SUPPORT: Failed to apply or refresh IPv6 ACL 2000 rule 1 to the inbound direction of interface Ethernet 3/1/2. The ACL is not supported.
日志说明	因系统不支持ACL规则而导致无法在接口的某个方向上应用或更新ACL规则
处理建议	检查ACL规则并删除不支持的配置

120.19 PFILTER_IF_RES_CONFLICT

日志内容	Failed to apply or refresh [STRING] ACL [UINT] to the [STRING] direction of interface [STRING]. [STRING] ACL [UINT] has already been applied to the interface.
参数解释	$1：ACL版本 $2：ACL编号 $3：流量方向 $4：接口名称 $5：ACL类型 $6：ACL编号
日志等级	3
举例	PFILTER/3/PFILTER_IF_RES_CONFLICT: Failed to apply or refresh IPv6 ACL 2000 to the inbound direction of interface Ethernet 3/1/2. IPv6 ACL 3000 has already been applied to the interface.
日志说明	IPv4、IPv6、MAC类型的ACL在接口某方向上应用了，系统无法在此方向上应用或更新相同类型的ACL规则
处理建议	删除相同类型的ACL

120.20 PFILTER_IF_UNK_ERR

日志内容	Failed to apply or refresh [STRING] ACL [UINT] [STRING] to the [STRING] direction of interface [STRING].
参数解释	$1：ACL版本 $2：ACL编号 $3：ACL规则的ID及内容 $4：流量方向 $5：接口名称
日志等级	3
举例	PFILTER/3/PFILTER_IF_UNK_ERR: Failed to apply or refresh IPv6 ACL 2000 rule 1 to the inbound direction of interface Ethernet 3/1/2.
日志说明	因故障系统无法在接口的某个方向上应用或更新ACL规则
处理建议	无

120.21 PFILTER_IPV6_STATIS_INFO

日志内容	[STRING] ([STRING]): Packet-filter IPv6 [UINT32] [STRING] [STRING] [UINT64] packet(s).
参数解释	$1：ACL应用目的地 $2：流量方向 $3：ACL编号 $4：ACL规则的ID及内容 $5：匹配上规则的报文个数
日志等级	6
举例	ACL/6/PFILTER_IPV6_STATIS_INFO: Ethernet0/4/0 (inbound): Packet-filter IPv6 2000 rule 0 permit source 1:1::/64 logging 1000 packet(s).
日志说明	匹配上报文过滤中的IPv6 ACL规则的报文数量发生变化
处理建议	无

120.22 PFILTER_STATIS_INFO

日志内容	[STRING] ([STRING]): Packet-filter [UINT32] [STRING] [UINT64] packet(s).
参数解释	$1：ACL应用目的地 $2：流量方向 $3：ACL编号 $4：ACL规则的ID及内容 $5：匹配上规则的报文个数
日志等级	6
举例	ACL/6/PFILTER_STATIS_INFO: Ethernet0/4/0 (inbound): Packet-filter 2000 rule 0 permit source 1.1.1.1 0 logging 10000 packet(s).
日志说明	匹配上报文过滤中的IPv4 ACL规则的报文数量发生变化
处理建议	无

120.23 PFILTER_VLAN_IPV4_DACT_NO_RES

日志内容	Failed to apply or refresh the IPv4 default action to the [STRING] direction of VLAN [UINT16]. The resources are insufficient.
参数解释	$1：流量方向 $2：VLAN ID
日志等级	3
举例	PFILTER/3/PFILTER_VLAN_IPV4_DACT_NO_RES: Failed to apply or refresh the IPv4 default action to the inbound direction of VLAN 1. The resources are insufficient.
日志说明	因硬件资源不足，系统无法在VLAN的某个方向上应用或更新IPv4缺省动作
处理建议	使用**display qos-acl resource**命令检查硬件资源使用情况

120.24 PFILTER_VLAN_IPV4_DACT_UNK_ERR

日志内容	Failed to apply or refresh the IPv4 default action to the [STRING] direction of VLAN [UINT16].
参数解释	$1：流量方向 $2：VLAN ID
日志等级	3
举例	PFILTER/3/PFILTER_VLAN_IPV4_DACT_UNK_ERR: Failed to apply or refresh the IPv4 default action to the inbound direction of VLAN 1.
日志说明	因故障系统无法在VLAN的某个方向上应用或更新IPv4缺省动作
处理建议	无

120.25 PFILTER_VLAN_IPV6_DACT_NO_RES

日志内容	Failed to apply or refresh the IPv6 default action to the [STRING] direction of VLAN [UINT16]. The resources are insufficient.
参数解释	$1：流量方向 $2：VLAN ID
日志等级	3
举例	PFILTER/3/PFILTER_VLAN_IPV6_DACT_NO_RES: Failed to apply or refresh the IPv6 default action to the inbound direction of VLAN 1. The resources are insufficient.
日志说明	因硬件资源不足，系统无法在VLAN的某个方向上应用或更新IPv6缺省动作
处理建议	使用**display qos-acl resource**命令检查硬件资源使用情况

120.26 PFILTER_VLAN_IPV6_DACT_UNK_ERR

日志内容	Failed to apply or refresh the IPv6 default action to the [STRING] direction of VLAN [UINT16].
参数解释	$1：流量方向 $2：VLAN ID
日志等级	3
举例	PFILTER/3/PFILTER_VLAN_IPV6_DACT_UNK_ERR: Failed to apply or refresh the IPv6 default action to the inbound direction of VLAN 1.
日志说明	因故障系统无法在VLAN的某个方向上应用或更新IPv6缺省动作
处理建议	无

120.27 PFILTER_VLAN_MAC_DACT_NO_RES

日志内容	Failed to apply or refresh the MAC default action to the [STRING] direction of VLAN [UINT16]. The resources are insufficient.
参数解释	$1：流量方向 $2：VLAN ID
日志等级	3
举例	PFILTER/3/PFILTER_VLAN_MAC_DACT_NO_RES: Failed to apply or refresh the MAC default action to the inbound direction of VLAN 1. The resources are insufficient.
日志说明	因硬件资源不足，系统无法在VLAN的某个方向上应用或更新MAC缺省动作
处理建议	使用**display qos-acl resource**命令检查硬件资源使用情况

120.28 PFILTER_VLAN_MAC_DACT_UNK_ERR

日志内容	Failed to apply or refresh the MAC default action to the [STRING] direction of VLAN [UINT16].
参数解释	$1：流量方向 $2：VLAN ID
日志等级	3
举例	PFILTER/3/PFILTER_VLAN_MAC_DACT_UNK_ERR: Failed to apply or refresh the MAC default action to the inbound direction of VLAN 1.
日志说明	因故障系统无法在VLAN的某个方向上应用或更新MAC缺省动作
处理建议	无

120.29 PFILTER_VLAN_NO_RES

日志内容	Failed to apply or refresh [STRING] ACL [UINT] [STRING] to the [STRING] direction of VLAN [UINT16]. The resources are insufficient.
参数解释	$1：ACL版本 $2：ACL编号 $3：ACL规则的ID及内容 $4：流量方向 $5：VLAN ID
日志等级	3
举例	PFILTER/3/PFILTER_VLAN_NO_RES: Failed to apply or refresh IPv6 ACL 2000 rule 1 to the inbound direction of VLAN 1. The resources are insufficient.
日志说明	因硬件资源不足，系统无法在VLAN的某个方向上应用或更新ACL规则
处理建议	使用**display qos-acl resource**命令检查硬件资源使用情况

120.30 PFILTER_VLAN_NOT_SUPPORT

日志内容	Failed to apply or refresh [STRING] ACL [UINT] [STRING] to the [STRING] direction of VLAN [UINT16]. The ACL is not supported.
参数解释	$1：ACL版本 $2：ACL编号 $3：ACL规则的ID及内容 $4：流量方向 $5：VLAN ID
日志等级	3
举例	PFILTER/3/PFILTER_VLAN_NOT_SUPPORT: Failed to apply or refresh ACL 2000 rule 1 to the inbound direction of VLAN 1. The ACL is not supported.
日志说明	因系统不支持ACL规则而导致无法在VLAN的某个方向上应用或更新ACL规则
处理建议	检查ACL规则并删除不支持的配置

120.31 PFILTER_VLAN_RES_CONFLICT

日志内容	Failed to apply or refresh [STRING] ACL [UINT] to the [STRING] direction of VLAN [UINT16]. [STRING] ACL [UINT] has already been applied to the VLAN.
参数解释	$1：ACL版本 $2：ACL编号 $3：流量方向 $4：VLAN ID $5：ACL类型 $6：ACL编号
日志等级	3
举例	PFILTER/3/PFILTER_VLAN_RES_CONFLICT: Failed to apply or refresh IPv6 ACL 2000 to the inbound direction of VLAN 1. IPv6 ACL 3000 has already been applied to the VLAN.
日志说明	IPv4、IPv6、MAC类型的ACL已经在VLAN的某方向上应用了，系统无法在此方向上应用或更新相同类型的ACL规则
处理建议	删除相同类型的ACL

120.32 PFILTER_VLAN_UNK_ERR

日志内容	Failed to apply or refresh [STRING] ACL [UINT] [STRING] to the [STRING] direction of VLAN [UINT16].
参数解释	$1：ACL版本 $2：ACL编号 $3：ACL规则的ID及内容 $4：流量方向 $5：VLAN ID
日志等级	3
举例	PFILTER/3/PFILTER_VLAN_UNK_ERR: Failed to apply or refresh ACL 2000 rule 1 to the inbound direction of VLAN 1.
日志说明	因故障系统无法在VLAN的某个方向上应用或更新ACL规则
处理建议	无

121 PIM

本节介绍 PIM 模块输出的日志信息。

121.1 PIM_NBR_DOWN

日志内容	[STRING] Neighbor [STRING] ([STRING]) is down.
参数解释	$1：公网侧PIM邻居down时，该参数为空；私网侧PIM邻居down时，该参数为“(*VPN实例的名称*)” $2：PIM邻居的IP地址 $3：接口名称
日志等级	4
举例	PIM/4/PIM_NBR_DOWN: Neighbor 10.1.1.1(Vlan-interface10) is down.
日志说明	PIM邻居的状态变为down
处理建议	检查PIM配置是否错误以及检查网络是否发生故障

121.2 PIM_NBR_UP

日志内容	[STRING] Neighbor [STRING] ([STRING]) is up.
参数解释	$1：公网侧PIM邻居up时，该参数为空；私网侧PIM邻居up时，该参数为“(*VPN实例的名称*)” $2：PIM邻居的IP地址 $3：接口名称
日志等级	4
举例	PIM/4/PIM_NBR_UP: Neighbor 10.1.1.1(Vlan-interface10) is up.
日志说明	PIM邻居的状态变为up
处理建议	无

122 PING

本节介绍 ping 模块输出的日志信息。

122.1 PING_STATISTICS

日志内容	[STRING] statistics for [STRING]: [UINT32] packets transmitted, [UINT32] packets received, [DOUBLE]% packet loss, round-trip min/avg/max/std-dev = [DOUBLE]/[DOUBLE]/[DOUBLE]/[DOUBLE] ms.
参数解释	$1：Ping或Ping6 $2：目的IP地址，IPv6地址，或主机名 $3：发送的回显请求数量 $4：接收的回显应答数量 $5：没有回复的报文占总请求报文比 $6：最小往返时间 $7：平均往返时间 $8：最大往返时间 $9：往返时间标准差
日志等级	6
举例	PING/6/PING_STATISTICS: Ping statistics for 192.168.0.115: 5 packets transmitted, 5 packets received, 0.0% packet loss, round-trip min/avg/max/std-dev = 0.000/0.800/2.000/0.748 ms.
日志说明	用户执行**ping**命令查看公网中对端是否可达
处理建议	如果没有收到报文，请检查接口是否DOWN，并查找路由表，看是否存在有效路由

122.2 PING_VPN_STATISTICS

日志内容	[STRING] statistics for [STRING] in VPN instance [STRING] : [UINT32] packets transmitted, [UINT32] packets received, [DOUBLE]% packet loss, round-trip min/avg/max/std-dev = [DOUBLE]/[DOUBLE]/[DOUBLE]/[DOUBLE] ms.
参数解释	$1：Ping或Ping6 $2：目的IP地址，IPv6地址，或主机名 $3：VPN实例名 $3：发送的回显请求数量 $4：接收的回显应答数量 $5：没有回复的报文占总请求报文比 $6：最小往返时间 $7：平均往返时间 $8：最大往返时间 $9：往返时间标准差
日志等级	6
举例	PING/6/PING_VPN_STATISTICS: Ping statistics for 192.168.0.115 in VPN instance vpn1: 5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss, round-trip min/avg/max/std-dev = 0.000/0.800/2.000/0.748 ms.
日志说明	用户执行**ping**命令查看VPN中的对端是否可达
处理建议	如果没有收到报文，请检查接口是否DOWN，并查找路由表，看是否存在有效路由

123 PKI

本节包含 PKI 日志消息。

123.1 REQUEST_CERT_FAIL

日志内容	Failed to request certificate of domain [STRING].
参数解释	$1：PKI域名
日志等级	5
举例	PKI/5/REQUEST_CERT_FAIL: Failed to request certificate of domain abc.
日志说明	为PKI域申请证书失败
处理建议	检查设备和CA服务器的配置和其间的网络

123.2 REQUEST_CERT_SUCCESS

日志内容	Request certificate of domain [STRING] successfully.
参数解释	$1：PKI域名
日志等级	5
举例	PKI/5/REQUEST_CERT_SUCCESS: Request certificate of domain abc successfully.
日志说明	为PKI域申请证书成功
处理建议	无

124 PKT2CPU

本节包含 PKT2CPU 日志消息。

124.1 PKT2CPU_NO_RESOURCE

日志内容	-Interface=[STRING]-ProtocolType=[UINT32]-MacAddr=[STRING]; The resources are insufficient. -Interface=[STRING]-ProtocolType=[UINT32]-SrcPort=[UINT32]-DstPort=[UINT32]; The resources are insufficient.
参数解释	$1：接口名 $2：协议类型 $3：MAC地址或源端口 $4：目的端口
日志等级	4
举例	PKT2CPU/4/PKT2CPU_NO_RESOURCE: -Interface=Ethernet0/0/2-ProtocolType=21-MacAddr=0180-c200-0014; The resources are insufficient.
日志说明	硬件资源不足
处理建议	取消配置

125 PKTCPT

本节介绍 PKTCPT（Packet Capture）模块输出的日志信息。

125.1 PKTCPT_AP_OFFLINE

日志内容	Failed to start packet capture. Reason: AP was offline.
参数解释	无
日志等级	6
举例	PKTCPT/6/PKTCPT_AP_OFFLINE: Failed to start packet capture. Reason: AP was offline.
日志说明	指定报文捕获的AP没有上线，报文捕获启动失败
处理建议	检查配置，AP上线后再次开启报文捕获

125.2 PKTCPT_AREADY_EXIT

日志内容	Failed to start packet capture. Reason: The AP was uploading frames captured during the previous capturing operation.
参数解释	无
日志等级	6
举例	PKTCPT/6/PKTCPT_AREADY_EXIT: Failed to start packet capture. Reason: The AP was uploading frames captured during the previous capturing operation.
日志说明	AC/FIT AP组网，当AC上的报文捕获功能先停止时，AP还在上传捕获的报文。此时用户再次开启报文捕获功能，报文捕获功能会启动失败
处理建议	请稍后重新开启报文捕获功能

125.3 PKTCPT_CONN_FAIL

日志内容	Failed to start packet capture. Reason: Failed to connect to the FTP server.
参数解释	无
日志等级	6
举例	PKTCPT/6/PKTCPT_CONN_FAIL: Failed to start packet capture. Reason: Failed to connect to the FTP server.
日志说明	无法连接到与设备在同一网段的FTP服务器，报文捕获功能启动失败
处理建议	• 检查 URL 是否合法。可能情况包括：指定的 FTP 服务器的 IP 地址不存在；指定的 IP 地址不是 FTP 服务器的地址；指定的 FTP 服务器的接口处于关闭状态 • 检查 URL 中域名解析是否成功 • 检查开启报文捕获服务设备与 FTP 服务器是否可达 • 检查 FTP 服务器是否上线

125.4 PKTCPT_INVALID_FILTER

日志内容	Failed to start packet capture. Reason: Invalid expression for matching packets to be captured.
参数解释	无
日志等级	6
举例	PKTCPT/6/PKTCPT_INVALD_FILTER: Failed to start packet capture. Reason: Invalid expression for matching packets to be captured.
日志说明	捕获过滤规则非法，启动报文捕获功能失败
处理建议	修改捕获过滤规则

125.5 PKTCPT_LOGIN_DENIED

日志内容	Packet capture aborted. Reason: FTP server login failure.
参数解释	无
日志等级	6
举例	PKTCPT/6/PKTCPT_LOGIN_DENIED: Packet capture aborted. Reason: FTP server login failure.
日志说明	登录FTP服务器失败，报文捕获退出
处理建议	检查用户名密码是否正确

125.6 PKTCPT_MEMORY_ALERT

日志内容	Packet capture aborted. Reason: Memory threshold reached.
参数解释	无
日志等级	6
举例	PKTCPT/6/PKTCPT_MEMORY_ALERT: Packet capture aborted. Reason: Memory threshold reached.
日志说明	设备达到内存门限时，报文捕获功能退出
处理建议	无

125.7 PKTCPT_OPEN_FAIL

日志内容	Failed to start packet capture. Reason: File for storing captured frames not opened.
参数解释	无
日志等级	6
举例	PKTCPT/6/PKTCPT_OPEN_FAIL: Failed to start packet capture. Reason: File for storing captured frames not opened.
日志说明	将报文文件保存到FLASH时，文件路径无法打开，报文捕获功能启动失败
处理建议	• 若用户不具有写文件权限，请配置写权限 • 若指定的文件名是已经存在并被其它程序占用，请使用其它文件名

125.8 PKTCPT_OPERATION_TIMEOUT

日志内容	Failed to start or continue packet capture. Reason: Operation timed out.
参数解释	无
日志等级	6
举例	PKTCPT/6/PKTCPT_OPERATION_TIMEOUT: Failed to start or continue packet capture. Reason: Operation timed out.
日志说明	由于指定的与设备在不同网段的FTP服务器不可达，连接超时导致报文捕获启动失败；由于指定的与设备在不同网段的FTP服务器不在线，上传捕获的报文超时，导致报文捕获退出
处理建议	• 检查 FTP 服务器是否可达 • 检查 FTP 服务器是否在线

125.9 PKTCPT_SERVICE_FAIL

日志内容	Failed to start packet capture. Reason: TCP or UDP port binding faults.
参数解释	无
日志等级	6
举例	PKTCPT/6/PKTCPT_SERVICE_FAIL: Failed to start packet capture. Reason: TCP or UDP port binding faults.
日志说明	由于TCP或者UDP端口绑定冲突等原因导致报文捕获功能启动失败
处理建议	• 如果之前打开的报文捕获客户端（第三方软件 wireshark）没有关闭，请关闭后重新启动报文捕获功能 • 绑定新的端口号，重新启动报文捕获功能

125.10 PKTCPT_UNKNOWN_ERROR

日志内容	Failed to start or continue packet capture. Reason: Unknown error.
参数解释	无
日志等级	6
举例	PKTCPT/6/PKTCPT_UNKNOWN_ERROR: Failed to start or continue the packet capture. Reason: Unknown error.
日志说明	其它未知原因导致服务启动失败或者退出
处理建议	无

125.11 PKTCPT_UPLOAD_ERROR

日志内容	Packet capture aborted. Reason: Failed to upload captured frames.
参数解释	无
日志等级	6
举例	PKTCPT/6/PKTCPT_UPLOAD_ERROR: Packet capture aborted. Reason: Failed to upload captured frames.
日志说明	由于上传捕获的数据报文失败，导致报文捕获退出
处理建议	• 检查是否试图改变 FTP 的工作目录 • 检查指定 FTP 服务器上文件是否有写权限 • 检查 FTP 服务器是否下线 • 检查与 FTP 服务器是否可达 • 检查 FTP 服务器是否已满 • 检查报文捕获服务是否退出

125.12 PKTCPT_WRITE_FAIL

日志内容	Packet capture aborted. Reason: Not enough space to store captured frames.
参数解释	无
日志等级	6
举例	PKTCPT/6/PKTCPT_WRITE_FAIL: Packet capture aborted. Reason: Not enough space to store captured frames.
日志说明	报文文件保存到FLASH时，FLASH已满，报文捕获功能退出
处理建议	删除无用文件释放磁盘空间

126 PORT

本节介绍 PORT 模块输出的日志信息。

126.1 OMA

日志内容	[STRING]: Transceiver module has I/O errors. Please check the transceiver module.
参数解释	$1：接口名
日志等级	4
举例	PORT/4/OMA: -MDC=1-Slot=2; GigabitEthernet2/1/1: Transceiver module has I/O errors. Please check the transceiver module.
日志说明	CSPEX类单板、CEPC类单板接口上的光模块出现I/O读写故障
处理建议	**1.** 请确认接口是否支持该光模块，如不支持，请更换成支持的光模块；如支持，请更换该故障的光模块 **2.** 请联系技术支持

127 PORTAL

本节介绍 Portal 模块输出的日志信息。

127.1 PORTAL_INFO

日志内容	The [STRING] configuration conflicts with user-vlan configuration. To avoid conflicts, do not configure both features on interface [STRING].
参数解释	$1：配置名称，取值包括： • portal enable：IPv4 Portal 认证配置 • portal ipv6 enable：IPv6 Portal 认证配置 $2：子接口名称
日志等级	4
举例	DPORTAL/4/PORTAL_INFO: -MDC=1-Slot=4; The portal enable configuration conflicts with user-vlan configuration. To avoid conflicts, do not configure both features on interface Route-Aggregation1.2.
日志说明	子接口上同时配置了用户VLAN终结特性和Portal认证（**portal [ipv6] enable**）特性，存在配置冲突
处理建议	**1.** 子接口视图下使用 **display this** 命令查看是否同时存在用户 VLAN 终结配置和 Portal 认证配置，然后使用 **undo** 命令删除其中一类配置命令 **2.** 如果问题仍然存在，联系技术支持

127.2 PORTAL_DIAG

日志内容	PORTAL session$1 get no enough resource when adding a port to a link-aggregation group. This session will not take effect.
参数解释	$1：会话ID
日志等级	4
举例	DPORTAL/4/PORTAL_DIAG:PORTAL session 896 get no enough resource when adding a port to a link-aggregation group. This session will not take effect.
日志说明	当端口加入已处于在线状态的Portal会话的聚合口时，因系统资源不足，Portal会话部分功能（例如会话计费、限速等功能）对该端口上所接入的用户不生效
处理建议	1. 执行 **display qos-acl resource** 命令显示当前单板上资源的使用情况，删除一些没有必要多余的资源 2. 请联系技术支持

127.3 PORTAL_LIMIT_GLOBAL

日志内容	User failed to come online. Reason=BAS global access limit already reached.
参数解释	无
日志等级	6
举例	PORTAL/6/PORTAL_LIMIT_GLOBAL: -MDC=1; User failed to come online. Reason=BAS global access limit already reached.
日志说明	上线用户数达到全局最大用户数
处理建议	无

127.4 PORTAL_LIMIT_IF

日志内容	User failed to come online through interface [STRING]. Reason=BAS access limit of the interface already reached.
参数解释	$1：接口名
日志等级	6
举例	PORTAL/6/PORTAL_LIMIT_IF: -MDC=1-Slot=4; User failed to come online through interface GigabitEthernet4/2/20. Reason=BAS access limit of the interface already reached.
日志说明	上线用户数达到接口最大用户数
处理建议	无

127.5 PORTAL_USER_LOGOFF

日志内容	-UserName=[STRING]-IPAddr=[IPADDR]-IfName=[STRING]-OuterVLAN=[UINT16]-InnerVLAN=[UINT16]-MACAddr=[MAC]-Reason=[STRING]-Input Octets=[UINT32]-Output Octets=[UINT32]-Input Gigawords=[UINT32]-Output Gigawords=[UINT32]; User went offline.
参数解释	$1：用户名 $2：IP地址 $3：接口名 $4：外层VLAN ID $5：内层VLAN ID $6：MAC地址 $7：User request $8：Input Octets $9：Output Octets $10：Input Gigawords $11：Output Gigawords
日志等级	6
举例	PORTAL/6/PORTAL_USER_LOGOFF: -UserName=abc-IPAddr=1.1.1.2-IfName=Route-Aggregation1023.4000-OuterVLAN=N/A-InnerVLAN=4000-MACAddr=0230-0103-5601-Reason=User request-Input Octets=100-Output Octets=200-Input Gigawords=100-Output Gigawords=200; User went offline.
日志说明	用户正常下线
处理建议	无

127.6 PORTAL_USER_LOGOFF_ABNORMAL

日志内容	-UserName=[STRING]-IPAddr=[IPADDR]-IfName=[STRING]-OuterVLAN=[UINT16]-InnerVLAN=[UINT16]-MACAddr=[MAC]-Reason=[STRING]-Input Octets=[UINT32]-Output Octets=[UINT32]-Input Gigawords=[UINT32]-Output Gigawords=[UINT32]; User went offline abnormally.
参数解释	$1：用户名 $2：IP地址 $3：接口名 $4：外层VLAN ID $5：内层VLAN ID $6：MAC地址 $7：下线原因，具体取值请见表65-4 $8：Input Octets $9：Output Octets $10：Input Gigawords $11：Output Gigawords
日志等级	6
举例	PORTAL/6/PORTAL_USER_LOGOFF_ABNORMAL: -UserName=abc-IPAddr=1.1.1.2-IfName=Route-Aggregation1023.4000-OuterVLAN=100-InnerVLAN=4000-MACAddr=0230-0103-5601-Reason=Port down-Input Octets=100-Output Octets=200-Input Gigawords=100-Output Gigawords=200; User went offline abnormally.
日志说明	用户异常下线
处理建议	请根据下线异常原因选择相应的处理方式，详见表65-4

表127-1 下线异常原因列表

下线原因	说明	处理建议
DHCP lease timeout.	DHCP租约过期	无
DHCP user request.	客户端主动请求释放IP地址	无
DHCP configuration changed.	DHCP配置变化引起用户下线	请检查DHCP服务器配置
Idle timeout.	用户在规定时间内的流量没有达到设定阈值	无
Session timeout.	用户上线时间达到了规定值	无
User detection failure	用户在线探测失败	无
The RADIUS server forcibly logged out the user.	RADIUS服务器强制用户下线	无
Interface down.	接入接口状态为Down	请确保用户接入接口网线连接正常且检查接口下没有配置**shutdown**命令

下线原因	说明	处理建议
Interface inactive.	接入接口状态为Deactive	• 请确保用户接入接口网线连接正常 • 请确保用户接入单板或者子卡正常且没有被拔出
Port was removed from VLAN.	VLAN接口接入Portal，二层端口离开VLAN	请确保用户接入的二层端口开启了漫游功能
Authorization ACL for the online user was deleted.	线用户授权的ACL被删除	无
The device forcibly logged out the user.	设备强制用户下线	请确保接口上的Portal功能正常
Failed to synchronize user information with the server.	设备和服务器进行用户信息同步失败	• 请确保服务器配置用户心跳间隔小于等于设备上配置的用户同步超时时长 • 请确保服务器处于可达状态
User recovery failure	用户恢复失败	• 请确保上线接口状态为 Up • 请确保上线接口的 Portal 功能正常 • 请确保用户仍剩余有在线时长
Authorization ACL for the online user changed.	在线用户的授权ACL内容更改导致下线	• 请确保 ACL 重新授权成功 • 确保接口下没有配置了 ACL 严格检查
Authorization user profile for the online user changed.	在线用户的授权User Profile内容更改导致下线	• 请通过 **display user profile** 命令检查授权是否失败 • 确保接口下没有配置 User Profile 严格检查
The RADIUS server doesn't reply to the accounting request.	RADIUS服务器无法回应计费请求	• 请确保设备与 RADIUS 服务器之间的通信正常 • 请确保 RADIUS 服务器状态正常
Accounting update failure.	计费更新失败	• 请确保设备与 RADIUS 服务器之间的通信正常 • 请确保 RADIUS 服务器状态正常
No AAA response for the accounting start packet was received.	用户在报文超时时间内未收到认证服务器的回应（开始计费阶段）	• 请确保设备与 RADIUS 服务器之间的通信正常 • 请确保 RADIUS 服务器状态正常
Failed to send the accounting request for the user.	用户计费请求发送失败	• 请确保设备与 RADIUS 服务器之间的通信正常 • 请确保 RADIUS 服务器状态正常
Traffic threshold for the user was reached.	用户的流量达到了阈值	无

127.7 PORTAL_USER_LOGON_FAIL

日志内容	-UserName=[STRING]-IPAddr=[IPADDR]-IfName=[STRING]-OuterVLAN=[UINT16]-InnerVLAN=[UINT16]-MACAddr=[MAC]-Reason=[STRING]; User failed to come online.
参数解释	$1：用户名 $2：IP地址 $3：接口名 $4：外层VLAN ID $5：内层VLAN ID $6：MAC地址 $7：上线失败原因，取值请参见表65-3
日志等级	6
举例	PORTAL/6/PORTAL_USER_LOGON_FAIL: -UserName=abc-IPAddr=1.1.1.2-IfName=Route-Aggregation1023.4000-OuterVLAN=100-InnerVLAN=4000-MACAddr=0230-0103-5601-Reason=Authentication failure; User failed to come online.
日志说明	用户上线失败
处理建议	请根据上线失败详细原因选择相应的处理方式，详见表65-3

表127-2 上线失败详细原因列表

上线失败原因	说明	处理建议
Authentication failure.	认证失败	• 请确保设备与认证服务器之间的通信正常 • 请确保设备与认证服务器之间的共享密钥相同 • 请确保用户名合法 • 请确保密码正确 • 请确保设备上的认证域配置正确
Authorization failure.	授权失败	• 请确保设备与授权服务器之间的通信正常 • 请确保授权服务器下发的授权属性在设备上存在且配置正确 • 请确保设备支持授权服务器下发的授权属性
Authentication ACK message was not received from the RADIUS server.	设备没有收到RADIUS服务器回应的认证ACK报文	请确保设备到RADIUS服务器路由可达
The device failed to send the authentication request to the RADIUS server.	设备向RADIUS服务器发送认证请求失败	• 请确保设备与 RADIUS 服务器之间的通信正常 • 通过 **display radius scheme** 命令检查 RADIUS 服务器状态，确认其状态为 active
The RADIUS server rejected the authentication request.	RADIUS服务器回应认证拒绝	请确保用户用户名或密码信息正确
Failed to add authorization information for the	添加用户授权信息失败	请检查授权服务器下发的授权属性在设备上是否存在并配置正确

上线失败原因	说明	处理建议
user.		
Local authentication request was rejected.	本地认证被拒绝	请确保本地用户用户名或密码信息正确
No authentication response was received from the authentication server.	用户在认证超时时间内未收到认证服务器的回应	• 检查设备与 RADIUS 服务器之间的通信是否正常 • 检查 RADIUS 服务器状态是否正常
Maximum number of concurrent logins for the account already reached.	一个帐号允许接入的用户数超过了限制	• 检查一个帐号上线用户数 • 通过 **access-limit** 命令修改限制
Local user doesn't exist on the device.	设备上未配置该本地用户	请检查设备本地用户相关配置
Failed to assign a user rule.	用户规则下发失败	硬件内存空间不足，请释放内存
Failed to obtain physical information.	上线过程中获取物理信息失败	无
Authorization ACL doesn't exist.	授权ACL不存在	请确保授权的ACL配置是否存在

127.8 PORTAL_USER_LOGON_SUCCESS

日志内容	-UserName=[STRING]-IPAddr=[IPADDR]-IfName=[STRING]-OuterVLAN=[UINT16]-InnerVLAN=[UINT16]-MACAddr=[MAC]: User came online successfully.
参数解释	$1：用户名 $2：IP地址 $3：接口名 $4：外层VLAN ID $5：内层VLAN ID $6：MAC地址
日志等级	6
举例	PORTAL/6/PORTAL_USER_LOGON_SUCCESS: -UserName=abc-IPAddr=1.1.1.2-IfName=Route-Aggregation1023.4000-OuterVLAN=100-InnerVLAN=4000-MACAddr=0230-0103-5601; User came online successfully.
日志说明	用户上线成功
处理建议	无

127.9 USER_TRACEINFO

日志内容	[objectID=[UINT16]][slotID=[UINT16]][STRING][user info: [STRING]][trace info: [STRING]]
参数解释	$1：业务跟踪对象的编号 $2：接入用户所属的槽位号 $3：业务跟踪阶段，目前有Portal和IPoE两个阶段 $4：用户信息。各用户信息含义请参见表65-6 $5：跟踪详细信息。Portal阶段的详细跟踪信息请参见**表129-5**，IPoE阶段的详细跟踪信息请参见IPoE模块的USER_TRACEINFO日志
日志等级	7
举例	USER/7/USER_TRACEINFO:[objectID=1][slotID=0][portal][user info: MAC address: 0800-2700-acb8 IP address: 80.1.1.1 Access interface: GigabitEthernet1/0/1 User name: abc] [trace info: Sent packet to portal authentication server newpt: Verion: 2.0 Type: ACK_AUTH Method: PAP Serial No: 160 Request ID: 0 User IP: 80.1.1.1 Error code: 0 Attribute count: 3]
日志说明	跟踪接入用户在Portal或IPoE阶段的详细信息
处理建议	无

表127-3 被跟踪用户信息描述表

字段	描述
MAC address	接入用户的MAC地址
Access interface	接入用户接入接口
Service VLAN	接入用户的外层VLAN ID
Customer VLAN	接入用户的内层VLAN ID
Username	接入用户的用户名
IP address	接入用户的IP地址
Access mode	业务跟踪对象的接入模式

表127-4 被跟踪详细信息描述表（Portal）

字段	描述
Sent logon request to IPoE	Portal向IPoE发送认证请求消息
Received logon success message from IPoE	Portal收到IPoE发送的上线成功消息
Received logon failure message from IPoE	Portal收到IPoE发送的上线失败消息
Sent logoff request to IPoE	Portal向IPoE发送下线请求消息
Received logoff response from IPoE	Portal收到IPoE发送的下线应答消息
Received forced-logoff message from IPoE	Portal收到IPoE发送的强制用户下线消息
Received message for user informaiton transparent transmission from IPoE	Portal收到IPoE发送的待透传的用户信息
Received MAC binding query request from IPoE	Portal收到IPoE发送的MAC地址绑定查询消息
Sent MAC binding query response to IPoE	Portal向IPoE发送MAC地址绑定查询应答消息
Received MAC-trigger user online message from IPoE	Portal收到IPoE发送的MAC地址绑定用户上线通知消息
Received MAC-trigger user offline message from IPoE.	Portal收到IPoE发送的MAC地址绑定用户下线通知消息
Received user roaming message from IPoE	Portal收到IPoE发送的用户漫游消息
Received authentication-continue message from IPoE	Portal收到IPoE发送的认证持续消息
Received packet from portal authentication server *server-name*	接收到Portal认证服务器*server-name*发送的报文
Sent packet to portal authentication server *server-name*	已发送报文给Portal认证服务器*server-name*
Version	Portal协议报文的版本号，取值包括： • 1.0：版本 1 • 2.0：版本 2 • 3.0：版本 2
Type	Portal协议报文类型： • REQ_CHALLENGE • ACK_CHALLENGE • REQ_AUTH • ACK_AUTH • REQ_LOGOUT • ACK_LOGOUT • AFF_ACK_AUTH • NTF_LOGOUT • REQ_INFO • ACK_INFO

字段	描述
	• NTF_USER_DISCOVER • NTF_USER_IP_CHANGE • AFF_NTF_USER_IP_CHANGE • ACK_NTF_LOGOUT • NTF_HEART • NTF_USER_HEART • ACK_NTF_USER_HEART • NTF_CHALLENGE • NTF_USER_NOTIFY • AFF_NTF_USER_NOTIFY • REQ_MACBIND_INFO • ACK_MACBIND_INFO • NTF_USER_LOGON • NTF_USER_LOGOUT • REQ_USER_OFFLINE • UNKNOWN
Method	Portal的认证方法： • EAP：EAP 认证方法 • CHAP：CHAP 认证方法 • PAP：PAP 认证方法
Serial numner	Portal报文序列号
Reqest ID	Portal报文的请求ID
User IP	Portal用户的IP地址
Error code	错误码
Attribute count	Portal报文携带的属性个数

128 PORTSEC

本节介绍端口安全模块输出的日志信息。

128.1 PORTSEC_ACL_FAILURE

日志内容	-IfName=[STRING]-MACAddr=[STRING]; ACL authorization failed because[STRING].
参数解释	$1：接口名 $2：MAC地址 $3：下发ACL失败的原因
日志等级	5
举例	PORTSEC/5/PORTSEC_ACL_FAILURE:-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9; ACL authorization failed because the specified ACL didn't exist.
日志说明	下发授权ACL失败，及其原因 下发ACL失败的原因，包括如下取值： • the specified ACL didn't exist.：下发的 ACL 不存在 • this type of ACL is not supported.：不支持此 ACL 类型 • hardware resources were insufficient.：内存不足 • the specified ACL conflicted with other ACLs applied to the interface.：下发的 ACL 与接口上应用的其他 ACL 冲突 • the specified ACL didn't contain any rules.：下发的 ACL 中未包含规则
处理建议	根据失败原因修改配置

128.2 PORTSEC_LEARNED_MACADDR

日志内容	-IfName=[STRING]-MACAddr=[STRING]-VLANID=[STRING]; A new MAC address was learned.
参数解释	$1：接口名 $2：MAC地址 $3：VLAN ID
日志等级	6
举例	PORTSEC/6/PORTSEC_LEARNED_MACADDR:-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9-VLANID=444; A new MAC address was learned.
日志说明	学到一个新的安全MAC地址
处理建议	无

128.3 PORTSEC_NTK_NOT_EFFECTIVE

日志内容	The NeedToKnow feature is configured but is not effective on interface [STRING].
参数解释	$1：接口名
日志等级	3
举例	PORTSEC/3/PORTSEC_NTK_NOT_EFFECTIVE: The NeedToKnow feature is configured but is not effective on interface Ethernet3/1/2.
日志说明	NeedToKnow模式在接口上不生效，因为该接口不支持NeedToKnow模式
处理建议	无

128.4 PORTSEC_PORTMODE_NOT_EFFECTIVE

日志内容	The port security mode is configured but is not effective on interface [STRING].
参数解释	$1：接口名
日志等级	3
举例	PORTSEC/3/PORTSEC_PORTMODE_NOT_EFFECTIVE: The port security mode is configured but is not effective on interface Ethernet3/1/2.
日志说明	端口安全模式在接口上不生效，因为该接口不支持这种端口安全模式
处理建议	改变端口安全模式或关闭接口的端口安全特性

128.5 PORTSEC_PROFILE_FAILURE

日志内容	-IfName=[STRING]-MACAddr=[STRING]; Failed to assign a user profile to driver.
参数解释	$1：接口名 $2：MAC地址
日志等级	5
举例	PORTSEC/5/PORTSEC_PROFILE_FAILURE:-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9; Failed to assign a user profile to driver.
日志说明	下发user-profile到驱动失败
处理建议	无

128.6 PORTSEC_VIOLATION

日志内容	-IfName=[STRING]-MACAddr=[STRING]-VLANID=[STRING]-IfStatus=[STRING]; Intrusion protection was triggered.
参数解释	$1：接口名 $2：MAC地址 $3：VLAN ID $4：接口状态
日志等级	5
举例	PORTSEC/5/PORTSEC_VIOLATION:-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9-VLANID=444-IfStatus=Up; Intrusion protection was triggered.
日志说明	触发入侵检测
处理建议	检查配置情况或改变端口安全模式

129 PPP

本节介绍 PPP 模块输出的日志信息。

129.1 IPPOOL_ADDRESS_EXHAUSTED

日志内容	The address pool [STRING] was exhausted.
参数解释	$1：地址池名称
日志等级	5
举例	PPP/5/IPPOOL_ADDRESS_EXHAUSTED: The address pool aaa was exhausted.
日志说明	当地址池里最后一个地址分配出去时，打印本信息
处理建议	向地址池里添加地址

129.2 PPP_USER_LOGON_SUCCESS

日志内容	-UserName=[STRING]-IPAddr=[IPADDR]-IfName=[STRING]-OuterVLAN=[UINT16]-InnerVLAN=[UINT16]-MACAddr=[MAC]; The user came online successfully.
参数解释	$1：用户名 $2：IP地址 $3：接口名称 $4：外层VLAN ID $5：内层VLAN ID $6：MAC地址
日志等级	6
举例	PPP/6/PPP_USER_LOGON_SUCCESS: -UserName=abc-IPAddr=1.1.1.2-IfName=Route-Aggregation1023.4000-OuterVLAN=1000-InnerVLAN=4000-MACAddr=0230-0103-5601; The user came online successfully.
日志说明	用户上线成功
处理建议	无

129.3 PPP_USER_LOGON_FAILED

日志内容	-UserName=[STRING]-IPAddr=[IPADDR]-IfName=[STRING]-OuterVLAN=[UINT16]-InnerVLAN=[UINT16]-MACAddr=[MAC]-Reason=[STRING]; The user failed to come online.
参数解释	$1：用户名 $2：IP地址 $3：接口名称 $4：外层VLAN ID $5：内层VLAN ID $6：MAC地址 $7：上线失败原因，取值请参见表129-1
日志等级	5
举例	PPP/5/PPP_USER_LOGON_FAILED: -UserName=abc-IPAddr=1.1.1.2-IfName=Route-Aggregation1023.4000-OuterVLAN=1000-InnerVLAN=4000-MACAddr=0230-0103-5601-Reason=Authentication failed; The user failed to come online.
日志说明	用户上线失败
处理建议	具体处理建议请见表129-1

表129-1 上线失败原因列表

上线失败原因	说明	处理建议
Authentication failed	认证失败	• 检查设备与认证服务器之间的通信是否正常 • 检查用户名是否合法

上线失败原因	说明	处理建议
		• 检查密码是否正确 • 检查设备上的认证域是否正确
Authentication method error	配置的认证方法错误。通常是用户请求的认证类型与端口下配置的认证类型不一致导致上线失败	检查配置的认证方式是否正确
Authorization failed	授权失败	• 检查设备与授权服务器之间的通信是否正常 • 检查授权服务器下发的授权属性在设备上是否存在并正确配置 • 检查设备是否支持授权服务器下发的授权属性
IP assignment failed	分配IP失败	检查地址池中地址是否已经耗尽
Accounting failed	计费失败	• 检查设备与计费服务器之间的通信是否正常 • 检查认证计费服务器状态是否正常
AAA access limit reached	一个帐号允许接入的用户数超过了限制	• 检查一个帐号上线用户数 • 通过 **access-limit** 命令将使用当前本地用户名接入设备的最大用户数调整为更大的值
The local user does not exist	未配置该本地用户	• 检查拨号用户是否为合法用户 • 如果是合法用户接入，但设备上不存在对应本地用户，则需要在本地添加该用户
Local authentication failed: wrong password	用户密码错误导致本地认证被拒绝	• 检查用户名是否合法 • 检查密码是否正确
No AAA response during authentication	设备在认证超时时间内未收到认证服务器的回应	• 检查认证服务器是否可达 • 检查认证服务器状态是否正常 • 检查设备与认证服务器上配置的共享密钥是否相同
RADIUS authentication reject	RADIUS服务器回应认证拒绝	• 检查用户名是否合法 • 检查密码是否正确
AAA authorization information error	添加用户授权信息失败	检查授权服务器下发的授权属性在设备上是否存在并正确配置
Authentication request to AAA failed	设备向AAA服务器发送认证请求失败	• 检查设备与认证服务器之间的通信是否正常 • 检查认证服务器状态是否正常
Accounting request to AAA failed	设备向AAA服务器发送计费请求失败	• 检查设备与计费服务器之间的通信是否正常 • 检查计费服务器状态是否正常
No authentication ACK from AAA	设备没有收到AAA服务器回应的认证ACK报文	• 检查设备与认证服务器之间的通信是否正常 • 检查认证服务器状态是否正常
TACACS authentication reject	TACACS服务器回应认证失败	• 检查用户名是否合法 • 检查密码是否正确
DHCP decline	DHCP拒绝IP地址申请	检查是否有可用的IP地址

上线失败原因	说明	处理建议
No response from DHCP server	DHCP server服务器没有应答	检查DHCP server服务器是否可达
Failed to allocate public network ports in a CGN network	NAT分配公网端口失败	检查在CGN组网中的NAT配置是否正确以及端口块资源是否耗尽（端口块中的所有端口都被使用）

129.4 PPP_USER_LOGOFF

日志内容	-UserName=[STRING]-IPAddr=[IPADDR]-IfName=[STRING]-OuterVLAN=[UINT16]-InnerVLAN=[UINT16]-MACAddr=[MAC]-Reason=[STRING]; The user logged off.
参数解释	$1：用户名 $2：IP地址 $3：接口名称 $4：外层VLAN ID $5：内层VLAN ID $6：MAC地址 $7：下线原因，取值请参见表129-2
日志等级	6
举例	PPP/6/PPP_USER_LOGOFF: -UserName=abc-IPAddr=1.1.1.2-IfName=Route-Aggregation1023.4000-OuterVLAN=1000-InnerVLAN=4000-MACAddr=0230-0103-5601-Reason=Use request; The user logged off.
日志说明	用户正常下线
处理建议	无

表129-2 正常下线原因列表

下线原因	说明
User request	用户主动要求终止连接

129.5 PPP_USER_LOGOFF_ABNORMAL

日志内容	-UserName=[STRING]-IPAddr=[IPADDR]-IfName=[STRING]-OuterVLAN=[UINT16]-InnerVLAN=[UINT16]-MACAddr=[MAC]-Reason=[STRING]; The user logged off abnormally.
参数解释	$1：用户名 $2：IP地址 $3：接口名称 $4：外层VLAN ID $5：内层VLAN ID $6：MAC地址 $7：下线原因，具体原因请见表129-3
日志等级	6
举例	PPP/6/PPP_USER_LOGOFF_ABNORMAL: -UserName=abc-IPAddr=1.1.1.2-IfName=Route-Aggregation1023.4000-OuterVLAN=1000-InnerVLAN=4000-MACAddr=0230-0103-5601-Reason=Lost Carrier; The user logged off abnormally.
日志说明	用户异常下线
处理建议	具体处理建议请见表129-3

表129-3 异常下线原因列表

下线原因	说明	处理建议
Lost carrier	协议保活报文丢失。通常由BAS下一级网络设备（含该设备）到用户设备间的故障引起	请将相关日志信息保存到本地，并联系H3C技术支持
Lost service	业务服务器（例如：L2TP）主动发起终止用户业务服务的报文	无
BAS error	由于BAS内部软件处理异常造成用户掉线	请将相关日志信息保存到本地，并联系H3C技术支持
BAS reboot	BAS异常重启前发送断线信息，以进行非管理性的重启	请将相关日志信息保存到本地，并联系H3C技术支持
Admin reset	由于管理的需要，管理员在用户接入接口配置**shutdown**命令，临时中断用户的连接	无
BAS request	其它未规定的掉线原因	请将相关日志信息保存到本地，并联系H3C技术支持
Session timeout	用户上线时间达到了规定值	通知用户流量耗尽或则去续费
Traffic quota limit reached	用户的流量达到了规定值	通知用户流量耗尽或则去续费
Logged off by the RADIUS server	AAA服务器强制下线	无
Accounting update failure	计费更新失败	• 检查设备与计费服务器之间的通信是否正常

下线原因	说明	处理建议
		• 检查计费服务器状态是否正常
Port error	BAS主动检测到用户接入端口的错误	检查用户接入单板或者端口是否异常
Admin reboot	管理员通过**reboot**命令重启设备	无
No AAA response during realtime accounting	用户在超时时间内未收到计费服务器的回应（实时计费阶段）	• 检查设备与计费服务器之间的通信是否正常 • 检查计费服务器状态是否正常
No AAA response for accounting start	用户在超时时间内未收到认证服务器的回应（开始计费阶段）	• 检查设备与计费服务器之间的通信是否正常 • 检查计费服务器状态是否正常
No AAA response for accounting stop	用户在超时时间内未收到认证服务器的回应（停止计费阶段）	• 检查设备与计费服务器之间的通信是否正常 • 检查计费服务器状态是否正常
PPP negotiation terminated	PPP协商过程被中断	检查配置是否正确
Repeated LCP negotiation packets	收到重复的LCP协商报文	客户端断开重新发起连接
The interface that the user accesses goes down	用户接入接口状态为Down	• 检查用户接入接口网线连接是否正常 • 检查用户接入单板或者子卡是否异常或被拔出
The interface that the user accesses is shut down	用户接入接口状态为Down	检查用户接入端口是否配置了命令**shutdown**
Failed to set up an L2TP session	L2TP会话建立失败	请将相关日志信息保存到本地，并联系H3C技术支持
L2TP tunnel reset by command	设备上执行**reset l2tp tunnel**命令，导致L2TP用户下线	无
L2TP tunnel terminated by the peer	对端LAC/LNS设备检测到用户下线，拆除隧道	无
The peer did not respond to control packets	对端设备不响应。L2TP隧道内所有的协议报文一直没有得到对接设备的响应导致隧道Down	• 检查对端设备是否可达 • 检查对端设备 L2TP 协议状态是否正确
Realtime accounting request to AAA failed	设备向AAA服务器发送实时计费请求失败	• 检查设备与计费服务器之间的通信是否正常 • 检查计费服务器状态是否正常
Session idle cut	用户在规定时间内的流量没有达到设定值	无
DHCP lease timeout	DHCP租约过期	通知用户地址租约到期
DHCP user request	用户主动请求下线	无
DHCP configuration change	DHCP配置变化引起用户下线	检查DHCP相关配置
IP conflict on DHCP	DHCP server服务器上发现IP地址冲突	检查是否授权了重复的IP地址

下线原因	说明	处理建议
server		
Failed to obtain an IP address of the type specified for basic services of users	由于主业务依赖的IP地址分配失败导致用户异常下线	• 检查主业务相关配置是否正确，例如：**basic-service-ip-type** 命令是否指定了正确的 IP 地址类型 • 检查用于给用户分配主业务 IP 地址的地址池（DHCP 地址池或 PPP 地址池）配置是否正确
Internal Error	未知内部错误	请将相关日志信息保存到本地，并联系H3C技术支持
Released public network ports in a CGN network	CGN单板被拔出或CGN单板处于异常状态导致NAT释放公网端口	检查CGN单板是否被拔出或处于异常状态
Magic number check failed	魔术字检查失败导致用户下线	• 检查链路两端接口是否配置了 **ppp magic-number-check** 命令 • 检查链路两端是否都正常在电运行 • 链路任意一端重新发起连接
MAC conflict	MAC地址冲突导致用户异常下线	• 检查是否通过 **pppoe-server session-limit per-mac** 命令配置了每个用户所能创建 PPPoE 会话的最大数目为 1（缺省为 1） • 检查是否有相同 MAC 地址的用户上线

129.6 PPPOES_LIMIT

日志内容	Maximum number of PPPoE sessions already reached.
参数解释	无
日志等级	3
举例	PPPOES/3/PPPOES_LIMIT: Maximum number of PPPoE sessions already reached.
日志说明	PPPoE用户上线已达到系统允许上线的最大数目，新用户无法上线
处理建议	1. 确认 **pppoe-server session-limit total** 配置 2. 执行 **display pppoe-server session summary slot** 命令查看当前单板上的 PPPoE 会话数是否已达到系统允许创建的最大数目 3. 如果非上述原因导致新用户无法上线，请联系 H3C 技术支持

129.7 PPPOES_LIMIT_VLAN

日志内容	Maximum number of PPPoE sessions for the VLAN already reached.
参数解释	无
日志等级	3
举例	PPPOES/3/PPPOES_LIMIT_VLAN: Maximum number of PPPoE sessions for the VLAN already reached.
日志说明	PPPoE用户上线已达到每个VLAN创建会话最大数目，新用户无法上线
处理建议	1. 确认 **pppoe-server session-limit per-vlan** 配置 2. 执行 **display pppoe-server session summary interface** 命令查看当前接口上的 PPPoE 会话数是否已达到 VLAN 允许创建的最大数目 3. 如果非上述原因导致新用户无法上线，请联系 H3C 技术支持

129.8 PPPOES_LIMIT_IF

日志内容	Maximum number of PPPoE sessions for the interface already reached.
参数解释	无
日志等级	3
举例	PPPOES/3/PPPOES_LIMIT_IF: Maximum number of PPPoE sessions for the interface already reached.
日志说明	PPPoE用户上线已达到接口创建会话最大数目，新用户无法上线
处理建议	1. 确认 **pppoe-server session-limit** 配置 2. 执行 **display pppoe-server session summary interface** 命令查看当前接口上的 PPPoE 会话数是否已达到接口允许创建的最大数目 3. 如果非上述原因导致新用户无法上线，请联系 H3C 技术支持

129.9 PPPOES_LIMIT_MAC

日志内容	Maximum number of PPPoE sessions for the user already reached.
参数解释	无
日志等级	3
举例	PPPOES/3/PPPOES_LIMIT_MAC: Maximum number of PPPoE sessions for the user already reached.
日志说明	PPPoE用户上线已达到每个用户创建会话最大数目，新用户无法上线
处理建议	1. 确认 **pppoe-server session-limit per-mac** 配置 2. 执行 **display pppoe-server session summary interface** 命令查看当前接口上的 PPPoE 会话数是否已达到用户允许创建的最大数目 3. 如果非上述原因导致新用户无法上线，请联系 H3C 技术支持

129.10 PPPOES_MAC_THROTTLE

日志内容	The MAC [STRING] triggered MAC throttle on interface [STRING].
参数解释	$1：MAC 地址 $2：接口名称
日志等级	5
举例	PPPOES/5/PPPOES_MAC_THROTTLE: -MDC=1; The MAC 001b-21a8-0949 triggered MAC throttle on interface GigabitEthernet1/0/1.
日志说明	在监视时间段内某PPPoE用户建立会话请求数目已达到接入接口允许每个用户会话请求数目的最大值，在扼制时间内接入接口直接丢弃该用户的会话请求
处理建议	1. 确认 **pppoe-server throttle per-mac** 配置 2. 执行 **display pppoe-server throttled-mac** 命令查看用户接入接口上被扼制用户的剩余扼制时间 3. 如果非上述原因导致新用户无法上线，请联系 H3C 技术支持

129.11 USER_TRACEINFO

日志内容	[objectID=[UINT16]][slotID=[UINT16]][STRING][user info: [STRING]][trace info:[STRING]]
参数解释	$1：业务跟踪对象的编号 $2：接入用户所属的槽位号 $3：业务跟踪阶段，目前有PPPoE、L2TP、PPP和AAA四个阶段 $4：用户信息。各用户信息含义请参见表65-6 $5：跟踪详细信息。PPPoE、L2TP、PPP和AAA阶段的详细跟踪信息请分别参见表129-5、表129-6、表129-7和表65-8
日志等级	7
举例	USER/7/USER_TRACEINFO:[objectID=1][slotID=1][PPPoE][user info: MAC address:000c-29b9-c92e Access interface:GigabitEthernet1/0/1 Access mode:PPPoE] [trace info: Receive a PADI packet 11 09 00 00 0a 00 01 01 00 00 01 03 00 02 00 01]
日志说明	编号为1业务跟踪对象在PPPoE阶段，从1号槽位的GigabitEthernet1/0/1接口收到一个PADI报文
处理建议	无

表129-4 被跟踪用户信息描述表

字段	描述
MAC address	接入用户的MAC地址
Access interface	接入用户接入接口
Service VLAN	接入用户的外层VLAN ID
Customer VLAN	接入用户的内层VLAN ID
Tunnel ID	接入用户的L2TP隧道ID
Username	接入用户的用户名
IP address	接入用户的IP地址
Access mode	业务跟踪对象的接入模式

表129-5 被跟踪详细信息描述表（PPPoE）

字段	描述
Received a PADI packet	PPPoE Sever收到PPPoE Client的PADI报文
Sent a PADO packet	PPPoE Server向PPPoE Client发送PADO报文
Received a PADR packet	PPPoE Sever收到PPPoE Client的PADR报文
Sent a PADS packet	PPPoE Server向PPPoE Client发送PADS报文

字段	描述
Established a PPPoE session successfully. Notified PPP Start Session (session ID=1)	建立PPPoE会话，通知PPP开始会话协商
Received a PADT packet	PPPoE Sever收到PPPoE Client的PADT报文
Deleted the PPPoE session successfully.	删除PPPoE会话

表129-6 被跟踪详细信息描述表（L2TP）

字段	描述
PPP notified LAC up and L2TP started a tunnel establishment process	PPP通知LAC up事件，LAC端发起L2TP隧道协商
PPP notified LAC up and L2TP started establishing a session within a middle state L2TP tunnel	PPP通知LAC up事件，LAC端在一个中间状态的L2TP隧道中发起L2TP会话协商
PPP notified LAC up and L2TP started establishing a session within an L2TP tunnel	PPP通知LAC up事件，LAC端在一个已经建立的L2TP隧道中发起L2TP会话协商
Sent an ICRQ packet to LNS, TunnelID=1, SessionID=2	LAC端向LNS端发送ICRQ报文
Received an ICRP packet, TunnelID=1, SessionID=2	LAC端收到ICRP报文
Sent an ICCN packet to LNS, TunnelID=1, SessionID=2	LAC端向LNS端发送ICCN报文
Received an ICCN packet and processed successfully, TunnelID=1, SessionID=2	LNS端收到ICCN报文，处理成功
Received an invalid ICCN packet and failed to process it, TunnelID=1, SessionID=2	LNS端收到非法ICCN报文，处理失败
Received an ICCN packet but failed to allocate resources, TunnelID=1, SessionID=2	LNS端收到ICCN报文，资源不足处理失败
Received an ICCN packet but failed to process it, TunnelID=1, SessionID=2	LNS端收到ICCN报文，但处理失败
An L2TP session on LAC was going offline, TunnelID=1, SessionID=2	LAC端L2TP会话正在下线
An L2TP session on LNS was going offline, TunnelID=1, SessionID=2	LNS端L2TP会话正在下线
Sent a CDN packet to the peer, TunnelID=1, SessionID=2	本端向对端发送CDN报文
Received a CDN packet, TunnelID=1, SessionID=2	本端收到对端发送的CDN报文
Deleted an L2TP session, TunnelID=1, SessionID=2	删除本地L2TP会话

表129-7 被跟踪详细信息描述表（PPP）

字段	描述
Received interface up event	PPP收到接口up事件
LCP FSM open event	PPP LCP状态机open事件

字段	描述
Determined negotiation parameters during LCP initialization	LCP初始化，确定LCP需要协商参数
LCP FSM up event	PPP LCP状态机up事件
Sent an LCP Configuration Request packet	PPP发送LCP Configure-Request报文
Received an LCP negotiation packet or Echo keepalive packet	PPP收到LCP协商报文或echo保活报文
Received an LCP Configuration Request packet	PPP收到LCP Configure-Request报文
Sent an LCP Configuration Ack packet	PPP发送LCP Configure-Ack报文
Received an LCP Configuration Ack packet	PPP收到LCP Configure-Ack报文
LCP up event	PPP LCP 协商成功
LCP FSM down event	PPP LCP状态机down事件
LCP down event	PPP收到LCP down事件
Logged out the user as requested	PPP收到下线请求，用户下线
LCP FSM close event	PPP LCP状态机close事件
Started authentication after LCP negotiation succeeded	PPP LCP 协商阶段成功，进入认证阶段
Sent a CHAP Challenge packet	PPP CHAP认证阶段发送Challenge报文
Received a CHAP authentication packet in authentication phase	PPP在认证阶段收到CHAP认证类型报文
Received a CHAP Request packet	PPP收到CHAP认证请求报文
Sent an authentication request to AAA	PPP向AAA发送认证请求，进行认证
Received a CHAP authentication success message from AAA	PPP收到AAA的CHAP认证成功消息
Sent a CHAP Ack to the client	PPP向客户端发送CHAP认证成功报文
CHAP authentication succeeded	PPP CHAP认证成功
Received a CHAP authentication failure message from AAA	PPP收到AAA的CHAP认证失败消息
Sent a CHAP Nak to the client	PPP向客户端发送CHAP认证失败报文
Received a PAP authentication packet in authentication phase	PPP在认证阶段收到PAP认证类型报文
Received a PAP Request packet	PPP收到PAP认证请求报文
Received a PAP authentication success message from AAA	PPP收到AAA的PAP认证成功消息
Sent a PAP Ack to the client	PPP向客户端发送PAP认证成功报文
PAP authentication succeeded	PPP PAP认证成功
PAP authentication failed	PPP PAP认证失败
Received a PAP authentication failure message from	PPP收到AAA的PAP认证失败消息

字段	描述
AAA	
Sent a PAP Nak to the client	PPP向客户端发送PAP认证失败报文
Received an LCP Termination Request packet	PPP收到LCP Terminate-Request报文
Sent an LCP Termination Ack packet	PPP发送LCP Terminate-Ack报文
Started NCP negotiation	PPP 进入NCP协商阶段
IPCP FSM open event	PPP IPCP状态机open事件
Determined negotiation parameters during IPCP initialization	初始化IPCP协商选项
IPCP FSM up event	PPP IPCP状态机up事件
Sent an IPCP Configuration Request packet	PPP发送IPCP Configure-Request报文
Received an IPCP negotiation packet in IPCP negotiation phase	PPP在IPCP协商阶段收到IPCP协商报文
Received an IPCP Configuration Request packet	PPP收到IPCP Configure-Request报文
Received an IPCP Configuration Ack packet	PPP收到IPCP Configure-Ack报文
Sent an IPCP Configuration Nak packet	PPP发送IPCP Configure-Nak报文
Sent an IPCP Configuration Ack packet	PPP发送IPCP Configure-Ack报文
IPCP negotiation succeeded	PPP IPCP 协商成功
User came online successfully	用户成功上线
Logged out the user as lost carrier	协议保活报文丢失。通常由BAS下一级网络设备（含该设备）到用户设备间的故障引起
Logged out the user as lost service	业务服务器（例如：L2TP）主动发起终止用户业务服务的报文
Logged out the user as BAS error	由于BAS内部软件处理异常造成用户掉线
Logged out the user as BAS reboot	BAS异常重启前发送断线信息，以进行非管理性的重启
Logged out the user as admin reset	由于管理的需要，管理员在用户接入接口配置**shutdown**命令，临时中断用户的连接
Logged out the user as BAS request	其它未规定的掉线原因
Logged out the user as session timeout	用户上线时间达到了规定值
Logged out the user as RADIUS server	AAA服务器强制下线
Logged out the user as session idle cut	用户在规定时间内的流量没有达到设定值
Logged out the user as accounting update failure	计费更新失败
Logged out the user as port error	BAS主动检测到用户接入端口的错误
Logged out the user as admin reboot	管理员通过**reboot**命令重启设备
Logged out the user as authentication failure	认证失败
Logged out the user as authorization failure	授权失败

字段	描述
Logged out the user as ip assignment failure	分配IP失败
Logged out the user as accounting failure	计费失败
Free ip address	PPP释放IP地址
Sent an LCP Echo Request packet	PPP发送Echo-Request报文
Received an LCP Echo Reply packet	PPP收到Echo-Reply报文
Received interface down event	PPP收到接口down事件
IPCP FSM down event	PPP IPCP状态机down事件
IPCP down event	PPP收到IPCP down事件
IPCP FSM close event	PPP IPCP状态机close事件
Notify NCP down	LCP通知上层协议NCP down
PPP L2TP prenego started	PPP L2TP预协商开始
PPP L2TP prenego finished	PPP L2TP预协商结束
Mandatory-lcp, LCP renego started	强制LCP重协商，开始LCP重协商
Mandatory-chap, CHAP renego started	强制CHAP验证，开始CHAP验证
L2TP mandatory-chap needed the authentication mode of CHAP on VT	配置强制CHAP验证，但VT口上没有配置CHAP认证方式
LCP prenego for L2TP failed	LCP预协商失败
PPP L2TP prenego CHAP started	CHAP认证预协商开始
PPP L2TP prenego CHAP finished	CHAP认证预协商结束
PPP L2TP prenego PAP started	PAP认证预协商开始
PPP L2TP prenego PAP finished	PAP认证预协商结束
PPP L2TP prenego MSCHAP started	MSCHAP认证预协商开始
PPP L2TP prenego MSCHAP finished	MSCHAP认证预协商结束
PPP L2TP prenego authentication failed	PPP L2TP认证预协商失败

表129-8 被跟踪详细信息描述表（AAA）

字段	描述
LocalAuth: Authentication request initiated	本地认证：认证请求初始化
LocalAuth: Authentication succeeded	本地认证：认证成功
LocalAuth: Authorization request initiated	本地认证：授权请求初始化
LocalAuth: Authorization succeeded	本地认证：授权成功
LocalAuth: Accounting start request initiated	本地认证：计费开始请求初始化
LocalAuth: Accounting start succeeded	本地认证：计费开始成功

字段	描述
LocalAuth: Accounting stop request initiated	本地认证：计费停止请求初始化
LocalAuth: Accounting stop succeeded	本地认证：计费停止成功
LocalAuth: Authentication failed/Wrong password	本地认证：密码错误导致认证失败
LocalAuth: Authorization failed/Wrong password	本地认证：密码错误导致授权失败
LocalAuth: Accounting start failed/Wrong password	本地认证：密码错误导致计费开始失败
LocalAuth: Accounting stop failed/Wrong password	本地认证：密码错误导致计费停止失败
LocalAuth: Authentication failed/User blocked	本地认证：用户状态为block导致认证失败
LocalAuth: Authorization failed/User blocked	本地认证：用户状态为block导致授权失败
LocalAuth: Accounting start failed/User blocked	本地认证：用户状态为block导致计费开始失败
LocalAuth: Accounting stop failed/User blocked	本地认证：用户状态为block导致计费停止失败
LocalAuth: Authentication failed/Service type mismatch	本地认证：用户接入类型不匹配，导致认证失败
LocalAuth: Authorization failed/Service type mismatch	本地认证：用户接入类型不匹配导致授权失败
LocalAuth: Accounting start failed/Service type mismatch	本地认证：用户接入类型不匹配导致计费开始失败
LocalAuth: Accounting stop failed/Service type mismatch	本地认证：用户接入类型不匹配导致计费停止失败
LocalAuth: Authentication failed/Binding attribute mismatch	本地认证：用户绑定属性与实际属性不符，导致认证失败
LocalAuth: Authorization failed/Binding attribute mismatch	本地认证：用户绑定属性与实际属性不符导致授权失败
LocalAuth: Accounting start failed/Binding attribute mismatch	本地认证：用户绑定属性与实际属性不符导致计费开始失败
LocalAuth: Accounting stop failed/Binding attribute mismatch	本地认证：用户绑定属性与实际属性不符导致计费停止失败
LocalAuth: Accounting start failed/Access limit reached	本地认证：用户接入数达到上限导致计费开始失败
LocalAuth: Authentication failed/User doesn’t exist	本地认证：用户不存在导致认证失败
LocalAuth: Authorization failed/User doesn’t exist	本地认证：用户不存在导致授权失败
LocalAuth: Accounting start failed/User doesn’t exist	本地认证：用户不存在导致计费开始失败
LocalAuth: Accounting stop failed/User doesn’t exist	本地认证：用户不存在导致计费停止失败
RADIUS: Authentication request initiated	RADIUS：认证请求初始化
RADIUS: Authentication succeeded	RADIUS：认证成功
RADIUS: Accounting start request initiated	RADIUS：计费开始请求初始化
RADIUS: Accounting start succeeded	RADIUS：计费开始成功
RADIUS: Accounting stop request initiated	RADIUS：计费停止请求初始化

字段	描述
RADIUS: Accounting stop succeeded	RADIUS：计费停止成功
RADIUS: Authentication failed/Server reject	RADIUS：因用户密码错误等原因RADIUS服务器返回拒绝
RADIUS: Authentication failed/System error	RADIUS：因指定的RADIUS方案不存在等原因的系统错误，导致认证失败
RADIUS: Accounting start failed/System error	RADIUS：因指定的RADIUS方案不存在等原因的系统错误导致计费开始失败
RADIUS: Accounting update failed/System error	RADIUS：因指定的RADIUS方案不存在等原因的系统错误导致计费更新失败
RADIUS: Accounting stop failed/System error	RADIUS：因指定的RADIUS方案不存在等原因的系统错误导致计费停止失败
RADIUS: Authentication failed/Response timeout	RADIUS：因请求回应超时导致认证失败
RADIUS: Accounting start failed/Response timeout	RADIUS：因请求回应超时导致计费开始失败
RADIUS: Accounting update failed/Response timeout	RADIUS：因请求回应超时导致计费更新失败
RADIUS: Accounting stop failed/Response timeout	RADIUS：因请求回应超时导致计费停止失败
RADIUS: Accounting update request initiated	RADIUS：计费更新请求初始化
RADIUS：Authentication failed/Server blocked	RADIUS：因指定RADIUS方案下配置的所有认证服务器均无回应导致认证失败
RADIUS: Accounting start failed/Server blocked	RADIUS：因指定RADIUS方案下配置的所有计费服务器均无回应导致计费开始失败
RADIUS: Accounting update failed/Server blocked	RADIUS：因指定RADIUS方案下配置的所有计费服务器均无回应导致计费更新失败
RADIUS: Accounting stop failed/Server blocked	RADIUS：因指定RADIUS方案下配置的所有计费服务器均无回应导致计费停止失败

130 PPPoE

本节介绍 PPPoE 模块输出的日志信息。

130.1 PPPOE_DAPI

日志内容	No enough resource
参数解释	N/A
日志等级	4
举例	DPPPOE/4/PPPOE_DAPI: -MDC=1; No enough resource
日志说明	当设备切换成DP工作在转控分离模式时，添加VBRAS协议上送硬件资源不足
处理建议	1. 执行 **display qos-acl resource** 命令查看当前单板上 IPv4 ACL 与 IPv6 ACL 资源的使用情况 2. 请联系技术支持

130.2 PPPOE_PADI

日志内容	No enough resource.
参数解释	无
日志等级	4
举例	DPPPOE/4/PPPOE_PADI: -MDC=1; No enough resource.
日志说明	对于CSPEX类单板（除CSPEX-1204之外）、CEPC类单板上的PADI防攻击，产品已经达到规格限制
处理建议	请联系技术支持

130.3 PADI_DEFEND

日志内容	ARP MAC entries do not have enough resources.
参数解释	无
日志等级	4
举例	DPPPOE/4/PADI_DEFEND: -MDC=1-Slot=3; ARP MAC entries do not have enough resources.
日志说明	对于CSPEX类单板（除CSPEX-1204之外）、CEPC类单板上的PADI防攻击，产品已经达到规格限制
处理建议	无

130.4 PPPOE_ENABLE

日志内容	The resources are insufficient.
参数解释	无
日志等级	4
举例	DPPPOE/4/PPPOE_ENABLE: -MDC=1-Slot=3; The resources are insufficient.
日志说明	在某接口上启用PPPoE Server协议，将该接口与虚拟模板接口绑定时，因TCAM资源不足导致DHCPv6协议下发失败
处理建议	1. 通过关闭所绑定 VT 口下的无用协议，或减少某些无用接口与 VT 口的绑定的方式，释放出足够的 TCAM 资源，然后先取消绑定 VT 口，再重新绑定 VT 口 2. 如果仅仅是通过 DHCPv6 分配 IPv6 地址，在不释放 TCAM 资源的情况下，可通过其它地址分配方式（例如：客户端通过 ND 协议中的 RA 报文获得 IPv6 地址前缀）为客户端分配地址

130.5 PPPOE_TABLE

日志内容	No enough resource
参数解释	N/A
日志等级	4
举例	DPPPOE/4/PPPOE_TABLE: -MDC=1; No enough resource
日志说明	PPPoE会话或硬件资源不足，无法完成当前操作。例如，PPPoE用户上线已达到系统最大规格，新用户无法上线
处理建议	1. 执行 display pppoe-server session summary slot 命令查看当前单板上的 PPPoE 会话数是否超过产品规格的最大数 2. 执行 display qos-acl resource 命令查看当前单板上资源的使用情况 3. 请联系技术支持

131 PS

本节介绍 PS 模块输出的日志信息。

131.1 PS_SWITCH_WTOP

日志内容	Tunnel-bundle[STRING]: Switched from working tunnel [STRING] to protection tunnel [STRING].
参数解释	$1：Tunnel-bundle隧道信息 $2：主隧道信息 $3：备隧道信息
日志等级	4
举例	PS/4/PS_SWITCH_WTOP: Tunnel-bundle1: Switched from working tunnel tunnel1 to protection tunnel tunnel2.
日志说明	当主隧道缺陷，切换到备隧道时，触发该日志
处理建议	无

131.2 PS_SWITCH_PTOW

日志内容	Tunnel-bundle[STRING]: Switched from protection tunnel [STRING] to working tunnel [STRING].
参数解释	$1：Tunnel-bundle隧道信息 $2：备隧道信息 $3：主隧道信息
日志等级	4
举例	PS/4/PS_SWITCH_PTOW: Tunnel-bundle1: Switched from protection tunnel tunnel1 to working tunnel tunnel2.
日志说明	当主隧道主缺陷恢复，回切到主隧道时，触发该日志
处理建议	无

132 PTP

本节介绍 PTP 模块输出的日志信息。

132.1 PTP_CLOCK_SOURCE_CLASS_BELOW_THRESHOLD

日志内容	The clock source class fell below the threshold.
参数解释	无
日志等级	4
举例	PTP/4/PTP_CLOCK_SOURCE_CLASS_BELOW_THRESHOLD: The clock source class fell below the threshold.
日志说明	时钟源劣化告警阈值，原因包括： • 当设备通过 PTP 输入接口中分组报文获取时钟源时，当前选用 PTP 本地时钟源的时钟等级低于时钟等级阈值，且 PTP 时钟源的 stepsRemoved 值为 0 • 当设备通过 TOD 输入接口获取时钟源时，当前选用 TOD 外接时钟源的时钟等级低于时钟等级阈值
处理建议	使用**display ptp clock**命令，查看Class字段显示当前时钟源等级是否低于告警阈值 • 若低于告警阈值，在时钟源所在设备上调高时钟等级或者切换时钟源为时钟等级更高的时钟源，查看告警是否打印 PTP_CLOCK_SOURCE_CLASS_RECOVER 日志 ◦ 若查看到 PTP_CLOCK_SOURCE_CLASS_RECOVER 日志，正常告警 ◦ 若未查看到此日志，则收集告警、日志和配置信息，联系技术支持 • 若高于告警阈值，收集告警、日志和配置信息，联系技术支持

132.2 PTP_CLOCK_SOURCE_CLASS_RECOVER

日志内容	The clock source class crossed the threshold.
参数解释	无
日志等级	4
举例	PTP/4/PTP_CLOCK_SOURCE_CLASS_RECOVER: The clock source class crossed the threshold.
日志说明	时钟源输入时钟等级高于或者等于劣化告警阈值
处理建议	无

132.3 PTP_EXT_TIME_PORT_DISCONNECT

日志内容	The external time port became disconnect. (ExtTimePortType=[STRING])
参数解释	$1：外部时钟源的接口类型，取值包括： ○ ToD0：第一路 ToD 时钟 ○ ToD1：第一路 ToD 时钟
日志等级	4
举例	PTP/4/PTP_EXT_TIME_PORT_DISCONNECT: The external time port became disconnect. (ExtTimePortType=ToD0)
日志说明	设备无法接收到外部时钟源的时钟信号或外部时钟源断开与本端设备的连接
处理建议	请确认连接外部时钟源的PTP接口是否UP： • PTP 接口 UP，则收集告警、日志和配置信息，联系技术支持 • PTP 接口 DOWN，则表示链路故障或接口 DOWN，排除故障恢复链路

132.4 PTP_EXT_TIME_PORT_RECOVER

日志内容	The external time port status resumed. (ExtTimePortType=[STRING])
参数解释	$1：外部时钟源的端口类型，取值包括： ○ ToD0：第一路 ToD 时钟 ○ ToD1：第一路 ToD 时钟
日志等级	4
举例	PTP/4/PTP_EXT_TIME_PORT_RECOVER: The external time port status resumed. (ExtTimePortType=ToD0)
日志说明	设备重新接收到外部时钟源的时钟信号，外部时钟源与本设备相连的物理链路恢复连接
处理建议	无

132.5 PTP_FREQUENCY_LOCK

日志内容	Clock frequency resumed to locked state.
参数解释	无
日志等级	3
举例	PTP/3/PTP_FREQUENCY_LOCK: Clock frequency resumed to locked state.
日志说明	时钟从频率失锁状态中恢复为正常
处理建议	无

132.6 PTP_FREQUENCY_NOT_LOCK

日志内容	Clock frequency not in locked state.
参数解释	无
日志等级	3
举例	PTP/3/PTP_FREQUENCY_NOT_LOCK: Clock frequency not in locked state.
日志说明	时钟频率失锁告警，原因包括： • 以太频率同步模式下，参考源频偏过大 • 1588v2 频率同步模式下，时间戳异常 • 系统时钟的输出频率频偏超过+/-10ppm

处理建议	设备打印该告警以后，是否打印了PTP_FREQUENCY_LOCK日志
	• 若查看到 PTP_FREQUENCY_LOCK 日志，则表示设备刚启动或者频率发生震荡，正常告警
	• 若未查看到此日志，则查看 PTP 配置信息是否发生改变
	  ○ 若 PTP 配置信息发生改变，则恢复配置
	  ○ 若 PTP 配置信息未发生改变，则收集告警、日志和配置信息，联系技术支持

132.7 PTP_MASTER_CLOCK_CHANGE

日志内容	PTP master clock property changed. (OldMasterClockId=[STRING], CurrentMasterClockId=[STRING], NewSourceIfIndex=[UINT16], OldSourcePortNum=[UINT16], CurrentSourcePortNum=[UINT16], OldSourcePortName=[STRING], CurrentSourcePortName=[STRING])
参数解释	$1：原来主时钟ID $2：当前主时钟ID $3：新的时钟源索引 $4：曾为本设备提供时钟源的接口编号 $5：当前为本设备提供时钟源的接口编号 $6：曾为本设备提供时钟源的接口名称 $7：当前为本设备提供时钟源的接口名称
日志等级	4
举例	PTP/4/PTP_MASTER_CLOCK_CHANGE: PTP master clock property changed. (OldMasterClockId=000FE2-FFFE-FF0000, CurrentMasterClockId=000FE2-FFFE-FF0000, NewSourceIfIndex=1, OldSourcePortNum=2, CurrentSourcePortNum=1, OldSourcePortName=G1/0/2, CurrentSourcePortName=G1/0/1)
日志说明	主时钟源属性发生改变，原因包括： • PTP 域内的时钟设备属性发生变化，导致出现了优先级更高的时钟源或获取时钟源的路径发生了改变 • 接入了优先级更高的时钟源 • 接收时钟源信号的 PTP 接口所在链路故障或者 PTP 接口 DOWN

处理建议	使用**display ptp interface brief**命令查看是否存在PTP接口处于Fault状态
	• 若存在接口处于 Fault 状态，则表示该状态为 PTP 协议的错误状态（即检测到错误），接口不处理 PTP 协议报文；收集告警、日志和配置信息，联系技术支持
	• 若不存在接口处于 Fault 状态，则查看 PTP 配置信息是否发生改变
	  ○ 若 PTP 配置信息发生改变，则恢复配置
	  ○ 若 PTP 配置信息未发生改变，则收集告警、日志和配置信息，联系技术支持

132.8 PTP_PKTLOST_RECOVER

日志内容	PTP packets lost were recovered. (PktType=[STRING])
参数解释	$1：PTP报文类型，取值包括： ○ Delay_Resp：PTP Delay_Resp 报文 ○ Announce：PTP Announce 报文 ○ Sync：PTP Sync 报文 ○ Pdelay_Resp：PTP Pdelay_Resp 报文
日志等级	4
举例	PTP/4/PTP_PKTLOST_RECOVER: PTP packets lost were recovered. (PktType =Announce)
日志说明	从PTP报文丢失告警状态中恢复正常。只有当Slave端口检测Announce、Delay_Resp、Sync报文超时后又重新收到Announce、Delay_Resp报文或者超时时间过长设备自身由从时钟转变为主时钟时，才会打印此日志
处理建议	无

132.9 PTP_PKTLOST

日志内容	PTP packets were lost. (PktType=[STRING])
参数解释	$1：PTP报文类型，取值包括： ○ Delay_Resp：PTP Delay_Resp 报文 ○ Announce：PTP Announce 报文 ○ Sync：PTP Sync 报文 ○ Pdelay_Resp：PTP Pdelay_Resp 报文
日志等级	4
举例	PTP/4/PTP_PKTLOST: PTP packets were lost. (PktType=Announce)
日志说明	Slave端口检测Announce、Delay_Resp、Sync报文，超过检测时间没有收到报文，则认为报文丢失
处理建议	在打印该日志的PTP从时钟设备上使用**display ptp statistics**命令查看接收报文统计计数是否增长 • 若增长，则表示链路延时过长导致的超时，无须处理 • 若不增长，则在 PTP 主时钟设备使用 **display ptp statistics** 命令查看发送报文统计计数是否增长 ○ 若增长，则表示链路故障导致对端超时没收到报文，排除故障恢复链路 ○ 若不增长，则收集告警、日志和配置信息，联系技术支持

132.10 PTP_PORT_BMCINFO_CHANGE

日志内容	The BMC info for port [UINT16] changed. (PortName=[STRING], PortSourceId=[STRING], PortSourcePortNum=[UINT16], PortSourceStepsRemoved=[UINT16], CurrentMasterClockId=[STRING])
参数解释	$1：PTP接口索引 $2：PTP接口名称 $3：PTP接口接收到的时钟源ID $4：PTP接口接收到的时钟源端口号 $5：PTP接口接收到的时钟源跳数 $6：设备当前主时钟ID
日志等级	5
举例	PTP/5/PTP_PORT_BMCINFO_CHANGE: The BMC info for port 1 changed. (PortName=G1/0/1, PortSourceId=000FE2-FFFE-FF0001, PortSourcePortNum=1, PortSourceStepsRemoved=5, CurrentMasterClockId=000FE2-FFFE-FF0000)
日志说明	PTP接口收到的时钟源ID、时钟源端口号或时钟源跳数等时钟源信息发生变化
处理建议	无

132.11 PTP_PORT_STATE_CHANGE

日志内容	PTP port state changed. (IfIndex=[UINT16], PortName=[STRING], PortState=[STRING], OldPortState=[STRING])
参数解释	$1：PTP接口索引 $2：PTP接口名称 $3：PTP接口当前的状态，取值包括： ○ Master：接口状态为 Master，对外发布时间信息 ○ Slave：接口状态为 Slave，跟踪外部时间信息 ○ Passive：接口状态为 Passive（接口收到对端的 Announce 报文后，计算出的状态），不跟踪外部时间信息，也不对外发布时间信息 ○ Listening：接口状态为 Listening（接口初始化后，即进入 Listening 状态），不跟踪外部时间信息，也不对外发布时间信息 ○ Faulty：接口状态为 Faulty，该状态为 PTP 协议的错误状态（即检测到错误），接口不处理 PTP 协议报文 ○ Initializing：接口状态为 Initializing，接口位于初始化状态，接口不处理协议报文 ○ Premaster：接口状态为 Premaster，Master 状态前的临时状态 ○ Disable：接口状态为 Disabled，接口上 PTP 协议未运行，接口不处理协议报文 ○ Uncalibrated：接口状态为 Uncalibrated，Slave 状态前的临时状态 $4：PTP接口变化前的状态，取值包括： ○ Master：接口状态为 Master，对外发布时间信息 ○ Slave：接口状态为 Slave，跟踪外部时间信息 ○ Passive：接口状态为 Passive（接口收到对端的 Announce 报文后，计算出的状态），不跟踪外部时间信息，也不对外发布时间信息 ○ Listening：接口状态为 Listening（接口初始化后，即进入 Listening 状态），不跟踪外部时间信息，也不对外发布时间信息 ○ Faulty：接口状态为 Faulty，该状态为 PTP 协议的错误状态（即检测到错误），接口不处理 PTP 协议报文 ○ Initializing：接口状态为 Initializing，接口位于初始化状态，接口不处理协议报文 ○ Premaster：接口状态为 Premaster，Master 状态前的临时状态 ○ Disable：接口状态为 Disabled，接口上 PTP 协议未运行，接口不处理协议报文 ○ Uncalibrated：接口状态为 Uncalibrated，Slave 状态前的临时状态
日志等级	5
举例	PTP/5/PTP_PORT_STATE_CHANGE: PTP port state changed. (IfIndex=1, PortName=G1/0/1, PortState=Slave, OldPortState=Master)
日志说明	PTP接口状态发生改变，原因包括： • PTP 域内的时钟设备属性发生变化，比如优先级、时钟等级、时钟精度、接口的 NotSlave 属性等 • 接入了优先级更高的时钟源 • PTP 接口所在链路故障或者 PTP 接口 DOWN
处理建议	使用**display ptp interface brief**命令查看是否存在PTP接口处于Fault状态

	• 若存在接口处于 Fault 状态，则表示链路故障或接口 DOWN，排除故障恢复链路
	• 若不存在接口处于 Fault 状态，则查看 PTP 配置信息是否发生改变
	  ○ 若 PTP 配置信息发生改变，则恢复配置
	  ○ 若 PTP 配置信息未发生改变，则收集告警、日志和配置信息，联系技术支持

132.12 PTP_SRC_CHANGE

日志内容	Clock source property changed. (SourceName=[STRING], Priority1=[UCHAR], Priority2=[UCHAR], ClockClass=[UINT16], ClockAccuracy=[UINT16]], ClockSourceType=[STRING])

参数解释	$1：时钟源，取值包括：
	  ○ Local：本地时钟
	  ○ Tod1：第一路 ToD 时钟
	  ○ Tod2：第二路 ToD 时钟
	$2：第一优先级
	$3：第二优先级
	$4：时钟源的时间等级
	$5：时钟源的时间精度
	$6：最优时钟的时钟类别，取值包括：
	  ○ Atomic clock：原子时钟
	  ○ GPS：Global Positioning System，全球定位系统
	  ○ Handset：手持设备
	  ○ Internal oscillator：内部振荡器
	  ○ NTP：Network Time Protocol，网络时间协议
	  ○ Other：其他
	  ○ PTP：Precision Time Protocol，精确时间协议
	  ○ Terrestrial radio：陆基无线电
	  ○ Unknown：未知

日志等级	5
举例	PTP/5/PTP_SRC_CHANGE: Clock source property changed. (SourceName=Tod1, Priority1=1, Priority2=2, ClockClass=6, ClockAccuracy=20, ClockSourceType=Atomic clock)
日志说明	时钟源属性发生改变，原因包括： • 用户通过命令行改变时钟源属性 • 接收到了精度更高的外接时钟源
处理建议	无

132.13 PTP_SRC_SWITCH

日志内容	Clock source switched. (LastClockID=[STRING], CurrentClockID=[STRING])
参数解释	$1：原来的时钟源ID $2：当前的时钟源ID
日志等级	4
举例	PTP/4/PTP_SRC_SWITCH: Clock source switched.(LastSource=000FE2-FFFE-FF0000, CurrentSource=000FE2-FFFE-FF0001)
日志说明	新的更好的时钟源加入PTP域，设备跟踪的时钟源发生切换
处理建议	无

132.14 PTP_TIME_LOCK

日志内容	Time resumed to locked state.
参数解释	无
日志等级	3
举例	PTP/3/PTP_TIME_LOCK: Time resumed to locked state.
日志说明	时钟从失锁状态中恢复为正常
处理建议	无

132.15 PTP_TIME_NOT_LOCK

日志内容	Time not in locked state.
参数解释	无
日志等级	3
举例	PTP/3/PTP_TIME_NOT_LOCK: Time not in locked state.
日志说明	时钟失锁告警，原因包括： • 频率失锁 • 子卡逻辑或者时钟扣板硬件故障 • DSP 收到的时间戳不变或者时戳错误

处理建议	检查PTP Slave接口是否链路故障或接口DOWN
	• 若链路故障或接口 DOWN，排除故障恢复链路
	• 接口正常，则查看 PTP 配置信息是否发生改变
	  ○ 若 PTP 配置信息发生改变，则恢复配置
	  ○ 若 PTP 配置信息未发生改变，则收集告警、日志和配置信息，联系技术支持

132.16 PTP_TIME_OFFSE_EXCEED_THRESHOLD

日志内容	The PTP time offset exceeded the threshold. (TimeOffset=[UINT16], AlarmThresholdTimeOffset=[UINT16])
参数解释	$1：源绝对时间差 $2：源绝对时间差告警阈值
日志等级	4
举例	PTP/4/PTP_TIME_OFFSET_EXCEED_THRESHOLD: The PTP time offset exceeded the threshold. (TimeOffset=500, AlarmThresholdTimeOffset=400)
日志说明	PTP源绝对时间差超过阈值。比较外部基准参考时间和PTP时间，获取两者时间差值，差值超过时间偏差告警阈值，则打印此信息
处理建议	使用**ptp asymmetry-correction**命令配置非对称延迟校正时间，调整当前设备的PTP时钟源时间，使与外部基准时间一致，查看设备是否打印PTP_TIME_OFFSET_RECOVER日志 • 若查看到 PTP_TIME_OFFSET_RECOVER 日志，则问题解决 • 若未查看到此日志，则收集告警、日志和配置信息，联系技术支持

132.17 PTP_TIME_OFFSET_RECOVER

日志内容	The PTP standard time offset resumed. (TimeOffset=[UINT16], AlarmThresholdTimeOffset=[UINT16])
参数解释	$1：源绝对时间差 $2：源绝对时间差告警阈值
日志等级	4
举例	PTP/4/PTP_STANDARD_TIME_OFFSET_RECOVER: The PTP standard time offset resumedl. (TimeOffset=300, AlarmThresholdTimeOffset=400)
日志说明	PTP源绝对时间差恢复为正常状态
处理建议	无

132.18 PTP_TIME_SYNC

日志内容	Time resumed to synchronized state.
参数解释	无
日志等级	4
举例	PTP/4/PTP_TIME_SYNC: Time resumed to synchronized state.
日志说明	设备恢复到时钟同步的正常状态
处理建议	无

132.19 PTP_TIME_UNSYNC

日志内容	Time changed to unsynchronized state.
参数解释	无
日志等级	4
举例	PTP/4/PTP_TIME_UNSYNC: Time changed to unsynchronized state.
日志说明	设备处于无法进行时钟同步的状态，原因包括： • 链路故障或者接口 DOWN 导致设备没有跟踪的时钟源 • 本设备时钟源优先级配置得太高，使得本设备处于 local 状态，无法同步其他设备的时间信号
处理建议	1. 使用 **displsy ptp interface brief** 命令查看设备是否存在 PTP Slave 接口 ○ 是：请联系技术支持 ○ 否：执行步骤 2 2. 使用 **display ptp clock** 命令，查看 Clock type 字段显示是否为 ToD 外接时钟源类型 ○ 是：执行步骤 3 ○ 否：设备没有时钟源可以同步，正常打印 3. 检查是否通过 **ptp { tod0 | tod1 } input** 命令配置了 ToD 时钟信号的入方向接收延迟校正时间 ○ 是：请联系技术支持 ○ 否：执行步骤 4 4. 执行 **ptp { tod0 | tod1 } input** 命令校正 ToD 时钟信号为入方向接收延迟校正时间，查看设备是否打印 PTP_TIME_SYNC 日志 ○ 是：问题解决 ○ 否：收集告警、日志和配置信息，联系技术支持

132.20 PTP_TIMESTAMP_CHANGE

日志内容	The timestamp state turned to normal.
参数解释	无
日志等级	3
举例	PTP/3/PTP_TIMESTAMP_CHANGE: The timestamp state turned to normal.
日志说明	本设备接收到的报文中携带的时间戳恢复为持续变化，时间戳状态正常 正常情况下设备接收到的PTP报文中的时间戳是持续变化的，当时间戳不变化时表示状态异常，只有时间戳从异常状态恢复到正常状态时，才会输出该日志
处理建议	无

132.21 PTP_TIMESTAMP_UNCHANGE

日志内容	The timestamp state turned to abnormal.
参数解释	无
日志等级	3
举例	PTP/3/PTP_TIMESTAMP_UNCHANGE: The timestamp state turned to abnormal.
日志说明	本设备接收到的报文中携带的时间戳不变化，时间戳状态异常 正常情况下设备接收到的PTP报文中的时间戳是持续变化的，当时间戳不变化时表示状态异常

处理建议	使用**display ptp statistics**命令查看Sync报文统计计数是否增长
	• 若增长，则收集告警、日志和配置信息，并联系技术支持
	• 若不增长，则检查链路是否故障，并待链路故障解除后，查看设备是否打印PTP_TIMESTAMP_CHANGED 日志
	  ○ 若查看到 PTP_TIMESTAMP_CHANGED 日志，则表示时间戳状态恢复正常
	  ○ 若未查看到此日志，则收集告警、日志和配置信息，联系技术支持

133 PWDCTL

本节介绍 Password control 模块输出的日志信息。

133.1 PWDCTL_ADD_BLACKLIST

日志内容	[STRING] was added to the blacklist for failed login attempts.
参数解释	$1：用户名
日志等级	6
举例	PWDCTL/6/PWDCTRL_ADD_BLACKLIST: hhh was added to the blacklist for failed login attempts.
日志说明	因为用户输入密码错误，用户登录设备失败，被加入密码控制黑名单
处理建议	无

133.2 PWDCTL_CHANGE_PASSWORD

日志内容	[STRING] changed the password because [STRING].
参数解释	$1：用户名 $2：更改密码原因 o it was the first login of the account：用户首次登录 o the password had expired：密码已经过期 o the password was too short：密码长度过短 o the password was not complex enough：密码复杂度不满足要求 o the password was default password：密码是缺省密码
日志等级	6
举例	PWDCTL/6/PWDCTL_CHANGE_PASSWORD: hhh changed the password because It was the first login of the account.
日志说明	由于某种原因，用户改变用户密码。例如该用户的账户第一次登录设备
处理建议	无

133.3 PWDCTL_FAILED_TO_OPENFILE

日志内容	Failed to open the password file.
参数解释	N/A
日志等级	3
举例	PWDCTL/3/FAILED_TO_OPENFILE: Failed to open the password file.
日志说明	因文件系统异常导致创建或打开*.dat文件失败
处理建议	请检查设备文件系统存储空间是否充足

133.4 PWDCTL_FAILED_TO_WRITEPWD

日志内容	Failed to write the password records to file.
参数解释	N/A
日志等级	3
举例	PWDCTL/3/PWDCTL_FAILED_TO_WRITEPWD: Failed to write the password records to file.
日志说明	设备无法将用户密码写入密码记录文件
处理建议	请检查设备文件系统存储空间是否充足

133.5 PWDCTL_UPDATETIME

日志内容	Last login time updated after clock update.
参数解释	无
日志等级	6
举例	PWDCTL/6/PWDCTL_UPDATETIME: Last login time updated after clock update.
日志说明	用户最近登录时间已同步更新
处理建议	无

134 QACL

本节介绍 ACL 和 QoS 模块输出的日志信息。

134.1 ACL

日志内容	Insufficient resources for the portal session. Some functions of the session didn't take effect.
参数解释	无
日志等级	4
举例	QACL/4/ACL: -MDC=1-Slot=5 ; Insufficient resources for the portal session. Some functions of the session didn't take effect.
日志说明	添加Portal会话时，因系统资源不足，新增的Portal会话部分功能（例如会话计费、限速等功能）不生效
处理建议	1. 执行 **display qos-acl resource** 命令显示当前单板上资源的使用情况，删除一些没有必要多余的资源 2. 请联系技术支持

134.2 ACL

日志内容	Due to insufficient hardware resources, the CAR action and the CBQ action applied to interface [STRING] did not work as expected.
参数解释	$1：三层聚合接口的名称
日志等级	4
举例	QACL/4/ACL: -MDC=1-Slot=4; Due to insufficient hardware resources, the CAR action and the CBQ action applied to interface RAGG1000 did not work as expected.
日志说明	当三层聚合组的成员端口在选中和非选中状态之间变化时，如果硬件资源不足，聚合口上配置的QoS策略里的CAR或者CBQ限速达不到配置的效果
处理建议	1. 重新配置三层聚合接口上的 QoS 策略限速参数 2. 请联系技术支持

134.3 DrvDebug

日志内容	After you configure the qos trust auto command for a serial interface on a CPOS subcard in an MPE-1104 card, the command takes effect on all serial interfaces created for the CPOS interface to which the configured serial interface belongs. If the configured serial interface belongs to the first CPOS interface on the CPOS subcard, the command also takes effect on all MP-group interfaces on the CPOS subcard.
参数解释	无
日志等级	4
举例	DRVPLAT/4/DrvDebug: -MDC=1-Slot=5; After you configure the qos trust auto command for a serial interface on a CPOS subcard in an MPE-1104 card, the command takes effect on all serial interfaces created for the CPOS interface to which the configured serial interface belongs. If the configured serial interface belongs to the first CPOS interface on the CPOS subcard, the command also takes effect on all MP-group interfaces on the CPOS subcard.
日志说明	在CMPE-1104单板的CPOS接口通道化出来的串口上配置qos trust auto命令行，对以下接口也会生效： • 从该 CPOS 接口通道化出来的其它串口 • 如果该 CPOS 接口是接口子卡的第一个 CPOS 接口，该接口子卡上创建的所有 MP-group 接口
处理建议	无

134.4 DrvDebug

日志内容	After you configure the qos trust auto command for an MP-group interface on a CPOS subcard in an MPE-1104 card, the command takes effect on all MP-group interfaces on the CPOS subcard and all serial interfaces of the first CPOS interface on the CPOS subcard.
参数解释	无
日志等级	4
举例	DRVPLAT/4/DrvDebug: -MDC=1-Slot=5; After you confi gure the qos trust auto command for an MP-group interface on a CPOS subcard in a n MPE-1104 card, the command takes effect on all MP-group interfaces on the CPOS subcard and all serial interfaces of the first CPOS interface on the CPOS subca rd.
日志说明	在CMPE-1104单板的MP-group接口上配置qos trust auto命令行，对以下接口也会生效： • 该接口子卡上第一个 CPOS 口通道化出来的串口 • 该接口子卡上创建的其它 MP-group 接口
处理建议	无

134.5 DrvDebug

日志内容	After you configure the qos trust auto command for a serial (or MP-group) interface on a MIC-ET16L subcard in an MPE-1104 card, the command takes effect on all serial (or MP-group) interfaces on the MIC-ET16L subcard.
参数解释	无
日志等级	4
举例	DRVPLAT/4/DrvDebug: -MDC=1-Slot=5; After you configure the qos trust auto command for a serial (or MP-group) interface on a MIC-ET16L subcard in an MPE-1104 card, the command takes effect on all serial (or MP-group) interfaces on the MIC-ET16L subcard.
日志说明	在CMPE-1104单板的MIC-ET16L接口子卡上只要有一个接口配置**qos trust auto**命令行，则该接口子卡的所有接口都会变成信任报文模式
处理建议	无

134.6 DrvDebug

日志内容	Failed to synchronize the QoS policy on an aggregate interface to a new member port. Not enough hardware resources available.
参数解释	无
日志等级	4
举例	DRVPLAT/4/DrvDebug:-MDC=1-Slot=5; Failed to synchronize the QoS policy on an aggregate interface to a new member port. Not enough hardware resources available.
日志说明	在三层聚合接口上添加三层聚合成员接口时，由于该聚合成员接口所在单板硬件资源不足，不能同步三层聚合接口上的QoS策略
处理建议	• 将三层聚合成员接口退出三层聚合接口 • 在三层聚合接口上重新配置 QoS 策略 • 请联系技术支持

134.7 QoS

日志内容	Not enough WFQ resources to modify the weight value of queue [INT 32] in a queue scheduling profile.
参数解释	$1：队列号
日志等级	4
举例	QACL/4/QoS : -MDC=1-Slot=9; Not enough WFQ resources to modify the weight value of queue [INT 32] in a queue scheduling profile.
日志说明	动态修改qmprofile的队列WFQ weight值时，WFQ资源不足
处理建议	• 请删除不需要的 WFQ weight，以便释放 WFQ 资源 • 请联系技术支持

134.8 QoS

日志内容	The rate limiting configuration on interface [STRING] didn't work as expected due to insufficient hardware resources
参数解释	$1：三层聚合接口的名称
日志等级	4
举例	QACL/4/QOS: -MDC=1-Slot=4; The rate limiting configuration on interface RAGG1 didn't work as expected due to insufficient hardware resources.
日志说明	当三层聚合组的成员端口在选中和非选中状态之间变化时，如果硬件资源不足，三层聚合接口上配置的以下QoS功能无法达到配置的效果，具体包括： • 三层聚合接口下发的限速功能 • 三层聚合接口下发的独占带宽功能 • 三层聚合接口下发的限速功能和独占带宽功能
处理建议	• 请联系技术支持

134.9 QoS

日志内容	Due to insufficient hardware resources, the outgoing traffic for the newly added member port of a Layer 3 aggregation group was sent out of another Selected port.
参数解释	无
日志等级	4
举例	QACL/4/QoS:-MDC=1-Slot=4; Due to insufficient hardware resources, the outgoing traffic for the newly added member port of a Layer 3 aggregation group was sent out of another Selected port.
日志说明	一个三层聚合接口已有8成员接口，当第九个成员接口加入且被选中时，则由于硬件资源不足，该成员接口出方向的流量由其他成员接口转发
处理建议	• 将之前未选中的成员接口退出该三层聚合接口，以释放硬件资源 • 联系技术支持

134.10 QoS

日志内容	Not enough hardware queue resources for ATM
参数解释	无
日志等级	4
举例	QACL/4/QoS:-MDC=1-Slot=4;Not enough hardware queue resources for ATM.
日志说明	在ATM接口上创建PVC或者切换service时，单板的队列硬件资源不足导致操作失败
处理建议	• 请联系技术支持

134.11 QOS_CAR_APPLYIF_FAIL

日志内容	[STRING]; Failed to apply the [STRING] CAR in [STRING] profile [STRING] to interface [STRING]. Reason: [STRING].
参数解释	$1：CAR应用的端口信息 $2：CAR应用方向 $3：Profile类型：取值为user $4：Profile名称 $5：接口名称 $6：失败原因 • The CAR is not supported：不支持 CAR • The resources are insufficient：资源不足
日志等级	4
举例	QOS/4/QOS_CAR_APPLYIF_FAIL: Port=GigabitEthernet3/1/1; Failed to apply the inbound CAR in user profile a to interface GigabitEthernet3/1/1. Reason: The resources are insufficient.
日志说明	• 接口下应用 user profile 时，下发配置的 CAR 信息失败 • 接口下已经应用 user profile，在该 user profile 下增加或修改 CAR 配置失败
处理建议	删除profile下的CAR配置或修改CAR的相关参数

134.12 QOS_QMPROFILE_RESTORE_FAIL

日志内容	Failed to restore the configuration of queue scheduling profile [STRING] on interface [STRING], because [STRING].
参数解释	$1：队列调度策略名称 $2：接口名称 $3：失败原因 ◦ the minimum bandwidth exceeds the interface bandwidth：队列调度策略中配置的最小带宽超过接口带宽
日志等级	4
举例	QOS/4/QOS_QMPROFILE_RESTORE_FAIL: Failed to restore the configuration of queue scheduling profile b on interface GigabitEthernet1/0/1, because the minimum bandwidth exceeds the interface bandwidth.
日志说明	队列调度策略恢复失败
处理建议	修改队列调度策略中的最小带宽或接口带宽，重新应用队列调度策略

134.13 TE

日志内容	The MPLS TE reservable bandwidth configuration on Layer 3 aggregate interface [STRING] didn't work as expected due to insufficient hardware resources.
参数解释	$1：三层聚合接口的编号
日志等级	6
举例	QACL/6/TE: -MDC=1-Slot=4; The MPLS TE reservable bandwidth configuration on Layer 3 aggregate interface [STRING] didn't work as expected due to insufficient hardware resources.
日志说明	当三层聚合组的成员端口在选中和非选中状态之间变化时，如果硬件资源不足，三层聚合接口上配置的MPLS TE带宽预留无法达到配置的效果
处理建议	• 请重新配置三层聚合接口上的 MPLS TE 带宽保证配置 • 请联系技术支持

135 QOS

本节介绍 QoS 模块输出的日志信息。

135.1 EDSG_CONFIG_CONFLICT

日志内容	Failed to activate EDSG service policy [UINT32] on user [UINT32]. The EDSG service policy conflicts with existing configurations in the [STRING] direction.
参数解释	$1：EDSG业务策略ID $2：User ID $3：下发方向
日志等级	3
举例	QOS/3/EDSG_ CONFIG_CONFLICT: Failed to activate EDSG service policy 1 on user 0x30000072. The EDSG service policy conflicts with existing configurations in the outbound direction.
日志说明	• EDSG 业务策略与 User-profile 视图下的 QMProfile、GTS 或 qos queue 两两互斥 • EDSG 业务策略与用户上线接口上配置的 HQoS 互斥
处理建议	• 如果 User-profile 视图下存在 QMProfile、GTS 或 qos queue 的配置，请调整这部分配置 • 如果用户上线接口视图下存在 HQoS 配置，请调整 HQoS 配置

135.2 EDSG_EXCEED_LIMIT

日志内容	Failed to activate EDSG service policy [UINT32] on user [UINT32]. The EDSG service policy ID is out of range.
参数解释	$1：EDSG业务策略ID $2：User ID
日志等级	3
举例	QOS/3/EDSG_ EXCEED_LIMIT: Failed to activate EDSG service policy 1 on user 0x30000072. The EDSG service policy ID is out of range.
日志说明	EDSG业务策略应用失败，原因是：RADIUS服务器下发的EDSG业务策略ID不在设备支持的范围内
处理建议	请根据业务板类型确认设备是否支持在同一用户上激活多个EDSG业务策略： • 同一用户上仅支持激活一个 EDSG 业务策略，则策略 ID 取值必须为 1 • 同一用户上支持激活 N 个 EDSG 业务策略，则策略 ID 取值范围为 1～N 修改RADIUS服务器下发的EDSG业务策略ID为设备支持的合理范围

135.3 EDSG_LRMODE_CONFLICT

日志内容	Failed to activate EDSG service policy [UINT32] on user [UINT32]. The rate limit mode for the EDSG service policy is different from the rate limit mode for an existing EDSG service policy.
参数解释	$1：EDSG业务策略ID $2：User ID
日志等级	3
举例	QOS/3/EDSG_LRMODE_CONFLICT: Failed to activate EDSG service policy 1 on user 0x30000072. The rate limit mode for the EDSG service policy is different from the rate limit mode for an existing EDSG service policy.
日志说明	EDSG业务策略应用失败，原因是：RADIUS服务器下发EDSG业务策略的流量限速模式不一致，后下发的EDSG业务策略应用失败
处理建议	请修改RADIUS服务器下发的EDSG业务策略的流量限速模式

135.4 EDSG_MODE_CONFLICT

日志内容	Failed to activate EDSG service policy [UINT32] on user [UINT32]. The status of the separate rate limiting function for the EDSG service policy is different from the status of this function for an existing EDSG service policy.
参数解释	$1：EDSG业务策略ID $2：User ID
日志等级	3
举例	QOS/3/EDSG_ EXCEED_LIMIT: Failed to activate EDSG service policy 1 on user 0x30000072. The status of the separate rate limiting function for the EDSG service policy is different from the status of this function for an existing EDSG service policy.
日志说明	EDSG业务策略应用失败，原因是：RADIUS服务器下发EDSG业务策略的双栈业务流量独立限速功能状态不一致，后下发的EDSG业务策略应用失败
处理建议	无

135.5 EDSG_NOT_SUPPORT

日志内容	Failed to activate service [UINT32] on user [UINT32]. The EDSG service policy is not supported.
参数解释	$1：EDSG业务策略ID $2：User ID
日志等级	3
举例	QOS/3/EDSG_NOT_SUPPORT: Failed to activate service 1 on user 0x30000072. The EDSG service policy is not supported.
日志说明	EDSG业务策略应用失败，原因是：不支持EDSG业务限速（together模式下的带内带宽）下发
处理建议	建议用户从其他类型接口上线

135.6 QOS_CAR_APPLYUSER_FAIL

日志内容	[STRING]; Failed to apply the [STRING] CAR in [STRING] profile [STRING] to the user. Reason: [STRING].
参数解释	$1：用户标识信息 $2：CAR应用方向 $3：Profile类型 $4：Profile名称 $5：失败原因
日志等级	4
举例	QOS/4/QOS_CAR_APPLYUSER_FAIL: -MAC=1111-2222-3333-IP=192.168.1.2-SVLAN=100-VPN=”N/A”-Port=GigabitEthernet5/1/5; Failed to apply the inbound CAR in user profile a to the user. Reason: The resources are insufficient.
日志说明	• 用户上线，下发配置的 CAR 信息失败 • 用户已经上线，修改 CAR 信息或者增加 CAR 应用失败
处理建议	取消CAR在profile下的应用或者修改CAR的相关参数信息

135.7 QOS_CBWFQ_REMOVED

日志内容	CBWFQ is removed from [STRING].
参数解释	$1：接口名称
日志等级	3
举例	QOS/3/QOS_CBWFQ_REMOVED: CBWFQ is removed from GigabitEthernet4/0/1.
日志说明	因接口最大带宽或接口速率更改后低于接口上原来配置的CBWFQ要求的带宽或速率，系统从接口上删除CBWFQ
处理建议	增大接口最大带宽或接口速率后重新应用被删除的CBWFQ

135.8 QOS_DIFFSERV_CFG_FAIL

日志内容	Failed to configure the MPLS Diffserv mode in VPN instance [STRING]. Reason: [STRING].
参数解释	$1：VPN实例名称 $2：失败原因： ○ 业务板不支持配置 MPLS 的差分服务模式：The card does not support MPLS Diffserv mode
日志等级	4
举例	QOS/4/QOS_DIFFSERV_CFG_FAIL: -MDC=1-Chassis=1-Slot=5; Failed to configure the MPLS Diffserv mode in VPN instance vpn1. Reason: The card does not support MPLS Diffserv mode.
日志说明	在VPN实例中配置MPLS的差分服务模式失败
处理建议	无

135.9 QOS_GTS_APPLYINT_FAIL

日志内容	Failed to apply the gts configuration to the interface [STRING]. [STRING]
参数解释	$1：接口名称 $2：失败原因
日志等级	4
举例	QOS/4/QOS_GTS_APPLYINT_FAIL; Failed to apply the gts configuration to the interface Route-Aggregation1. The operation is not supported.
日志说明	单板上的接口不支持应用GTS
处理建议	无

135.10 QOS_GTS_APPLYUSER_FAIL

日志内容	[STRING]; Failed to apply the [STRING] GTS to the traffic of user profile a in [STRING] in [STRING] profile [STRING] to the user. Reason: [STRING].
参数解释	$1：用户标识信息 $2：GTS应用方向 $3：GTS应用范围 $4：Profile类型 $5：User profile名称 $6：失败原因
日志等级	4
举例	QOS/4/QOS_GTS_APPLYUSER_FAIL: -MAC=1111-2222-3333-IP=192.168.1.2/16-CVLAN=100-Port=GigabitEthernet5/1/5; Failed to apply the inbound GTS to the traffic of user profile a in queue 0. Reason: The resources are insufficient. QOS/4/QOS_GTS_APPLYUSER_FAIL: -MAC=1111-2222-3333-IP=192.168.1.2/16-CVLAN=100-Port=GigabitEthernet5/1/5; Failed to apply the inbound GTS to the traffic of user profile a in all queues. Reason: The resources are insufficient. QOS/4/QOS_GTS_APPLYUSER_FAIL: -MAC=1111-2222-3333-IP=192.168.1.2/16-CVLAN=100-Port=GigabitEthernet5/1/5; Failed to apply the inbound GTS to the traffic of session group profile a in queue 0. Reason: The GTS configuration conflicts with the CAR configuration in an EDSG service policy.
日志说明	• 用户上线，下发配置的 GTS 失败 • 用户已经上线，修改 GTS 配置或者增加 GTS 应用失败 • 用户已经上线，GTS 的配置与 EDSG 业务流量限速配置冲突
处理建议	取消GTS在user profile下的应用或者修改GTS的相关参数信息

135.11 QOS_MEMORY_WARNING

日志内容	The system does not have enough memory.
参数解释	无
日志等级	4
举例	QOS/4/QOS_MEMORY_WARNING: The system does not have enough memory.
日志说明	QoS响应系统内存门限告警
处理建议	等待系统内存恢复

135.12 QOS_NOT_ENOUGH_BANDWIDTH

日志内容	Policy [STRING] requested bandwidth [UINT32](kbps). Only [UINT32](kbps) is available on [STRING].
参数解释	$1：QoS策略名称 $2：CBWFQ需要的带宽 $3：接口可用带宽 $4：接口名称
日志等级	3
举例	QOS/3/QOS_NOT_ENOUGH_BANDWIDTH: Policy d requested bandwidth 10000(kbps). Only 80(kbps) is available on GigabitEthernet4/0/1.
日志说明	因CBWFQ要求的带宽大于接口最大带宽，CBWFQ配置失败
处理建议	增大接口最大带宽值或减小CBWFQ要求的带宽值

135.13 QOS_POLICY_APPLYCOPP_CBFAIL

日志内容	Failed to apply classifier-behavior [STRING] in policy [STRING] to the [STRING] direction of control plane slot [UINT32]. [STRING].
参数解释	$1：CB对名称 $2：QoS策略名称 $3：流量方向 $4：槽位号 $5：失败原因 ○ The behavior is empty：流行为为空 ○ Only one rate-limiting action is supported in one behavior to be applied to the control plane：一个流行为中仅支持配置一个限速动作
日志等级	4
举例	QOS/4/QOS_POLICY_APPLYCOPP_CBFAIL: Failed to apply classifier-behavior d in policy b to the inbound direction of control plane slot 3. The behavior is empty.
日志说明	系统在控制平面的某个方向上应用或更新QoS策略中的某个CB对失败
处理建议	请根据失败原因，修改策略中的配置

135.14 QOS_POLICY_APPLYCOPP_FAIL

日志内容	Failed to apply or refresh QoS policy [STRING] to the [STRING] direction of control plane slot [UINT32]. [STRING].
参数解释	$1：QoS策略名称 $2：流量方向 $3：槽位号 $4：失败原因
日志等级	4
举例	QOS/4/QOS_POLICY_APPLYCOPP_FAIL: Failed to apply or refresh QoS policy b to the inbound direction of control plane slot 3. The operation is not supported.
日志说明	系统在控制平面的某个方向上应用或更新QoS策略失败
处理建议	请根据失败原因，修改策略中的配置

135.15 QOS_POLICY_APPLYGLOBAL_CBFAIL

日志内容	Failed to apply classifier-behavior [STRING] in policy [STRING] to the [STRING] direction globally. [STRING].
参数解释	$1：CB对名称 $2：QoS策略名称 $3：流量方向 $4：失败原因
日志等级	4
举例	QOS/4/QOS_POLICY_APPLYGLOBAL_CBFAIL: Failed to apply classifier-behavior a in policy b to the outbound direction globally. The behavior is empty.
日志说明	系统在某个方向上全局应用或更新QoS策略中的某个CB对失败
处理建议	请根据失败原因，修改策略中的配置

135.16 QOS_POLICY_APPLYGLOBAL_FAIL

日志内容	Failed to apply or refresh QoS policy [STRING] to the [STRING] direction globally. [STRING].
参数解释	$1：QoS策略名称 $2：流量方向 $3：失败原因
日志等级	4
举例	QOS/4/QOS_POLICY_APPLYGLOBAL_FAIL: Failed to apply or refresh QoS policy b to the inbound direction globally. The operation is not supported.
日志说明	系统在某个方向上全局应用或更新QoS策略失败
处理建议	请根据失败原因，修改策略中的配置

135.17 QOS_POLICY_APPLYIF_CBFAIL

日志内容	Failed to apply classifier-behavior [STRING] in policy [STRING] to the [STRING] direction of interface [STRING]. [STRING].
参数解释	$1：CB对名称 $2：QoS策略名称 $3：流量方向 $4：接口名称 $5：失败原因 ○ The behavior is empty.：流行为为空，未配置任何动作 ○ Only one service class marking action is supported for the same EXP value on the same interface and the service calss value can't be modified except that the old value has been deleted.：对于同一个 EXP 值，同一接口上仅支持配置一个重新标记报文的 MPLS TE 隧道转发类值的动作；且仅支持通过删除并重新配置的方式进行修改
日志等级	4
举例	QOS/4/QOS_POLICY_APPLYIF_CBFAIL: Failed to apply classifier-behavior b in policy b to the inbound direction of interface Ethernet3/1/2. The behavior is empty.
日志说明	系统在接口的某个方向上应用或更新QoS策略中的某个CB对失败
处理建议	请根据失败原因，修改策略中的配置

135.18 QOS_POLICY_APPLYIF_FAIL

日志内容	Failed to apply or refresh QoS policy [STRING] to the [STRING] direction of interface [STRING]. [STRING].
参数解释	$1：QoS策略名称 $2：流量方向 $3：接口名称 $4：失败原因
日志等级	4
举例	QOS/4/QOS_POLICY_APPLYIF_FAIL: Failed to apply or refresh QoS policy b to the inbound direction of interface Ethernet3/1/2. The operation is not supported.
日志说明	系统在接口的某个方向上应用或更新QoS策略失败
处理建议	请根据失败原因，修改策略中的配置

135.19 QOS_POLICY_APPLYUSER_FAIL

日志内容	[STRING]; Failed to apply the [STRING] QoS policy [STRING] in user profile [STRING] to the user.Reason: [STRING].
参数解释	$1：用户标识信息 $2：QoS policy应用方向 $3：QoS policy名称 $4：User profile名称 $5：失败原因
日志等级	4
举例	QOS/4/QOS_POLICY_APPLYUSER_FAIL: -MAC=1111-2222-3333-IP=192.168.1.2/16-CVLAN=100-Port=GigabitEthernet5/1/5; Failed to apply the inbound QoS policy p in user profile a to the user.Reason: The QoS policy is not supported.
日志说明	• 用户上线，下发配置的 QoS policy 信息失败 • 用户已经上线，修改 QoS Policy 信息或者增加 QoS Policy 应用失败
处理建议	取消QoS policy在User profile下的应用或者修改QoS Profile的信息

135.20 QOS_POLICY_APPLYVLAN_CBFAIL

日志内容	Failed to apply classifier-behavior [STRING] in policy [STRING] to the [STRING] direction of VLAN [UINT32]. [STRING].
参数解释	$1：CB对名称 $2：QoS策略名称 $3：流量方向 $4：VLAN ID $5：失败原因
日志等级	4
举例	QOS/4QOS_POLICY_APPLYVLAN_CBFAIL: Failed to apply classifier-behavior b in policy b to the inbound direction of VLAN 2. The behavior is empty.
日志说明	系统在VLAN的某个方向上应用或更新QoS策略中的某个CB对失败
处理建议	请根据失败原因，修改策略中的配置

135.21 QOS_POLICY_APPLYVLAN_FAIL

日志内容	Failed to apply or refresh QoS policy [STRING] to the [STRING] direction of VLAN [UINT32]. [STRING].
参数解释	$1：QoS策略名称 $2：流量方向 $3：VLAN ID $4：失败原因
日志等级	4
举例	QOS/4/QOS_POLICY_APPLYVLAN_FAIL: Failed to apply or refresh QoS policy b to the inbound direction of VLAN 2. The operation is not supported.
日志说明	系统在VLAN的某个方向上应用或更新QoS策略失败
处理建议	请根据失败原因，修改策略中的配置

135.22 QOS_QMPROFILE_APPLYINT_FAIL

日志内容	Failed to apply the queue management profile to the [STRING] direction of interface [STRING]. [STRING]
参数解释	$1：流量方向，包括： • inbound • outbound $2：接口名称 $3：失败原因，包括： • 单板上的接口不支持应用队列调度策略 • 资源不足导致接口应用队列调度策略失败
日志等级	4
举例	QOS/4/QOS_QMPROFILE_APPLYINT_FAIL: Failed to apply the queue management profile to the outbound direction of interface Route-Aggregation1. The operation is not supported.
日志说明	单板上的接口不支持应用队列调度策略
处理建议	设备资源不足时，请删除部分已应用的ACL规则，释放部分资源

135.23 QOS_QMPROFILE_APPLYUSER_FAIL

日志内容	[STRING]; Failed to apply queue management profile [STRING] in [STRING] profile [STRING] to the user. Reason: [STRING].
参数解释	$1：用户标识信息 $2：Queue management Profile名称 $3：Profile类型 $4：Profile名称 $5：失败原因
日志等级	4
举例	QOS/4/QOS_QMPROFILE_APPLYUSER_FAIL: -MAC=1111-2222-3333-IP=192.168.1.2/16-SVLAN=100-Port=GigabitEthernet5/1/5; Failed to apply queue management profile b in session group profile a to the user. Reason: The QMProfile is not supported. QOS/4/QOS_QMPROFILE_APPLYUSER_FAIL: -MAC=1111-2222-3333-IP=192.168.1.2/16-CVLAN=100-Port=GigabitEthernet5/1/5; Failed to apply queue scheduling profile b in session group profile a to the user. Reason: The queue scheduling profile configuration conflicts with the CAR configuration in an EDSG service policy.
日志说明	• 用户上线，下发配置的 QMProfile 信息失败 • 用户已经上线，修改 QMProfile 信息或者增加 QMProfile 应用失败 • 用户已经上线，修改后的 QMProfile 信息或者增加 QMProfile 与 EDSG 业务流量限速配置冲突
处理建议	取消QMProfile在 profile下的应用或者修改QMProfile的相关信息

135.24 QOS_QMPROFILE_MODIFYQUEUE_FAIL

日志内容	Failed to configure queue [UINT32] in queue management profile [STRING]. [STRING].
参数解释	$1：队列编号 $2：Profile名称 $3：失败原因
日志等级	4
举例	QOS/4/QOS_QMPROFILE_MODIFYQUEUE_FAIL: Failed to configure queue 1 in queue management profile myqueue. The value is out of range.
日志说明	qmprofile成功应用到端口后，再对某队列进行修改，新的参数超出端口能力范围
处理建议	取消此profile在对应板的应用再修改队列参数

135.25 QOS_PRIORITY_APPLYUSER_FAIL

日志内容	Failed to identify the [STRING] priority of the user. Reason: [STRING].
参数解释	$1：流量方向 $2：失败原因
日志等级	4
举例	QOS/4/QOS_PRIORITY_APPLYUSER_FAIL: Failed to identify the inbound priority of the user. Reason: The priority type is not supported.
日志说明	根据用户的优先级在入方向修改该用户对应报文的优先级失败或者根据用户优先级入队列失败
处理建议	取消根据用户优先级入队列或者修改该用户对应报文的优先级

135.26 QOS_LR_APPLYIF_CONFIGFAIL

日志内容	Failed to apply the rate limiting configuration to the [STRING] direction of the interface [STRING]. [STRING].
参数解释	$1：流量方向 $2：接口名称 $3：失败原因
日志等级	4
举例	QOS/4/QOS_LR_APPLYIF_CONFIGFAIL: Failed to apply the rate limiting configuration to the outbound direction of the interface Bridge-Aggregation 1. The operation is not supported.
日志说明	LR限速配置应用到接口上，某些板可能会下发失败
处理建议	请根据失败原因，修改限速配置

135.27 QOS_ITACAR_APPLYUSER_FAIL

日志内容	[STRING]; Failed to apply the ITA CAR at level [STRING] to the user. Reason: [STRING].
参数解释	$1：用户标识信息 $2：ITA CAR的级别 $3：失败原因
日志等级	4
举例	QOS/4/QOS_ITACAR_APPLYUSER_FAIL: -MAC=1111-2222-3333-IP=192.168.1.2/16-SVLAN=100-Port=GigabitEthernet5/1/5; Failed to apply the ITA CAR at level 7 to the user. Reason: The ITA CAR is not supported.
日志说明	• 通过 COA 消息，RADIUS 服务器为已上线用户授权 ITA 业务策略，ITA 业务策略中流量计费级别的流量监管应用失败 • 通过 COA 消息，RADIUS 服务器修改已上线用户 ITA 业务策略，ITA 业务策略中流量计费级别的流量监管参数修改失败
处理建议	RADIUS服务器取消应用ITA业务策略或者修改ITA业务策略中流量计费级别的流量监管参数

135.28 QOS_WEIGHT_APPLYUSER_FAIL

日志内容	[STRING]; Failed to apply the [STRING] weight in [STRING] profile [STRING] to the user. Reason: [STRING].
参数解释	$1：用户标识信息 $2：Weight应用方向 $3：Profile类型 $4：Profile名称 $5：失败原因
日志等级	4
举例	QOS/4/QOS_WEIGHT_APPLYUSER_FAIL: -MAC=1111-2222-3333-IP=192.168.1.2-SVLAN=100-VPN=”N/A”-Port=GigabitEthernet5/1/5; Failed to apply the outbound weight in user profile a to the user. Reason: The resources are insufficient. QOS/4/QOS_WEIGHT_APPLYUSER_FAIL: -MAC=1111-2222-3333-IP=192.168.1.2-SVLAN=100-VPN=”N/A”-Port=GigabitEthernet5/1/5; Failed to apply the outbound weight in user profile a to the user. Reason: The weight configuration conflicts with the CAR configuration in an EDSG service policy.
日志说明	1.用户上线，下发配置的Weight信息失败 2.用户已经上线，修改Weight信息或者增加Weight应用失败 3.用户已经上线，修改后的Weight信息或者增加Weight与EDSG业务流量限速配置冲突
处理建议	取消Weight在profile下的应用或者修改Weight的相关参数信息

136 RADIUS

本节介绍 RADIUS 模块输出的日志信息。

136.1 RADIUS_AUTH_FAILURE

日志内容	User [STRING] from [STRING] failed authentication.
参数解释	$1：用户名称 $2：IP地址
日志等级	5
举例	RADIUS/5/RADIUS_AUTH_FAILURE: User abc@system from 192.168.0.22 failed authentication.
日志说明	RADIUS服务器了拒绝用户的认证请求
处理建议	无

136.2 RADIUS_AUTH_SUCCESS

日志内容	User [STRING] from [STRING] was authenticated successfully.
参数解释	$1：用户名称 $2：IP地址
日志等级	6
举例	RADIUS/6/RADIUS_AUTH_SUCCESS: User abc@system from 192.168.0.22 was authenticated successfully.
日志说明	RADIUS服务器接收了用户的认证请求
处理建议	无

136.3 RADIUS_DELETE_HOST_FAIL

日志内容	Failed to delete servers in scheme [STRING].
参数解释	$1：方案名称
日志等级	4
举例	RADIUS/4/RADIUS_DELETE_HOST_FAIL: Failed to delete servers in scheme abc.
日志说明	删除RADIUS方案中的服务器失败
处理建议	无

137 RDDC

本节介绍 RDDC（redundancy）模块输出的日志信息。

137.1 RDDC_ACTIVENODE_CHANGE

日志内容	Redundancy group [STRING] active node changed to [STRING], because of [STRING].
参数解释	$1：冗余组名称 $2：激活节点信息 $3：状态变化原因 ○ manual switchover：表示状态变化由手动切换引起 ○ group's configuration changed：表示状态变化由冗余组配置变化引起 ○ node's weight changed：表示状态变化由冗余组节点权重变化引起
日志等级	5
举例	RDDC/5/RDDC_ACTIVENODE_CHANGE: Redundancy group 1 active node changed to node 1 (chassis 1), because of manual switchover.
日志说明	由于用户配置了手工倒换，配置变更或权重变换，冗余组激活节点发生切换
处理建议	无

138 RIP

本节介绍 RIP 模块输出的日志信息。

138.1 RIP_MEM_ALERT

日志内容	RIP Process received system memory alert [STRING] event.
参数解释	$1：内存告警类型
日志等级	5
举例	RIP/5/RIP_MEM_ALERT: RIP Process received system memory alert start event.
日志说明	RIP模块收到内存告警信息
处理建议	当超过各级内存门限时，检查系统内存占用情况，对占用内存较多的模块进行调整，尽量释放可用内存

138.2 RIP_RT_LMT

日志内容	RIP [UINT32] Route limit reached
参数解释	$1：RIP进程ID
日志等级	3
举例	RIP/3/RIP_RT_LMT: RIP 1 Route limit reached.
日志说明	RIP进程的路由数达到了上限值
处理建议	检查是否受到攻击或者减少网络路由数

139 RIPNG

本节介绍 RIPng 模块输出的日志信息。

139.1 RIPNG_MEM_ALERT

日志内容	RIPng Process receivedsystem memory alert [STRING] event.
参数解释	$1：内存告警类型
日志等级	5
举例	RIPNG/5/RIPNG_MEM_ALERT: RIPNG Process received system memory alert start event.
日志说明	RIPng模块收到内存告警信息
处理建议	当超过各级内存门限时，检查系统内存占用情况，对占用内存较多的模块进行调整，尽量释放可用内存

139.2 RIPNG_RT_LMT

日志内容	RIPng [UINT32] Route limit reached
参数解释	$1：RIPng进程ID
日志等级	3
举例	RIPNG/3/RIPNG_RT_LMT: RIPng 1 Route limit reached.
日志说明	RIPng进程的路由数达到了上限值
处理建议	检查是否受到攻击或者减少网络路由数

140 RM

本节介绍 RM 模块输出的日志信息。

140.1 RM_ACRT_REACH_LIMIT

日志内容	Max active [STRING] routes [UINT32] reached in URT of [STRING]
参数解释	$1：IPv4或IPv6 $2：最大激活路由数 $3：VPN实例名
日志等级	4
举例	RM/4/RM_ACRT_REACH_LIMIT: Max active IPv4 routes 100000 reached in URT of VPN1
日志说明	VPN实例单播路由表中的激活路由数达到了上限值
处理建议	检查所有的路由并删除不需要的路由

140.2 RM_ACRT_REACH_THRESVALUE

日志内容	Threshold value [UINT32] of max active [STRING] routes reached in URT of [STRING]
参数解释	$1：最大激活路由数告警百分比 $2：IPv4或IPv6 $3：VPN实例名
日志等级	4
举例	RM/4/RM_ACRT_REACH_THRESVALUE: Threshold value 50% of max active IPv4 routes reached in URT of vpn1
日志说明	VPN实例单播路由表中的激活路由数达到了最大路由数告警百分比
处理建议	修改最大路由数告警百分比或路由数上限值

140.3 RM_THRESHLD_VALUE_REACH

日志内容	Threshold value [UINT32] of active [STRING] routes reached in URT of [STRING]
参数解释	$1：最大激活路由数 $2：IPv4或IPv6 $3：VPN实例名
日志等级	4
举例	RM/4/RM_THRESHLD_VALUE_REACH: Threshold value 10000 of active IPv4 routes reached in URT of vpn1
日志说明	VPN实例单播路由表中的激活路由数达到了上限值
处理建议	修改路由数上限值

141 RPR

本节介绍 RPR 模块输出的日志信息。

141.1 RPR_EXCEED_MAX_SEC_MAC

日志内容	A maximum number of secondary MAC addresses exceeded defect is present on the ring corresponding to RPR logical interface [STRING].
参数解释	$1：接口名称
日志等级	4
举例	RPR/4/RPR_EXCEED_MAX_SEC_MAC: A maximum number of secondary MAC addresses exceeded defect is present on the ring corresponding to RPR logical interface RPR-Router1.
日志说明	RPR环上次级MAC地址的数量超过了最大数量
处理建议	关闭RPR环上配有VRRP功能站点的VRRP功能

141.2 RPR_EXCEED_MAX_SEC_MAC_OVER

日志内容	A maximum number of secondary MAC addresses exceeded defect is cleared on the ring corresponding to RPR logical interface [STRING].
参数解释	$1：接口名称
日志等级	5
举例	RPR/5/RPR_EXCEED_MAX_SEC_MAC_OVER: A maximum number of secondary MAC addresses exceeded defect is cleared on the ring corresponding to RPR logical interface RPR-Router1.
日志说明	RPR环上次级MAC地址的数量不再超过最大数量
处理建议	无

141.3 RPR_EXCEED_MAX_STATION

日志内容	A maximum number of stations exceeded defect is present on the ring corresponding to RPR logical interface [STRING].
参数解释	$1：接口名称
日志等级	4
举例	RPR/4/RPR_EXCEED_MAX_STATION: A maximum number of stations exceeded defect is present on the ring corresponding to RPR logical interface RPR-Router1.
日志说明	RPR环上站点的数量超过了最大数量
处理建议	减少RPR环上站点的数量

141.4 RPR_EXCEED_MAX_STATION_OVER

日志内容	A maximum number of stations exceeded defect is cleared on the ring corresponding to RPR logical interface [STRING].
参数解释	$1：接口名称
日志等级	5
举例	RPR/5/RPR_EXCEED_MAX_STATION_OVER: A maximum number of stations exceeded defect is cleared on the ring corresponding to RPR logical interface RPR-Router1.
日志说明	RPR环上站点的数量不再超过最大数量
处理建议	无

141.5 RPR_EXCEED_RESERVED_RATE

日志内容	An excess reserved rate defect is present on ringlet0/ringlet1 corresponding to RPR logical interface [STRING].
参数解释	$1：接口名称
日志等级	3
举例	RPR/3/RPR_EXCEED_RESERVED_RATE: An excess reserved rate defect is present on ringlet0 corresponding to RPR logical interface RPR-Router1.
日志说明	RPR环上站点配置的预留带宽总和超过了环路带宽
处理建议	减少站点的预留带宽，使其总和不大于环路带宽

141.6 RPR_EXCEED_RESERVED_RATE_OVER

日志内容	An excess reserved rate defect is cleared on ringlet0/ringlet1 corresponding to RPR logical interface [STRING].
参数解释	$1：接口名称
日志等级	5
举例	RPR/5/RPR_EXCEED_RESERVED_RATE_OVER: An excess reserved rate defect is cleared on ringlet0 corresponding to RPR logical interface RPR-Router1.
日志说明	RPR环上站点配置的预留带宽总和不再超过环路带宽
处理建议	无

141.7 RPR_IP_DUPLICATE

日志内容	A duplicate IP address defect is present on the ring corresponding to RPR logical interface [STRING].
参数解释	$1：接口名称
日志等级	3
举例	RPR/3/RPR_IP_DUPLICATE: A duplicate IP address defect is present on the ring corresponding to RPR logical interface RPR-Router1.
日志说明	RPR环上至少两个站点间的IP地址重复
处理建议	找到IP地址相同的站点，并修改其IP地址

141.8 RPR_IP_DUPLICATE_OVER

日志内容	A duplicate IP address defect is cleared on the ring corresponding to RPR logical interface [STRING].
参数解释	$1：接口名称
日志等级	5
举例	RPR/5/RPR_IP_DUPLICATE_OVER: A duplicate IP address defect is cleared on the ring corresponding to RPR logical interface RPR-Router1.
日志说明	RPR环上站点的IP地址不再相同
处理建议	无

141.9 RPR_JUMBO_INCONSISTENT

日志内容	A jumbo configuration defect is present on the ring corresponding to RPR logical interface [STRING].
参数解释	$1：接口名称
日志等级	6
举例	RPR/6/RPR_JUMBO_INCONSISTENT: A jumbo configuration defect is present on the ring corresponding to RPR logical interface RPR-Router1.
日志说明	RPR环上至少两个站点间的Jumbo帧配置不一致
处理建议	找到Jumbo帧配置不一致的站点，并修改其Jumbo帧配置

141.10 RPR_JUMBO_INCONSISTENT_OVER

日志内容	A jumbo configuration defect is cleared on the ring corresponding to RPR logical interface [STRING].
参数解释	$1：接口名称
日志等级	6
举例	RPR/6/RPR_JUMBO_INCONSISTENT_OVER: A jumbo configuration defect is cleared on the ring corresponding to RPR logical interface RPR-Router1.
日志说明	RPR环上站点的Jumbo帧配置一致
处理建议	无

141.11 RPR_LAGGCONFIG_INCONSISTENT

日志内容	An inconsistent LAGG configuration is present on the ring corresponding to RPR logical interface [STRING].
参数解释	$1：RPR逻辑接口名称
日志等级	4
举例	RPR/4/RPR_LAGGCONFIG_INCONSISTENT: An inconsistent LAGG configuration is present on the ring corresponding to RPR logical interface RPR-Router1.
日志说明	RPR环上，本站点与邻居站点的RPR逻辑接口的聚合配置不一致
处理建议	使用**display link-aggregation verbose**命令检查本站点和邻居站点的RPR逻辑接口的聚合配置，确保本站点和邻居站点上的聚合配置保持一致

141.12 RPR_LAGGCONFIG_INCONSISTENT_OVER

日志内容	An inconsistent LAGG configuration is cleared on the ring corresponding to RPR logical interface [STRING].
参数解释	$1：RPR逻辑接口名称
日志等级	5
举例	RPR/5/RPR_LAGGCONFIG_INCONSISTENT: An inconsistent LAGG configuration is cleared on the ring corresponding to RPR logical interface RPR-Router1.
日志说明	RPR环上，本站点与邻居站点的RPR逻辑接口的聚合配置已经更改为一致
处理建议	无

141.13 RPR_MISCABLING

日志内容	A miscabling defect is present on ringlet0/ringlet1 corresponding to RPR logical interface [STRING].
参数解释	$1：接口名称
日志等级	3
举例	RPR/3/RPR_MISCABLING: A miscabling defect is present on ringlet0 corresponding to RPR logical interface RPR-Router1.
日志说明	站点的西向/东向边连接到了其它站点的西向/东向边
处理建议	检查站点与其它站点间的RPR物理端口是否连接错误

141.14 RPR_MISCABLING_OVER

日志内容	A miscabling defect is cleared on ringlet0/ringlet1 corresponding to RPR logical interface [STRING].
参数解释	$1：接口名称
日志等级	5
举例	RPR/5/RPR_MISCABLING_OVER: A miscabling defect is cleared on ringlet0 corresponding to RPR logical interface RPR-Router1.
日志说明	站点与其它站点间的RPR物理端口连接正确
处理建议	无

141.15 RPR_PROTECTION_INCONSISTENT

日志内容	A protection configuration defect is present on the ring corresponding to RPR logical interface [STRING].
参数解释	$1：接口名称
日志等级	3
举例	RPR/3/RPR_PROTECTION_INCONSISTENT: A protection configuration defect is present on the ring corresponding to RPR logical interface RPR-Router1.
日志说明	RPR环上至少两个站点间的保护模式配置不一致
处理建议	找到保护模式配置不一致的站点，并修改其保护模式配置

141.16 RPR_PROTECTION_INCONSISTENT_OVER

日志内容	A protection configuration defect is cleared on the ring corresponding to RPR logical interface [STRING].
参数解释	$1：接口名称
日志等级	5
举例	RPR/5/RPR_PROTECTION_INCONSISTENT_OVER: A protection configuration defect is cleared on the ring corresponding to RPR logical interface RPR-Router1.
日志说明	RPR环上站点的保护模式配置一致
处理建议	无

141.17 RPR_SEC_MAC_DUPLICATE

日志内容	A duplicate secondary MAC addresses defect is present on the ring corresponding to RPR logical interface [STRING].
参数解释	$1：接口名称
日志等级	3
举例	RPR/3/RPR_SEC_MAC_DUPLICATE: A duplicate secondary MAC addresses defect is present on the ring corresponding to RPR logical interface RPR-Router1.
日志说明	RPR环上至少两个站点间的次级MAC地址重复
处理建议	找到次级MAC地址相同的站点，并修改其次级MAC地址

141.18 RPR_SEC_MAC_DUPLICATE_OVER

日志内容	A duplicate secondary MAC addresses defect is cleared on the ring corresponding to RPR logical interface [STRING].
参数解释	$1：接口名称
日志等级	5
举例	RPR/5/RPR_SEC_MAC_DUPLICATE_OVER: A duplicate secondary MAC addresses defect is cleared on the ring corresponding to RPR logical interface RPR-Router1.
日志说明	RPR环上站点的次级MAC地址不再相同
处理建议	无

141.19 RPR_TOPOLOGY_INCONSISTENT

日志内容	An inconsistent topology defect is present on the ring corresponding to RPR logical interface [STRING].
参数解释	$1：接口名称
日志等级	3
举例	RPR/3/RPR_TOPOLOGY_INCONSISTENT: An inconsistent topology defect is present on the ring corresponding to RPR logical interface RPR-Router1.
日志说明	站点上不同端口收集的拓扑信息不一致
处理建议	在链路上依次执行**shutdown**和**undo shutdown**命令，使站点重新收集拓扑信息

141.20 RPR_TOPOLOGY_INCONSISTENT_OVER

日志内容	An inconsistent topology defect is cleared on the ring corresponding to RPR logical interface [STRING].
参数解释	$1：接口名称
日志等级	5
举例	RPR/5/RPR_TOPOLOGY_INCONSISTENT_OVER: An inconsistent topology defect is cleared on the ring corresponding to RPR logical interface RPR-Router1.
日志说明	站点上不同端口收集的拓扑信息已一致
处理建议	无

141.21 RPR_TOPOLOGY_INSTABILITY

日志内容	A topology instability defect is present on the ring corresponding to RPR logical interface [STRING].
参数解释	$1：接口名称
日志等级	4
举例	RPR/4/RPR_TOPOLOGY_INSTABILITY: A topology instability defect is present on the ring corresponding to RPR logical interface RPR-Router1.
日志说明	RPR环的拓扑不稳定
处理建议	无

141.22 RPR_TOPOLOGY_INSTABILITY_OVER

日志内容	A topology instability defect is cleared on the ring corresponding to RPR logical interface [STRING].
参数解释	$1：接口名称
日志等级	5
举例	RPR/5/RPR_TOPOLOGY_INSTABILITY_OVER: A topology instability defect is cleared on the ring corresponding to RPR logical interface RPR-Router1.
日志说明	RPR环的拓扑已稳定
处理建议	无

141.23 RPR_TOPOLOGY_INVALID

日志内容	A topology invalid defect is present on the ring corresponding to RPR logical interface [STRING].
参数解释	$1：接口名称
日志等级	4
举例	RPR/4/RPR_TOPOLOGY_INVALID: A topology invalid defect is present on the ring corresponding to RPR logical interface RPR-Router1.
日志说明	站点收集的拓扑信息无效
处理建议	在链路上依次执行**shutdown**和**undo shutdown**命令，使站点重新收集拓扑信息

141.24 RPR_TOPOLOGY_INVALID_OVER

日志内容	A topology invalid defect is cleared on the ring corresponding to RPR logical interface [STRING].
参数解释	$1：接口名称
日志等级	5
举例	RPR/5/RPR_TOPOLOGY_INVALID_OVER: A topology invalid defect is cleared on the ring corresponding to RPR logical interface RPR-Router1.
日志说明	站点收集的拓扑信息有效
处理建议	无

142 RRPP

本节介绍 RRPP 模块输出的日志信息。

142.1 RRPP_RING_FAIL

日志内容	Ring [UINT32] in Domain [UINT32] failed.
参数解释	$1：环ID $2：域ID
日志等级	4
举例	RRPP/4/RRPP_RING_FAIL: Ring 1 in Domain 1 failed.
日志说明	RRPP域下的环链路故障
处理建议	检测RRPP环的各个节点，清除网络故障

142.2 RRPP_RING_RESTORE

日志内容	Ring [UINT32] in Domain [UINT32] recovered.
参数解释	$1：环ID $2：域ID
日志等级	4
举例	RRPP/4/RRPP_RING_RESTORE: Ring 1 in Domain 1 recovered.
日志说明	RRPP域下的环故障恢复
处理建议	无

143 RSVP

本节介绍 RSVP 模块输出的日志信息。

143.1 RSVP_FRR_SWITCH

日志内容	Session ([STRING]): FRR is [STRING].
参数解释	$1：被保护隧道信息 $2：会话保护状态，如果有备份隧道信息，同时输出备隧道信息，取值包括： ready：绑定了快速重路由的旁路隧道，此时未进行切换 used：绑定了快速重路由的旁路隧道，此时已切换 disabled：解绑定快速重路由的旁路隧道
日志等级	5
举例	RSVP/5/RSVP_FRR_SWITCH: Session (DIP 2.2.2.2, SIP 1.1.1.1, TID 3, LSPID 5): FRR is ready. Bypass tunnel is Tunnel5.
日志说明	当隧道FRR保护成功、保护取消或发生切换时，触发该日志
处理建议	无

143.2 RSVP_P2MP_FRR_SWITCH

日志内容	Session ([STRING]): FRR is [STRING].
参数解释	$1：被保护隧道信息 $2：会话保护状态，如果有备份隧道信息，同时输出备隧道信息，取值包括： ready：绑定了快速重路由的旁路隧道，此时未进行切换 used：绑定了快速重路由的旁路隧道，此时已切换 disabled：解绑定快速重路由的旁路隧道
日志等级	5
举例	RSVP/5/RSVP_P2MP_FRR_SWITCH: P2MP session (DIP 2.2.2.2, SIP 1.1.1.1, P2MPID 0x1010101, TID 3, LSPID 5): FRR is ready. Bypass tunnel is Tunnel5.
日志说明	当隧道FRR保护成功、保护取消或发生切换时，触发该日志
处理建议	无

144 RTM

本节介绍 EAA 的 RTM（Real-Time Management）模块输出的日志信息。

144.1 RTM_ENVIRONMENT

日志内容	Can't find environment variable [STRING].
参数解释	$1：环境变量的名字
日志等级	4
举例	RTM/4/RTM_ENVIRONMENT: Can't find environment variable TestEnv.
日志说明	CLI监控策略替换环境变量时没有找到对应的环境变量，CLI监控策略执行失败
处理建议	请先定义环境变量再使用环境变量

144.2 RTM_TCL_LOAD_FAILED

日志内容	Failed to load the Tcl script file of policy [STRING].
参数解释	$1：Tcl监控策略的名称
日志等级	4
举例	RTM/4/RTM_TCL_LOAD_FAILED: Failed to load the Tcl script file of policy [STRING].
日志说明	Tcl监控策略对应的文件加载到内存失败
处理建议	无

144.3 RTM_TCL_MODIFY

日志内容	Failed to execute Tcl-defined policy [STRING] because the policy's Tcl script file had been modified.
参数解释	$1：Tcl监控策略的名称
日志等级	4
举例	RTM/4/RTM_TCL_MODIFY: Failed to execute Tcl-defined policy aaa because the policy's Tcl script file had been modified.
日志说明	Tcl监控策略触发执行时，对应的文件被修改
处理建议	确保Tcl监控策略对应的文件与注册文件相同或者重新创建Tcl监控策略

144.4 RTM_TCL_NOT_EXIST

日志内容	Failed to execute Tcl-defined policy [STRING] because the policy's Tcl script file was not found.
参数解释	$1：Tcl监控策略的名称
日志等级	4
举例	RTM/4/RTM_TCL_NOT_EXIST: Failed to execute Tcl-defined policy aaa because the policy's Tcl script file was not found.
日志说明	Tcl监控策略触发执行时对应的文件不存在
处理建议	确保Tcl监控策略对应的文件存在或者重新创建Tcl监控策略

145 RXTX

本节介绍 RXTX 模块输出的日志信息。

145.1 INIT

日志内容	IRF physical port protection occurred. Please check the affected port for VLAN configuration errors to restore the port state. IRF physical port=[INT32].
参数解释	$1：IRF物理端口
日志等级	4
举例	RXTX/4/INIT: IRF physical port protection occurred. Please check the affected port for VLAN configuration errors to restore the port state. IRF physical port=Ten1/3/0/24.
日志说明	当IRF成员设备间采用非直连方式组网时，IRF物理链路上VLAN配置有误，导致链路存在环路，IRF物理端口启动保护措施
处理建议	(1) 执行**shutdown**命令关闭提示的IRF物理端口 (2) 请分别检查提示出错的IRF物理端口以及与其连接的中继设备端口的VLAN配置，查找配置错误的端口 (3) 修改错误的IRF物理端口的VLAN及中继设备对应端口VLAN的配置。由于每条IRF物理链路的IRF协议报文需要隔离传输，请为每条IRF物理链路划分不同的VLAN，且同一条IRF物理链路两端的端口配置的VLAN ID必须相同 (4) 执行**undo shutdown**命令开启上述IRF物理端口

146 SCM

本节介绍 SCM（服务控制管理）模块输出的日志信息。

146.1 PROCESS_ABNORMAL

日志内容	The process [STRING] exited abnormally.
参数解释	$1：进程名
日志等级	5
举例	SCM/5/PROCESS_ABNORMAL: The process devd exited abnormally.
日志说明	服务异常退出
处理建议	1. 通常情况下，进程异常退出后，会立即自动重启。可使用 **display process** 命令查看进程是否存在。如果进程存在，则进程已恢复 2. 如果进程未恢复，请搜集以下信息： o 在 probe 视图下，执行 view /var/log/trace.log > trace.log，然后将设备存储目录下的 trace.log 文件通过 FTP 或 TFTP 功能，上传到服务器 o **display process log** 命令查看进程信息，如果 core 字段显示为 Y，则表示进程退出时产生 core 文件 o 如果产生 core 文件，请使用 **display exception context** 命令搜集进程异常信息，并将该异常信息保存到一个文件中；通过 **display exception filepath** 命令查看 core 文件目录，并通过 FTP 或 TFTP 功能，将 core 文件和记载了异常信息的文件上传到服务器 o 联系工程师，将上述文件，发送给工程师进行分析，并保留现场，以便工程师进行进一步分析定位 3. 如果进程已恢复，但仍需要定位进程异常退出的原因，请执行（2） 备注：当使用FTP功能将文件上传到服务器时，请使用binary传输模式

146.2 PROCESS_ACTIVEFAILED

日志内容	The standby process [STRING] failed to switch to the active process due to uncompleted synchronization, and was restarted.
参数解释	$1：进程名
日志等级	4
举例	SCM/4/PROCESS_ACTIVEFAILED: The standby process [STRING] failed to switch to the active process due to uncompleted synchronization, and was restarted.
日志说明	备用进程还未完成同步时主进程意外退出，导致备进程倒换成主进程失败。进程重启
处理建议	无

146.3 SCM_ABNORMAL_REBOOT

日志内容	形式一： The process [STRING] can't be restored. Reboot now.（集中式设备） 形式一： The process [STRING] can't be restored. Reboot [STRING] now.（分布式设备－独立运行模式）（集中式IRF设备）（分布式设备－IRF模式）
参数解释	形式一： $1：进程名 形式二： $1：进程名 $2：chassis编号+slot编号或slot编号
日志等级	3
举例	SCM/3/SCM_ABNORMAL_REBOOT: The process ipbased can't be restored. Reboot slot 2 now.
日志说明	形式一： 进程在设备启动过程中，异常退出，尝试自动重启多次后，仍不能恢复，则自动重启设备 形式二： 进程在指定slot启动过程中，异常退出，尝试自动重启多次后，仍不能恢复，则系统会自动重启指定slot
处理建议	1. 等单板重启后，使用 **display process** 命令查看进程是否恢复 2. 若多次重启后仍不能恢复，联系工程师解决

146.4 SCM_ABNORMAL_REBOOTMDC

日志内容	The process [STRING] in [STRING] [UINT16] can't be restored. Reboot [STRING] [UINT16] now.
参数解释	$1：进程名 $2：取值为MDC或Context $3：MDC或Context的编号 $4：取值为MDC或Context $5：MDC或Context的编号
日志等级	3
举例	SCM/3/SCM_ABNORMAL_REBOOTMDC: The process ipbased in MDC 2 can't be restored. Reboot MDC 2 now.
日志说明	在主用主控板上的用户MDC的在启动过程中，或者在引擎组中主引擎上的Context启动过程中，进程异常退出，尝试自动重启多次后，仍不能恢复，则重启此MDC或Context。此日志在MDC 1或Context 1中输出
处理建议	1. 等单板重启后，使用 **display process** 命令查看进程是否恢复 2. 若多次重启后仍不能恢复，联系工程师解决

146.5 SCM_ABORT_RESTORE

日志内容	The process [STRING] can't be restored, abort it.
参数解释	$1：进程名
日志等级	3
举例	SCM/3/SCM_ABORT_RESTORE: The process ipbased can't be restored, abort it.
日志说明	进程在系统运行中异常退出，尝试自动重启多次后，仍不能恢复，系统放弃恢复该进程
处理建议	1. 任意视图下执行 **display process log** 命令查看进程退出详细信息 2. 重启异常进程所在单板或 MDC，尝试恢复 3. 提供 **display process log** 命令的显示信息，联系工程师解决

146.6 SCM_INSMOD_ADDON_TOOLONG

日志内容	Failed to finish loading [STRING] in [UINT32] minutes.
参数解释	$1：内核文件的名称 $1：已加载时间
日志等级	4
举例	SCM/4/SCM_INSMOD_ADDON_TOOLONG: Failed to finish loading addon.ko in 30 minutes.
日志说明	设备启动过程中加载内核文件超时
处理建议	**1.** 重启单板，尝试恢复 **2.** 联系工程师解决

146.7 SCM_KERNEL_INIT_TOOLONG

日志内容	Kernel init in sequence [STRING] function [STRING] failed to finish in [UINT32] minutes.
参数解释	$1：内核事件的阶段 $2：内核事件阶段对应的函数的地址 $3：所用时间
日志等级	4
举例	SCM/4/SCM_KERNEL_INIT_TOOLONG: Kernel init in sequence 0x25e7 function 0x6645ffe2 failed to finish in 15 minutes.
日志说明	内核初始化时，某个阶段某函数运行时间过长
处理建议	**1.** 重启单板，尝试恢复 **2.** 联系工程师解决

146.8 SCM_PROCESS_STARTING_TOOLONG

日志内容	The process [STRING] on [STRING] [UINT16] has not finished starting in [UINT32] hours.
参数解释	$1：进程名 $2：取值为MDC或Context（不支持MDC或者Context的设备，不会输出该信息） $3：MDC或Context的编号（不支持MDC或者Context的设备，不会输出该信息） $4：所用时间
日志等级	4
举例	SCM/4/ SCM_PROCESS_STARTING_TOOLONG: The process ipbased on MDC 2 has not finished starting in 1 hours.
日志说明	进程长时间未启动完成。可能是因为配置太多导致进程启动慢，也可能是进程异常
处理建议	1. 大量配置的情况下，设备启动需要较长时间，如果等待 6 小时后，仍提示进程未完成启动，则可以认为进程已经异常 2. 重启单板/MDC/Context，尝试恢复。等单板/MDC/Context 重启后，使用 **display process** 命令查看进程是否恢复 3. 联系工程师解决

146.9 SCM_PROCESS_STILL_STARTING

日志内容	The process [STRING] on [STRING] [UINT16] is still starting for [UINT32] minutes.
参数解释	$1：进程的名称 $2：取值为MDC或Context（不支持MDC或者Context的设备，不会输出该信息） $3：MDC或Context编号（不支持MDC或者Context的设备，不会输出该信息） $4：所用时间
日志等级	6
举例	SCM/6/SCM_PROCESS_STILL_STARTING: The process ipbased on MDC 2 is still starting for 20 minutes.
日志说明	某进程一直处于启动状态
处理建议	正常提示，无须处理

146.10 SCM_SKIP_PROCESS

日志内容	The process [STRING] was skipped because it failed to start within 6 hours.
参数解释	$1：进程名
日志等级	4
举例	SCM/4/SCM_SKIP_PROCESS: The process ipbased was skipped because it failed to start within 6 hours.
日志说明	单板/MDC/Context启动过程中，有进程超过6小时未启动完成，跳过该进程继续启动
处理建议	1. 重启单板/MDC/Context 尝试恢复。等单板/MDC/Context 重启后，使用 **display process** 命令查看进程是否恢复 2. 联系工程师解决

146.11 SCM_SKIP_PROCESS

日志内容	The process [STRING] on [STRING] [UINT16] was skipped because it failed to start within 6 hours.
参数解释	$1：进程名 $2：取值为MDC或Context（不支持MDC或者Context的设备，不会输出该信息） $3：MDC或Context的编号（不支持MDC或者Context的设备，不会输出该信息）
日志等级	3
举例	SCM/3/SCM_SKIP_PROCESS: The process ipbased on MDC 2 was skipped because it failed to start within 6 hours.
日志说明	某进程超过6小时未启动完成，系统跳过该进程，继续启动
处理建议	1. 重启单板/MDC/Context，尝试恢复。等单板/MDC/Context 重启后，使用 **display process** 命令查看进程是否恢复 2. 联系工程师解决

147 SCRLSP

本节介绍静态 CRLSP 模块输出的日志信息。

147.1 SCRLSP_LABEL_DUPLICATE

日志内容	Incoming label [INT32] for static CRLSP [STRING] is duplicate.
参数解释	$1：入标签值 $2：静态CRLSP名称
日志等级	4
举例	SCRLSP/4/SCRLSP_LABEL_DUPLICATE: Incoming label 1024 for static CRLSP aaa is duplicate.
日志说明	静态CRLSP的入标签被静态PW或者静态LSP占用。触发该日志的原因可能有： **1.** 在 MPLS 已使能的情况下，配置了一条入标签被静态 PW 或者静态 LSP 占用的静态 CRLSP **2.** 在入标签被静态 PW 或静态 LSP 占用的静态 CRLSP 存在的情况下，使能 MPLS
处理建议	删除该CRLSP，重新配置一条静态CRLSP，并指定一个新的入标签

148 SESSION

本节介绍 SESSION 模块输出的日志信息。

148.1 SESSION_DRV_EXCEED

日志内容	The number of session entries ([UINT32]) supported by hardware already reached.
参数解释	$1：产品硬件支持的最大会话表项的数目
日志等级	2
举例	SESSION/2/SESSION_DRV_EXCEED: The number of session entries (65535) supported by hardware already reached.
日志说明	会话表项数目达到硬件支持的最大规格时会发送该日志
处理建议	无

148.2 SESSION_DRV_RECOVERY

日志内容	Session resources supported by hardware had been released.
参数解释	无
日志等级	2
举例	SESSION/2/SESSION_DRV_RECOVERY: Session resources supported by hardware had been released.
日志说明	会话表项资源从用尽状态恢复时会发送该日志
处理建议	无

148.3 SESSION_IPV4_FLOW

日志内容	Protocol(1001)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];NATSrcIPAddr(1005)=[IPADDR];NATSrcPort(1006)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];NATDstIPAddr(1009)=[IPADDR];NATDstPort(1010)=[UINT16];InitPktCount(1044)=[UINT32];InitByteCount(1046)=[UINT32];RplyPktCount(1045)=[UINT32];RplyByteCount(1047)=[UINT32];RcvVPNInstance(1042)=[STRING];SndVPNInstance(1043)=[STRING];RcvDSLiteTunnelPeer(1040)=[STRING];SndDSLiteTunnelPeer(1041)=[STRING];BeginTime_e(1013)=[STRING];EndTime_e(1014)=[STRING];Event(1048)=([UNIT16])[STRING];
参数解释	$1：协议类型 $2：源IP地址 $3：源端口号 $4：转换后的源IP地址 $5：转换后的源端口号 $6：目的IP地址 $7：目的端口号 $8：转换后的目的IP地址 $9：转换后的目的端口号 $10：入方向的报文总数 $11：入方向的字节总数 $12：出方向的报文总数 $13：出方向的字节总数 $14：源VPN名称 $15：目的VPN名称 $16：源DS-Lite Tunnel $17：目的DS-Lite Tunnel $18：创建会话的时间 $19：会话删除时间 $20：日志类型 $21：日志类型描述信息，包括： • Session created：会话创建日志 • Active flow threshold：流量或时间阈值日志 • Normal over：正常流结束，会话删除日志 • Aged for timeout：会话老化删除日志 • Aged for reset or config-change：通过配置删除会话日志 • Other：其他原因删除会话日志，如由其他模块删除
日志等级	6
举例	SESSION/6/SESSION_IPV4_FLOW: Protocol(1001)=UDP;SrcIPAddr(1003)=10.10.10.1;SrcPort(1004)=1024;NATSrcIPAddr(1005)=10.10.10.1;NATSrcPort(1006)=1024;DstIPAddr(1007)=20.20.20.1;DstPort(1008)=21;NATDstIPAddr(1009)=20.20.20.1;NATDstPort(1010)=21;InitPktCount(1044)=1;InitByteCount(1046)=50;RplyPktCount(1045)=0;RplyByteCount(1047)=0;RcvVPNInstance(1042)=;SndVPNInstance(1043)=;RcvDSLiteTunnelPeer(1040)=;SndDSLiteTunnelPeer(1041)=;BeginTime_e(1013)=03182024082546;EndTime_e(1014)=;Event(1048)=(8)Session created;

日志说明	创建、删除IPv4会话时会发送该日志 IPv4会话过程中会定时发送该日志 IPv4会话的流量或时间达到指定的阈值时会发送该日志
处理建议	无

148.4 SESSION_IPV6_FLOW

日志内容	Protocol(1001)=[STRING];SrcIPv6Addr(1036)=[IPADDR];SrcPort(1004)=[UINT16];DstIPv6Addr(1037)=[IPADDR];DstPort(1008)=[UINT16];InitPktCount(1044)=[UINT32];InitByteCount(1046)=[UINT32];RplyPktCount(1045)=[UINT32];RplyByteCount(1047)=[UINT32];RcvVPNInstance(1042)=[STRING];SndVPNInstance(1043)=[STRING];BeginTime_e(1013)=[STRING];EndTime_e(1014)=[STRING];Event(1048)=([UNIT16])[STRING];
参数解释	$1：协议类型 $2：源IPv6地址 $3：源端口号 $3：目的IPv6地址 $4：目的端口号 $5：入方向的报文总数 $6：入方向的字节总数 $7：出方向的报文总数 $8：出方向的字节总数 $9：源VPN名称 $10：目的VPN名称 $11：创建会话的时间 $12：会话删除时间 $13：日志类型 $14：日志类型描述信息，包括： • Session created：会话创建日志 • Active flow threshold：流量或时间阈值日志 • Normal over：正常流结束，会话删除日志 • Aged for timeout：会话老化删除日志 • Aged for reset or config-change：通过配置删除会话日志 • Other：其他原因删除会话日志，如由其他模块删除
日志等级	6
举例	SESSION/6/SESSION_IPV6_FLOW: Protocol(1001)=UDP;SrcIPv6Addr(1036)=2001::2;SrcPort(1004)=1024;DstIPv6Addr(1037)=3001::2;DstPort(1008)=53;InitPktCount(1044)=1;InitByteCount(1046)=110;RplyPktCount(1047)=0;RplyByteCount(1047)=0;RcvVPNInstance(1042)=;SndVPNInstance(1043)=;BeginTime_e(1013)=03182024082901;EndTime_e(1014)=;Event(1048)=(8)Session created;
日志说明	创建、删除IPv6会话时会发送该日志 IPv6会话过程中会定时发送该日志 IPv6会话的流量或时间达到指定的阈值时会发送该日志
处理建议	无

149 SFLOW

本节介绍 sFlow 模块输出的日志信息。

149.1 SFLOW_HARDWARE_ERROR

日志内容	Failed to [STRING] on interface [STRING] due to [STRING].
参数解释	$1：流采样模式配置，显示为：update sampling mode $2：接口名 $3：失败的原因，目前只有不支持的操作一个原因，显示为：not supported operation
日志等级	4
举例	SFLOW/4/SFLOW_HARDWARE_ERROR: Failed to update sampling mode on interface GigabitEthernet1/0/1 due to not supported operation.
日志说明	用户执行的配置不会生效。触发该日志的原因可能有：设备不支持的流采样模式
处理建议	改用其它采样模式

150 SHELL

本节介绍 SHELL 模块输出的日志信息。

150.1 SHELL_CMD

日志内容	-Line=[STRING]-IPAddr=[STRING]-User=[STRING]; Command is [STRING]
参数解释	$1：用户线名（如果不涉及该参数，显示为**） $2：IP地址（如果不涉及该参数，显示为**） $3：用户名（如果不涉及该参数，显示为**） $4：命令字符串
日志等级	6
举例	SHELL/6/SHELL_CMD: -Line=aux0-IPAddr=**-User=**; Command is quit
日志说明	记录设备执行过的命令
处理建议	无

150.2 SHELL_CMD_CONFIRM

日志内容	Confirm option of command [STRING] is [STRING].
参数解释	$1：命令字符串 $2：确认选项
日志等级	6
举例	SHELL/6/SHELL_CMD_CONFIRM: Confirm option of command save is no.
日志说明	记录需要用户确认命令的用户选项操作结果
处理建议	无

150.3 SHELL_CMD_EXECUTEFAIL

日志内容	-User=[STRING]-IPAddr=[STRING]; Command [STRING] in view [STRING] failed to be executed.
参数解释	$1：用户名 $2：IP地址 $3：命令字符串 $4：当前命令模式
日志等级	4
举例	SHELL/4/SHELL_CMD_EXECUTEFAIL: -User=**-IPAddr=192.168.62.138; Command save in view system failed to be executed.
日志说明	后台程序下发的命令执行失败
处理建议	定位命令执行失败的具体原因

150.4 SHELL_CMD_INPUT

日志内容	Input string for the [STRING] command is [STRING].
参数解释	$1：命令字符串 $2：输入字符串
日志等级	6
举例	SHELL/6/SHELL_CMD_INPUT: Input string for the save command is startup.cfg. SHELL/6/SHELL_CMD_INPUT: Input string for the save command is CTRL_C. SHELL/6/SHELL_CMD_INPUT: Input string for the save command is the Enter key.
日志说明	当用户执行命令时，如果需要输入相关信息以进行下一步操作，则输入的字符内容将被记录，并产生日志信息 例如： • 在执行 **save** 命令保存配置时，需要用户输入配置文件名和路径，用户输入的该信息将被记录 • 在执行 **save** 命令保存配置时，需要用户输入配置文件名和路径，用户输入 CTRL_C 取消了保存配置操作，则该信息将被记录 • 在执行 **save** 命令保存配置时，需要用户输入配置文件名和路径，用户输入回车，则该信息将被记录
处理建议	无

150.5 SHELL_CMD_INPUT_TIMEOUT

日志内容	Operation timed out: Getting input for the [STRING] command.
参数解释	$1：命令字符串
日志等级	6
举例	SHELL/6/SHELL_CMD_INPUT_TIMEOUT: Operation timed out: Getting input for the fdisk command.
日志说明	当用户执行命令时，如果需要输入额外信息确认操作，而用户在一定时间内未输入信息，则产生输入超时的日志信息
处理建议	无

150.6 SHELL_CMD_LOCKEDBYOTHER

日志内容	SHELL/6/SHELL_CMD_LOCKEDBYOTHER: The system has been locked by [STRING].
参数解释	$1：配置会话的类型
日志等级	6
举例	SHELL/6/SHELL_CMD_LOCKEDBYOTHER: The system has been locked by NETCONF.
日志说明	其他用户占有全局配置锁，导致命令行命令下发失败
处理建议	等待其他用户释放全局配置锁后再配置

150.7 SHELL_CMD_MATCHFAIL

日志内容	-User=[STRING]-IPAddr=[STRING]; Command [STRING] in view [STRING] failed to be matched.
参数解释	$1：用户名 $2：IP地址 $3：命令字符串 $4：当前命令模式
日志等级	4
举例	SHELL/4/SHELL_CMD_MATCHFAIL: -User=**-IPAddr=192.168.62.138; Command description 10 in view system failed to be matched.
日志说明	由于命令输入错误，或者当前模式错误等，造成命令匹配错误
处理建议	定位命令匹配失败的具体原因

150.8 SHELL_CMDDENY

日志内容	-Line=[STRING]-IPAddr=[STRING]-User=[STRING]; Command=[STRING] is denied.
参数解释	$1：用户线名（如果不涉及该参数，显示为**） $2：IP地址（如果不涉及该参数，显示为**） $3：用户名（如果不涉及该参数，显示为**） $4：命令字符串
日志等级	5
举例	SHELL/5/SHELL_CMDDENY: -Line=vty0-IPAddr=192.168.62.138-User=**; Command vlan 10 is permission denied.
日志说明	命令执行失败。用户权限不够
处理建议	无

150.9 SHELL_CMDFAIL

日志内容	Command [STRING] failed to restore the configuration.
参数解释	$1：命令字符串
日志等级	6
举例	SHELL/6/SHELL_CMDFAIL: The “save” command failed to restore the configuration.
日志说明	文本配置恢复操作失败
处理建议	无

150.10 SHELL_COMMIT_FAIL

日志内容	-Line=[STRING]-IPAddr=[STRING]-User=[STRING]; Failed to commit the target configuration.
参数解释	$1：用户线名（如果不涉及该参数，显示为**） $2：IP地址（如果不涉及该参数，显示为**） $3：用户名（如果不涉及该参数，显示为**）
日志等级	4
举例	SHELL/4/SHELL_COMMIT_FAIL: -Line=aux0-IPAddr=**-User=**; Failed to commit the target configuration.
日志说明	私有模式或独占模式下，下发目标配置失败
处理建议	无

150.11 SHELL_COMMIT_ROLLBACK

日志内容	The configuration commit delay is overtime, a configuration rollback will be performed.
参数解释	无
日志等级	5
举例	SHELL/5/ SHELL_COMMIT_ROLLBACK: The configuration commit delay is overtime, a configuration rollback will be performed.
日志说明	下发目标配置时指定了超时回滚时间，设备达到超时回滚时间进行配置回滚，配置回滚开始的提示
处理建议	无

150.12 SHELL_COMMIT_ROLLBACKDONE

日志内容	The configuration rollback has been performed.
参数解释	无
日志等级	5
举例	SHELL/5/ SHELL_COMMIT_ROLLBACKDONE: The configuration rollback has been performed.
日志说明	下发目标配置时指定了超时回滚时间，设备达到超时回滚时间，配置回滚完成的提示
处理建议	无

150.13 SHELL_COMMIT_ROLLBACKFAIL

日志内容	Failed to roll back the configuration from the uncommitted changes.
参数解释	无
日志等级	5
举例	SHELL/5/ SHELL_COMMIT_ROLLBACKFAIL: Failed to roll back the configuration from the uncommitted changes.
日志说明	下发目标配置时指定了超时回滚时间，设备达到超时回滚时间进行配置回滚时，回滚失败
处理建议	请根据需要手工处理

150.14 SHELL_COMMIT_SUCCESS

日志内容	-Line=[STRING]-IPAddr=[STRING]-User=[STRING]; Target configuration successfully committed.
参数解释	$1：用户线名（如果不涉及该参数，显示为**） $2：IP地址（如果不涉及该参数，显示为**） $3：用户名（如果不涉及该参数，显示为**）
日志等级	5
举例	SHELL/5/SHELL_COMMIT_SUCCESS: -Line=aux0-IPAddr=**-User=**; Target configuration successfully committed.
日志说明	私有模式或独占模式下，下发目标配置成功
处理建议	无

150.15 SHELL_CRITICAL_CMDFAIL

日志内容	-User=[STRING]-IPAddr=[STRING]; Command=[STRING] .
参数解释	$1：用户名 $2：IP地址 $3：命令字符串
日志等级	6
举例	SHELL/6/SHELL_CRITICAL_CMDFAIL: -User=admin-IPAddr=169.254.0.7; Command is save.
日志说明	命令执行失败
处理建议	无

150.16 SHELL_LOGIN

日志内容	[STRING] logged in from [STRING].
参数解释	$1：用户名 $2：用户线名
日志等级	5
举例	SHELL/5/SHELL_LOGIN: Console logged in from console0.
日志说明	用户成功登录 用户线名为“local”时，表示用户登录到备用主控板自身
处理建议	无

150.17 SHELL_LOGOUT

日志内容	[STRING] logged out from [STRING].
参数解释	$1：用户名 $2：用户线名
日志等级	5
举例	SHELL/5/SHELL_LOGOUT: Console logged out from console0.
日志说明	用户退出登录 用户线名为“local”时，表示用户从备用主控板自身退出登录
处理建议	无

150.18 SHELL_SAVE_FAILED

日志内容	Failed to save running configuration to configuration file for configuration rollback.
参数解释	N/A
日志等级	5
举例	SHELL/5/SHELL_SAVE_FAILED: Failed to save running configuration to configuration file for configuration rollback.
日志说明	系统保存下发目标配置前的配置到配置文件失败，无法进行配置回滚。系统保存下发目标配置前的配置到配置文件的时机有： • 执行 **commit** 命令后下发目标配置失败 • 执行 **commit confirmed** 命令指定了超时回滚时间，但在超时回滚时间内没有再次执行 **commit** 命令确认下发目标配置
处理建议	如需将当前配置回滚到下发目标配置前的配置，请手动恢复

150.19 SHELL_SAVE_SUCCESS

日志内容	Saved running configuration to configuration file for configuration rollback.
参数解释	N/A
日志等级	5
举例	SHELL/5/SHELL_SAVE_SUCCESS: Saved running configuration to configuration file for configuration rollback.
日志说明	系统成功地保存下发目标配置前的配置到配置文件，以进行配置回滚。系统保存下发目标配置前的配置到配置文件的时机有： • 执行 **commit** 命令后下发目标配置失败 • 执行 **commit confirmed** 命令指定了超时回滚时间，但在超时回滚时间内没有再次执行 **commit** 命令确认下发目标配置
处理建议	无

150.20 SHELL_SAVEPOINT_EXIST

日志内容	The running configuration at this rollback point is the same as the configuration at the previous rollback point.
参数解释	N/A
日志等级	5
举例	SHELL/5/SHELL_SAVEPOINT_EXIST: The running configuration at this rollback point is the same as the configuration at the previous rollback point.
日志说明	新创建的配置回滚点与上次创建的配置回滚点对应的配置相同
处理建议	无

150.21 SHELL_SAVEPOINT_FAILED

日志内容	Failed to create a new rollback point.
参数解释	N/A
日志等级	5
举例	SHELL/5/SHELL_SAVEPOINT_FAILED: Failed to create a new rollback point.
日志说明	创建新配置回滚点失败
处理建议	如需保留对应配置回滚点，可以手动恢复回滚点对应配置，然后检查文件系统（例如文件系统剩余存储空间是否充足），再执行**commit**命令

150.22 SHELL_SAVEPOINT_SUCCESS

日志内容	Created a new rollback point.
参数解释	N/A
日志等级	5
举例	SHELL/5/SHELL_SAVEPOINT_SUCCESS: Created a new rollback point.
日志说明	成功创建一个新配置回滚点
处理建议	无

151 SLSP

本节介绍静态 LSP 模块输出的日志信息。

151.1 SLSP_LABEL_DUPLICATE

日志内容	Incoming label [INT32] for static LSP [STRING] is duplicate.
参数解释	$1：入标签值 $2：静态LSP名称
日志等级	4
举例	SLSP/4/SLSP_LABEL_DUPLICATE: Incoming label 1024 for static LSP aaa is duplicate.
日志说明	静态LSP的入标签被静态PW或者静态CRLSP占用。触发该日志的原因可能有： • 在 MPLS 已使能的情况下，配置了一条入标签被静态 PW 或静态 CRLSP 占用的静态 LSP • 在入标签被静态 PW 或静态 CRLSP 占用的静态 LSP 存在的情况下，使能 MPLS
处理建议	删除该LSP，重新配置一条静态LSP，并指定一个新的入标签

152 SMLK

本节介绍 Smart Link 模块输出的日志信息。

152.1 SMLK_LINK_SWITCH

日志内容	Status of port [STRING] in smart link group [UINT16] changes to active.
参数解释	$1：端口名称 $2：Smart Link组ID
日志等级	4
举例	SMLK/4/SMLK_LINK_SWITCH: Status of port GigabitEthernet0/1/4 in smart link group 1 changes to active.
日志说明	从端口接替故障主端口转发流量
处理建议	清除网络故障

153 SNMP

本节介绍 SNMP 模块输出的日志信息。

153.1 SNMP_ACL_RESTRICTION

日志内容	SNMP [STRING] from [STRING] is rejected due to ACL restriction.
参数解释	$1：SNMP团体名/用户名/组名 $2：NMS的IP地址
日志等级	3
举例	SNMP/3/SNMP_ACL_RESTRICTION: SNMP community public from 192.168.1.100 is rejected due to ACL restrictions.
日志说明	当SNMP报文因ACL限制被拒绝通过时，打印系统日志
处理建议	检查SNMP agent上的ACL配置，及agent是否被攻击

153.2 SNMP_AUTHENTICATION_FAILURE

日志内容	Failed to authenticate SNMP message.
参数解释	无
日志等级	4
举例	SNMP/4/SNMP_AUTHENTICATION_FAILURE: Failed to authenticate SNMP message.
日志说明	NMS向Agent发起SNMP请求，当认证失败时，Agent记录此日志信息
处理建议	无

153.3 SNMP_GET

日志内容	-seqNO=[UINT32]-srcIP=[STRING]-op=GET-node=[STRING]-value=[STRING]; The agent received a message.
参数解释	$1：SNMP操作日志的序列号 $2：NMS的IP 地址 $3：Get操作的MIB节点名及对应的OID $4：请求报文的取值字段
日志等级	6
举例	SNMP/6/SNMP_GET: -seqNO=1-srcIP=192.168.28.28-op=GET-node=sysLocation(1.3.6.1.2.1.1.6.0)-value=; The agent received a message.
日志说明	NMS向Agent发送Get请求报文。如果SNMP日志功能开启，SNMP模块将记录Get请求相关信息
处理建议	无

153.4 SNMP_INFORM_LOST

日志内容	Inform failed to reach NMS [STRING]: Inform [STRING][STRING].
参数解释	$1：NMS主机地址及端口号 $2：告警名称及对应的OID $3：告警携带的MIB节点名称、OID及相应的值 o 如果告警未携带 MIB 节点，此参数部分不会出现 o 如果告警携带有 MIB 节点，此参数部分以“ with ”（空格 with 空格）开头，节点间以“;”（分号）作为分隔符
日志等级	3
举例	SNMP/3/SNMP_INFORM_LOST: Inform failed to reach NMS 192.168.111.222(163): Inform coldStart(1.3.6.1.6.3.1.1.5.1).
日志说明	设备给NMS发送Inform报文后，未收到NMS的响应报文，则认为NMS不可达。设备会打印该日志方便用户定位 当日志携带多个参数导致日志超长时，系统会自动将当前日志拆分为多条日志发送，且添加定位符标识“-PART=xx”，xx表示拆分后生成的日志的序号
处理建议	检查设备到NMS是否路由可达

153.5 SNMP_NOTIFY

日志内容	Notification [STRING][STRING].
参数解释	$1：告警名称及对应的OID $2：告警携带的MIB节点名称、OID及相应的值 o 如果告警未携带 MIB 节点，此参数部分不会出现 o 如果告警携带有 MIB 节点，此参数部分以“ with ”（空格 with 空格）开头，节点间以“;”（分号）作为分隔符
日志等级	6
举例	未拆分的日志举例： SNMP/6/SNMP_NOTIFY: Notification hh3cLogIn(1.3.6.1.4.1.25506.2.2.1.1.3.0.1) with hh3cTerminalUserName(1.3.6.1.4.1.25506.2.2.1.1.2.1.0)=;hh3cTerminalSource(1.3.6.1.4.1.25506.2.2.1.1.2.2.0)=Console. 被拆分的日志举例： SNMP/6/SNMP_NOTIFY: -MDC=1; -PART=1; Notification syslogMsgNotification(1.3.6.1.2.1.192.0.1) with syslogMsgFacility(1.3.6.1.2.1.192.1.2.1.2.1)=23;syslogMsgSeverity(1.3.6.1.2.1.192.1.2.1.3.1)=6;syslogMsgVersion(1.3.6.1.2.1.192.1.2.1.4.1)=1;syslogMsgTimeStamp(1.3.6.1.2.1.192.1.2.1.5.1)=07-e2-04-12-12-26-35-00-00-00-2d-00-00[hex];syslogMsgHostName(1.3.6.1.2.1.192.1.2.1.6.1)=H3C;syslogMsgAppName(1.3.6.1.2.1.192.1.2.1.7.1)=SHELL;syslogMsgProcID(1.3.6.1.2.1.192.1.2.1.8.1)=-;syslogMsgMsgID(1.3.6.1.2.1.192.1.2.1.9.1)=SHELL_CMD;syslogMsgSDParams(1.3.6.1.2.1.192.1.2.1.10.1)=4;syslogMsgMsg(1.3.6.1.2.1.192.1.2.1.11.1)= Command is snmp-agent trap enable syslog;syslogMsgSDParamValue(1.3.6.1.2.1.192.1.3.1.4.1.1.12.83.121.115.76.111.99.64.50.53.53.48.54.3.77.68.67)=1;syslogMsgSDParamValue(1.3.6.1.2.1.192.1.3.1.4.1.2.12.65.112.112.76.111.99.64.50.53.53.48.54.4.76.105.110.101)=con0. SNMP/6/SNMP_NOTIFY: -MDC=1; -PART=2; Notification syslogMsgNotification(1.3.6.1.2.1.192.0.1) with syslogMsgSDParamValue(1.3.6.1.2.1.192.1.3.1.4.1.3.12.65.112.112.76.111.99.64.50.53.53.48.54.6.73.80.65.100.100.114)=**;syslogMsgSDParamValue(1.3.6.1.2.1.192.1.3.1.4.1.4.12.65.112.112.76.111.99.64.50.53.53.48.54.4.85.115.101.114)=**.
日志说明	Agent发送告警给NMS。如果SNMP告警日志功能开启，Agent将记录SNMP告警信息 当日志携带多个参数导致日志超长时，系统会自动将当前日志拆分为多条日志发送，且添加定位符标识“-PART=xx”，xx表示拆分后生成的日志的序号
处理建议	无

153.6 SNMP_SET

日志内容	-seqNO=[UINT32]-srcIP=[STRING]-op=SET-errorIndex=[UINT32]-errorStatus=[STRING]-node=[STRING]-value=[STRING]; The agent received a message.
参数解释	$1：SNMP操作日志的序列号 $2：NMS的IP地址 $3：Set操作的差错索引 $4：Set操作的差错状态 $5：Set操作的MIB节点名及对应的OID $6：Set操作设置的MIB节点的值
日志等级	6
举例	SNMP/6/SNMP_SET: -seqNO=3-srcIP=192.168.28.28-op=SET-errorIndex=0-errorStatus=noError-node=sysLocation(1.3.6.1.2.1.1.6.0)-value=Hangzhou China; The agent received a message.
日志说明	NMS向Agent发送Set请求。如果SNMP日志功能开启，SNMP模块将记录Set操作
处理建议	无

153.7 SNMP_USM_NOTINTIMEWINDOW

日志内容	-User=[STRING]-IPAddr=[STRING]; SNMPv3 message is not in the time window.
参数解释	$1：用户名 $2：NMS的IP地址
日志等级	4
举例	SNMP/4/SNMP_USM_NOTINTIMEWINDOW: -User=admin-IPAddr=169.254.0.7; SNMPv3 message is not in the time window.
日志说明	SNMPv3消息不在时间窗
处理建议	无

154 SSHC

本节介绍 SSHC（SSH client，SSH 客户端）模块输出的日志信息。

154.1 SSHC_ALGORITHM_MISMATCH

日志内容	Failed to log in to SSH server [STRING] because of [STRING] algorithm mismatch.
参数解释	$1：SSH服务端IP地址 $2：算法类型:encryption（加密）、key exchange（密钥交换）、MAC（message authentication code）或者public key（公钥）
日志等级	6
举例	SSHC/6/SSHC_ALGORITHM_MISMATCH: Failed to log in to SSH server 192.168.30.11 because of encryption algorithm mismatch.
日志说明	算法不匹配，SSH客户端登录服务器失败
处理建议	修改算法，使SSH客户端和服务器使用相同算法

155 SSHS

本节介绍 SSHS（SSH server，SSH 服务器）模块输出的日志信息。

155.1 SSHS_ACL_DENY

日志内容	The SSH Connection [IPADDR]([STRING]) request was denied according to ACL rules.
参数解释	$1：SSH客户端IP地址 $2：SSH客户端IP地址所在VPN
日志等级	5
举例	SSHS/5/SSH_ACL_DENY: The SSH Connection 1.2.3.4(vpn1) request was denied according to ACL rules.
日志说明	SSH ACL规则限制登录IP地址。该日志在SSH服务端检测到非法客户端尝试登录时输出
处理建议	无

155.2 SSHS_ALGORITHM_MISMATCH

日志内容	SSH client [STRING] failed to log in because of [STRING] algorithm mismatch.
参数解释	$1：SSH客户端IP地址 $2：算法类型，encryption（加密）、key exchange（密钥交换）、MAC（message authentication code）或者public key（公钥）
日志等级	6
举例	SSHS/6/SSHS_ALGORITHM_MISMATCH: SSH client 192.168.30.117 failed to log in because of encryption algorithm mismatch.
日志说明	算法不匹配，SSH客户端登录失败
处理建议	修改算法，使SSH客户端和服务器使用相同算法

155.3 SSHS_AUTH_EXCEED_RETRY_TIMES

日志内容	SSH user [STRING] (IP: [STRING]) failed to log in, because the number of authentication attempts exceeded the upper limit.
参数解释	$1：用户名 $2：SSH客户端IP地址
日志等级	6
举例	SSHS/6/SSHS_AUTH_EXCEED_RETRY_TIMES: SSH user David (IP: 192.168.30.117) failed to log in, because the number of authentication attempts exceeded the upper limit.
日志说明	SSH用户登录失败，认证尝试次数达到了最大值
处理建议	请SSH用户确认登录信息，并尝试重新登录

155.4 SSHS_AUTH_FAIL

日志内容	SSH user [STRING] (IP: [STRING]) didn't pass public key authentication for [STRING].
参数解释	$1：用户名 $2：SSH客户端IP地址 $3：失败原因： • wrong public key algorithm （公钥算法错误） • wrong public key（公钥错误） • wrong digital signature（数字签名错误）
日志等级	5
举例	SSHS/5/SSHS_AUTH_FAIL: SSH user David (IP: 192.168.30.117) didn't pass public key authentication for wrong public key algorithm.
日志说明	SSH用户没有通过公钥认证
处理建议	请SSH用户重新登录

155.5 SSHS_AUTH_TIMEOUT

日志内容	Authentication timed out for [IPADDR].
参数解释	$1：用户IP地址
日志等级	6
举例	SSHS/6/SSHS_AUTH_TIMEOUT: Authentication timed out for 1.1.1.1.
日志说明	SSH用户认证超时。该日志在SSH服务端检测到用户认证超时时输出
处理建议	建议用户检查是否没有及时输入认证信息

155.6 SSHS_CONNECT

日志内容	SSH user [STRING] (IP: [STRING]) connected to the server successfully.
参数解释	$1：用户名 $2：SSH客户端IP地址
日志等级	6
举例	SSHS/6/SSHS_CONNECT: SSH user David (IP: 192.168.30.117) connected to the server successfully.
日志说明	SSH用户成功登录服务器
处理建议	无

155.7 SSHS_DECRYPT_FAIL

日志内容	The packet from [STRING] failed to be decrypted with [STRING].
参数解释	$1：SSH客户端IP地址 $2：加密算法（比如aes256-cbc）
日志等级	5
举例	SSHS/5/SSHS_DECRYPT_FAIL: The packet from 192.168.30.117 failed to be decrypted with aes256-cbc.
日志说明	来自SSH客户端的报文解密失败
处理建议	无

155.8 SSHS_DISCONNECT

日志内容	SSH user [STRING] (IP: [STRING]) disconnected from the server.
参数解释	$1：用户名 $2：SSH客户端IP地址
日志等级	6
举例	SSHS/6/SSHS_DISCONNECT: SSH user David (IP: 192.168.30.117) disconnected from the server.
日志说明	SSH用户退出登录
处理建议	无

155.9 SSHS_ENCRYPT_FAIL

日志内容	The packet to [STRING] failed to be encrypted with [STRING].
参数解释	$1：SSH客户端IP地址 $2：加密算法（比如aes256-cbc）
日志等级	5
举例	SSHS/5/SSHS_ENCRYPT_FAIL: The packet to 192.168.30.117 failed to be encrypted with aes256-cbc.
日志说明	发往SSH客户端的报文加密失败
处理建议	无

155.10 SSHS_LOG

日志内容	Authentication failed for [STRING] from [STRING] port [INT32] because of invalid username or wrong password.
参数解释	$1：SSH客户端IP地址 $2：用户名 $3：端口号
日志等级	6
举例	SSHS/6/SSHS_LOG: Authentication failed for David from 140.1.1.46 port 16266 because of invalid username or wrong password.
日志说明	SSH用户密码认证失败
处理建议	无

155.11 SSHS_MAC_ERROR

日志内容	SSH server received a packet with wrong message authentication code (MAC) from [STRING].
参数解释	$1：SSH客户端IP地址
日志等级	6
举例	SSHS/6/SSHS_MAC_ERROR: SSH server received a packet with wrong message authentication code (MAC) from 192.168.30.117.
日志说明	SSH服务器从客户端收到一个MAC错误的报文
处理建议	无

155.12 SSHS_REACH_SESSION_LIMIT

日志内容	SSH client [STRING] failed to log in. The current number of SSH sessions is [NUMBER]. The maximum number allowed is [NUMBER].
参数解释	$1：SSH客户端IP地址 $2：当前的SSH会话数 $3：设备允许建立的SSH会话数
日志等级	6
举例	SSHS/6/SSHS_REACH_SESSION_LIMIT: SSH client 192.168.30.117 failed to log in. The current number of SSH sessions is 10. The maximum number allowed is 10.
日志说明	SSH客户端登录失败，SSH会话数达到了最大值
处理建议	无

155.13 SSHS_REACH_USER_LIMIT

日志内容	SSH client [STRING] failed to log in, because the number of users reached the upper limit.
参数解释	$1：SSH客户端IP地址
日志等级	6
举例	SSHS/6/SSHS_REACH_USER_LIMIT: SSH client 192.168.30.117 failed to log in, because the number of users reached the upper limit.
日志说明	SSH客户端登录失败，SSH用户数达到了最大值
处理建议	无

155.14 SSHS_SCP_OPER

日志内容	User [STRING] at [IPADDR] requested operation: [STRING].
参数解释	$1：用户名称. $2：用户IP地址. $3：用户请求内容，包括文件操作信息 • get file "*name*"：下载名为 *name* 的文件 • put file "*name*"：上传名为 *name* 的文件
日志等级	6
举例	SSHS/6/SSHS_SCP_OPER: -MDC=1; User user1 at 1.1.1.1 requested operation: put file "aa".
日志说明	SCP服务器收到SCP用户请求执行相关操作
处理建议	无

155.15 SSHS_SFTP_OPER

日志内容	User [STRING] at [IPADDR] requested operation: [STRING].
参数解释	$1：用户名称. $2：用户IP地址. $3：用户请求内容，包括文件操作和目录操作等信息 • open dir "*path*"：打开目录 *path* • open "*file*" (attribute code *code*) in *MODE* mode：在 *MODE* 模式下，打开文件 *file*，该文件的属性代码为 *code* • remove file "*path*"：删除文件 *path* • mkdir "*path*" (attribute code *code*)：创建新目录 *path*，该目录的属性代码为 *code* • rmdir "*path*"：删除目录 *path* • rename old "*old-name*" to new "*new-name*"：改变旧文件或文件夹的名称 *old-name* 为 *new-name*
日志等级	6
举例	SSHS/6/SSHS_SFTP_OPER: User user1 at 1.1.1.1 requested operation: open dir "flash:/".
日志说明	SFTP用户请求相关操作信息。该日志在SFTP服务端收到用户请求执行相关命令时输出
处理建议	无

155.16 SSHS_SRV_UNAVAILABLE

日志内容	The [STRING] server is disabled or the [STRING] service type is not supported.
参数解释	$1：服务类型，包括Stelnet、SCP、SFTP、NETCONF
日志等级	6
举例	SSHS/6/SSHS_SRV_UNAVAILABLE: The SCP server is disabled or the SCP service type is not supported.
日志说明	Stelnet/SCP/SFTP/NETCONF over SSH服务不可用，服务器正在断开连接
处理建议	检查服务状态或用户配置

155.17 SSHS_VERSION_MISMATCH

日志内容	SSH client [STRING] failed to log in because of version mismatch.
参数解释	$1：SSH客户端IP地址
日志等级	6
举例	SSHS/6/SSHS_VERSION_MISMATCH: SSH client 192.168.30.117 failed to log in because of version mismatch.
日志说明	SSH客户端和服务器的SSH版本号不匹配
处理建议	修改版本，使SSH客户端和服务器使用相同SSH版本

156 STAMGR

本节介绍 STAMGR 模块输出的日志信息。

156.1 STAMGR_ADD_FAILVLAN

日志内容	-SSID=[STRING]-UserMAC=[STRING]; Added a user to the Fail VLAN [STRING].
参数解释	$1：用户上线的无线服务名称 $2：用户的MAC地址 $3：用户加入的Fail-VLAN的VLAN ID
日志等级	5
举例	STAMGR/5/STAMGR_ADD_FAILVLAN:-SSID=text-wifi-UserMAC=3ce5-a616-28cd; Added a user to the Fail VLAN 5.
日志说明	用户认证失败加入Fail-VLAN
处理建议	无

156.2 STAMGR_ADDBAC_INFO

日志内容	Add BAS AC [STRING].
参数解释	$1：BAS AC的MAC地址
日志等级	6
举例	STAMGR/6/STAMGR_ADDBAC_INFO: Add BAS AC 3ce5-a616-28cd.
日志说明	Master AC与BAS AC建立连接
处理建议	无

156.3 STAMGR_ADDSTA_INFO

日志内容	Add client [STRING].
参数解释	$1：客户端的MAC地址
日志等级	6
举例	STAMGR/6/STAMGR_ADDSTA_INFO: Add client 3ce5-a616-28cd.
日志说明	客户端成功连接到BAS AC
处理建议	无

156.4 STAMGR_AUTHORACL_FAILURE

日志内容	-SSID=[STRING]-UserMAC=[STRING]; Failed to assign an ACL. Reason: [STRING].
参数解释	$1：用户上线的无线服务名称 $2：用户的MAC地址 $3：授权ACL失败的原因 • The ACL doesn't exist：指定的 ACL 不存在 • ACL type not supported：不支持指定的 ACL 类型 • Not enough hardware resources：内存不足 • The ACL conflicts with other ACLs：指定的 ACL 与其他 ACL 冲突 • The ACL doesn't contain any rules：指定 ACL 没有包含任何规则 • Unknown error：未知错误
日志等级	5
举例	STAMGR/5/STAMGR_AUTHORACL_FAILURE:-SSID=text-wifi-UserMAC=3ce5-a616-28cd; Failed to assign an ACL.Reason: The ACL doesn’t exist.
日志说明	下发ACL失败
处理建议	无

156.5 STAMGR_AUTHORUSERPROFILE_FAILURE

日志内容	-SSID=[STRING]-UserMAC=[STRING]; Failed to assign a user profile
参数解释	$1：用户上线的无线服务名称 $2：用户的MAC地址
日志等级	5
举例	STAMGR/5/STAMGR_AUTHORUSERPROFILE_FAILURE:-SSID=text-wifi-UserMAC=3ce5-a616-28cd; Failed to assign a user profile
日志说明	下发user profile失败
处理建议	无

156.6 STAMGR_CLIENT_OFFLINE

日志内容	Client [STRING] went offline from BSS [STRING] with [STRING]. State changed to Unauth.
参数解释	$1：客户端的MAC地址 $2：BSSID $3：服务模板的SSID
日志等级	6
举例	STAMGR/6/STAMGR_CLIENT_OFFLINE: Client 0023-8933-2147 went offline from BSS 0023-12ef-78dc with SSID abc. State changed to Unauth.
日志说明	客户端在BSS下线，状态变为未认证状态
处理建议	• 若客户端主动下线，则不用排查问题 • 若客户端异常下线，需要查看 AP 和 Radio 是否处于正常工作状态，若有异常根据调试信息定位并解决问题

156.7 STAMGR_CLIENT_ONLINE

日志内容	Client [STRING] went online from BSS [STRING] with SSID [STRING]. State changed to Run.
参数解释	$1：客户端的MAC地址 $2：BSSID $3：无线服务模板的SSID
日志等级	6
举例	STAMGR/6/STAMGR_CLIENT_ONLINE: Client 0023-8933-2147 went online from BSS 0023-12ef-78dc with SSID abc. State changed to Run.
日志说明	客户端在BSS上线，状态变为运行状态
处理建议	无

156.8 STAMGR_DELBAC_INFO

日志内容	Delete BAS AC [STRING].
参数解释	$1：BAS AC的MAC地址
日志等级	6
举例	STAMGR/6/STAMGR_DELBAC_INFO: Delete BAS AC 3ce5-a616-28cd.
日志说明	Master AC断开与BAS AC的连接
处理建议	无

156.9 STAMGR_DELSTA_INFO

日志内容	Delete client [STRING].
参数解释	$1：客户端的MAC地址
日志等级	6
举例	STAMGR/6/STAMGR_DELSTA_INFO: Delete client 3ce5-a616-28cd.
日志说明	客户端断开与BAS AC的连接
处理建议	无

156.10 STAMGR_DOT1X_LOGIN_FAILURE

日志内容	-Username=[STRING]-UserMAC=[STRING]-SSID=[STRING]-VLANID=[STRING]; A user failed 802.1X authentication.
参数解释	$1：用户名 $2：用户的MAC地址 $3：用户上线的无线服务名称 $4：用户上线的VLAN ID
日志等级	5
举例	STAMGR/5/STAMGR_DOT1X_LOGIN_FAILURE:-Username=Dot1X-UserMAC=3ce5-a616-28cd-SSID=text-wifi-VLANID=11; A user failed 802.1X authentication.
日志说明	用户802.1X认证失败。触发该日志的原因可能有：AAA服务器不可用、用户名或密码设置不正确
处理建议	• 检查设备与 AAA 服务器的网络连接是否正常 • 检查 AAA 服务器是否正常工作 • 检查用户名和密码设置是否和 AAA 服务器上的设置一致

156.11 STAMGR_DOT1X_LOGIN_SUCC

日志内容	-Username=[STRING]-UserMAC=[STRING]-SSID=[STRING]-VLANID=[STRING]; A user passed 802.1X authentication and came online.
参数解释	$1：用户名 $2：用户的MAC地址 $3：用户上线的无线服务名称 $4：用户上线的VLAN ID
日志等级	6
举例	STAMGR/6/STAMGR_DOT1X_LOGIN_SUCC:-Username=Dot1X-UserMAC=3ce5-a616-28cd-SSID=text-wifi-VLANID=11; A user passed 802.1X authentication and came online.
日志说明	用户通过802.1X认证
处理建议	无

156.12 STAMGR_DOT1X_LOGOFF

日志内容	Username=[STRING]-UserMAC=[STRING]-SSID=[STRING]-VLANID=[STRING]; Session for an 802.1X user was terminated.
参数解释	$1：用户名 $2：用户的MAC地址 $3：用户上线的无线服务名称 $4：用户上线的VLAN ID
日志等级	6
举例	STAMGR/6/STAMGR_DOT1X_LOGOFF:-Username=Dot1X-UserMAC=3ce5-a616-28cd-SSID=text-wifi-VLANID=11; Session for an 802.1X user was terminated.
日志说明	802.1X用户下线
处理建议	无

156.13 STAMGR_MACA_LOGIN_FAILURE

日志内容	-Username=[STRING]-UserMAC=[STRING]-SSID=[STRING]-VLANID=[STRING]-UsernameFormat=[STRING]; A user failed MAC authentication.
参数解释	$1：用户名 $2：用户的MAC地址 $3：用户上线的无线服务名称 $4：用户上线的VLAN ID $5：用户名格式 • fixed：固定用户名格式 • MAC address：MAC 地址格式
日志等级	5
举例	STAMGR/5/STAMGR_MACA_LOGIN_FAILURE:-Username=MAC-UserMAC=3ce5-a616-28cd-SSID=text-wifi-VLANID=11-UsernameFormat=fixed; A user failed MAC authentication.
日志说明	用户MAC地址认证失败。触发该日志的原因可能有：AAA服务器不可用、用户名或密码设置不正确
处理建议	• 检查设备与 AAA 服务器的网络连接是否正常 • 检查 AAA 服务器是否正常工作 • 检查用户名和密码设置是否和 AAA 服务器上的设置一致

156.14 STAMGR_MACA_LOGIN_SUCC

日志内容	-Username=[STRING]-UserMAC=[STRING]-SSID=[STRING]-VLANID=[STRING]-UsernameFormat=[STRING]; A user passed MAC authentication and came online.
参数解释	$1：用户名 $2：用户的MAC地址 $3：用户上线的无线服务名称 $4：用户上线的VLAN ID $5：用户名格式 • fixed：固定用户名格式 • MAC address：MAC 地址格式
日志等级	6
举例	STAMGR/6/STAMGR_MACA_LOGIN_SUCC:-Username=MAC-UserMAC=3ce5-a616-28cd-SSID=text-wifi-VLANID=11-UsernameFormat=fixed; A user passed MAC authentication and came online.
日志说明	用户通过MAC地址认证
处理建议	无

156.15 STAMGR_MACA_LOGOFF

日志内容	-Username=[STRING]-UserMAC=[STRING]-SSID=[STRING]-VLANID=[STRING]-UsernameFormat=[STRING]; Session for a MAC authentication user was terminated.
参数解释	$1：用户名 $2：用户的MAC地址 $3：用户上线的无线服务名称 $4：用户上线的VLAN ID $5：用户名格式 • fixed：固定用户名格式 • MAC address：MAC 地址格式
日志等级	6
举例	STAMGR/6/STAMGR_MACA_LOGOFF:-Username=MAC-UserMAC=3ce5-a616-28cd-SSID=text-wifi-VLANID=11-UsernameFormat=fixed; Session for a MAC authentication user was terminated.
日志说明	用户下线
处理建议	无

156.16 STAMGR_STAIPCHANGE_INFO

日志内容	IP address of client [STRING] changed to [STRING].
参数解释	$1：客户端的MAC地址 $2：客户端更新的IP地址
日志等级	6
举例	STAMGR/6/STAMGR_STAIPCHANGE_INFO: IP address of client 3ce5-a616-28cd changed to 4.4.4.4.
日志说明	客户端更新IP地址
处理建议	无

156.17 STAMGR_TRIGGER_IP

日志内容	-SSID=[STRING]-UserMAC=[STRING]-VLANID=[STRING]; Intrusion protection triggered. Action: [STRING].
参数解释	$1：用户上线的无线服务名称 $2：用户的MAC地址 $3：用户上线的VLAN ID $4：入侵检测模式 • Added the user to the blocked MAC address list：将用户加入 Block-MAC 表中 • Closed the user's BSS temporarily：关闭用户所在 BSS 一段时间 • Closed the user's BSS permanently：永久关闭用户所在的 BSS
日志等级	5
举例	STAMGR/5/STAMGR_TRIGGER_IP:-SSID=text-wifi-UserMAC=3ce5-a616-28cd-VLANID=11; Intrusion protection triggered, the intrusion protection action: added a user to the list of Block-MAC.
日志说明	触发入侵检测，并显示入侵检测模式
处理建议	无

157 STM

本节介绍 STM（IRF）模块输出的日志信息。

157.1 STM_AUTO_UPDATE_FAILED

日志内容	形式一： Slot [UINT32] auto-update failed. Reason: [STRING]. 形式二： Chassis [UINT32] slot [UINT32] auto-update failed. Reason: [STRING].
参数解释	形式一： $1：成员设备编号 $2：失败原因： ○ Timeout when loading：加载超时 ○ Wrong description when loading：软件包中记录的文件描述信息和软件包当前的属性不一致 ○ Disk full when writing to disk：备设备存储介质上的空间不够 形式二： $1：成员设备编号 $2：主控板槽位号 $3：失败原因： ○ Timeout when loading：加载超时 ○ Wrong description when loading：软件包中记录的文件描述信息和软件包当前的属性不一致 ○ Disk full when writing to disk：主控板存储介质上的空间不够
日志等级	4
举例	STM/4/STM_AUTO_UPDATE_FAILED: Slot 5 auto-update failed. Reason: Timeout when loading.
日志说明	形式一： 在加入IRF时，设备从主设备自动加载启动软件包失败 形式二： 在加入IRF时，备用主控板从全局主用主控板自动加载启动软件包失败
处理建议	1. 如果失败原因为 Timeout when loading，请检查 IRF 链路是否畅通 2. 如果失败原因为 Wrong description when loading，可能是软件包被损坏了，请重新下载软件包 3. 如果失败原因为 Disk full when writing to disk，请先清理备设备的存储介质，删除一些暂时不用的文件 4. 请手动升级即将加入 IRF 的设备的软件包后，再将该设备和 IRF 相连

157.2 STM_AUTO_UPDATE_FINISHED

日志内容	形式一： File loading finished on slot [UINT32]. 形式二： File loading finished on chassis [UINT32] slot [UINT32].
参数解释	形式一： $1：成员设备编号 形式二： $1：成员设备编号 $2：主控板槽位号
日志等级	5
举例	STM/5/STM_AUTO_UPDATED_FINISHED: File loading finished on slot 3.
日志说明	形式一： 成员设备完成启动文件加载 形式二： 主控板完成启动文件加载
处理建议	无

157.3 STM_AUTO_UPDATING

日志内容	形式一： Don't reboot the slot [UINT32]. It is loading files. 形式二： Don't reboot the chassis [UINT32] slot [UINT32]. It is loading files.
参数解释	形式一： $1：成员设备编号 形式二： $1：成员设备编号 $2：主控板槽位号
日志等级	5
举例	STM/5/STM_AUTO_UPDATING: Don't reboot the slot 2. It is loading files.
日志说明	形式一： 如果成员设备正在加载文件，请不要重启该设备 形式二： 如果主控板正在加载文件，请不要重启该主控板
处理建议	无

157.4 STM_LINK_DOWN

日志内容	IRF port [UINT32] went down.
参数解释	$1：IRF端口名
日志等级	3
举例	STM/3/STM_LINK_DOWN: IRF port 2 went down.
日志说明	IRF端口关闭。当绑定的所有物理端口都关闭时，IRF端口关闭
处理建议	检查绑定到IRF端口的物理端口，确保至少有一个物理端口处于UP状态，可以正常工作

157.5 STM_LINK_TIMEOUT

日志内容	IRF port [UINT32] went down because the heartbeat timed out.
参数解释	$1：IRF端口名
日志等级	2
举例	STM/2/STM_LINK_TIMEOUT: IRF port 1 went down because the heartbeat timed out.
日志说明	由于心跳检测超时，IRF端口关闭
处理建议	检查IRF链路是否故障

157.6 STM_LINK_UP

日志内容	IRF port [UINT32] came up.
参数解释	$1：IRF端口名
日志等级	6
举例	STM/6/STM_LINK_UP: IRF port 1 came up.
日志说明	IRF链路可以正常工作
处理建议	无

157.7 STM_MERGE

日志内容	IRF merge occurred.
参数解释	无
日志等级	4
举例	STM/4/STM_MERGE: IRF merge occurred.
日志说明	IRF合并事件发生
处理建议	无

157.8 STM_MERGE_NEED_REBOOT

日志内容	IRF merge occurred. This IRF system needs a reboot.
参数解释	无
日志等级	4
举例	STM/4/STM_MERGE_NEED_REBOOT: IRF merge occurred. This IRF system needs a reboot.
日志说明	由于本IRF系统在主设备选举中失败，请重启本IRF系统来完成IRF合并
处理建议	登录到本IRF，使用**reboot**命令重启本IRF

157.9 STM_MERGE_NOT_NEED_REBOOT

日志内容	IRF merge occurred. This IRF system does not need to reboot.
参数解释	无
日志等级	5
举例	STM/5/STM_MERGE_NOT_NEED_REBOOT: IRF merge occurred. This IRF system does not need to reboot.
日志说明	由于本IRF系统在主设备选举中取胜，无须重启本IRF系统即可完成IRF合并
处理建议	重启对端IRF完成合并

157.10 STM_SAMEMAC

日志内容	Failed to stack because of the same bridge MAC addresses.
参数解释	无
日志等级	4
举例	STM/4/STM_SAMEMAC: Failed to stack because of the same bridge MAC addresses.
日志说明	因为桥MAC地址相同，无法形成IRF
处理建议	检查设备桥MAC地址是否相同

157.11 STM_SOMER_CHECK

日志内容	Neighbor of IRF port [UINT32] cannot be stacked.
参数解释	$1：IRF端口名
日志等级	3
举例	STM/3/STM_SOMER_CHECK: Neighbor of IRF port 1 cannot be stacked.
日志说明	IRF口连接的设备无法加入本设备所在的IRF
处理建议	请检查以下事项： • 设备型号是否允许组成 IRF • IRF 配置是否正确 要获取更多信息，请参见该型号设备的IRF配置指导

158 STP

本节介绍生成树模块输出的日志信息。

158.1 STP_BPDU_PROTECTION

日志内容	BPDU-Protection port [STRING] received BPDUs.
参数解释	$1：接口名
日志等级	4
举例	STP/4/STP_BPDU_PROTECTION: BPDU-Protection port GigabitEthernet1/0/1 received BPDUs.
日志说明	使能了BPDU保护功能的接口收到BPDU报文
处理建议	检查下行设备是否是用户终端，是否存在恶意攻击

158.2 STP_BPDU_RECEIVE_EXPIRY

日志内容	Instance [UINT32]'s port [STRING] received no BPDU within the rcvdInfoWhile interval. Information of the port aged out.
参数解释	$1：生成树实例编号 $2：接口名
日志等级	5
举例	STP/5/STP_BPDU_RECEIVE_EXPIRY: Instance 0's port GigabitEthernet1/0/1 received no BPDU within the rcvdInfoWhile interval. Information of the port aged out.
日志说明	非指定端口因在BPDU超时之前没有收到任何BPDU报文，端口状态发生改变
处理建议	检查上行设备的STP状态及是否存在恶意攻击

158.3 STP_CONSISTENCY_RESTORATION

日志内容	Consistency restored on VLAN [UINT32]'s port [STRING].
参数解释	$1：VLAN ID $2：接口名
日志等级	6
举例	STP/6/STP_CONSISTENCY_RESTORATION: Consistency restored on VLAN 10's port GigabitEthernet1/0/1.
日志说明	接口类型不一致或者PVID不一致的保护状态解除
处理建议	无

158.4 STP_DETECTED_TC

日志内容	[STRING] [UINT32]'s port [STRING] detected a topology change.
参数解释	$1：生成树实例或VLAN $2：生成树实例编号或VLAN ID $3：接口名
日志等级	6
举例	STP/6/STP_DETECTED_TC: Instance 0's port GigabitEthernet1/0/1 detected a topology change.
日志说明	接口所在生成树实例或VLAN拓扑发生变化，本端设备检测到拓扑变化
处理建议	检查拓扑变化的原因。如果是有链路down了，就恢复此故障链路

158.5 STP_DISABLE

日志内容	STP is now disabled on the device.
参数解释	无
日志等级	6
举例	STP/6/STP_DISABLE: STP is now disabled on the device.
日志说明	设备全局去使能了生成树特性
处理建议	无

158.6 STP_DISCARDING

日志内容	Instance [UINT32]'s port [STRING] has been set to discarding state.
参数解释	$1：生成树实例编号 $2：接口名
日志等级	6
举例	STP/6/STP_DISCARDING: Instance 0's port GigabitEthernet1/0/1 has been set to discarding state.
日志说明	MSTP在计算实例内端口状态，该接口被置为discarding状态
处理建议	无

158.7 STP_ENABLE

日志内容	STP is now enabled on the device.
参数解释	无
日志等级	6
举例	STP/6/STP_ENABLE: STP is now enabled on the device.
日志说明	设备全局使能了生成树特性
处理建议	无

158.8 STP_FORWARDING

日志内容	Instance [UINT32]'s port [STRING] has been set to forwarding state.
参数解释	$1：生成树实例编号 $2：接口名
日志等级	6
举例	STP/6/STP_FORWARDING: Instance 0's port GigabitEthernet1/0/1 has been set to forwarding state.
日志说明	STP在计算实例内端口状态，该接口被置为forwarding状态
处理建议	无

158.9 STP_LOOP_PROTECTION

日志内容	Instance [UINT32]'s LOOP-Protection port [STRING] failed to receive configuration BPDUs.
参数解释	$1：生成树实例编号 $2：接口名
日志等级	4
举例	STP/4/STP_LOOP_PROTECTION: Instance 0's LOOP-Protection port GigabitEthernet1/0/1 failed to receive configuration BPDUs.
日志说明	使能了环路保护功能的接口不能接受BPDU配置报文
处理建议	检查上行设备的STP状态及是否存在恶意攻击

158.10 STP_NOT_ROOT

日志内容	The current switch is no longer the root of instance [UINT32].
参数解释	$1：生成树实例编号
日志等级	5
举例	STP/5/STP_NOT_ROOT: The current switch is no longer the root of instance 0.
日志说明	本设备某生成树实例配置为根桥，但它收到比自身更优的BPDU报文后，就不再是此实例的根桥
处理建议	检查桥优先级配置及是否存在恶意攻击

158.11 STP_NOTIFIED_TC

日志内容	[STRING] [UINT32]'s port [STRING] was notified a topology change.
参数解释	$1：生成树实例或VLAN $2：生成树实例编号或VLAN ID $3：接口名
日志等级	6
举例	STP/6/STP_NOTIFIED_TC: Instance 0's port GigabitEthernet1/0/1 was notified a topology change.
日志说明	远端相连设备通知本设备某接口所在生成树实例或VLAN的拓扑发生变化
处理建议	检查拓扑变化的原因。如果是有链路down了，就恢复此故障链路

158.12 STP_PORT_TYPE_INCONSISTENCY

日志内容	Access port [STRING] in VLAN [UINT32] received PVST BPDUs from a trunk or hybrid port.
参数解释	$1：接口名 $2：VLAN ID
日志等级	4
举例	STP/4/STP_PORT_TYPE_INCONSISTENCY: Access port GigabitEthernet1/0/1 in VLAN 10 received PVST BPDUs from a trunk or hybrid port.
日志说明	Access接口收到了对端Trunk或Hybrid接口发出的PVST报文
处理建议	检查两端的接口类型配置是否一致

158.13 STP_PVID_INCONSISTENCY

日志内容	Port [STRING] with PVID [UINT32] received PVST BPDUs from a port with PVID [UINT32].
参数解释	$1：接口名 $2：VLAN ID $3：VLAN ID
日志等级	4
举例	STP/4/STP_PVID_INCONSISTENCY: Port GigabitEthernet1/0/1 with PVID 10 received PVST BPDUs from a port with PVID 20.
日志说明	接口收到了PVID不一致的报文
处理建议	检查两端的接口PVID配置是否一致

158.14 STP_PVST_BPDU_PROTECTION

日志内容	PVST BPDUs were received on port [STRING], which is enabled with PVST BPDU protection.
参数解释	$1：接口名
日志等级	4
举例	STP/4/STP_PVST_BPDU_PROTECTION: PVST BPDUs were received on port GigabitEthernet1/0/1, which is enabled with PVST BPDU protection.
日志说明	在MSTP模式下，设备上使能了PVST报文保护功能的端口收到了PVST报文
处理建议	检查其他设备是否发出了PVST BPDU

158.15 STP_ROOT_PROTECTION

日志内容	Instance [UINT32]'s ROOT-Protection port [STRING] received superior BPDUs.
参数解释	$1：生成树实例编号 $2：接口名
日志等级	4
举例	STP/4/STP_ROOT_PROTECTION: Instance 0's ROOT-Protection port Ethernet1/0/2 received superior BPDUs.
日志说明	使能了根保护功能的接口收到了比自身BPDU报文更优的BPDU报文
处理建议	检查桥优先级配置及是否存在恶意攻击

159 SWFA

本节介绍 SWFA 模块输出的日志信息。

159.1 FWD

日志内容	Erroneous packets detected on an internal port of chassis [UINT32] slot [UINT32].
参数解释	$1：设备在IRF中的成员编号 $2：单板所在槽位号
日志等级	3
举例	SWFA/3/FWD: Erroneous packets detected on an internal port of chassis 1 slot 3.
日志说明	检测到内部互连端口（HG口）上有错误报文，打印syslog，不会修复故障
处理建议	请联系技术支持

159.2 FWD

日志内容	Erroneous packets detected on an internal port of slot [UINT32].
参数解释	$1：单板所在槽位号
日志等级	3
举例	SWFA/3/FWD: Erroneous packets detected on an internal port of slot 3.
日志说明	检测到内部互连端口（HG口）上有错误报文，打印syslog，不会修复故障
处理建议	请联系技术支持

160 SYSEVENT

本节介绍系统事件模块输出的日志信息。

160.1 EVENT_TIMEOUT

日志内容	Module [UINT32]'s processing for event [UINT32] timed out. Module [UINT32]'s processing for event [UINT32] on [STRING] timed out.
参数解释	$1：模块ID $2：事件ID $3：MDC *MDC-ID*或Context *Context-ID*
日志等级	6
举例	SYSEVENT/6/EVENT_TIMEOUT: -MDC=1; Module 0x1140000's processing for event 0x20000010 timed out. SYSEVENT/6/EVENT_TIMEOUT: -Context=1; Module 0x33c0000's processing for event 0x20000010 on Context 16 timed out.
日志说明	应用模块处理事件超时 非缺省MDC/Context上打印的日志信息不包含MDC *MDC-ID*或Context *Context-ID* 缺省MDC/Context上打印的本MDC/Context的日志信息不包含MDC *MDC-ID*或Context *Context-ID* 缺省MDC/Context上打印的其它MDC/Context的日志信息包含MDC *MDC-ID*或Context *Context-ID*
处理建议	无

161 SYSLOG

本节包含 syslog 日志消息。

161.1 SYSLOG_FILE_DECOMPRESS_ERROR

日志内容	Failed to decompress [STRING].
参数解释	$1：待解压的日志文件的名称和路径
日志等级	4
举例	SYSLOG/4/SYSLOG_FILE_DECOMPRESS_ERROR: Failed to decompress flash:/logfile/logfile1.log.gz.
日志说明	解压日志文件失败
处理建议	1. 在用户视图下，通过 **dir** 命令查看存储介质是否空间不足，如果空间不足则使用 **delete /unreserved** 命令删除部分不再使用的文件 2. 其它情况请联系技服人员解决

161.2 SYSLOG_LOGFILE_FULL

日志内容	Log file space is full.
参数解释	无
日志等级	4
举例	SYSLOG/4/SYSLOG_LOGFILE_FULL: Log file space is full.
日志说明	日志空间已满
处理建议	备份日志文件后将其删除，然后根据需要使能端口

161.3 SYSLOG_RESTART

日志内容	System restarted -- [STRING] [STRING] Software.
参数解释	$1：公司名称 $2：软件名称
日志等级	6
举例	SYSLOG/6/SYSLOG_RESTART: System restarted -- H3C Comware Software
日志说明	系统重启日志
处理建议	无

161.4 SYSLOG_RTM_EVENT_BUFFER_FULL

日志内容	In the last minute, [String] syslog logs were not monitored because the buffer was full.
参数解释	$1：过去1分钟内SYSLOG模块没有发送给EAA模块的日志的条数
日志等级	5
举例	SYSLOG/5/SYSLOG_RTM_EVENT_BUFFER_FULL: In the last minute, 100 syslog logs were not monitored because the buffer was full.
日志说明	设备在短时间内产生大量日志，导致EAA监控的日志缓冲区被占满，有多条日志没来得及匹配便被丢弃了
处理建议	• 找到日志的来源，减少日志的生成 • 使用 **rtm event syslog buffer-size** 命令增大 EAA 监控的日志缓冲区的大小

162 SYSM

本节介绍 SYSM 模块输出的日志信息

162.1 DrvDebug

日志内容	The board in chassis [UINT32] slot [UINT32] doesn't support VLAN 4094.
参数解释	$1：设备在IRF中的成员编号，chassis参数仅在IRF模式下可见 $2：单板所在的槽位号
日志等级	2
举例	DRVPLAT/2/DrvDebug: -MDC=1-Chassis=2-Slot=3; The board in chassis 2 slot 3 doesn't support VLAN 4094.
日志说明	CSPC 类单板（CSPC-GE16XP4L-E、CSPC-GE24L-E 和 CSPC-GP24GE8XP2L-E 除外）和 CMPE-1104 单板不支持 VLAN 4094
处理建议	无

162.2 DrvDebug

日志内容	The subcard [INT32] of slot [INT32] is not steady!
参数解释	$1：接口子卡槽位号 $2：单板所在的全局槽位号（独立运行模式为单板所在的槽位号，IRF模式为（IRF中的成员编号-1）x 18+单板所在的槽位号）
日志等级	5
举例	DRVPLAT/5/DrvDebug: The subcard1 of slot 2 is not steady!
日志说明	接口子卡没有安装到位或存在硬件问题
处理建议	重新拔插子卡，确保子卡已经插好。使用**display device**命令查看该子卡是否存在，如果还是不存在，请将该子卡更换子卡槽位进行检查： • 更换槽位后使用 **display device** 命令查看，如果该子卡存在了，说明可能是子卡槽位坏了，请联系技术支持 • 更换槽位后使用 **display device** 命令查看，如果该子卡还是不存在，说明可能是该子卡坏了，请联系技术支持

162.3 DrvDebug

日志内容	Warning: Overtemperature condition is detected on power module [INT32] Please check it.
参数解释	$1：电源风扇号
日志等级	5
举例	DRVPLAT/5/DrvDebug: Warning: Overtemperature condition is detected on power module 2. Please check it.
日志说明	风扇模块温度过高
处理建议	**1.** 如果环境温度较高，请检查设备所在机房的空调运行是否正常 **2.** 请检查设备出风口是否被阻塞 **3.** 请检查设备风扇是否正常运行，设备出风口是否有正常出风 **4.** 请检查是否所有槽位上都正确插了单板或者假面板 **5.** 请联系技术支持

162.4 DrvDebug

日志内容	Warning: Fan of power module [INT32] fails to operate. Please check it.
参数解释	$1：电源风扇号
日志等级	5
举例	DRVPLAT/5/DrvDebug: Warning: Fan of power module 2 fails to operate. Please check it.
日志说明	电源风扇无法工作
处理建议	请联系技术支持

162.5 DrvDebug

日志内容	Power Error, there is no input in Power 1.
参数解释	无
日志等级	5
举例	DRVPLAT/5/DrvDebug:Power Error, there is no input in Power 1.
日志说明	设备的电源模块无电流输入
处理建议	**1.** 检查电源线的连接。如果电源线松动，请重新插好电源线；如果电源线损坏，请更换电源线 **2.** 检查电源模块的安装。如果没有安装到位，请重新安装电源模块来确保电源模块和设备背板可靠连接 **3.** 检查连接的供电系统。确认供电系统正常供电，电压正常 **4.** 请联系技术支持

162.6 DrvDebug

日志内容	Power Error, there is no input in Power 2.
参数解释	无
日志等级	5
举例	DRVPLAT/5/DrvDebug:Power Error, there is no input in Power 2
日志说明	设备的电源模块无电流输入
处理建议	**1.** 检查电源线的连接。如果电源线松动，请重新插好电源线；如果电源线损坏，请更换电源线 **2.** 检查电源模块的安装。如果没有安装到位，请重新安装电源模块来确保电源模块和设备背板可靠连接 **3.** 检查连接的供电系统。确认供电系统正常供电，电压正常 **4.** 请联系技术支持

162.7 DrvDebug

日志内容	Warning: Only one power exist!
参数解释	无
日志等级	5
举例	DRVPLAT/5/DrvDebug: Only one power exist!
日志说明	当前设备上只有一个电源槽位安装了电源模块
处理建议	请确保选配电源模块的系统最大输出功率大于路由器整机功耗（建议预留20%的功率余量）

162.8 DrvDebug

日志内容	Warning: Power 1 differs from power 2 in types!
参数解释	无
日志等级	5
举例	DRVPLAT/5/DrvDebug: Warning: Power 1 differs from power 2 in types!
日志说明	对于同一台设备上出现不同型号的电源模块
处理建议	不同型号的电源模块不能混插在同一台设备上，请尽快更换

162.9 DrvDebug

日志内容	Frame [INT32] fan [STRING] state error!
参数解释	$1：风扇框号 $2：风扇号
日志等级	5
举例	DRVPLAT/5/DrvDebug: Frame 1 fan 2 state error!
日志说明	风扇状态报错，可能风扇与主用主控板之间的通信存在异常
处理建议	请联系技术支持

162.10 DrvDebug

日志内容	The airflow directions for the two fan trays must be the same. Please check it.
参数解释	无
日志等级	5
举例	DRVPLAT/5/DrvDebug: The airflow directions for the two fan trays must be the same. Please check it.
日志说明	风扇出风方向一致，当设备检测到抽风和吹风风扇框同时存在时，首先会产生此告警信息，然后自动处理成抽风风扇框全速工作，吹风风扇框按最低速率工作
处理建议	请联系技术支持

162.11 DrvDebug

日志内容	Warning: Chassis [INT32] Fan [INT32] is absent!
参数解释	$1：设备在IRF中的成员编号. $2：风扇框号
日志等级	5
举例	DRVPLAT/5/DrvDebug: Warning: Chassis 1 Fan 2 is absent!
日志说明	系统检测到设备上缺少风扇框或者风扇框没有安装到位
处理建议	• 请将风扇框安装到位。安装完成之后查看主控板上风扇框状态指示灯（FAN），OK灯常亮的话就表示安装到位了 • 请联系技术支持

162.12 DrvDebug

日志内容	Warning: Fan [INT32] is absent!
参数解释	$1：风扇框号
日志等级	5
举例	DRVPLAT/5/DrvDebug: Warning: Fan 2 is absent!
日志说明	系统检测到设备上缺少风扇框或者风扇框没有安装到位
处理建议	• 请将风扇框安装到位。安装完成之后查看主控板上风扇框状态指示灯（FAN），OK灯常亮的话就表示安装到位了 • 请联系技术支持

162.13 DrvDebug

日志内容	The max-ecmp-num configuration should be the same on devices in one IRF. Please check it on the neighbor device connected to IRF-port [INT32].
参数解释	$1：端口索引
日志等级	5
举例	DRVPLAT/5/DrvDebug: The max-ecmp-num configuration should be the same on devices in one IRF. Please check it on the neighbor device connected to IRF-port 3.
日志说明	IRF中每台设备设置的最大等价路由条数不一致
处理建议	请使用**max-ecmp-num** 命令将IRF中每台设备的最大等价路由设置成相同值。有关**max-ecmp-num**命令的介绍，请参见“三层技术-IP路由配置指导”中的“IP路由基础”

162.14 DrvDebug

日志内容	The Systemworking mode configuration should be the same on devices in one IRF. Please check it on the neighbor device connected to IRF-port [INT32].
参数解释	$1：端口索引
日志等级	5
举例	DRVPLAT/5/DrvDebug: The Systemworking mode configuration should be the same on devices in one IRF.Please check it on the neighbor device connected to IRF-port 3.
日志说明	IRF中本设备与其他相邻成员设备的工作模式不一致
处理建议	**1.** 使用 **system-working-mode** 命令将本设备和邻居设备设置成相同的堆叠工作模式；有关 **system-working-mode** 命令的介绍，请参见“基础配置 配置指导”中的“设备管理配置” **2.** 请联系技术支持

162.15 DrvDebug

日志内容	IRF fabrics of this router series can't use a ring topology. Please modify the configuration or network connection and reboot the member devices.
参数解释	无
日志等级	4
举例	DRVPLAT/4/DrvDebug: -MDC=1; IRF fabrics of this router series can't use a ring topology. Please modify the configuration or network connection and reboot the member devices. DRVPLAT/4/DrvDebug: -MDC=1-Chassis=2-Slot=4; IRF fabrics of this router series can't use a ring topology. Please modify the configuration or network connection and reboot the member devices.
日志说明	当用户配置两框IRF，不支持配置IRF拓扑为环形拓扑
处理建议	**1.** 检查设备 IRF 的配置连接情况，是否存在环型 IRF 拓扑情况 **2.** 删除环形 IRF 拓扑的错误配置，将 IRF 拓扑修改为链型拓扑 **3.** 正确的配置连接后，保存配置，重启 IRF 设备恢复业务

162.16 DrvDebug

日志内容	Port [STRING] became inactive, because it received error packets.
参数解释	$1：IRF物理端口号
日志等级	4
举例	DRVPLAT/4/DrvDebug: -MDC=1-Chassis=4-Slot=2; Port Ten-GigabitEthernet4/2/0/1 became inactive, because it received error packets.
日志说明	由于IRF物理端口持续收到错误的数据包，IRF堆叠口状态切换成inactive
处理建议	**1.** 请更换 IRF 物理端口所在链路的光模块或光纤 **2.** 请联系技术支持

162.17 DrvDebug

日志内容	The device does not support board in chassis [INT32] slot [INT32] ,type is unknown(0x[STRING]), Please check.
参数解释	$1：IRF的成员编号 $2：单板所在的槽位号 $3：单板类型
日志等级	5
举例	DRVPLAT/5/DrvDebug: The device does not support board in chassis 1 slot 3 ,type is unknown(0x80), Please check.
日志说明	IRF模式下，提示设备不支持该单板
处理建议	请联系技术支持

162.18 DrvDebug

日志内容	The device does not support board in slot [INT32] ,type is unknown(0x[STRING]), Please check.
参数解释	$1：单板所在的槽位号 $2：单板类型
日志等级	5
举例	DRVPLAT/5/DrvDebug: The device does not support board in slot3 ,type is unknown(0x80), Please check.
日志说明	独立运行模式下，提示设备不支持该单板
处理建议	请联系技术支持

162.19 DrvDebug

日志内容	Configuration error for IRF physical interface [STRING]. Make sure the interface is bound to an IRF port with a port index different than the peer IRF physical interface.
参数解释	$1：IRF物理端口
日志等级	4
举例	DRVPLAT/4/DrvDebug: -MDC=1-Chassis=1-Slot=1; Configuration error for IRF physical interface Ten1/1/0/45. Make sure the interface is bound to an IRF port with a port index different than the peer IRF physical interface.
日志说明	当用户配置IRF时，两台IRF成员设备同时使用IRF端口1或者IRF端口2
处理建议	修改两台IRF成员设备的IRF端口配置。其中一台使用IRF端口1，另一台使用IRF端口2

162.20 DrvDebug

日志内容	Error: slot [INT32] and slot [INT32] can't be intermixed.
参数解释	$1：业务板或网板所在的槽位号 $2：业务板或网板所在的槽位号
日志等级	2
举例	DRVPLAT/2/DrvDebug: -MDC=1; Error: slot 17 and slot 16 can't be intermixed.

日志说明	当存在以下情况时，会打印该日志：
	• E 类网板与其他类型的网板混插
	• CSFC-12E 网板与以下业务板同时在位：CSPC-GP24LA1、CSPC-XP2LA1、CSPC-GT48LA1、CSPC-XP8LB、CSPC-GP48LB、CSPC-GP24XP2LB、CSPC-XP4LB、CSPC-CP2LB、CMPE-1104、CSPEX-1204、CSPEX-1104-E、CSPC-GE24L-E、CSPC-GP24GE8XP2L-E、CSPC-GE16XP4L-E
	• CSFC-16E 或 CSFC-08E 网板与除下列单板之外的其他单板同时在位：
	  ○ CSPEX 类单板（除 CSPEX-1204）
	  ○ CEPC 类单板
	  ○ IM-NGFWX-IV 单板、IM-OAPX 单板
	• CSPEX-1602X 单板与非 E 类网板同时在位

处理建议	1. 请将同一设备上的网板更换成同一型号 2. CSFC-12E 网板在位时，如需继续使用 CSPC-GP24LA1、CSPC-XP2LA1、CSPC-GT48LA1、CSPC-XP8LB、CSPC-GP48LB、CSPC-GP24XP2LB、CSPC-XP4LB、CSPC-CP2LB、CMPE-1104、CSPEX-1204、CSPEX-1104-E、CSPC-GE24L-E、CSPC-GP24GE8XP2L-E、CSPC-GE16XP4L-E 业务板，请将 CSFC-12E 网板更换为其他型号的网板。如需继续使用 CSFC-12E 网板，请拔出这些业务板 3. CSFC-16E 网板或 CSFC-08E 网板在位时，如需继续使用除 CSPEX 类单板（除 CSPEX-1204）、CEPC 类单板、IM-NGFWX-IV、IM-OAPX 之外的其它单板，请将 CSFC-16E 网板或 CSFC-08E 网板更换为其他型号的网板。如需继续使用 CSFC-16E 网板或 CSFC-08E 网板，请拔出这些业务板 4. 如要继续使用 CSPEX-1602X 单板，请将网板更换成 CSFC-12E 或者 CSFC-08E、CSFC-16E 网板；如不需要使用 CSPEX-1602X 单板，请拔出该单板

162.21 DrvDebug

日志内容	Error: chassis [INT 32] slot [INT32] and chassis [INT 32] slot [INT32] can't be intermixed.
参数解释	$1：设备在IRF中的成员编号 $2：业务板或网板所在的槽位号 $3：设备在IRF中的成员编号 $4：业务板或网板所在的槽位号
日志等级	2
举例	DRVPLAT/2/DrvDebug: -MDC=1; Error: chassis 3 slot 17 and chassis 3 slot 16 can't be intermixed.

日志说明	当存在以下情况时，会打印该日志：
	• E 类网板与其他类型的网板混插
	• CSFC-12E 网板与以下业务板同时在位：CSPC-GP24LA1、CSPC-XP2LA1、CSPC-GT48LA1、CSPC-XP8LB、CSPC-GP48LB、CSPC-GP24XP2LB、CSPC-XP4LB、CSPC-CP2LB、CMPE-1104、CSPEX-1204、CSPEX-1104-E、CSPC-GE24L-E、CSPC-GP24GE8XP2L-E、CSPC-GE16XP4L-E
	• CSFC-16E 或 CSFC-08E 网板与除下列单板之外的其他单板同时在位：
	  ○ CSPEX 类单板（除 CSPEX-1204）
	  ○ CEPC 类单板
	  ○ IM-NGFWX-IV 单板、IM-OAPX 单板
	• CSPEX-1602X 单板与非 E 类网板同时在位

处理建议	1. 请将同一设备上的网板更换成同一型号 2. CSFC-12E 网板在位时，如需继续使用 CSPC-GP24LA1、CSPC-XP2LA1、CSPC-GT48LA1、CSPC-XP8LB、CSPC-GP48LB、CSPC-GP24XP2LB、CSPC-XP4LB、CSPC-CP2LB、CMPE-1104、CSPEX-1204、CSPEX-1104-E、CSPC-GE24L-E、CSPC-GP24GE8XP2L-E、CSPC-GE16XP4L-E 业务板，请将 CSFC-12E 网板更换为其他型号的网板。如需继续使用 CSFC-12E 网板，请拔出这些业务板 3. CSFC-16E 网板或 CSFC-08E 网板在位时，如需继续使用除 CSPEX 类单板（除 CSPEX-1204）、CEPC 类单板、IM-NGFWX-IV、IM-OAPX 之外的其它单板，请将 CSFC-16E 网板或 CSFC-08E 网板更换为其他型号的网板。如需继续使用 CSFC-16E 网板或 CSFC-08E 网板，请拔出这些业务板 4. 如要继续使用 CSPEX-1602X 单板，请将网板更换成 CSFC-12E 或者 CSFC-08E、CSFC-16E 网板；如不需要使用 CSPEX-1602X 单板，请拔出该单板

162.22 DrvDebug

日志内容	Route-Aggregation[INT32] on chassis [INT32] slot [INT32] does not support the dot1q ethernet-type configuration.
参数解释	$1：三层聚合接口的编号 $2：设备在IRF中的成员编号（chassis参数仅在IRF模式下显示） $3：单板所在的槽位号
日志等级	2
举例	DRVPLAT/2/DrvDebug: -MDC=1-Slot=3; Route-Aggregation100 on chassis 1 slot 3 does not support the dot1q ethernet-type configuration.
日志说明	三层聚合接口有成员端口属于CSPC类单板和CMPE-1104单板时，不支持配置VLAN Tag的TPID值
处理建议	1. 在该三层聚合接口视图下使用 **undo dot1q ethernet-type** 命令删除配置 2. 确保该三层聚合接口的成员端口都属于 CSPEX 单板和 CEPC 类单板，然后再为该三层聚合接口配置 **dot1q ethernet-type** 命令

162.23 DrvDebug

日志内容	Incorrect IRF bridge MAC address. Make sure the lowest 11 bits of the IRF bridge MAC address are all zeros.
参数解释	无
日志等级	4
举例	DRVPLAT/4/DrvDebug: -MDC=1; Incorrect IRF bridge MAC address. Make sure the lowest 11 bits of the IRF bridge MAC address are all zeros.
日志说明	当前配置的IRF桥MAC地址不合理，最低11比特位必须为0
处理建议	使用**irf mac-address**命令配置IRF的桥MAC地址时，确保其最低11比特位为0，例如000F-E2FA-9800（最后两个字节0x98和0x00对应的二进制为10011**000 00000000**）

162.24 DrvDebug

日志内容	Incorrect IRF bridge MAC address. Make sure the lowest 9 bits of the IRF bridge MAC address are all zeros.
参数解释	无
日志等级	4
举例	DRVPLAT/4/DrvDebug: -MDC=1; Incorrect IRF bridge MAC address. Make sure the lowest 9 bits of the IRF bridge MAC address are all zeros.
日志说明	当前配置的IRF桥MAC地址不合理，最低9比特位必须为0
处理建议	使用**irf mac-address**命令配置IRF的桥MAC地址时，确保其最低9比特位为0

162.25 DrvDebug

日志内容	Chassis [INT 32] Slot [INT 32]：IRF-Connect mode setting has been changed. To have this change take effect, please save the configuration and reboot the module.
参数解释	$1：设备在IRF中的成员编号 $2：单板所在槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: -MDC=1-Chassis=1-Slot=4; Chassis 1 Slot 9 : IRF-Connect mode setting has been changed. To have this change take effect, please save the configuration and reboot the module.
日志说明	单板的IRF连接模式发生修改，需要保存配置并重新启动该单板
处理建议	保存配置并重新启动该单板

162.26 DrvDebug

日志内容	Chassis [INT 32] slot [INT 32]: Can't configure the module to operate in IRF-Connect mode. Please disable IRF-Connect mode on the module, save the configuration, and then reboot the module.
参数解释	$1：设备在IRF中的成员编号 $2：单板所在槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: -MDC=1-Chassis=3-Slot=0; Chassis 3 Slot 3: Can't configure the module to operate in IRF-Connect mode. Please disable IRF-Connect mode on the module, save the configuration, and then reboot the module.
日志说明	该单板不支持配置成IRF专用单板
处理建议	请取消将单板配置为IRF专用单板的配置，并重新启动该单板

162.27 DrvDebug

日志内容	Power modules in power frame [UINT32] of chassis [UINT32] are of different models.
参数解释	$1：电源框号 $2：设备在IRF中的成员编号
日志等级	2
举例	DRVPLAT/2/DrvDebug: -MDC=1; Power modules in power frame1 of chassis 1 are of different models.
日志说明	同一个电源适配器内所插的电源不是同一型号
处理建议	请将所插的电源更换为同一型号

162.28 DrvDebug

日志内容	Power modules in power frame [UINT32] are of different models.
参数解释	$1：电源框号
日志等级	2
举例	DRVPLAT/2/DrvDebug: -MDC=1; Power modules in power frame 1 are of different models.
日志说明	同一个电源适配器内所插的电源不是同一型号
处理建议	请将所插的电源更换为同一型号

162.29 DrvDebug

日志内容	Only one power module is installed in power frame [UINT32] of chassis [UINT32].
参数解释	$1：电源框号 $2：设备在IRF中的成员编号
日志等级	2
举例	DRVPLAT/2/DrvDebug: -MDC=1; Only one power module is installed in power frame 1 of chassis 1.
日志说明	一个电源适配器内只插了一个电源
处理建议	请再插入一个电源

162.30 DrvDebug

日志内容	Only one power module is installed in power frame [UINT32].
参数解释	$1：电源框号
日志等级	2
举例	DRVPLAT/2/DrvDebug: -MDC=1; Only one power module is installed in power frame 1.
日志说明	一个电源适配器内只插了一个电源
处理建议	请再插入一个电源

162.31 DrvDebug

日志内容	Power modules in power frames [UINT32] and [UINT32] of chassis [UINT32] are of different models.
参数解释	$1：电源框号 $2：电源框号 $3：设备在IRF中的成员编号
日志等级	2
举例	DRVPLAT/2/DrvDebug: -MDC=1; Power modules in power frames 1 and 2 of chassis 1 are of different models.
日志说明	两个电源框内电源型号不一致
处理建议	请更换为相同型号的电源

162.32 DrvDebug

日志内容	Power modules in power frames [UINT32] and [UINT32] are of different models.
参数解释	$1：电源框号 $2：电源框号
日志等级	2
举例	DRVPLAT/2/DrvDebug: -MDC=1; Power modules in power frames 1 and 2 are of different models.
日志说明	两个电源框内电源型号不一致
处理建议	请更换为相同型号的电源

162.33 FUNCMV

日志内容	The subcard in subslot [INT32] is not installed correctly. Please remove the subcard and install it again.
参数解释	$1：子卡所在的子槽号
日志等级	1
举例	PORT/1/FUNCMV: -MDC=1-Slot=7; The subcard in subslot 1 is not installed correctly. Please remove the subcard and install it again.
日志说明	当前槽位的子卡未安装到位，无法正常使用
处理建议	**1.** 请将子卡拔出后重新安装 **2.** 请联系技术支持

162.34 SUBCARD

日志内容	Slot [STRING] subslot [STRING]:Power error.
参数解释	$1：单板所在的槽位号 $2：子卡所在的槽位号
日志等级	2
举例	BSP/2/SUBCARD: Slot 1 subslot 2:Power error.
日志说明	子卡电源故障，无法正常启动
处理建议	• 请更换出现故障的子卡 • 请联系技术支持

162.35 SUBCARD

日志内容	Chassis [STRING] slot [STRING] subslot [STRING]:Power error.
参数解释	$1：设备在IRF中的成员编号 $2：单板所在的槽位号 $3：子卡所在的槽位号
日志等级	2
举例	BSP/2/SUBCARD: Chassis 1 slot 1 subslot 2:Power error.
日志说明	子卡电源故障，无法正常启动
处理建议	• 请更换出现故障的子卡 • 请联系技术支持

162.36 SUBCARD

日志内容	The type of current subcard is [STRING]. It doesn't match with the previous subcard [STRING] in Chassis [INT32] Slot [INT32] SubSlot [INT32].
参数解释	$1：当前子卡型号 $2：以前的子卡型号 $3：设备在IRF中的成员编号 $4：CSPEX-1204、CSPEX-1812X、CSPEX-1104-E单板所在的槽位号 $5：子槽所在的槽位号
日志等级	2
举例	DSYSM/2/SUBCARD: The type of current subcard is PIC-PS2G4L. It doesn't match with the previous subcard PIC-PSP4L in Chassis 2 Slot 6 SubSlot 1.
日志说明	2号成员设备6号槽位的CSPEX-1204单板上，1号槽位的子卡由PIC-PSP4L子卡变成PIC-PS2G4L子卡
处理建议	• 当 CSPEX-1204、CSPEX-1812X、CSPEX-1104-E 单板正常工作时，请不要将位于此单板同一槽位上的子卡更换成不同型号的子卡 • 如需将位于 CSPEX-1204、CSPEX-1812X、CSPEX-1104-E 单板同一槽位上的子卡更换成其他型号时，请先将 CSPEX-1204、CSPEX-1812X、CSPEX-1104-E 单板拔出，更换子卡后再重新插入

162.37 SUBCARD

日志内容	The type of current subcard is [STRING]. It doesn't match with the previous subcard [STRING] in Slot [INT32] SubSlot [INT32].
参数解释	$1：当前子卡型号 $2：以前的子卡型号 $3：CSPEX-1204、CSPEX-1812X、CSPEX-1104-E单板所在的槽位号 $4：子槽所在的槽位号
日志等级	2
举例	DSYSM/2/SUBCARD: The type of current subcard is PIC-PS2G4L. It doesn't match with the previous subcard PIC-PSP4L in Slot 6 SubSlot 1
日志说明	6号槽位的CSPEX-1204单板上，1号槽位的子卡由PIC-PSP4L子卡变成PIC-PS2G4L子卡
处理建议	• 当 CSPEX-1204、CSPEX-1812X、CSPEX-1104-E 单板正常工作时，请不要将位于此单板同一槽位上的子卡更换成不同型号的子卡 • 如需将位于 CSPEX-1204、CSPEX-1812X、CSPEX-1104-E 单板同一槽位上的子卡更换成其他型号时，请先将 CSPEX-1204、CSPEX-1812X、CSPEX-1104-E 单板拔出，更换子卡后再重新插入

162.38 SUBCARD

日志内容	The subcard is not supported in chassis [INT32] slot [INT32] subslot [INT32].
参数解释	$1：设备在IRF中的成员编号 $2：单板槽位号 $3：子卡槽位号
日志等级	2
举例	DSYSM/2/SUBCARD: -MDC=1-Slot=2; The subcard is not supported in chassis 2 slot 2 subslot 4.
日志说明	2号成员设备上2号单板的4号槽位不支持该子卡
处理建议	请将子卡更换为该槽位所支持的子卡

162.39 SUBCARD

日志内容	The subcard is not supported in slot [INT32] subslot [INT32].
参数解释	$1：单板槽位号 $2：子卡槽位号
日志等级	2
举例	DSYSM/2/SUBCARD: -MDC=1-Slot=2; The subcard is not supported in slot 2 subslot 4.
日志说明	2号单板上的4号槽位不支持该子卡
处理建议	请将子卡更换为该槽位所支持的子卡

162.40 SUBCARD

日志内容	In IRF mode, the card in slot [UINT] on chassis [UINT] doesn't support WAN subcards when the card has IRF physical interfaces.
参数解释	$1：单板所在的槽位号 $2：设备在IRF中的成员编号
日志等级	4
举例	DSYSM/4/SUBCARD: In IRF mode, the card in slot 5 on chassis 4 doesn't support WAN subcards when the card has IRF physical interfaces.
日志说明	IRF模式下，如果有一块CSPEX类单板（除CSPEX-1204之外）上的接口作为IRF物理端口，则该单板不支持WAN类型的子卡启动
处理建议	IRF模式下，CSPEX类单板（除CSPEX-1204之外）单板上的接口作为IRF物理端口时，不能安装WAN类型的子卡，如果需要使用WAN类型子卡，请先取消该单板上IRF的配置，并重启该单板

163 TACACS

本节介绍 TACACS 模块输出的日志信息。

163.1 TACACS_AUTH_FAILURE

日志内容	User [STRING] from [STRING] failed authentication.
参数解释	$1：用户名称 $2：IP地址
日志等级	5
举例	TACACS/5/TACACS_AUTH_FAILURE: User cwf@system from 192.168.0.22 failed authentication.
日志说明	TACACS服务器了拒绝用户的认证请求
处理建议	无

163.2 TACACS_AUTH_SUCCESS

日志内容	User [STRING] from [STRING] was authenticated successfully.
参数解释	$1：用户名称 $2：IP地址
日志等级	6
举例	TACACS/6/TACACS_AUTH_SUCCESS: User cwf@system from 192.168.0.22 was authenticated successfully.
日志说明	TACACS服务器接收了用户的认证请求
处理建议	无

163.3 TACACS_DELETE_HOST_FAIL

日志内容	Failed to delete servers in scheme [STRING].
参数解释	$1：方案名称
日志等级	4
举例	TACACS/4/TACACS_DELETE_HOST_FAIL: Failed to delete servers in scheme abc.
日志说明	删除TACACS方案中的服务器失败
处理建议	无

164 TBDL

本节介绍 TBDL 模块输出的日志信息。

164.1 TBDL_SWICH_P

日志内容	Tunnel-bundle[STRING]: Switched from working tunnel [STRING] to protection tunnel [STRING].
参数解释	$1：Tunnel-bundle隧道信息 $2：主隧道信息 $3：备隧道信息
日志等级	4
举例	TBDL/4/TBDL_SWITCH_P: Tunnel-bundle1: Switched from working tunnel tunnel1 to protection tunnel tunnel2.
日志说明	当主隧道缺陷，切换到备隧道时，触发该日志
处理建议	无

164.2 TBDL_SWICH_W

日志内容	Tunnel-bundle[STRING]: Switched from protection tunnel [STRING] to working tunnel [STRING].
参数解释	$1：Tunnel-bundle隧道信息 $2：备隧道信息 $3：主隧道信息
日志等级	4
举例	TBDL/4/TBDL_SWITCH_W: Tunnel-bundle1: Switched from protection tunnel tunnel1 to working tunnel tunnel2.
日志说明	当主隧道主缺陷恢复，回切到主隧道时，触发该日志
处理建议	无

165 TE

本节介绍 TE 模块输出的日志信息。

165.1 TE_BACKUP_SWITCH

日志内容	Tunnel [UNIT] ([STRING]): [STRING]. [STRING]
参数解释	$1：主隧道信息 $2：LSP信息 $3：会话保护状态，取值包括： • Backup tunnel ready：热备隧道保护状态，此时未进行切换 • Backup tunnel used：热备隧道保护使用状态，此时已切换 • Backup tunnel disabled：不需要保护 • Main tunnel recovered：主链路恢复，切换回主链路 $4：LSP路径信息，包括LSP经过的LSR节点的接口IP地址、LSR ID或使用的标签值。仅当状态为Backup tunnel used或Main tunnel recovered时打印
日志等级	5
举例	TE/5/TE_BACKUP_SWITCH: Tunnel 5 (IngressLsrID=1.1.1.8 EgressLsrID=2.2.2.8 LSPID=100 Bandwidth=1000kbps): Backup tunnel used. Current LSP path is 10.1.1.1/32(flag=0x00) - 10.1.1.2/32(flag=0x00) - 1151(flag=0x01) - 2.2.2.8/32(flag=0x20).
日志说明	当热备隧道或Segment Routing隧道建立、取消和热备切换时，触发该日志
处理建议	无

165.2 TE_MBB_SWITCH

日志内容	Tunnel [STRING] ([STRING]): Make before break triggered by [STRING]. [STRING]
参数解释	$1：主隧道信息 $2：LSP信息 $3：Make-before-break重建隧道，取值包括： • configuration change：配置变化，触发重建隧道 • FRR used：FRR 主隧道已切换，触发重建主隧道 • reoptimize timer expiration：重优化时间到，触发重建隧道 • automatic bandwidth adjustment: 自动带宽调整，触发重建隧道 • stateful PCE updated：接收 Stateful PCE PCUpd 消息，触发重建隧道 $4：LSP路径信息
日志等级	5
举例	TE/5/TE_MBB_SWITCH: Tunnel 5 (IngressLsrID=1.1.1.8 EgressLsrID=2.2.2.8 LSPID=100 Bandwidth=1000kbps): Make-before-break triggered by configuration change. Current LSP path is 10.1.1.1/32(flag=0x00) - 10.1.1.2/32(flag=0x00) - 1151(flag=0x01) - 2.2.2.8/32(flag=0x20).
日志说明	当make-before-break重建隧道时，触发该日志
处理建议	无

166 TELNETD

本节介绍 TELNETD（Telnet Daemon）模块输出的日志信息。

166.1 TELNETD_ACL_DENY

日志内容	The Telnet Connection [IPADDR]([STRING]) request was denied according to ACL rules.
参数解释	$1：Telnet客户端IP地址 $2：Telnet客户端IP地址所在VPN
日志等级	5
举例	TELNETD/5/TELNETD_ACL_DENY: The Telnet Connection 1.2.3.4(vpn1) request was denied according to ACL rules.
日志说明	Telnet ACL规则限制登录IP地址。该日志在Telnet服务端检测到非法客户端尝试登录时输出
处理建议	无

166.2 TELNETD_REACH_SESSION_LIMIT

日志内容	Telnet client [STRING] failed to log in. The current number of Telnet sessions is [NUMBER]. The maximum number allowed is ([NUMBER]).
参数解释	$1：Telnet客户端IP地址 $2：当前的Telnet会话数 $3：设备允许建立的Telnet会话数
日志等级	6
举例	TELNETD/6/TELNETD_REACH_SESSION_LIMIT: Telnet client 1.1.1.1 failed to log in. The current number of Telnet sessions is 10. The maximum number allowed is (10).
日志说明	Telnet登录用户达到上限。该日志在Telnet服务端检测到登录客户端数达到上限时输出
处理建议	请根据需要使用命令**aaa session-limit**配置允许的Telnet最大登录用户数

167 TRILL

本节介绍 TRILL 模块输出的日志信息。

167.1 TRILL_DUP_SYSTEMID

日志内容	Duplicate System ID [STRING] in [STRING] PDU sourced from RBridge 0x[HEX].
参数解释	$1：System ID $2：PDU类型 $3：源RBridge的Nickname
日志等级	5
举例	TRILL/5/TRILL_DUP_SYSTEMID: Duplicate System ID 0011.2200.1501 in LSP PDU sourced from RBridge 0xc758.
日志说明	本地RBridge收到的LSP或者IIH PDU中的System ID和本地RBridge的System ID相同。可能的原因包括： • 为本地 RBridge 和远端 RBridge 分配了相同的 System ID • 本地 RBridge 收到了一个自己产生、携带了旧的 Nickname 的 LSP PDU
处理建议	检查TRILL网络中RBridge的System ID

167.2 TRILL_INTF_CAPABILITY

日志内容	The interface [STRING] does not support TRILL.
参数解释	$1：接口名称
日志等级	4
举例	TRILL/4/TRILL_INTF_CAPABILITY: The interface GigabitEthernet0/1/3 does not support TRILL.
日志说明	不支持TRILL的端口被加入到了聚合组中
处理建议	将不支持TRILL的端口从聚合组中删除

167.3 TRILL_LICENSE_EXPIRED

日志内容	The TRILL feature is being disabled, because its license has expired.
参数解释	无
日志等级	5
举例	TRILL/5/TRILL_LICENSE_EXPIRED: The TRILL feature is being disabled, because its license has expired.
日志说明	TRILL的License已经过期
处理建议	检查TRILL的License

167.4 TRILL_MEM_ALERT

日志内容	TRILL process receive system memory alert [STRING] event.
参数解释	$1：内存告警事件的类型
日志等级	5
举例	TRILL/5/TRILL_MEM_ALERT: TRILL process receive system memory alert start event.
日志说明	TRILL从系统收到一个内存告警事件
处理建议	检查系统内存

167.5 TRILL_NBR_CHG

日志内容	TRILL [UINT32], [STRING] adjacency [STRING] ([STRING]), state changed to [STRING].
参数解释	$1：TRILL进程ID $2：邻居级别 $3：邻居的System ID $4：接口名 $5：当前邻居状态 o up：表示邻居关系已建立，可以正常工作 o initializing：表示初始状态 o down：表示邻居关系结束
日志等级	5
举例	TRILL/5/TRILL_NBR_CHG: TRILL 1, Level-1 adjacency 0011.2200.1501 (GigabitEthernet0/1/3), state changed to down.
日志说明	一个TRILL邻居的状态发生改变
处理建议	当邻居状态变为down或者initializing时，请根据状态变化的原因检查TRILL配置和网络状态

167.6 TRILL_NO_LICENSE

日志内容	The TRILL feature has no license.
参数解释	无
日志等级	5
举例	TRILL/5/TRILL_NO_LICENSE: The TRILL feature has no license.
日志说明	TRILL没有License
处理建议	请为TRILL安装有效的License

168 TUNNEL

本节介绍 TUNNEL 模块输出的日志信息。

168.1 L3_TUNNEL

日志内容	No enough resource
参数解释	无
日志等级	6
举例	L3/6/L3_TUNNEL: -MDC=1-Slot=4; No enough resource
日志说明	硬件资源不足，无法完成当前操作。例如，当系统Tunnel资源耗尽时，无法创建新的GRE隧道
处理建议	联系技术支持

168.2 L3_TUNNEL

日志内容	The Board Slot [INT32] Create Tunnel Failed, Because No Enough Resource!
参数解释	$1：单板所在的槽位号
日志等级	3
举例	L3/3/L3_TUNNEL: -MDC=1-Slot=2; The Board Slot 2 Create Tunnel Failed, Because No Enough Resource!
日志说明	当单板的NH（NextHop）资源耗尽或者主控板L3 INTF资源不足时创建隧道，会提示该信息。此时创建的隧道无法使用，需要待资源恢复后重新创建此隧道
处理建议	1. 在 Probe 视图下执行 **debug ipv4-drv show statistics slot** *slot-number* 命令查看当前单板上资源的使用情况 2. 清除 ARP 表项，释放 NH 资源 3. 再次查看单板上资源的使用情况，确认资源已经恢复 4. 在 Probe 视图下执行 **display hardware internal l3 np tunnel index** *index* 命令查看隧道索引 ID 对应的隧道接口编号，并重新创建此隧道 5. 再次创建隧道还是提示，在 Probe 视图下执行 display hardware internal indexq handle 1234FF00 slot *slot-number* chip *chip-number* 查看主控板资源使用情况 6. 联系技术支持

169 USER

本节介绍 User 模块输出的日志信息。

169.1 USER_RECOVER_NORMAL

日志内容	形式一： The user number on slot [INT32] has recovered to normal state. 形式二： The user number on chassis [INT32] slot [INT32] has recovered to normal state.
参数解释	形式一： $1：slot编号 形式二： $1：chassis编号 $2：slot编号
日志等级	5
举例	USER/5/ USER_RECOVER_NORMAL: The user number on slot 5 has recovered to normal state.
日志说明	指定slot上接入用户数从上限阈值重新恢复到设定的正常范围
处理建议	无

169.2 USER_UPPER_THRESHOLD

日志内容	形式一： The user number on slot [INT32] is above the upper warning threshold (UpperThreshold=[INT32]). 形式二： The user number on chassis [INT32] slot [INT32] is above the upper warning threshold (UpperThreshold=[INT32]).
参数解释	形式一： $1：slot编号 $2：接入用户数告警阈值 形式二： $1：chassis编号 $2：slot编号 $3：接入用户数告警阈值
日志等级	4
举例	USER/4/USER_UPPER_THRESHOLD: The user number on slot 5 is above the upper warning threshold (UpperThreshold=20).
日志说明	指定slot上接入用户数超过上限阈值
处理建议	确认是否存在大量非法IPoE和PPPoE用户上线

170 VLAN

本节介绍接口 VLAN 模块输出的日志信息。

170.1 VLAN_FAILED

日志内容	Failed to add interface [STRING] to the default VLAN.
参数解释	$1：接口名称
日志等级	4
举例	VLAN/4/VLAN_FAILED: Failed to add interface S-Channel4/2/0/19:100 to the default VLAN.
日志说明	在硬件资源不足的时候创建一个S-Channel接口，此S-Channel接口不能加入到缺省VLAN
处理建议	无

170.2 VLAN_VLANMAPPING_FAILED

日志内容	The configuration failed because of resource insufficiency or conflicts on [STRING].
参数解释	$1：接口名称
日志等级	4
举例	VLAN/4/VLAN_VLANMAPPING_FAILED: The configuration failed because of resource insufficiency or conflicts on Ethernet0/0.
日志说明	因本接口硬件资源不足或者接口加入或离开二层聚合组，所以部分或全部VLAN映射配置丢失
处理建议	无

170.3 VLAN_VLANTRANSPARENT_FAILED

日志内容	The configuration failed because of resource insufficiency or conflicts on [STRING].
参数解释	$1：接口名称
日志等级	4
举例	VLAN/4/VLAN_VLANTRANSPARENT_FAILED: The configuration failed because of resource insufficiency or conflicts on Ethernet0/0.
日志说明	因本接口硬件资源不足或者接口加入或离开二层聚合组，所以部分或全部VLAN透传配置丢失
处理建议	无

171 VRRP

本节介绍 VRRP 模块输出的日志信息。

171.1 VRRP_STATUS_CHANGE

日志内容	The status of [STRING] virtual router [UINT32] (configured on [STRING]) changed from [STRING] to [STRING]: [STRING].
参数解释	$1：VRRP协议版本 $2：VRRP备份组号 $3：VRRP备份组所在接口的名称 $4：先前状态 $5：当前状态 $6：状态变化原因： • Interface event received：收到接口事件 • IP address deleted：虚地址删除 • The status of the tracked object changed：Track 对象状态变化 • VRRP packet received：收到 VRRP 报文 • Current device has changed to IP address owner：当前设备成为地址拥有者 • Master-down-timer expired：Master down 定时器超时 • Zero priority packet received：收到 0 优先级的报文 • Preempt：发生了抢占 • Master group drove：管理备份组驱动
日志等级	6
举例	VRRP/6/VRRP_STATUS_CHANGE: The status of IPv4 virtual router 10 (configured on Ethernet0/0) changed (from Backup to Master): Master-down-timer expired.
日志说明	VRRP备份组中的Master或Backup路由器状态发生变化。可能的原因包括：收到接口事件、虚地址删除、Track对象状态变化、收到VRRP报文、当前设备成为地址拥有者、Master down定时器超时、收到0优先级的报文、发生了抢占或者管理备份组驱动
处理建议	检查VRRP备份组中的Master或Backup路由器状态，确保备份组工作正常

171.2 VRRP_VF_STATUS_CHANGE

日志内容	The [STRING] virtual router [UINT32] (configured on [STRING]) virtual forwarder [UINT32] detected status change (from [STRING] to [STRING]): [STRING].
参数解释	$1：VRRP协议版本 $2：VRRP备份组号 $3：VRRP备份组所在接口的名称 $4：VF ID $5：VF先前状态 $6：VF当前状态 $7：状态变化原因
日志等级	6
举例	VRRP/6/VRRP_VF_STATUS_CHANGE: The IPv4 virtual router 10 (configured on GigabitEthernet5/1) virtual forwarder 2 detected status change (from Active to Initialize): Weight changed.
日志说明	虚拟转发器状态发生改变。可能的原因包括权重变化、定时器超时、VRRP备份组Down
处理建议	检查Track项的状态

171.3 VRRP_VMAC_INEFFECTIVE

日志内容	The [STRING] virtual router [UINT32] (configured on [STRING]) failed to add virtual MAC: [STRING].
参数解释	$1：VRRP协议版本 $2：VRRP备份组号 $3：VRRP备份组所在接口的名称 $4：出现错误的原因
日志等级	3
举例	VRRP/3/VRRP_VMAC_INEFFECTIVE: The IPv4 virtual router 10 (configured on Ethernet0/0) failed to add virtual MAC: Insufficient hardware resources.
日志说明	添加虚拟MAC地址失败
处理建议	确定操作失败的根因并解决

172 VSRP

本节介绍多机备份模块输出的日志信息。

172.1 VSRP_BIND_FAILED

日志内容	Failed to bind the IP addresses and the port on VSRP peer [STRING].
参数解释	$1：多机备份对端名称
日志等级	6
举例	VSRP/6/VSRP_BIND_FAILED: Failed to bind the IP addresses and the port on VSRP peer aaa.
日志说明	TCP端口正在被使用，创建到VSRP对端的TCP连接时接口绑定IP地址失败
处理建议	无

173 VXLAN

本节介绍 VXLAN 模块输出的日志信息。

173.1 VXLAN_LICENSE_UNAVAILABLE

日志内容	The VXLAN feature is disabled, because no licenses are valid.
参数解释	无
日志等级	3
举例	VXLAN/3/VXLAN_LICENSE_UNAVAILABLE: The VXLAN feature is disabled, because no licenses are valid.
日志说明	因为没有有效的License，VXLAN特性被禁用
处理建议	检查VXLAN的License，若要使用VXLAN特性，请安装有效的License

174 WAN

本节介绍 WAN（Wide Area Network）模块输出的日志信息。

174.1 ALARM

日志内容	[STRING] : Path [STRING] Alarm [STRING] [STRING]! Start Time : [STRING]!
参数解释	$1：CPOS接口名称 $2：高阶通道号 $3：高阶通道告警名称（如AIS/LOF/LOS/RDI/SD/SLM/TIM/UNEQ） $4：高阶通道告警的状态，包括告警恢复（recover）和告警上报（report） $5：告警恢复或上报的时间，显示格式为Y-M-D H:M:S:MS
日志等级	4
举例	WAN/4/ALARM: -MDC=1-Slot=5; Cpos5/1/1 : Path 1 Alarm AIS report! Start Time : 2014-04-04 11:40:53:533! WAN/4/ALARM: -MDC=1-Slot=5; Cpos5/1/1 : Path 1 Alarm AIS recover! Start Time : 2014-04-04 11:41:09:769!
日志说明	• 当高阶通道告警的状态为 recover 时，表示 CPOS 接口高阶通道告警消除的具体时间和告警类型 • 当高阶通道告警的状态为 report 时，表示 CPOS 接口高阶通道告警产生的具体时间和告警类型 触发该日志的可能原因有： • 对端 CPOS 接口通过 **shutdown** 命令被关闭 • 两端高阶通道开销字节配置不一致
处理建议	• 当高阶通道告警的状态为 recover 时，无须处理 • 当高阶通道告警的状态为 report 时，进行以下处理： **1.** 使用 display controller cpos 命令，检查接口的物理状态是否 UP • UP 表示该接口的物理状态正常，请按下一步检查 • DOWN (Administratively)表示该接口已经通过 **shutdown** 命令被关闭；请执行 **undo shutdown** 命令打开接口 • DOWN：表示该接口的管理状态为开启，但物理状态为关闭（可能因为线路故障或对端接口通过 **shutdown** 命令关闭了接口），请解决对应问题 **2.** 使用 display transceiver alarm 命令检查光模块是否出现故障 **3.** 进入接口视图，使用 **display this** 命令查看该接口和对端接口的开销字节（C2 或 J1）配置是否一致。如果不一致，请修改为一致 **4.** 请联系技术支持

174.2 ALARM

日志内容	[STRING] : VC4 1 TUG-3 [STRING] TUG-2 [STRING] TU12 [STRING] E1 Alarm [STRING] [STRING]! Start Time : [STRING]!
参数解释	$1：CPOS接口名称 $2：TUG-3编号 $3：TUG-2编号 $4：TU-12编号 $5：告警名称（如AIS/LOF/LOS/RDI/SD/SLM/TIM/UNEQ） $6：告警的状态，包括告警恢复（recover）和告警上报（report） $7：告警恢复或上报的时间，显示格式为Y-M-D H:M:S:MS
日志等级	4
举例	WAN/4/ALARM: -MDC=1-Slot=4; Cpos4/1/1 : VC4 1 TUG-3 1 TUG-2 1 TU12 1 E1 Alarm AIS report! Start Time : 2014-04-04 14:16:51:213!
日志说明	• 当告警的状态为 recover 时，表示 CPOS 接口帧格式为 SDH、AUG 的复用路径为 AU-4 时，低阶 E1 通道告警消除的具体时间和告警类型 • 当告警的状态为 report 时，表示 CPOS 接口帧格式为 SDH、AUG 的复用路径为 AU-4 时，低阶 E1 通道告警产生的具体时间和告警类型 触发该日志的可能原因有： • 对端 CPOS 接口下的 E1 通道被关闭 • 两端 E1 通道开销字节配置不一致
处理建议	• 当告警的状态为 recover 时，无须处理 • 当告警的状态为 report 时，进行以下处理： **1.** 使用 display controller cpos e1 命令，检查接口的物理状态是否 UP • UP 表示该接口的物理状态正常，请按下一步检查 • DOWN (Administratively)表示该接口已经通过 **shutdown** 命令被关闭；请执行 **undo shutdown** 命令打开接口 • DOWN：表示该接口的管理状态为开启，但物理状态为关闭（可能因为线路故障或对端接口通过 **shutdown** 命令关闭了接口），请解决对应问题 **2.** 使用 display transceiver alarm 命令检查光模块是否出现故障 **3.** 进入接口视图，使用 **display this** 命令查看该接口和对端接口的 E1 通道开销字节（C2 或 J2）配置是否一致。如果不一致，请修改为一致 **4.** 请联系技术支持

174.3 ALARM

日志内容	[STRING] : AUG 1 VC3 [STRING] TUG-2 [STRING] TU12 [STRING] E1 Alarm [STRING] [STRING]! Start Time : [STRING]!
参数解释	$1：CPOS接口名称 $2：VC3编号 $3：TUG-2编号 $4：TUG-12编号 $5：告警名称（如AIS/LOF/LOS/RDI/SD/SLM/TIM/UNEQ） $6：告警的状态，包括告警恢复（recover）和告警上报（report） $7：告警恢复或上报的时间，显示格式为Y-M-D H:M:S:MS
日志等级	4
举例	WAN/4/ALARM: -MDC=1-Slot=4; Cpos4/1/1 : AUG 1 VC3 1 TUG-2 1 TU12 1 E1 Alarm AIS report! Start Time : 2014-04-04 14:17:55:977! WAN/4/ALARM: -MDC=1-Slot=4; Cpos4/1/1 : AUG 1 VC3 1 TUG-2 1 TU12 1 E1 Alarm AIS recover! Start Time : 2014-04-04 14:17:47:928!
日志说明	• 当警的状态为 recover 时，表示 CPOS 接口帧格式为 SDH、AUG 的复用路径为 AU-3 时，低阶 E1 通道告警消除的具体时间和告警类型 • 当警的状态为 report 时，表示 CPOS 接口帧格式为 SDH、AUG 的复用路径为 AU-3 时，低阶 E1 通道告警产生的具体时间和告警类型 触发该日志的可能原因有： • 对端 CPOS 接口下的 E1 通道被关闭 • 两端 E1 通道开销字节配置不一致
处理建议	• 当告警的状态为 recover 时，无须处理 • 当告警的状态为 report 时，进行以下处理： **1.** 使用 display controller cpos e1 命令，检查接口的物理状态是否 UP • UP 表示该接口的物理状态正常，请按下一步检查 • DOWN (Administratively)表示该接口已经通过 **shutdown** 命令被关闭；请执行 **undo shutdown** 命令打开接口 • DOWN：表示该接口的管理状态为开启，但物理状态为关闭（可能因为线路故障或对端接口通过 **shutdown** 命令关闭了接口），请解决对应问题 **2.** 使用 display transceiver alarm 命令检查光模块是否出现故障 **3.** 进入接口视图，使用 **display this** 命令查看该接口和对端接口的 E1 通道开销字节（C2 或 J2）配置是否一致。如果不一致，请修改为一致 **4.** 请联系技术支持

174.4 ALARM

日志内容	[STRING] : OC-3 1 STS [STRING] VTG [STRING] VT2 [STRING] E1 Alarm [STRING] [STRING]! Start Time : [STRING]!
参数解释	$1：CPOS接口名称 $2：STS 编号 $3：VTG 编号 $4：VT2 编号 $5：告警名称（如AIS/LOF/LOS/RDI/SD/SLM/TIM/UNEQ） $6：告警的状态，包括告警恢复（recover）和告警上报（report） $7：告警恢复或上报的时间，显示格式为Y-M-D H:M:S:MS
日志等级	4
举例	WAN/4/ALARM: -MDC=1-Slot=4; Cpos4/1/1 : OC-3 1 STS 1 VTG 1 VT2 1 E1 Alarm AIS recover! Start Time : 2014-04-04 14:23:04:125!
日志说明	• 当告警的状态为 recover 时，表示 CPOS 接口帧格式为 SONET 时，低阶 E1 通道告警消除的具体时间和告警类型 • 当告警的状态为 report 时，表示 CPOS 接口帧格式为 SONET 时，低阶 E1 通道告警产生的具体时间和告警类型 触发该日志的可能原因有： • 对端 CPOS 接口下的 E1 通道被关闭 • 两端 E1 通道开销字节配置不一致
处理建议	• 当告警的状态为 recover 时，无须处理 • 当告警的状态为 report 时，进行以下处理： **1.** 使用 display controller cpos e1 命令，检查接口的物理状态是否 UP • UP 表示该接口的物理状态正常，请按下一步检查 • DOWN (Administratively)表示该接口已经通过 **shutdown** 命令被关闭；请执行 **undo shutdown** 命令打开接口 • DOWN：表示该接口的管理状态为开启，但物理状态为关闭（可能因为线路故障或对端接口通过 **shutdown** 命令关闭了接口），请解决对应问题 **2.** 使用 display transceiver alarm 命令检查光模块是否出现故障 **3.** 进入接口视图，使用 **display this** 命令查看该接口和对端接口的 E1 通道开销字节（C2 或 J2）配置是否一致。如果不一致，请修改为一致 **4.** 请联系技术支持

174.5 ALARM

日志内容	[STRING] : Alarm [STRING] [STRING]! Start Time : [STRING]!
参数解释	$1：CPOS接口名称 $2：告警名称（如AIS/LOF/LOS/RDI/SD/SLM/TIM/UNEQ） $3：告警状态，包括告警上报（report）和告警恢复（recover） $4：告警上报或恢复的时间，显示格式为Y-M-D H:M:S:MS
日志等级	4
举例	WAN/4/ALARM: -MDC=1-Slot=4; Cpos4/1/1 : Alarm LOS report! Start Time : 2014-04-04 14:14:47:263!
日志说明	• 当告警的状态为 recover 时，表示 CPOS 接口再生段和复用段告警消除的具体时间和告警类型 • 当警的状态为 report 时，表示 CPOS 接口再生段和复用段告警产生的具体时间和告警类型 触发该日志的可能原因有： • 对端 CPOS 接口被关闭 • 两端 CPOS 接口 SONET/SDH 帧的开销字节配置不一致 • 对端 CPOS 接口使用的线路时钟方式与本端相同
处理建议	• 当告警的状态为 recover 时，无须处理 • 当告警的状态为 report 时，进行以下处理： **1.** 使用 display controller cpos 命令，检查接口的物理状态是否 UP • UP 表示该接口的物理状态正常，请按下一步检查 • DOWN (Administratively)表示该接口已经通过 **shutdown** 命令被关闭；请执行 **undo shutdown** 命令打开接口 • DOWN：表示该接口的管理状态为开启，但物理状态为关闭（可能因为线路故障或对端接口通过 **shutdown** 命令关闭了接口），请解决对应问题 **2.** 使用 display transceiver alarm 命令检查光模块是否出现故障 **3.** 进入接口视图，使用 **display this** 命令查看该接口和对端接口的开销字节（J0）配置是否一致。如果不一致，请修改为一致 **4.** 使用 **display this** 命令查看该接口和对端接口使用的线路时钟方式是否一端为 Master，一端为 Slave。如果不是，请修改 **5.** 请联系技术支持

174.6 ALARM

日志内容	[STRING] : [STRING] [STRING] [STRING].
参数解释	$1：广域网接口名 $2：告警状态，包括告警上报（reports）和告警恢复（recovers） $3：告警级别：Section（再生段）、Line（复用段）、High Path（高阶通道）和Low Path（低阶通道） $4：告警名称（如AIS/LOF/LOS/RDI/SD/SLM/TIM/UNEQ）
日志等级	4
举例	WAN/4/ALARM: -MDC=1-Slot=2; Pos2/4/1 : reports Section TIM. WAN/4/ALARM: -MDC=1-Slot=2; Pos2/4/1 : reports High Path TIM.
日志说明	• 当告警的状态为 recover 时，表示 WAN 接口再生段、复用段、高阶通道或低阶通道告警消除的具体时间和告警类型 • 当告警的状态为 report 时，表示 WAN 接口再生段和复用段告警产生的具体时间和告警类型 WAN接口产生告警 触发该日志的可能原因有： • 对端 WAN 接口通过 **shutdown** 命令被关闭 • 对端 WAN 接口 SONET/SDH 帧的开销字节配置不一致 • 对端 WAN 接口使用的线路时钟方式与本端相同
处理建议	• 当告警的状态为 recover 时，无须处理 • 当告警的状态为 report 时，进行以下处理： **1.** 使用 **display interface** 命令，检查接口的物理状态是否 UP • UP 表示该接口的物理状态正常，请按下一步检查 • DOWN (Administratively)表示该接口已经通过 **shutdown** 命令被关闭；请执行 **undo shutdown** 命令打开接口 • DOWN：表示该接口的管理状态为开启，但物理状态为关闭（可能因为线路故障或对端接口通过 **shutdown** 命令关闭了接口），请解决对应问题 **2.** 使用 display transceiver alarm 命令检查光模块是否出现故障 **3.** 进入接口视图，使用 **display this** 命令查看该接口和对端接口的开销字节（J0、J1或 C2）配置是否一致。如果不一致，请修改为一致 **4.** 使用 **display this** 命令查看该接口和对端接口使用的线路时钟方式是否一端为 Master，一端为 Slave。如果不是，请修改 **5.** 请联系技术支持

174.7 ALARM

日志内容	[STRING] : [STRING] of [STRING] has lasted link-delay time!
参数解释	$1：广域网接口名 $2：告警状态，包括告警上报（Reporting）和告警恢复（Recovering） $3：告警类型（SD/SF/RDI）
日志等级	4
举例	WAN/4/ALARM: -MDC=1-Slot=2; Pos2/4/1 Reporting of Line RDI has lasted link-delay time!
日志说明	• 当告警的状态为 recover 时，表示 WAN 接口在 **link-delay** 命令配置的接口的物理连接状态抑制时间内收到 **alarm-detect** 命令指定的告警（SD、SF、RDI）已经消除 • 当告警的状态为 report 时，表示 WAN 接口在 **link-delay** 命令配置的接口的物理连接状态抑制时间内收到 **alarm-detect** 命令指定的告警（SD、SF、RDI）而产生的日志信息
处理建议	• 当告警的状态为 recover 时，无须处理 • 当告警的状态为 report 时，进行以下处理： **1.** 通过重新拔插光纤和更换光纤检查光纤连接是否正常 **2.** 使用 **display interface** 命令，检查接口的物理状态是否 UP • UP 表示该接口的物理状态正常，请按下一步检查 • DOWN (Administratively)表示该接口已经通过 **shutdown** 命令被关闭；请执行 **undo shutdown** 命令打开接口 • DOWN：表示该接口的管理状态为开启，但物理状态为关闭（可能因为线路故障或对端接口通过 **shutdown** 命令关闭了接口），请解决对应问题 **3.** 使用 display transceiver alarm 命令检查光模块是否出现故障 **4.** 请联系技术支持

174.8 ATM

日志内容	Operation Failed on pvc [UINT16]/[UINT16].
参数解释	$1：PVC的VPI/VCI
日志等级	3
举例	WAN/3/ATM: -MDC=1-Slot=4; Operation Failed on pvc 43/43
日志说明	在指定PVC上配置**service** { **cbrs** | **ubr** | **vbr-nrt** | **vbr-rt** }命令失败
处理建议	请联系H3C技术支持

175 WIPS

本节介绍 WIPS 模块输出的日志信息。

175.1 APFLOOD

日志内容	-VSD=[STRING]; AP flood detected.
参数解释	$1：VSD名字
日志等级	5
举例	WIPS/5/APFLOOD: -VSD=home; AP flood detected.
日志说明	指定VSD内检测到AP设备数量过多时触发日志
处理建议	检查是否存在攻击

175.2 AP_CHANNEL_CHANGE

日志内容	-VSD=[STRING]-SrcMAC=[MAC]; Channel change detected.
参数解释	$1：VSD名字 $2：AP的地址
日志等级	5
举例	WIPS/5/AP_CHANNEL_CHANGE: -VSD=home-SrcMAC=1122-3344-5566; Channel change detected.
日志说明	指定VSD内检测到指定AP信道改变时触发日志
处理建议	检查AP信道改变是否正常

175.3 ASSOCIATEOVERFLOW

日志内容	-VSD=[STRING]-SrcMAC=[MAC]; Association/Reassociation DoS attack detected.
参数解释	$1：VSD名字 $2：AP的地址
日志等级	5
举例	WIPS/5/ASSOCIATEOVERFLOW: -VSD=home-SrcMAC=1122-3344-5566; Association/Reassociation DoS attack detected.
日志说明	指定VSD内检测到指定AP回应status code为17的关联回应帧时触发日志
处理建议	检查AP是否受到攻击

175.4 HONEYPOT

日志内容	-VSD=[STRING]-SrcMAC=[MAC]; Honeypot AP detected.
参数解释	$1：VSD名字 $2：AP的地址
日志等级	5
举例	WIPS/5/HONEYPOT: -VSD=home-SrcMAC=1122-3344-5566; Honeypot AP detected.
日志说明	指定VSD内检测到指定AP为蜜罐时触发日志
处理建议	检查是否存在攻击

175.5 HTGREENMODE

日志内容	-VSD=[STRING]-SrcMAC=[MAC]; HT-Greenfield AP detected.
参数解释	$1：VSD名字 $2：AP的地址
日志等级	5
举例	WIPS/5/HTGREENMODE: -VSD=home-SrcMAC=1122-3344-5566; HT-Greenfield AP detected.
日志说明	指定VSD内检测到指定AP携带绿野模式时触发日志
处理建议	检查是否受到攻击

175.6 MAN_IN_MIDDLE

日志内容	-VSD=[STRING]-SrcMAC=[MAC]; Man-in-the-middle attack detected.
参数解释	$1：VSD名字 $2：client的地址
日志等级	5
举例	WIPS/5/MAN_IN_MIDDLE: -VSD=home-SrcMAC=1122-3344-5566; Man-in-the-middle attack detected.
日志说明	指定VSD内检测到指定client受到中间人攻击时触发日志
处理建议	检查client是否受到中间人攻击

175.7 WIPS_DOS

日志内容	-VSD=[STRING]; [STRING] rate attack detected.
参数解释	$1：VSD名字 $2：设备类型 • AP：AP • Client：客户端
日志等级	5
举例	WIPS/5/WIPS_DOS: -VSD=home; AP rate attack detected.
日志说明	设备指定VSD内的表项建立速率超过阈值时触发日志
处理建议	检查设备是否受到攻击

175.8 WIPS_FLOOD

日志内容	-VSD=[STRING]-SrcMAC=[MAC]; [STRING] flood detected.
参数解释	$1：VSD名字 $2：Flood攻击的MAC地址 $3：Flood帧类型 • Association request：Association 帧 • Authentication：Authentication 帧 • Disassociation：Disassociation 帧 • Reassociation request：Reassociation request 帧 • Deauthentication：Deauthentication 帧 • Null data：Null data 帧 • Beacon：Beacon 帧 • Probe request：Probe request 帧 • BlockAck：BlockAck 帧 • CTS：CTS 帧 • RTS：RTS 帧 • EAPOL start：EAPOL start 帧
日志等级	5
举例	WIPS/5/WIPS_FLOOD: -VSD=home-SrcMAC=1122-3344-5566; Association request flood detected.
日志说明	一定时间内在指定VSD内检测到同一类型的报文超过阈值时触发日志
处理建议	检查报文发送者的合法性

175.9 WIPS_MALF

日志内容	-VSD=[STRING]-SrcMAC=[MAC]; Error detected: [STRING].
参数解释	$1：VSD名字 $2：发送者的MAC地址 $3：畸形报文类型 • invalid ie length：非法 IE 长度 • duplicated ie：重复 IE • redundant ie：冗余 IE • invalid pkt length：报文长度无效 • illegal ibss ess：不合法 IBSS ESS • invalid source addr：无效源 MAC • overflow eapol key：EAPOL-Key 帧畸形 • malf auth：畸形认证 • malf assoc req：畸形关联请求 • malf ht ie：HT IE 畸形 • large duration：large duration 畸形 • null probe resp：null probe resp 畸形 • invalid deauth code：Deauthentication 畸形 • invalid disassoc code：解除关联码畸形 • over flow ssid：Overflow-ssid 畸形 • fata jack：fata jack 畸形
日志等级	5
举例	WIPS/5/WIPS_MALF: -VSD=home-SrcMAC=1122-3344-5566; Error detected: fata jack.
日志说明	指定VSD内检测到指定类型的畸形报文时触发日志
处理建议	检查报文发送者的合法性

175.10 WIPS_ROGUE

日志内容	-VSD=[STRING]-SrcMAC=[MAC]; Rogue AP detected by radio 1 of sensor [STRING] on channel 149 (RSSI=84).
参数解释	$1：VSD名字 $2：Rogue AP的MAC地址
日志等级	5
举例	WIPS/5/WIPS_ROGUE: -VSD=home-SrcMAC=1122-3344-5566; Rogue AP detected by radio 1 of sensor ap1 on channel 149 (RSSI=84).
日志说明	指定VSD内检测到Rogue AP
处理建议	网络存在Rogue AP,建议开启反制Rogue AP功能

175.11 WIPS_SPOOF

日志内容	-VSD=[STRING]-SrcMAC=[MAC]; [STRING] detected.
参数解释	$1：VSD名字 $2：仿冒的MAC地址 $3：仿冒类型 • AP spoofing AP：AP 仿冒为 AP • AP spoofing client：AP 仿冒为 client • AP spoofing ad-hoc：AP 仿冒为 ad-hoc • Ad-hoc spoofing AP：Ad-hoc 仿冒为 AP • Client spoofing AP：Client 仿冒为 AP
日志等级	5
举例	WIPS/5/WIPS_SPOOF: -VSD=home-SrcMAC=1122-3344-5566; AP spoofing AP detected.
日志说明	指定VSD内检测到设备仿冒时触发日志
处理建议	检查报文发送者的合法性

175.12 WIPS_UNAUTH

日志内容	-VSD=[STRING]-SrcMAC=[MAC];Unauthorized client detected by radio 1 of sensor [STRING] on channel 149 (RSSI=84).
参数解释	$1：VSD名字 $2：Unauth client的MAC地址
日志等级	5
举例	WIPS/5/WIPS_UNAUTH: -VSD=home-SrcMAC=1122-3344-5566; Unauthorized client detected by radio 1 of sensor ap1 on channel 149 (RSSI=84).
日志说明	指定VSD内检测到Unauth client
处理建议	检查网络中是否存在Unauth client

175.13 WIPS_WEAKIV

日志内容	-VSD=[STRING]-SrcMAC=[MAC]; Weak IV detected.
参数解释	$1：VSD名字 $2：发送者的MAC地址
日志等级	5
举例	WIPS/5/WIPS_WEAKIV: -VSD=home-SrcMAC=1122-3344-5566; Weak IV detected.
日志说明	指定VSD内检测到采用weak IV加密的报文
处理建议	使用安全级别更高的加密方法加密报文

175.14 WIRELESSBRIDGE

日志内容	-VSD=[STRING]-AP1=[MAC]-AP2=[MAC]]; Wireless bridge detected.
参数解释	$1：VSD名字 $2：AP的地址 $3：AP的地址
日志等级	5
举例	WIPS/5/WIRELESSBRIDGE: -VSD=home-AP1=1122-3344-5566-AP2=7788-9966-5544; Wireless bridge detected.
日志说明	指定VSD内检测到AP1和AP2建立无线网桥时触发日志
处理建议	检查无线网桥是否合法