UNIS 安全产品

日志信息参考（V7）

资料版本：6W600-20220316

Copyright ©2022 紫光恒越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。
除紫光恒越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 60
1.1 系统日志格式说明 60
1.2 快速日志格式说明 62
1.3 如何获取日志信息 63
1.3.1 通过控制台获取日志 63
1.3.2 通过监视终端获取日志 63
1.3.3 通过日志缓冲区获取日志 63
1.3.4 通过日志文件获取日志 63
1.3.5 通过日志主机获取日志 64
1.4 软件模块列表 64
1.5 文档使用说明 69
2 AAA 70
2.1 AAA_FAILURE 70
2.2 AAA_LAUNCH 71
2.3 AAA_SUCCESS 71
3 ACL 71
3.1 ACL_ACCELERATE_NO_RES 72
3.2 ACL_ACCELERATE_NOT_SUPPORT 72
3.3 ACL_ACCELERATE_NOT_SUPPORTHOPBYHOP 72
3.4 ACL_ACCELERATE_NOT_SUPPORTMULTITCPFLAG 73
3.5 ACL_ACCELERATE_NONCONTIGUOUSMASK 73
3.6 ACL_ACCELERATE_UNK_ERR 73
3.7 ACL_DYNRULE_COMMENT 74
3.8 ACL_DYNRULE_MDF 74
3.9 ACL_IPV6_STATIS_INFO 74
3.10 ACL_NO_MEM 75
3.11 ACL_RULE_REACH_MAXNUM 75
3.12 ACL_RULE_SUBID_EXCEED 75
3.13 ACL_STATIS_INFO 76
4 ADVPN 76
4.1 ADVPN_SESSION_DELETED 76
4.2 ADVPN_SESSION_STATE_CHANGED 77

5 AFT 77
5.1 AFT_V4TOV6_FLOW 78
5.2 AFT_V6TOV4_FLOW 79
6 ANCP 79
6.1 ANCP_INVALID_PACKET 80
7 ANTIVIRUS 80
7.1 ANTIVIRUS_IPV4_INTERZONE 81
7.2 ANTIVIRUS_IPV6_INTERZONE 83
7.3 ANTIVIRUS_WARNING 84
7.4 ANTIVIRUS_WARNING 84
7.5 ANTIVIRUS_WARNING 85
8 APMGR 85
8.1 AP_CREATE_FAILURE 85
8.2 AP_REBOOT_REASON 85
8.3 APMGR_ADDBAC_INFO 86
8.4 APMGR_AP_CFG_FAILED 86
8.5 APMGR_AP_ONLINE 86
8.6 APMGR_DELBAC_INFO 87
8.7 APMGR_GET_AP_MODEL_FAILURE 87
8.8 APMGR_LOG_ADD_AP_FAIL 87
8.9 APMGR_LOG_LACOFFLINE 88
8.10 APMGR_LOG_LACONLINE 88
8.11 APMGR_LOG_MEMALERT 88
8.12 APMGR_LOG_NOLICENSE 89
8.13 APMGR_LOG_OFFLINE 89
8.14 APMGR_LOG_ONLINE 89
8.15 APMGR_LOG_ONLINE_FAILED 90
8.16 APMGR_REACH_MAX_APNUMBER 90
8.17 APMGR_ERROR 91
8.18 CWC_AP_DOWN 91
8.19 CWC_AP_UP 92
8.20 CWC_AP_REBOOT 92
8.21 CWC_IMG_DOWNLOAD_COMPLETE 93
8.22 CWS_IMG_DOWNLOAD_FAILED 93
8.23 CWC_IMG_DOWNLOAD_START 93
8.24 CWC_IMG_NO_ENOUGH_SPACE 94

8.25 CWC_LOCALAC_DOWN 94
8.26 CWC_LOCALAC_UP 94
8.27 CWC_RUN_DOWNLOAD_COMPLETE 95
8.28 CWC_RUN_DOWNLOAD_START 95
8.29 CWC_RUN_NO_ENOUGH_SPACE 95
8.30 CWS_AP_DOWN 96
8.31 CWS_AP_UP 97
8.32 CWS_IMG_DOWNLOAD_COMPLETE 97
8.33 CWS_IMG_DOWNLOAD_FAILED 97
8.34 CWS_IMG_DOWNLOAD_START 98
8.35 CWS_IMG_ OPENFILE_FAILED 98
8.36 CWS_LOCALAC_DOWN 99
8.37 CWS_LOCALAC_UP 99
8.38 CWS_RUN_DOWNLOAD_COMPLETE 100
8.39 CWS_RUN_DOWNLOAD_START 100
8.40 RADIO 100
9 APR 100
9.1 NBAR_WARNING 101
9.2 NBAR_WARNING 101
9.3 NBAR_WARNING 101
9.4 NBAR_WARNING 102
10 ARP 102
10.1 ARP_ACTIVE_ACK_NO_REPLY 102
10.2 ARP_ACTIVE_ACK_NOREQUESTED_REPLY 103
10.3 ARP_BINDRULETOHW_FAILED 103
10.4 ARP_DYNAMIC 104
10.5 ARP_DYNAMIC_IF 104
10.6 ARP_DYNAMIC_SLOT 104
10.7 ARP_HOST_IP_CONFLICT 105
10.8 ARP_RATE_EXCEEDED 105
10.9 ARP_SENDER_IP_INVALID 105
10.10 ARP_SENDER_MAC_INVALID 106
10.11 ARP_SRC_MAC_FOUND_ATTACK 106
10.12 ARP_TARGET_IP_INVALID 106
10.13 DUPIFIP 107
10.14 DUPIP 107

10.15 DUPVRRPIP 107
11 ASPF 108
11.1 ASPF_IPV4_DNS 108
11.2 ASPF_IPV6_DNS 109
12 ATK 109
12.1 ATK_ICMP_ADDRMASK_REQ 110
12.2 ATK_ICMP_ADDRMASK_REQ_RAW 111
12.3 ATK_ICMP_ADDRMASK_REQ_RAW_SZ 111
12.4 ATK_ICMP_ADDRMASK_REQ_SZ 112
12.5 ATK_ICMP_ADDRMASK_RPL 113
12.6 ATK_ICMP_ADDRMASK_RPL_RAW 114
12.7 ATK_ICMP_ADDRMASK_RPL_RAW_SZ 114
12.8 ATK_ICMP_ADDRMASK_RPL_SZ 115
12.9 ATK_ICMP_ECHO_REQ 116
12.10 ATK_ICMP_ECHO_REQ_RAW 117
12.11 ATK_ICMP_ECHO_REQ_RAW_SZ 117
12.12 ATK_ICMP_ECHO_REQ_SZ 118
12.13 ATK_ICMP_ECHO_RPL 119
12.14 ATK_ICMP_ECHO_RPL_RAW 120
12.15 ATK_ICMP_ECHO_RPL_RAW_SZ 120
12.16 ATK_ICMP_ECHO_RPL_SZ 121
12.17 ATK_ICMP_FLOOD 121
12.18 ATK_ICMP_FLOOD_SZ 122
12.19 ATK_ICMP_INFO_REQ 122
12.20 ATK_ICMP_INFO_REQ_RAW 123
12.21 ATK_ICMP_INFO_REQ_RAW_SZ 123
12.22 ATK_ICMP_INFO_REQ_SZ 124
12.23 ATK_ICMP_INFO_RPL 125
12.24 ATK_ICMP_INFO_RPL_RAW 126
12.25 ATK_ICMP_INFO_RPL_RAW_SZ 126
12.26 ATK_ICMP_INFO_RPL_SZ 127
12.27 ATK_ICMP_LARGE 128
12.28 ATK_ICMP_LARGE_RAW 129
12.29 ATK_ICMP_LARGE_RAW_SZ 129
12.30 ATK_ICMP_LARGE_SZ 130
12.31 ATK_ICMP_PARAPROBLEM 131

12.32 ATK_ICMP_PARAPROBLEM_RAW 132
12.33 ATK_ICMP_PARAPROBLEM_RAW_SZ 132
12.34 ATK_ICMP_PARAPROBLEM_SZ 133
12.35 ATK_ICMP_PINGOFDEATH 134
12.36 ATK_ICMP_PINGOFDEATH_RAW 135
12.37 ATK_ICMP_PINGOFDEATH_RAW_SZ 135
12.38 ATK_ICMP_PINGOFDEATH_SZ 136
12.39 ATK_ICMP_REDIRECT 137
12.40 ATK_ICMP_REDIRECT_RAW 138
12.41 ATK_ICMP_REDIRECT_RAW_SZ 138
12.42 ATK_ICMP_REDIRECT_SZ 139
12.43 ATK_ICMP_SMURF 140
12.44 ATK_ICMP_SMURF_RAW 141
12.45 ATK_ICMP_SMURF_RAW_SZ 142
12.46 ATK_ICMP_SMURF_SZ 143
12.47 ATK_ICMP_SOURCEQUENCH 144
12.48 ATK_ICMP_SOURCEQUENCH_RAW 145
12.49 ATK_ICMP_SOURCEQUENCH_RAW_SZ 145
12.50 ATK_ICMP_SOURCEQUENCH_SZ 146
12.51 ATK_ICMP_TIMEEXCEED 147
12.52 ATK_ICMP_TIMEEXCEED_RAW 148
12.53 ATK_ICMP_TIMEEXCEED_RAW_SZ 148
12.54 ATK_ICMP_TIMEEXCEED_SZ 149
12.55 ATK_ICMP_TRACEROUTE 150
12.56 ATK_ICMP_TRACEROUTE_RAW 151
12.57 ATK_ICMP_TRACEROUTE_RAW_SZ 151
12.58 ATK_ICMP_TRACEROUTE_SZ 152
12.59 ATK_ICMP_TSTAMP_REQ 153
12.60 ATK_ICMP_TSTAMP_REQ_RAW 154
12.61 ATK_ICMP_TSTAMP_REQ_RAW_SZ 154
12.62 ATK_ICMP_TSTAMP_REQ_SZ 155
12.63 ATK_ICMP_TSTAMP_RPL 156
12.64 ATK_ICMP_TSTAMP_RPL_RAW 157
12.65 ATK_ICMP_TSTAMP_RPL_RAW_SZ 157
12.66 ATK_ICMP_TSTAMP_RPL_SZ 158
12.67 ATK_ICMP_TYPE 159
12.68 ATK_ICMP_TYPE_RAW 160

12.69 ATK_ICMP_TYPE_RAW_SZ 160
12.70 ATK_ICMP_TYPE_SZ 161
12.71 ATK_ICMP_UNREACHABLE 162
12.72 ATK_ICMP_UNREACHABLE_RAW 163
12.73 ATK_ICMP_UNREACHABLE_RAW_SZ 163
12.74 ATK_ICMP_UNREACHABLE_SZ 164
12.75 ATK_ICMPV6_DEST_UNREACH 165
12.76 ATK_ICMPV6_DEST_UNREACH_RAW 166
12.77 ATK_ICMPV6_DEST_UNREACH_RAW_SZ 166
12.78 ATK_ICMPV6_DEST_UNREACH_SZ 167
12.79 ATK_ICMPV6_ECHO_REQ 168
12.80 ATK_ICMPV6_ECHO_REQ_RAW 169
12.81 ATK_ICMPV6_ECHO_REQ_RAW_SZ 169
12.82 ATK_ICMPV6_ECHO_REQ_SZ 170
12.83 ATK_ICMPV6_ECHO_RPL 171
12.84 ATK_ICMPV6_ECHO_RPL_RAW 172
12.85 ATK_ICMPV6_ECHO_RPL_RAW_SZ 172
12.86 ATK_ICMPV6_ECHO_RPL_SZ 173
12.87 ATK_ICMPV6_FLOOD 173
12.88 ATK_ICMPV6_FLOOD_SZ 174
12.89 ATK_ICMPV6_GROUPQUERY 175
12.90 ATK_ICMPV6_GROUPQUERY_RAW 176
12.91 ATK_ICMPV6_GROUPQUERY_RAW_SZ 176
12.92 ATK_ICMPV6_GROUPQUERY_SZ 177
12.93 ATK_ICMPV6_GROUPREDUCTION 178
12.94 ATK_ICMPV6_GROUPREDUCTION_RAW 179
12.95 ATK_ICMPV6_GROUPREDUCTION_RAW_SZ 179
12.96 ATK_ICMPV6_GROUPREDUCTION_SZ 180
12.97 ATK_ICMPV6_GROUPREPORT 181
12.98 ATK_ICMPV6_GROUPREPORT_RAW 182
12.99 ATK_ICMPV6_GROUPREPORT_RAW_SZ 182
12.100 ATK_ICMPV6_GROUPREPORT_SZ 183
12.101 ATK_ICMPV6_LARGE 184
12.102 ATK_ICMPV6_LARGE_RAW 184
12.103 ATK_ICMPV6_LARGE_RAW_SZ 185
12.104 ATK_ICMPV6_LARGE_SZ 185
12.105 ATK_ICMPV6_PACKETTOOBIG 186

12.106 ATK_ICMPV6_PACKETTOOBIG_RAW 187
12.107 ATK_ICMPV6_PACKETTOOBIG_RAW_SZ 187
12.108 ATK_ICMPV6_PACKETTOOBIG_SZ 188
12.109 ATK_ICMPV6_PARAPROBLEM 189
12.110 ATK_ICMPV6_PARAPROBLEM_RAW 190
12.111 ATK_ICMPV6_PARAPROBLEM_RAW_SZ 190
12.112 ATK_ICMPV6_PARAPROBLEM_SZ 191
12.113 ATK_ICMPV6_TIMEEXCEED 192
12.114 ATK_ICMPV6_TIMEEXCEED_RAW 193
12.115 ATK_ICMPV6_TIMEEXCEED_RAW_SZ 193
12.116 ATK_ICMPV6_TIMEEXCEED_SZ 194
12.117 ATK_ICMPV6_TRACEROUTE 195
12.118 ATK_ICMPV6_TRACEROUTE_RAW 196
12.119 ATK_ICMPV6_TRACEROUTE_RAW_SZ 197
12.120 ATK_ICMPV6_TRACEROUTE_SZ 198
12.121 ATK_ICMPV6_TYPE 199
12.122 ATK_ICMPV6_TYPE_RAW 200
12.123 ATK_ICMPV6_TYPE_RAW_SZ 200
12.124 ATK_ICMPV6_TYPE_SZ 201
12.125 ATK_IP_OPTION 202
12.126 ATK_IP_OPTION_RAW 203
12.127 ATK_IP_OPTION_RAW_SZ 204
12.128 ATK_IP_OPTION_SZ 205
12.129 ATK_IP4_ACK_FLOOD 206
12.130 ATK_IP4_ACK_FLOOD_SZ 206
12.131 ATK_IP4_DIS_PORTSCAN 207
12.132 ATK_IP4_DIS_PORTSCAN_SZ 207
12.133 ATK_IP4_DNS_FLOOD 208
12.134 ATK_IP4_DNS_FLOOD_SZ 208
12.135 ATK_IP4_FIN_FLOOD 209
12.136 ATK_IP4_FIN_FLOOD_SZ 209
12.137 ATK_IP4_FRAGMENT 210
12.138 ATK_IP4_FRAGMENT_RAW 211
12.139 ATK_IP4_FRAGMENT_RAW_SZ 211
12.140 ATK_IP4_FRAGMENT_SZ 212
12.141 ATK_IP4_HTTP_FLOOD 212
12.142 ATK_IP4_HTTP_FLOOD_SZ 213

12.143 ATK_IP4_IMPOSSIBLE 213
12.144 ATK_IP4_IMPOSSIBLE_RAW 214
12.145 ATK_IP4_IMPOSSIBLE_RAW_SZ 214
12.146 ATK_IP4_IMPOSSIBLE_SZ 215
12.147 ATK_IP4_IPSWEEP 216
12.148 ATK_IP4_IPSWEEP_SZ 216
12.149 ATK_IP4_PORTSCAN 217
12.150 ATK_IP4_PORTSCAN_SZ 218
12.151 ATK_IP4_RST_FLOOD 218
12.152 ATK_IP4_RST_FLOOD_SZ 219
12.153 ATK_IP4_SLOW_ATTACK 219
12.154 ATK_IP4_SLOW_ATTACK_SZ 220
12.155 ATK_IP4_SYN_FLOOD 220
12.156 ATK_IP4_SYN_FLOOD_SZ 221
12.157 ATK_IP4_SYNACK_FLOOD 221
12.158 ATK_IP4_SYNACK_FLOOD_SZ 222
12.159 ATK_IP4_TCP_ALLFLAGS 222
12.160 ATK_IP4_TCP_ALLFLAGS_RAW 223
12.161 ATK_IP4_TCP_ALLFLAGS_RAW_SZ 223
12.162 ATK_IP4_TCP_ALLFLAGS_SZ 224
12.163 ATK_IP4_TCP_FINONLY 225
12.164 ATK_IP4_TCP_FINONLY_RAW 226
12.165 ATK_IP4_TCP_FINONLY_RAW_SZ 226
12.166 ATK_IP4_TCP_FINONLY_SZ 227
12.167 ATK_IP4_TCP_INVALIDFLAGS 228
12.168 ATK_IP4_TCP_INVALIDFLAGS_RAW 229
12.169 ATK_IP4_TCP_INVALIDFLAGS_RAW_SZ 230
12.170 ATK_IP4_TCP_INVALIDFLAGS_SZ 231
12.171 ATK_IP4_TCP_LAND 232
12.172 ATK_IP4_TCP_LAND_RAW 233
12.173 ATK_IP4_TCP_LAND_RAW_SZ 233
12.174 ATK_IP4_TCP_LAND_SZ 234
12.175 ATK_IP4_TCP_NULLFLAG 235
12.176 ATK_IP4_TCP_NULLFLAG_RAW 236
12.177 ATK_IP4_TCP_NULLFLAG_RAW_SZ 236
12.178 ATK_IP4_TCP_NULLFLAG_SZ 237
12.179 ATK_IP4_TCP_SYNFIN 238

12.180 ATK_IP4_TCP_SYNFIN_RAW 239
12.181 ATK_IP4_TCP_SYNFIN_RAW_SZ 239
12.182 ATK_IP4_TCP_SYNFIN_SZ 240
12.183 ATK_IP4_TCP_WINNUKE 241
12.184 ATK_IP4_TCP_WINNUKE_RAW 242
12.185 ATK_IP4_TCP_WINNUKE_RAW_SZ 242
12.186 ATK_IP4_TCP_WINNUKE_SZ 243
12.187 ATK_IP4_TEARDROP 244
12.188 ATK_IP4_TEARDROP_RAW 245
12.189 ATK_IP4_TEARDROP_RAW_SZ 245
12.190 ATK_IP4_TEARDROP_SZ 246
12.191 ATK_IP4_TINY_FRAGMENT 247
12.192 ATK_IP4_TINY_FRAGMENT_RAW 248
12.193 ATK_IP4_TINY_FRAGMENT_RAW_SZ 249
12.194 ATK_IP4_TINY_FRAGMENT_SZ 250
12.195 ATK_IP4_UDP_BOMB 251
12.196 ATK_IP4_UDP_BOMB_RAW 252
12.197 ATK_IP4_UDP_BOMB_RAW_SZ 252
12.198 ATK_IP4_UDP_BOMB_SZ 253
12.199 ATK_IP4_UDP_FLOOD 253
12.200 ATK_IP4_UDP_FLOOD_SZ 254
12.201 ATK_IP4_UDP_FRAGGLE 255
12.202 ATK_IP4_UDP_FRAGGLE_RAW 256
12.203 ATK_IP4_UDP_FRAGGLE_RAW_SZ 256
12.204 ATK_IP4_UDP_FRAGGLE_SZ 257
12.205 ATK_IP4_UDP_SNORK 258
12.206 ATK_IP4_UDP_SNORK_RAW 259
12.207 ATK_IP4_UDP_SNORK_RAW_SZ 259
12.208 ATK_IP4_UDP_SNORK_SZ 260
12.209 ATK_IP6_ACK_FLOOD 260
12.210 ATK_IP6_ACK_FLOOD_SZ 261
12.211 ATK_IP6_DIS_PORTSCAN 261
12.212 ATK_IP6_DIS_PORTSCAN_SZ 262
12.213 ATK_IP6_DNS_FLOOD 262
12.214 ATK_IP6_DNS_FLOOD_SZ 263
12.215 ATK_IP6_EXHEADER_ABNORMAL 263
12.216 ATK_IP6_EXHEADER_ABNORMAL_RAW 264

12.217 ATK_IP6_EXHEADER_ABNORMAL_RAW_SZ 264
12.218 ATK_IP6_EXHEADER_ABNORMAL_SZ 265
12.219 ATK_IP6_EXHEADER_EXCEED 266
12.220 ATK_IP6_EXHEADER_EXCEED_RAW 267
12.221 ATK_IP6_EXHEADER_EXCEED_RAW_SZ 267
12.222 ATK_IP6_EXHEADER_EXCEED_SZ 268
12.223 ATK_IP6_FIN_FLOOD 268
12.224 ATK_IP6_FIN_FLOOD_SZ 269
12.225 ATK_IP6_FRAGMENT 269
12.226 ATK_IP6_FRAGMENT_RAW 270
12.227 ATK_IP6_FRAGMENT_RAW_SZ 270
12.228 ATK_IP6_FRAGMENT_SZ 271
12.229 ATK_IP6_HTTP_FLOOD 271
12.230 ATK_IP6_HTTP_FLOOD_SZ 272
12.231 ATK_IP6_IMPOSSIBLE 272
12.232 ATK_IP6_IMPOSSIBLE_RAW 273
12.233 ATK_IP6_IMPOSSIBLE_RAW_SZ 273
12.234 ATK_IP6_IMPOSSIBLE_SZ 274
12.235 ATK_IP6_IPSWEEP 274
12.236 ATK_IP6_IPSWEEP_SZ 275
12.237 ATK_IP6_PORTSCAN 275
12.238 ATK_IP6_PORTSCAN_SZ 276
12.239 ATK_IP6_RST_FLOOD 276
12.240 ATK_IP6_RST_FLOOD_SZ 277
12.241 ATK_IP6_SLOW_ATTACK 277
12.242 ATK_IP6_SLOW_ATTACK_SZ 278
12.243 ATK_IP6_SYN_FLOOD 278
12.244 ATK_IP6_SYN_FLOOD_SZ 279
12.245 ATK_IP6_SYNACK_FLOOD 279
12.246 ATK_IP6_SYNACK_FLOOD_SZ 280
12.247 ATK_IP6_TCP_ALLFLAGS 280
12.248 ATK_IP6_TCP_ALLFLAGS_RAW 281
12.249 ATK_IP6_TCP_ALLFLAGS_RAW_SZ 281
12.250 ATK_IP6_TCP_ALLFLAGS_SZ 282
12.251 ATK_IP6_TCP_FINONLY 283
12.252 ATK_IP6_TCP_FINONLY_RAW 283
12.253 ATK_IP6_TCP_FINONLY_RAW_SZ 284

12.254 ATK_IP6_TCP_FINONLY_SZ 284
12.255 ATK_IP6_TCP_INVALIDFLAGS 285
12.256 ATK_IP6_TCP_INVALIDFLAGS_RAW 286
12.257 ATK_IP6_TCP_INVALIDFLAGS_RAW_SZ 286
12.258 ATK_IP6_TCP_INVALIDFLAGS_SZ 287
12.259 ATK_IP6_TCP_LAND 288
12.260 ATK_IP6_TCP_LAND_RAW 288
12.261 ATK_IP6_TCP_LAND_RAW_SZ 289
12.262 ATK_IP6_TCP_LAND_SZ 289
12.263 ATK_IP6_TCP_NULLFLAG 290
12.264 ATK_IP6_TCP_NULLFLAG_RAW 290
12.265 ATK_IP6_TCP_NULLFLAG_RAW_SZ 291
12.266 ATK_IP6_TCP_NULLFLAG_SZ 291
12.267 ATK_IP6_TCP_SYNFIN 292
12.268 ATK_IP6_TCP_SYNFIN_RAW 292
12.269 ATK_IP6_TCP_SYNFIN_RAW_SZ 293
12.270 ATK_IP6_TCP_SYNFIN_SZ 293
12.271 ATK_IP6_TCP_WINNUKE 294
12.272 ATK_IP6_TCP_WINNUKE_RAW 295
12.273 ATK_IP6_TCP_WINNUKE_RAW_SZ 295
12.274 ATK_IP6_TCP_WINNUKE_SZ 296
12.275 ATK_IP6_UDP_FLOOD 296
12.276 ATK_IP6_UDP_FLOOD_SZ 297
12.277 ATK_IP6_UDP_FRAGGLE 297
12.278 ATK_IP6_UDP_FRAGGLE_RAW 298
12.279 ATK_IP6_UDP_FRAGGLE_RAW_SZ 298
12.280 ATK_IP6_UDP_FRAGGLE_SZ 299
12.281 ATK_IP6_UDP_SNORK 300
12.282 ATK_IP6_UDP_SNORK_RAW 301
12.283 ATK_IP6_UDP_SNORK_RAW_SZ 301
12.284 ATK_IP6_UDP_SNORK_SZ 302
12.285 ATK_IPOPT_ABNORMAL 303
12.286 ATK_IPOPT_ABNORMAL_RAW 304
12.287 ATK_IPOPT_ABNORMAL_RAW_SZ 304
12.288 ATK_IPOPT_ABNORMAL_SZ 305
12.289 ATK_IPOPT_LOOSESRCROUTE 306
12.290 ATK_IPOPT_LOOSESRCROUTE_RAW 307

12.291 ATK_IPOPT_LOOSESRCROUTE_RAW_SZ 308
12.292 ATK_IPOPT_LOOSESRCROUTE_SZ 309
12.293 ATK_IPOPT_RECORDROUTE 310
12.294 ATK_IPOPT_RECORDROUTE_RAW 311
12.295 ATK_IPOPT_RECORDROUTE_RAW_SZ 312
12.296 ATK_IPOPT_RECORDROUTE_SZ 313
12.297 ATK_IPOPT_ROUTEALERT 314
12.298 ATK_IPOPT_ROUTEALERT_RAW 315
12.299 ATK_IPOPT_ROUTEALERT_RAW_SZ 316
12.300 ATK_IPOPT_ROUTEALERT_SZ 317
12.301 ATK_IPOPT_SECURITY 318
12.302 ATK_IPOPT_SECURITY_RAW 319
12.303 ATK_IPOPT_SECURITY_RAW_SZ 320
12.304 ATK_IPOPT_SECURITY_SZ 321
12.305 ATK_IPOPT_STREAMID 322
12.306 ATK_IPOPT_STREAMID_RAW 323
12.307 ATK_IPOPT_STREAMID_RAW_SZ 324
12.308 ATK_IPOPT_STREAMID_SZ 325
12.309 ATK_IPOPT_STRICTSRCROUTE 326
12.310 ATK_IPOPT_STRICTSRCROUTE_RAW 327
12.311 ATK_IPOPT_STRICTSRCROUTE_RAW_SZ 328
12.312 ATK_IPOPT_STRICTSRCROUTE_SZ 329
12.313 ATK_IPOPT_TIMESTAMP 330
12.314 ATK_IPOPT_TIMESTAMP_RAW 331
12.315 ATK_IPOPT_TIMESTAMP_RAW_SZ 332
12.316 ATK_IPOPT_TIMESTAMP_SZ 333
12.317 ATK_IPV6_EXT_HEADER 334
12.318 ATK_IPV6_EXT_HEADER_RAW 335
12.319 ATK_IPV6_EXT_HEADER_RAW_SZ 335
12.320 ATK_IPV6_EXT_HEADER_SZ 336
13 ATM 336
13.1 ATM_PVCDOWN 337
13.2 ATM_PVCUP 337
14 AUDIT 338
14.1 AUDIT_RULE_MATCH_AS_IPV4_LOG（系统日志） 339
14.2 AUDIT_RULE_MATCH_FILE_IPV4_LOG（系统日志） 340

14.3 AUDIT_RULE_MATCH_FORUM_IPV4_LOG（系统日志）……341
14.4 AUDIT_RULE_MATCH_IM_IPV4_LOG（系统日志）……342
14.5 AUDIT_RULE_MATCH_MAIL_IPV4_LOG（系统日志）……343
14.6 AUDIT_RULE_MATCH_OTHER_IPV4_LOG（系统日志）……344
14.7 AUDIT_RULE_MATCH_SEARCH_IPV4_LOG（系统日志）……345
14.8 AUDIT_RULE_MATCH_AS_IPV4_LOG（快速日志）……346
14.9 AUDIT_RULE_MATCH_FILE_IPV4_LOG（快速日志）……348
14.10 AUDIT_RULE_MATCH_FORUM_IPV4_LOG（快速日志）……350
14.11 AUDIT_RULE_MATCH_IM_IPV4_LOG（快速日志）……352
14.12 AUDIT_RULE_MATCH_MAIL_IPV4_LOG（快速日志）……354
14.13 AUDIT_RULE_MATCH_OTHER_IPV4_LOG（快速日志）……356
14.14 AUDIT_RULE_MATCH_SEARCH_IPV4_LOG（快速日志）……358
14.15 AUDIT_RULE_MATCH_AS_IPV6_LOG（系统日志）（快速日志）……360
14.16 AUDIT_RULE_MATCH_FILE_IPV6_LOG（系统日志）（快速日志）……361
14.17 AUDIT_RULE_MATCH_FORUM_IPV6_LOG（系统日志）（快速日志）……362
14.18 AUDIT_RULE_MATCH_IM_IPV6_LOG（系统日志）（快速日志）……363
14.19 AUDIT_RULE_MATCH_MAIL_IPV6_LOG（系统日志）（快速日志）……364
14.20 AUDIT_RULE_MATCH_OTHER_IPV6_LOG（系统日志）（快速日志）……366
14.21 AUDIT_RULE_MATCH_SEARCH_IPV6_LOG（系统日志）（快速日志）……367
15 AUTOCFG……368
15.1 AUTOCFG_URL_START_SUCCESS……368
15.2 AUTOCFG_URL_EXECUTE_SUCCESS……368
15.3 AUTOCFG_URL_EXECUTE_FAILURE……368
15.4 AUTOCFG_URL_START_FAILED……369
16 AVC……369
16.1 AVC_MATCH_IPV4_LOG……370
16.2 AVC_MATCH_IPV6_LOG……371
16.3 AVC_THRESHOLDWARNING_FASTLOGGING_FMT……372
16.4 AVC_THRESHOLDWARNING_FASTLOGGING_IPV6FMT……373
17 BFD……373
17.1 BFD_CHANGE_FSM……374
17.2 BFD_REACHED_UPPER_LIMIT……374
18 BGP……374
18.1 BGP_EXCEED_ROUTE_LIMIT……375
18.2 BGP_REACHED_THRESHOLD……375
18.3 BGP_MEM_ALERT……376

18.4 BGP_PEER_LICENSE_REACHED 376
18.5 BGP_ROUTE_LICENSE_REACHED 376
18.6 BGP_STATE_CHANGED 377
19 BLS 377
19.1 BLS_DIP_BLOCK 378
19.2 BLS_DIPV6_BLOCK 378
19.3 BLS_ENTRY_ADD 379
19.4 BLS_ENTRY_DEL 379
19.5 BLS_IP_BLOCK 380
19.6 BLS_IPV6_BLOCK 380
19.7 BLS_IPV6_ENTRY_ADD 380
19.8 BLS_IPV6_ENTRY_DEL 381
19.9 BLS_ENTRY_USER_ADD 381
19.10 BLS_ENTRY_USER_DEL 382
19.11 BLS_USER_IP_BLOCK 382
19.12 BLS_USER_IPV6_BLOCK 383
20 CC 383
20.1 CC_MATCH_IPV4_LOG 384
20.2 CC_MATCH_IPV6_LOG 385
21 CFD 386
21.1 CFD_CROSS_CCM 386
21.2 CFD_ERROR_CCM 386
21.3 CFD_LOST_CCM 387
21.4 CFD_REACH_LOWERLIMIT 387
21.5 CFD_REACH_UPPERLIMIT 388
21.6 CFD_RECEIVE_CCM 388
22 CFGLOG 388
22.1.1 CFGLOG_CFGOPERATE 389
23 CFGMAN 389
23.1 CFGMAN_ARCHIVE_FAIL 389
23.2 CFGMAN_CFGCHANGED 390
23.3 CFGMAN_OPTCOMPLETION 391
23.4 CFGMAN_REPLACE_CANCEL 392
23.5 CFGMAN_REPLACE_FAIL 392
23.6 CFGMAN_REPLACE_SOON 393

24 CGROUP 393
24.1 CGROUP_STATUS_CHANGE 393
25 CONNLMT 393
25.1 CONNLMT_IPV4_OVERLOAD 394
25.2 CONNLMT_IPV4_RECOVER 395
25.3 CONNLMT_IPV6_OVERLOAD 396
25.4 CONNLMT_IPV6_RECOVER 397
25.5 CONNLMT_IPV4_RATELIMIT 398
25.6 CONNLMT_IPV6_RATELIMIT 399
26 CONTEXT 399
26.1 CAR_DESTROY 400
26.2 CAR_MODIFY 400
26.3 SIB_BROADCAST_DROP 401
26.4 SIB_CORE_ATTACK_DROP 401
26.5 SIB_MAC_DUPLICATE 401
26.6 SIB_MAC_DUPLICATE 402
26.7 SIB_MULTICAST_DROP 402
27 DAC 402
27.1 DAC_STORE_STATE_STOREFULL 402
27.2 DAC_STORE_STATE_FULL 403
27.3 DAC_STORE_DELETE_FILE 403
27.4 DAC_HDD_FULL 404
28 DEV 404
28.1 BOARD_REBOOT 404
28.2 BOARD_REMOVED 405
28.3 BOARD_STATE_FAULT 405
28.4 BOARD_STATE_NORMAL 406
28.5 CFCARD_INSERTED 406
28.6 CFCARD_REMOVED 406
28.7 CHASSIS_REBOOT 407
28.8 DEV_CLOCK_CHANGE 407
28.9 DEV_FAULT_TOOLONG 407
28.10 FAN_ABSENT 408
28.11 FAN_DIRECTION_NOT_PREFERRED 408
28.12 FAN_FAILED 409
28.13 FAN_RECOVERED 409

28.14 MAD_DETECT 410
28.15 MAD_PROC 410
28.16 POWER_ABSENT 411
28.17 POWER_FAILED 411
28.18 POWER_FAILED_SHUTDOWN 412
28.19 POWER_MONITOR_ABSENT 412
28.20 POWER_MONITOR_FAILED 413
28.21 POWER_MONITOR_RECOVERED 413
28.22 POWER_RECOVERED 414
28.23 RPS_ABSENT 414
28.24 RPS_NORMAL 415
28.25 SUBCARD_FAULT 415
28.26 SUBCARD_INSERTED 416
28.27 SUBCARD_REBOOT 416
28.28 SUBCARD_REMOVED 416
28.29 SYSTEM_REBOOT 417
28.30 TEMPERATURE_ALARM 418
28.31 TEMPERATURE_LOW 419
28.32 TEMPERATURE_NORMAL 420
28.33 TEMPERATURE_SHUTDOWN 421
28.34 TEMPERATURE_WARNING 422
28.35 TIMER_CREATE_FAILED_FIRST 423
28.36 TIMER_CREATE_FAILED_MORE 423
28.37 VCHK_VERSION_INCOMPATIBLE 424
29 DFILTER 424
29.1 DFILTER_IPV4_LOG（系统日志） 425
29.2 DFILTER_IPV6_LOG（系统日志） 426
29.3 DFILTER_MATCH_IPV4_LOG（快速日志） 427
29.4 DFILTER_MATCH_IPV6_LOG（快速日志） 429
30 DHCP 430
30.1 DHCP_NOTSUPPORTED 430
30.2 DHCP_NORESOURCES 430
31 DHCPS 430
31.1 DHCPS_ALLOCATE_IP 431
31.2 DHCPS_CONFLICT_IP 431
31.3 DHCPS_EXTEND_IP 432

31.4 DHCPS_FILE 432
31.5 DHCPS_RECLAIM_IP 432
31.6 DHCPS_VERIFY_CLASS 433
32 DHCPS6 433
32.1 DHCPS6_ALLOCATE_ADDRESS 433
32.2 DHCPS6_ALLOCATE_PREFIX 434
32.3 DHCPS6_CONFLICT_ADDRESS 434
32.4 DHCPS6_EXTEND_ADDRESS 435
32.5 DHCPS6_EXTEND_PREFIX 435
32.6 DHCPS6_FILE 436
32.7 DHCPS6_RECLAIM_ADDRESS 436
32.8 DHCPS6_RECLAIM_PREFIX 437
33 DHCPSP4 437
33.1 DHCPSP4_FILE 437
34 DHCPSP6 437
34.1 DHCPSP6_FILE 438
35 DIAG 438
35.1 CORE_EXCEED_THRESHOLD 438
35.2 CORE_RECOVERY 439
35.3 CPU_EXCEED_THRESHOLD 439
35.4 CPU_RECOVER_THRESHOLD 439
35.5 CPU_USAGE_LASTMINUTE 440
35.6 DIAG_DEADLOOP_DETECT 440
35.7 DIAG_STORAGE_BELOW_THRESHOLD 440
35.8 DIAG_STORAGE_EXCEED_THRESHOLD 441
35.9 MEM_ALERT 442
35.10 MEM_BELOW_THRESHOLD 443
35.11 MEM_EXCEED_THRESHOLD 443
35.12 MEM_USAGE_EXCEED_THRESHOLD 444
35.13 MEM_USAGE_RECOVER_THRESHOLD 444
35.14 MEM_USAGE 444
36 DLDP 444
36.1 DLDP_AUTHENTICATION_FAILED 445
36.2 DLDP_LINK_BIDIRECTIONAL 445
36.3 DLDP_LINK_UNIDIRECTIONAL 445
36.4 DLDP_NEIGHBOR_AGED 446

36.5 DLDP_NEIGHBOR_CONFIRMED 446
36.6 DLDP_NEIGHBOR_DELETED 447
37 DNS 447
37.1 DNS_SNOOPING_LOG 448
38 DOT1X 449
38.1 DOT1X_LOGIN_FAILURE 450
38.2 DOT1X_LOGIN_SUCC 451
38.3 DOT1X_LOGOFF 452
38.4 DOT1X_NOTENOUGH_EADFREEIP_RES 453
38.5 DOT1X_NOTENOUGH_EADFREERULE_RES 453
38.6 DOT1X_NOTENOUGH_EADPORTREDIR_RES 453
38.7 DOT1X_NOTENOUGH_EADMACREDIR_RES 454
38.8 DOT1X_NOTENOUGH_ENABLEDOT1X_RES 454
38.9 DOT1X_NOTSUPPORT_EADFREEIP_RES 454
38.10 DOT1X_NOTSUPPORT_EADFREERULE_RES 455
38.11 DOT1X_NOTSUPPORT_EADMACREDIR_RES 455
38.12 DOT1X_NOTSUPPORT_EADPORTREDIR_RES 455
38.13 DOT1X_UNICAST_NOT_EFFECTIVE 456
38.14 DOT1X_WLAN_LOGIN_FAILURE 457
38.15 DOT1X_WLAN_LOGIN_SUCC 458
38.16 DOT1X_WLAN_LOGOFF 459
39 EDEV 460
39.1 EDEV_FAILOVER_GROUP_STATE_CHANGE 460
40 EIGRP 461
40.1 RID_CHANGE 461
40.2 PEER_CHANGE 461
41 ERPS 462
41.1 ERPS_STATE_CHANGED 462
42 ETHOAM 462
42.1 ETHOAM_CONNECTION_FAIL_DOWN 463
42.2 ETHOAM_CONNECTION_FAIL_TIMEOUT 463
42.3 ETHOAM_CONNECTION_FAIL_UNSATISF 463
42.4 ETHOAM_CONNECTION_SUCCEED 464
42.5 ETHOAM_DISABLE 464
42.6 ETHOAM_DISCOVERY_EXIT 464
42.7 ETHOAM_ENABLE 465

42.8 ETHOAM_ENTER_LOOPBACK_CTRLLED 465
42.9 ETHOAM_ENTER_LOOPBACK_CTRLLING 465
42.10 ETHOAM_LOCAL_DYING_GASP 466
42.11 ETHOAM_LOCAL_ERROR_FRAME 466
42.12 ETHOAM_LOCAL_ERROR_FRAME_PERIOD 466
42.13 ETHOAM_LOCAL_ERROR_FRAME_SECOND 467
42.14 ETHOAM_LOCAL_LINK_FAULT 467
42.15 ETHOAM_LOOPBACK_EXIT 467
42.16 ETHOAM_LOOPBACK_EXIT_ERROR_STATU 468
42.17 ETHOAM_LOOPBACK_NO_RESOURCE 468
42.18 ETHOAM_LOOPBACK_NOT_SUPPORT 468
42.19 ETHOAM_QUIT_LOOPBACK_CTRLLED 469
42.20 ETHOAM_QUIT_LOOPBACK_CTRLLING 469
42.21 ETHOAM_REMOTE_CRITICAL 469
42.22 ETHOAM_REMOTE_DYING_GASP 470
42.23 ETHOAM_REMOTE_ERROR_FRAME 470
42.24 ETHOAM_REMOTE_ERROR_FRAME_PERIOD 470
42.25 ETHOAM_REMOTE_ERROR_FRAME_SECOND 471
42.26 ETHOAM_REMOTE_ERROR_SYMBOL 471
42.27 ETHOAM_REMOTE_EXIT 471
42.28 ETHOAM_REMOTE_FAILURE_RECOVER 472
42.29 ETHOAM_REMOTE_LINK_FAULT 472
42.30 ETHOAM_NO_ENOUGH_RESOURCE 472
42.31 ETHOAM_NOT_CONNECTION_TIMEOUT 473
43 EVB 473
43.1 EVB_AGG_FAILED 473
43.2 EVB_LICENSE_EXPIRE 473
43.3 EVB_VSI_OFFLINE 474
43.4 EVB_VSI_ONLINE 474
44 EVIISIS 474
44.1 EVIISIS_LICENSE 474
44.2 EVIISIS_NBR_CHG 475
45 FCLINK 475
45.1 FCLINK_FDISC_REJECT_NORESOURCE 475
45.2 FCLINK_FLOGI_REJECT_NORESOURCE 476

46 FCOE 476
46.1 FCOE_INTERFACE_NOTSUPPORT_FCOE 476
47 FCZONE 476
47.1 FCZONE_DISTRIBUTE_FAILED 477
47.2 FCZONE_HARDZONE_DISABLED 477
47.3 FCZONE_HARDZONE_ENABLED 478
47.4 FCZONE_ISOLATE_ALLNEIGHBOR 478
47.5 FCZONE_ISOLATE_CLEAR_ALLVSAN 478
47.6 FCZONE_ISOLATE_CLEAR_VSAN 479
47.7 FCZONE_ISOLATE_NEIGHBOR 479
48 FFILTER 479
48.1 FFILTER_IPV4_LOG 480
48.2 FFILTER_IPV6_LOG 481
49 FILTER 482
49.1 FILTER_EXECUTION_ICMP 482
49.2 FILTER_EXECUTION_ICMPV6 483
49.3 FILTER_IPV4_EXECUTION 484
49.4 FILTER_IPV6_EXECUTION 485
49.5 FILTER_ZONE_IPV4_EXECUTION 486
49.6 FILTER_ZONE_IPV4_EXECUTION 487
49.7 FILTER_ZONE_IPV4_EXECUTION 488
49.8 FILTER_ZONE_IPV6_EXECUTION 489
49.9 FILTER_ZONE_IPV6_EXECUTION 490
49.10 FILTER_ZONE_IPV6_EXECUTION 491
49.11 FILTER_ZONE_EXECUTION_ICMP 492
49.12 FILTER_ZONE_EXECUTION_ICMP 493
49.13 FILTER_ZONE_EXECUTION_ICMP 494
49.14 FILTER_ZONE_EXECUTION_ICMPV6 495
49.15 FILTER_ZONE_EXECUTION_ICMPV6 496
49.16 FILTER_ZONE_EXECUTION_ICMPV6 497
50 FIPSNG 497
50.1 FIPSNG_HARD_RESOURCE_NOENOUGH 498
50.2 FIPSNG_HARD_RESOURCE_RESTORE 498
51 FS 498
51.1 FS_UNFORMATTED_PARTITION 498

52 FTP 498
52.1 FTP_ACL_DENY 499
52.2 FTP_REACH_SESSION_LIMIT 499
53 GLB 499
53.1 GLB_SCHED (快速日志) 500
53.2 GLB_SHCED_FAILURE (快速日志) 501
53.3 GLB_SYNCGROUP_CMD_DENY 501
53.4 GLB_SYNCGROUP_MEM_CONNECT 502
53.5 GLB_SYNCGROUP_MEM_DISCONNECT 502
53.6 GLB_SYNCGROUP_MEM_DISCONNECT 502
53.7 GLB_SYNCGROUP_MEM_DISCONNECT 503
53.8 GLB_SYNCGROUP_MEM_DISCONNECT 503
53.9 GLB_SYNCGROUP_MEM_DISCONNECT 503
53.10 GLB_SYNCGROUP_MEM_DISCONNECT 504
53.11 GLB_SYNCGROUP_MEM_DOMAINCONFLICT 504
53.12 GLB_SYNCGROUP_SYNC_CONFLICT 505
54 gRPC 505
54.1 GRPC_ENABLE_WITHOUT_TLS 506
55 HA 506
55.1 HA_BATCHBACKUP_FINISHED 506
55.2 HA_BATCHBACKUP_STARTED 506
55.3 HA_STANDBY_NOT_READY 507
55.4 HA_STANDBY_TO_MASTER 507
56 HLTH 507
56.1 LIPC_COMM_FAULTY 508
56.2 LIPC_COMM_RECOVER 508
57 HQOS 508
57.1 HQOS_DP_SET_FAIL 509
57.2 HQOS_FP_SET_FAIL 509
57.3 HQOS_POLICY_APPLY_FAIL 509
57.4 HQOS_POLICY_RECOVER_FAIL 510
58 HTTPD 510
58.1 HTTPD_CONNECT 510
58.2 HTTPD_CONNECT_TIMEOUT 511
58.3 HTTPD_DISCONNECT 511
58.4 HTTPD_FAIL_FOR_ACL 511

58.5 HTTPD_FAIL_FOR_ACP 512
58.6 HTTPD_REACH_CONNECT_LIMIT 512
59 IDENTITY 512
59.1 IDENTITY_AUTO_IMPORT_FINISHED 512
59.2 IDENTITY_AUTO_IMPORT_START 513
59.3 IDENTITY_CSV_IMPORT_FAILED 513
59.4 IDENTITY_IMC_IMPORT_FAILED_NO_MEMORY 513
59.5 IDENTITY_LDAP_IMPORT_FAILED_NO_MEMORY 514
59.6 IDENTITY_LDAP_IMPORT_GROUP_FAILED 514
59.7 IDENTITY_LDAP_IMPORT_USER_FAILED 515
60 IFNET 515
60.1 IF_JUMBOFRAME_WARN 515
60.2 INTERFACE_NOTSUPPRESSED 516
60.3 INTERFACE_SUPPRESSED 516
60.4 LINK_UPDOWN 516
60.5 PFC_WARNING 517
60.6 PHY_UPDOWN 517
60.7 PROTOCOL_UPDOWN 518
60.8 STORM_CONSTRAIN_BELOW 518
60.9 STORM_CONSTRAIN_CONTROLLED 519
60.10 STORM_CONSTRAIN_EXCEED 519
60.11 STORM_CONSTRAIN_NORMAL 520
60.12 TUNNEL_LINK_UPDOWN 520
60.13 TUNNEL_PHY_UPDOWN 521
60.14 VLAN_MODE_CHANGE 521
61 IKE 521
61.1 IKE_P1_SA_ESTABLISH_FAIL 522
61.2 IKE_P1_SA_TERMINATE 525
61.3 IKE_P2_SA_ESTABLISH_FAIL 527
61.4 IKE_P2_SA_TERMINATE 530
61.5 IKE_XAUTH_FAILE 532
62 IMA 533
62.1 IMA_ALLOCATE_FAILED 533
62.2 IMA_DATA_ERROR 534
62.3 IMA_FILE_HASH_FAILED 534
62.4 IMA_RM_FILE_MISS 534

62.5 IMA_RM_HASH_MISS ····· 535
62.6 IMA_TEMPLATE_ERROR ····· 535
63 IP6ADDR ····· 535
63.1 IP6ADDR_CREATEADDRESS_ERROR ····· 536
64 IPADDR ····· 536
64.1 IPADDR_HA_EVENT_ERROR ····· 537
64.2 IPADDR_HA_STOP_EVENT ····· 539
65 IPOE ····· 539
65.1 IPOE_USER_LOGON_SUCCESS ····· 539
65.2 IPOE_USER_LOGON_FAILED ····· 540
65.3 IPOE_USER_LOGOFF_NORMAL ····· 541
65.4 IPOE_USER_LOGOFF_ABNORMAL ····· 542
66 IPS ····· 543
66.1 IPS_IPV4_INTERZONE（系统日志）（快速日志） ····· 544
66.2 IPS_IPV6_INTERZONE（系统日志）（快速日志） ····· 547
66.3 IPS_WARNING（系统日志） ····· 549
66.4 IPS_WARNING（系统日志） ····· 550
66.5 IPS_WARNING（系统日志） ····· 550
66.6 IPS_WARNING（系统日志） ····· 550
66.7 IPS_WARNING（系统日志） ····· 551
66.8 IPS_WARNING（系统日志） ····· 551
66.9 IPS_WARNING（系统日志） ····· 551
66.10 IPS_WARNING（系统日志） ····· 552
66.11 IPS_WARNING（系统日志） ····· 552
66.12 IPS_WARNING（系统日志） ····· 552
67 IPSEC ····· 552
67.1 IPSEC_DEBUG_LOG ····· 553
67.2 IPSEC_FAILED_ADD_FLOW_TABLE ····· 553
67.3 IPSEC_KD3P_LOGINFO ····· 554
67.4 IPSEC_SA_ESTABLISH ····· 555
67.5 IPSEC_SA_ESTABLISH_FAIL ····· 557
67.6 IPSEC_SA_INITIATION ····· 561
67.7 IPSEC_SA_TERMINATE ····· 562
68 IPSG ····· 563
68.1 IPSG_ADDENTRY_ERROR ····· 563
68.2 IPSG_DELENTRY_ERROR ····· 564

69 IRDP 564
69.1 IRDP_EXCEED_ADVADDR_LIMIT 564
70 IRF 564
70.1 IRF_LINK_BLOCK 565
70.2 IRF_LINK_DOWN 565
70.3 IRF_LINK_UP 565
70.4 IRF_MEMBER_LEFT 566
70.5 IRF_MEMBERID_CONFLICT 566
70.6 IRF_MEMBERID_CONFLICT_REBOOT 566
70.7 IRF_MERGE 567
70.8 IRF_MERGE_NEED_REBOOT 567
70.9 IRF_MERGE_NOT_NEED_REBOOT 567
70.10 IRF_NEWMEMBER_JOIN 568
71 ISIS 568
71.1 ISIS_MEM_ALERT 568
71.2 ISIS_NBR_CHG 568
72 ISSU 569
72.1 ISSU_ROLLBACKCHECKNORMAL 569
72.2 ISSU_SWITCHOVER 569
72.3 ISSU_UPGRADE 570
73 KDNS 570
73.1 KDNS_BIND_PORT_ALLOCETED 571
74 KHTTP 571
74.1 KHTTP_BIND_PORT_ALLOCETED 571
74.2 KHTTP_BIND_ADDRESS_INUSED 572
75 L2PT 572
75.1 L2PT_SET_MULTIMAC_FAILED 572
75.2 L2PT_CREATE_TUNNELGROUP_FAILED 572
75.3 L2PT_ADD_GROUPMEMBER_FAILED 573
75.4 L2PT_ENABLE_DROP_FAILED 573
76 L2TPV2 573
76.1 L2TPV2_TUNNEL_EXCEED_LIMIT 573
76.2 L2TPV2_SESSION_EXCEED_LIMIT 574
77 L2VPN 574
77.1 L2VPN_BGPVC_CONFLICT_LOCAL 574
77.2 L2VPN_BGPVC_CONFLICT_REMOTE 575

77.3 L2VPN_HARD_RESOURCE_NOENOUGH 575
77.4 L2VPN_HARD_RESOURCE_RESTORE 575
77.5 L2VPN_LABEL_DUPLICATE 576
78 L3VPN 576
78.1 L3VPN_VRF_LICENSE_LIMIT 576
79 LAGG 576
79.1 LAGG_ACTIVE 577
79.2 LAGG_INACTIVE_AICFG 577
79.3 LAGG_INACTIVE_BFD 577
79.4 LAGG_INACTIVE_CONFIGURATION 578
79.5 LAGG_INACTIVE_DUPLEX 578
79.6 LAGG_INACTIVE_HARDWAREVALUE 578
79.7 LAGG_INACTIVE_LOWER_LIMIT 579
79.8 LAGG_INACTIVE_PARTNER 579
79.9 LAGG_INACTIVE_PHYSTATE 579
79.10 LAGG_INACTIVE_RESOURCE_INSUFICIE 580
79.11 LAGG_INACTIVE_SPEED 580
79.12 LAGG_INACTIVE_UPPER_LIMIT 580
80 LB 581
80.1 LB_CHANGE_DEFAULTLG_STATE_VS 581
80.2 LB_CHANGE_DEFAULTSF_STATE_VS 581
80.3 LB_CHANGE_DS_HCSTATUS 582
80.4 LB_CHANGE_DS_PROBERESULT 582
80.5 LB_CHANGE_DSQUOTE_HCSTATUS 583
80.6 LB_CHANGE_DSQUOTE_PROBERESULT 583
80.7 LB_CHANGE_LG_STATE_ACTION 584
80.8 LB_CHANGE_LG_STATUS 584
80.9 LB_CHANGE_LINK_BUSY_STATUS 585
80.10 LB_CHANGE_LINK_CONNNUM_OVER 585
80.11 LB_CHANGE_LINK_CONNRATE_OVER 586
80.12 LB_CHANGE_LINK_HCSTATUS 586
80.13 LB_CHANGE_LINK_MEMORY_ALERT 587
80.14 LB_CHANGE_LINK_PROBERESULT 587
80.15 LB_CHANGE_LINK_SHUTDOWN 587
80.16 LB_CHANGE_LINKQUOTE_CONNNUM_OVER 588
80.17 LB_CHANGE_LINKQUOTE_CONNRATE_OVER 588

80.18 LB_CHANGE_LINKQUOTE_HCSTATUS 589
80.19 LB_CHANGE_LINKQUOTE_PROBERESULT 589
80.20 LB_CHANGE_READ_WRITE_STATE_VS 590
80.21 LB_CHANGE_RS_CONNNUM_OVER 590
80.22 LB_CHANGE_RS_CONNRATE_OVER 591
80.23 LB_CHANGE_RS_HCSTATUS 591
80.24 LB_CHANGE_RS_MEMORY_ALERT 592
80.25 LB_CHANGE_RS_MONITORRESULT 592
80.26 LB_CHANGE_RS_PROBERESULT 593
80.27 LB_CHANGE_RS_SHUTDOWN 593
80.28 LB_CHANGE_RSQUOTE_CONNNUM_OVER 594
80.29 LB_CHANGE_RSQUOTE_CONNNUM_RECOVERY 594
80.30 LB_CHANGE_RSQUOTE_CONNRATE_OVER 595
80.31 LB_CHANGE_RSQUOTE_HCSTATUS 595
80.32 LB_CHANGE_RSQUOTE_PROBERESULT 596
80.33 LB_CHANGE_SF_STATE_ACTION 596
80.34 LB_CHANGE_SF_STATUS 597
80.35 LB_CHANGE_VS_CONNNUM_OVER 597
80.36 LB_CHANGE_VS_CONNRATE_OVER 598
80.37 LB_LINK_FLOW 598
80.38 LB_LINK_RECOVERFORM_SHUTDOWN 599
80.39 LB_LINK_STATE_ACTIVE 599
80.40 LB_LINK_STATE_INACTIVE 599
80.41 LB_NAT44_FLOW 600
80.42 LB_NAT46_FLOW 601
80.43 LB_NAT64_FLOW 602
80.44 LB_NAT66_FLOW 603
80.45 LB_PROTECTION_POLICY_CK(快速日志) 604
80.46 LB_PROTECTION_POLICY_IP(快速日志) 604
80.47 LB_RECOVERY_LINK_CONNNUM 605
80.48 LB_RECOVERY_LINK_CONNRATE 605
80.49 LB_RECOVERY_LINKQUOTE_CONNNUM 606
80.50 LB_RECOVERY_LINKQUOTE_CONNRATE 606
80.51 LB_RECOVERY_RS_CONNNUM 607
80.52 LB_RECOVERY_RS_CONNRATE 607
80.53 LB_RECOVERY_RSQUOTE_CONNRATE 608
80.54 LB_RECOVERY_VS_CONNNUM 608

80.55 LB_RECOVERY_VS_CONNRATE 609
80.56 LB_RS_RECOVERFORM_SHUTDOWN 609
80.57 LB_SLB_LICENSE_EXPIRED 609
80.58 LB_SLB_LICENSE_INSTALLED 610
80.59 LB_SLB_LICENSE_UNINSTALLED 610
81 LDP 610
81.1 LDP_MPLSLSRID_CHG 611
81.2 LDP_SESSION_CHG 612
81.3 LDP_SESSION_GR 613
81.4 LDP_SESSION_SP 613
82 LIPC 613
82.1 PORT_CHANGE 614
83 LLDP 614
83.1 LLDP_CREATE_NEIGHBOR 614
83.2 LLDP_DELETE_NEIGHBOR 615
83.3 LLDP_LESS_THAN_NEIGHBOR_LIMIT 615
83.4 LLDP_NEIGHBOR_AGE_OUT 616
83.5 LLDP_NEIGHBOR_AP_RESET 616
83.6 LLDP_PVID_INCONSISTENT 617
83.7 LLDP_REACH_NEIGHBOR_LIMIT 617
84 LOAD 617
84.1 BOARD_LOADING 618
84.2 LOAD_FAILED 618
84.3 LOAD_FINISHED 618
85 LOGIN 619
85.1 LOGIN_ACCOUNTING_FAILED 619
85.2 LOGIN_AUTHORIZATION_FAILED 619
85.3 LOGIN_FAILED 619
85.4 LOGIN_INVALID_USERNAME_PWD 620
85.5 LOGIN_PASSWORD_CHECK_FAILED 620
85.6 LOGIN_RECORD_OBTAIN_FAILED 620
86 LPDT 621
86.1 LPDT_LOOPED 621
86.2 LPDT_RECOVERED 621
86.3 LPDT_VLAN_LOOPED 621
86.4 LPDT_VLAN_RECOVERED 622

87 LS 622
87.1 LOCALSVR_PROMPTED_CHANGE_PWD 622
87.2 LS_ADD_USER_TO_GROUP 623
87.3 LS_AUTHEN_FAILURE 623
87.4 LS_AUTHEN_SUCCESS 624
87.5 LS_DEL_USER_FROM_GROUP 624
87.6 LS_DELETE_PASSWORD_FAIL 624
87.7 LS_PWD_ADDBLACKLIST 625
87.8 LS_PWD_CHGPWD_FOR_AGEDOUT 625
87.9 LS_PWD_CHGPWD_FOR_AGEOUT 625
87.10 LS_PWD_CHGPWD_FOR_COMPOSITION 626
87.11 LS_PWD_CHGPWD_FOR_FIRSTLOGIN 626
87.12 LS_PWD_CHGPWD_FOR_LENGTH 626
87.13 LS_PWD_FAILED2WRITEPASS2FILE 627
87.14 LS_PWD_MODIFY_FAIL 627
87.15 LS_PWD_MODIFY_SUCCESS 628
87.16 LS_REAUTHEN_FAILURE 628
87.17 LS_UPDATE_PASSWORD_FAIL 628
87.18 LS_USER_CANCEL 629
87.19 LS_USER_PASSWORD_EXPIRE 629
87.20 LS_USER_ROLE_CHANGE 629
88 LSPV 630
88.1 LSPV_PING_STATIS_INFO 630
89 MAC 630
89.1 MAC_NOTIFICATION 631
89.2 MAC_TABLE_FULL_GLOBAL 632
89.3 MAC_TABLE_FULL_PORT 632
89.4 MAC_TABLE_FULL_VLAN 632
90 MACA 632
90.1 MACA_ENABLE_NOT_EFFECTIVE 633
90.2 MACA_LOGIN_FAILURE 633
90.3 MACA_LOGIN_SUCC 634
90.4 MACA_LOGOFF 634
91 MACSEC 635
91.1 MACSEC_MKA_KEEPALIVE_TIMEOUT 635
91.2 MACSEC_MKA_PRINCIPAL_ACTOR 635

91.3 MACSEC_MKA_SAK_REFRESH 636
91.4 MACSEC_MKA_SESSION_REAUTH 636
91.5 MACSEC_MKA_SESSION_SECURED 636
91.6 MACSEC_MKA_SESSION_START 637
91.7 MACSEC_MKA_SESSION_STOP 637
91.8 MACSEC_MKA_SESSION_UNSECURED 638
92 MBFD 638
92.1 MBFD_TRACEROUTE_FAILURE 638
93 MBUF 638
93.1 DBL_FREE 639
93.2 MBUF_DATA_BLOCK_CREATE_FAIL 640
93.3 STEPMEM 641
94 MDC 641
94.1 MDC_CREATE_ERR 641
94.2 MDC_CREATE 642
94.3 MDC_DELETE 642
94.4 MDC_KERNEL_EVENT_TOOLONG 642
94.5 MDC_LICENSE_EXPIRE 643
94.6 MDC_NO_FORMAL_LICENSE 643
94.7 MDC_NO_LICENSE_EXIT 643
94.8 MDC_OFFLINE 644
94.9 MDC_ONLINE 644
94.10 MDC_STATE_CHANGE 644
95 MFIB 644
95.1 MFIB_MEM_ALERT 645
96 MGROUP 645
96.1 MGROUP_APPLY_SAMPLER_FAIL 645
96.2 MGROUP_RESTORE_CPUCFG_FAIL 646
96.3 MGROUP_RESTORE_IFCFG_FAIL 646
96.4 MGROUP_SYNC_CFG_FAIL 647
97 MPLS 647
97.1 MPLS_HARD_RESOURCE_NOENOUGH 647
97.2 MPLS_HARD_RESOURCE_RESTORE 647
98 MTLK 648
98.1 MTLK_UPLINK_STATUS_CHANGE 648

99 NAT 648
99.1 NAT_ADDR_BIND_CONFLICT 648
99.2 NAT_ADDRGRP_MEMBER_CONFLICT 649
99.3 NAT_ADDRGRP_RESOURCE_EXHAUST 649
99.4 NAT_FAILED_ADD_FLOW_RULE 649
99.5 NAT_FAILED_ADD_FLOW_TABLE 650
99.6 NAT_FLOW 651
99.7 NAT_INTERFACE_RESOURCE_EXHAUST 652
99.8 NAT_NOPAT_IP_USAGE_ALARM 652
99.9 NAT_PORTBLOCKGRP_ADDRESS_WARNING 653
99.10 NAT_SERVER_INVALID 653
99.11 NAT_SERVICE_CARD_RECOVER_FAILURE 654
99.12 NAT444_PORTBLOCK_USAGE_ALARM 655
100 ND 655
100.1 ND_CONFLICT 655
100.2 ND_DUPADDR 656
100.3 ND_HOST_IP_CONFLICT 656
100.4 ND_MAC_CHECK 657
100.5 ND_SET_PORT_TRUST_NORESOURCE 657
100.6 ND_SET_VLAN_REDIRECT_NORESOURCE 657
100.7 ND_MAXNUM_IF 658
100.8 ND_MAXNUM_DEV 658
101 NETCONF 日志 658
101.1 CLI 659
101.2 EDIT-CONFIG 660
101.3 NETCONF_MSG_DEL 661
101.4 ROW-OPERATION 662
101.5 REPLY 663
101.6 THREAD 663
102 NETSHARE 663
102.1 NETSHARE_IPV4_LOG 664
102.2 NETSHARE_IPV4_LOG 664
102.3 NETSHARE_IPV6_LOG 665
102.4 NETSHARE_IPV6_LOG 665
102.5 NETSHARE_IPV4_BLS_LOG 666
102.6 NETSHARE_IPV6_BLS_LOG 666

103 NQA 666
103.1 NQA_ENTRY_PROBE_RESULT 667
103.2 NQA_LOG_UNREACHABLE 667
103.3 NQA_SCHEDULE_FAILURE 667
103.4 NQA_SET_DRIVE_FAIL 668
103.5 NQA_SEVER_FAILURE 668
103.6 NQA_START_FAILURE 669
103.7 NQA_TWAMP_LIGHT_PACKET_INVALID 669
103.8 NQA_TWAMP_LIGHT_REACTION 670
103.9 NQA_TWAMP_LIGHT_START_FAILURE 670
104 NTP 670
104.1 NTP_CLOCK_CHANGE 671
104.2 NTP_LEAP_CHANGE 671
104.3 NTP_SOURCE_CHANGE 671
104.4 NTP_SOURCE_LOST 672
104.5 NTP_STRATUM_CHANGE 672
105 OBJP 672
105.1 OBJP_ACCELERATE_NO_RES 673
105.2 OBJP_ACCELERATE_NOT_SUPPORT 673
105.3 OBJP_ACCELERATE_UNK_ERR 673
105.4 OBJP_RULE_CREATE_SUCCESS 674
105.5 OBJP_RULE_CREATE_FAIL 674
105.6 OBJP_RULE_UPDATE_SUCCESS 675
105.7 OBJP_RULE_UPDATE_FAIL 676
105.8 OBJP_RULE_DELETE_SUCCESS 676
105.9 OBJP_RULE_DELETE_FAIL 676
105.10 OBJP_RULE_CLRSTAT_SUCCESS 677
105.11 OBJP_RULE_CLRSTAT_FAIL 677
105.12 OBJP_APPLY_POLICY_FAIL 677
105.13 OBJP_APPLAY_INFO 678
106 OFP 678
106.1 OFP_ACTIVE 678
106.2 OFP_ACTIVE_FAILED 678
106.3 OFP_CONNECT 679
106.4 OFP_FAIL_OPEN 679
106.5 OFP_FAIL_OPEN_FAILED 679

106.6 OFP_FLOW_ADD 680
106.7 OFP_FLOW_ADD_DUP 680
106.8 OFP_FLOW_ADD_FAILED 681
106.9 OFP_FLOW_ADD_TABLE_MISS 681
106.10 OFP_FLOW_ADD_TABLE_MISS_FAILED 682
106.11 OFP_FLOW_DEL 682
106.12 OFP_FLOW_DEL_L2VPN_DISABLE 683
106.13 OFP_FLOW_DEL_TABLE_MISS 683
106.14 OFP_FLOW_DEL_TABLE_MISS_FAILED 684
106.15 OFP_FLOW_DEL_VSIIF_DEL 684
106.16 OFP_FLOW_DEL_VXLAN_DEL 685
106.17 OFP_FLOW_MOD 685
106.18 OFP_FLOW_MOD_FAILED 686
106.19 OFP_FLOW_MOD_TABLE_MISS 686
106.20 OFP_FLOW_MOD_TABLE_MISS_FAILED 687
106.21 OFP_FLOW_RMV_GROUP 687
106.22 OFP_FLOW_RMV_HARDTIME 687
106.23 OFP_FLOW_RMV_IDLETIME 688
106.24 OFP_FLOW_RMV_METER 688
106.25 OFP_GROUP_ADD 688
106.26 OFP_GROUP_ADD_FAILED 689
106.27 OFP_GROUP_DEL 689
106.28 OFP_GROUP_MOD 689
106.29 OFP_GROUP_MOD_FAILED 690
106.30 OFP_METER_ADD 690
106.31 OFP_METER_ADD_FAILED 690
106.32 OFP_METER_DEL 691
106.33 OFP_METER_MOD 691
106.34 OFP_METER_MOD_FAILED 691
106.35 OFP_MISS_RMV_GROUP 692
106.36 OFP_MISS_RMV_HARDTIME 692
106.37 OFP_MISS_RMV_IDLETIME 692
106.38 OFP_MISS_RMV_METER 693
107 OPENSRC(RSYNC) 693
107.1 同步成功 693
107.2 同步失败 694

107.3 同步错误 694
108 OPTMOD 694
108.1 BIAS_HIGH 695
108.2 BIAS_LOW 695
108.3 BIAS_NORMAL 695
108.4 CFG_ERR 696
108.5 CHKSUM_ERR 696
108.6 IO_ERR 696
108.7 MOD_ALM_OFF 697
108.8 MOD_ALM_ON 697
108.9 MODULE_IN 697
108.10 MODULE_OUT 698
108.11 PHONY_MODULE 698
108.12 RX_ALM_OFF 698
108.13 RX_ALM_ON 699
108.14 RX_POW_HIGH 699
108.15 RX_POW_LOW 699
108.16 RX_POW_NORMAL 700
108.17 TEMP_HIGH 700
108.18 TEMP_LOW 700
108.19 TEMP_NORMAL 701
108.20 TX_ALM_OFF 701
108.21 TX_ALM_ON 701
108.22 TX_POW_HIGH 702
108.23 TX_POW_LOW 702
108.24 TX_POW_NORMAL 702
108.25 TYPE_ERR 703
108.26 VOLT_HIGH 703
108.27 VOLT_LOW 703
108.28 VOLT_NORMAL 704
109 OSPF 704
109.1 OSPF_DUP_RTRID_NBR 704
109.2 OSPF_IP_CONFLICT_INTRA 705
109.3 OSPF_LAST_NBR_DOWN 705
109.4 OSPF_MEM_ALERT 706
109.5 OSPF_NBR_CHG 706

109.6 OSPF_RT_LMT 706
109.7 OSPF_RTRID_CHG 707
109.8 OSPF_RTRID_CONFLICT_INTER 707
109.9 OSPF_RTRID_CONFLICT_INTRA 707
109.10 OSPF_VLINKID_CHG 708
110 OSPFV3 708
110.1 OSPFV3_LAST_NBR_DOWN 708
110.2 OSPFV3_MEM_ALERT 709
110.3 OSPFV3_NBR_CHG 709
110.4 OSPFV3_RT_LMT 709
111 PBB 710
111.1 PBB_JOINAGG_WARNING 710
112 PBR 710
112.1 PBR_HARDWARE_ERROR 710
113 PCAPWARE 711
113.1 PCAPWARE_STOP 711
114 PCE 711
114.1 PCE_PCEP_SESSION_CHG 712
115 PEX 712
115.1 PEX_CONFIG_ERROR 713
115.2 PEX_CONNECTION_ERROR 713
115.3 PEX_LINK_BLOCK 714
115.4 PEX_LINK_DOWN 714
115.5 PEX_LINK_FORWARD 715
115.6 PEX_REG_JOININ 715
115.7 PEX_REG_LEAVE 716
115.8 PEX_REG_REQUEST 716
116 PFILTER 716
116.1 PFILTER_APPLYUSER_FAIL 717
116.2 PFILTER_GLB_RES_CONFLICT 717
116.3 PFILTER_GLB_IPV4_DACT_NO_RES 718
116.4 PFILTER_GLB_IPV4_DACT_UNK_ERR 718
116.5 PFILTER_GLB_IPV6_DACT_NO_RES 718
116.6 PFILTER_GLB_IPV6_DACT_UNK_ERR 719
116.7 PFILTER_GLB_MAC_DACT_NO_RES 719
116.8 PFILTER_GLB_MAC_DACT_UNK_ERR 719

116.9 PFILTER_GLB_NO_RES 720
116.10 PFILTER_GLB_NOT_SUPPORT 720
116.11 PFILTER_GLB_UNK_ERR 721
116.12 PFILTER_IF_IPV4_DACT_NO_RES 721
116.13 PFILTER_IF_IPV4_DACT_UNK_ERR 721
116.14 PFILTER_IF_IPV6_DACT_NO_RES 722
116.15 PFILTER_IF_IPV6_DACT_UNK_ERR 722
116.16 PFILTER_IF_MAC_DACT_NO_RES 722
116.17 PFILTER_IF_MAC_DACT_UNK_ERR 723
116.18 PFILTER_IF_NO_RES 723
116.19 PFILTER_IF_NOT_SUPPORT 724
116.20 PFILTER_IF_RES_CONFLICT 724
116.21 PFILTER_IF_UNK_ERR 725
116.22 PFILTER_IPV6_STATIS_INFO 725
116.23 PFILTER_STATIS_INFO 726
116.24 PFILTER_VLAN_IPV4_DACT_NO_RES 726
116.25 PFILTER_VLAN_IPV4_DACT_UNK_ERR 726
116.26 PFILTER_VLAN_IPV6_DACT_NO_RES 727
116.27 PFILTER_VLAN_IPV6_DACT_UNK_ERR 727
116.28 PFILTER_VLAN_MAC_DACT_NO_RES 727
116.29 PFILTER_VLAN_MAC_DACT_UNK_ERR 728
116.30 PFILTER_VLAN_NO_RES 728
116.31 PFILTER_VLAN_NOT_SUPPORT 729
116.32 PFILTER_VLAN_RES_CONFLICT 729
116.33 PFILTER_VLAN_UNK_ERR 730
117 PHYD 730
117.1 DRV 730
118 PIM 733
118.1 PIM_NBR_DOWN 733
118.2 PIM_NBR_UP 733
119 PING 733
119.1 PING_STATISTICS 734
119.2 PING_VPN_STATISTICS 735
120 PKI 735
120.1 REQUEST_CERT_FAIL 735
120.2 REQUEST_CERT_SUCCESS 736

121 PKT2CPU 736
121.1 PKT2CPU_NO_RESOURCE 736
122 PKTCPT 736
122.1 PKTCPT_AP_OFFLINE 737
122.2 PKTCPT_AREADY_EXIT 737
122.3 PKTCPT_CONN_FAIL 737
122.4 PKTCPT_INVALID_FILTER 738
122.5 PKTCPT_LOGIN_DENIED 738
122.6 PKTCPT_MEMORY_ALERT 738
122.7 PKTCPT_OPEN_FAIL 739
122.8 PKTCPT_OPERATION_TIMEOUT 739
122.9 PKTCPT_SERVICE_FAIL 739
122.10 PKTCPT_UNKNOWN_ERROR 740
122.11 PKTCPT_UPLOAD_ERROR 740
122.12 PKTCPT_WRITE_FAIL 740
123 PORTAL 741
123.1 PORTAL_USER_LOGOFF 741
123.2 PORTAL_USER_LOGON_FAIL 743
123.3 PORTAL_USER_LOGON_SUCCESS 744
124 PORTSEC 744
124.1 PORTSEC_PORTMODE_NOT_EFFECTIVE 744
124.2 PORTSEC_NTK_NOT_EFFECTIVE 745
125 POSA 745
125.1 POSA_TCPLISTENPORT_NOT_OPEN 745
126 PPP 745
126.1 IPPOOL_ADDRESS_EXHAUSTED 745
126.2 PPPOES_MAC_THROTTLE 746
126.3 PPP_USER_LOGON_SUCCESS 746
126.4 PPP_USER_LOGON_FAILED 747
126.5 PPP_USER_LOGOFF 748
126.6 PPP_USER_LOGOFF_ABNORMAL 749
127 PREPROVISION 750
127.1 PREPROVISION_SLOT_MISMATCH 750
127.2 PREPROVISION_SUBSLOT_MISMATCH 751
128 PTS 751
128.1 PTS_AK_AUTH_FAILED 751

128.2 PTS_AK_INVALID 752
128.3 PTS_AK_NO_CERT 752
128.4 PTS_AK_NO_EXIST 752
128.5 PTS_AK_NO_LOAD 753
128.6 PTS_BTW_PCR_FAILED 753
128.7 PTS_CHECK_RM_VERSION_FAILED 753
128.8 PTS_CREATE_AGED_TIMER_FAILED 754
128.9 PTS_CREATE_CHECK_TIMER_FAILED 754
128.10 PTS_CREATE_CONTEXT_FAILED 754
128.11 PTS_CREATE_EPOLL_FAILED 755
128.12 PTS_CREATE_HASH_FAILED 755
128.13 PTS_CREATE_SELFVERIFY_COUNTER_FAILED 755
128.14 PTS_CREATE_SELFVERIFY_TIMER_FAILED 756
128.15 PTS_CREATE_SOCKET_FAILED 756
128.16 PTS_CREATE_TIMER_FAILED 756
128.17 PTS_FILE_HASH_FAILED 757
128.18 PTS_LOAD_KEY_FAILED 757
128.19 PTS_PARSE_IML_FAILED 757
128.20 PTS_PKG_PCR_FAILED 758
128.21 PTS_READ_PCR_FAILED 758
128.22 PTS_RM_FILE_FAILED 758
128.23 PTS_RUNTIME_PCR_FAILED 759
128.24 PTS_SELFVERIFY_FAILED 759
128.25 PTS_SELFVERIFY_START_FAILED 759
128.26 PTS_TEMPLATE_HASH_FAILED 760
129 PWDCTL 760
129.1 PWDCTL_ADD_BLACKLIST 760
129.2 PWDCTL_CHANGE_PASSWORD 761
129.3 PWDCTL_DELETEBLACLIST 761
129.4 PWDCTL_FAILED_COPYFILE 761
129.5 PWDCTL_FAILED_PROCMSG 762
129.6 PWDCTL_FAILED_TO_WRITEPWD 762
129.7 PWDCTL_LOCKBLACKLIST 762
129.8 PWDCTL_NOTIFYWRITEFILE 763
129.9 PWDCTL_RECFORMATCONV 763
129.10 PWDCTL_UNLOCKBLACKLIST 763

129.11 PWDCTL_UPDATETIME 764
129.12 PWDCTL_USERINLOCKING 764
130 QOS 764
130.1 QOS_AUTHCAR_APPLYUSER_FAIL 764
130.2 QOS_CAR_APPLYUSER_FAIL 765
130.3 QOS_CBWFQ_REMOVED 765
130.4 QOS_GTS_APPLYUSER_FAIL 766
130.5 QOS_NOT_ENOUGH_BANDWIDTH 766
130.6 QOS_POLICY_APPLYCOPP_CBFAIL 767
130.7 QOS_POLICY_APPLYCOPP_FAIL 767
130.8 QOS_POLICY_APPLYGLOBAL_CBFAIL 768
130.9 QOS_POLICY_APPLYGLOBAL_FAIL 768
130.10 QOS_POLICY_APPLYIF_CBFAIL 769
130.11 QOS_POLICY_APPLYIF_FAIL 769
130.12 QOS_POLICY_APPLYUSER_FAIL 770
130.13 QOS_POLICY_APPLYVLAN_CBFAIL 770
130.14 QOS_POLICY_APPLYVLAN_FAIL 771
130.15 QOS_QMPROFILE_APPLYUSER_FAIL 771
130.16 QOS_QMPROFILE_MODIFYQUEUE_FAIL 772
130.17 QOS_POLICY_REMOVE 772
130.18 QOS_POLICY_ACTIVATE 772
131 RADIUS 773
131.1 RADIUS_ACCT_SERVER_DOWN 773
131.2 RADIUS_ACCT_SERVER_UP 773
131.3 RADIUS_AUTH_FAILURE 774
131.4 RADIUS_AUTH_SERVER_DOWN 774
131.5 RADIUS_AUTH_SERVER_UP 775
131.6 RADIUS_AUTH_SUCCESS 775
131.7 RADIUS_REMOVE_SERVER_FAIL 775
132 RBM 776
132.1 CFG_BATCH_SYNC 776
132.2 CFG_BATCH_SYNC 776
132.3 CFG_BATCH_SYNC 776
132.4 CFG_BATCH_SYNC 777
132.5 CFG_COMPARE 777
132.6 CFG_COMPARE 777

132.7 CFG_COMPARE 778
132.8 CFG_COMPARE 778
132.9 DEVICE_ROLE 778
132.10 RBM_CFG_CONFLICT 779
132.11 RBM_CFG_ROLLBCK 779
132.12 RBM_CHANNEL 779
132.13 RBM_CHANNEL 780
132.14 RBM_CHANNEL_BIND_FAILED 780
133 RDDC 780
133.1 RDDC_ACTIVENODE_CHANGE 781
134 REPUTATION 781
134.1 REPUTATION_MATCH_IPV4_LOG 782
134.2 REPUTATION_MATCH_IPV6_LOG 783
135 RIP 784
135.1 RIP_MEM_ALERT 784
135.2 RIP_RT_LMT 784
136 RIPNG 784
136.1 RIPNG_MEM_ALERT 785
136.2 RIPNG_RT_LMT 785
137 RIR 785
137.1 RIR_BANDWIDTH_TOMAXIMUM 785
137.2 RIR_CFG_CHANGED 786
137.3 RIR_LINK_SELECT 786
137.4 RIR_LINKFAULT 787
137.5 RIR_QUALITY_DELAY 787
137.6 RIR_QUALITY_JITTER 788
137.7 RIR_QUALITY_OTHER 788
137.8 RIR_QUALITY_PKTLOSS 789
138 RM 789
138.1 RM_ACRT_REACH_LIMIT 789
138.2 RM_ACRT_REACH_THRESVALUE 790
138.3 RM_THRESHLD_VALUE_REACH 790
139 RPR 790
139.1 RPR_EXCEED_MAX_SEC_MAC 791
139.2 RPR_EXCEED_MAX_SEC_MAC_OVER 791
139.3 RPR_EXCEED_MAX_STATION 791

139.4 RPR_EXCEED_MAX_STATION_OVER 792
139.5 RPR_EXCEED_RESERVED_RATE 792
139.6 RPR_EXCEED_RESERVED_RATE_OVER 792
139.7 RPR_IP_DUPLICATE 793
139.8 RPR_IP_DUPLICATE_OVER 793
139.9 RPR_JUMBO_INCONSISTENT 793
139.10 RPR_JUMBO_INCONSISTENT_OVER 794
139.11 RPR_MISCABLING 794
139.12 RPR_MISCABLING_OVER 794
139.13 RPR_PROTECTION_INCONSISTENT 795
139.14 RPR_PROTECTION_INCONSISTENT_OVER 795
139.15 RPR_SEC_MAC_DUPLICATE 795
139.16 RPR_SEC_MAC_DUPLICATE_OVER 796
139.17 RPR_TOPOLOGY_INCONSISTENT 796
139.18 RPR_TOPOLOGY_INCONSISTENT_OVER 796
139.19 RPR_TOPOLOGY_INSTABILITY 797
139.20 RPR_TOPOLOGY_INSTABILITY_OVER 797
139.21 RPR_TOPOLOGY_INVALID 797
139.22 RPR_TOPOLOGY_INVALID_OVER 798
140 RRPP 798
140.1 RRPP_RING_FAIL 798
140.2 RRPP_RING_RESTORE 798
141 RTM 799
141.1 RTM_TCL_NOT_EXIST 799
141.2 RTM_TCL_MODIFY 799
141.3 RTM_TCL_LOAD_FAILED 799
142 SANDBOX 800
142.1 SANDBOX_DETECTION_IPV4_LOG 801
142.2 SANDBOX_DETECTION_IPV6_LOG 803
143 SCD 807
143.1 SCD_IPV4 808
144 SCMD 808
144.1 PROCESS_ABNORMAL 809
144.2 PROCESS_ACTIVEFAILED 809
144.3 PROCESS_CORERECORD 810
144.4 SCM_ABNORMAL_REBOOT 810

144.5 SCM_ABNORMAL_REBOOTMDC ····· 811
144.6 SCM_ABORT_RESTORE ····· 811
144.7 SCM_INSMOD_ADDON_TOOLONG ····· 812
144.8 SCM_KERNEL_INIT_TOOLONG ····· 812
144.9 SCM_KILL_PROCESS ····· 813
144.10 SCM_PROCESS_STARTING_TOOLONG ····· 814
144.11 SCM_PROCESS_STILL_STARTING ····· 815
144.12 SCM_SKIP_PROCESS ····· 815
145 SCRLSP ····· 816
145.1 SCRLSP_LABEL_DUPLICATE ····· 816
146 SECDIAG ····· 816
146.1 MONITOR_CONCURRENCY_EXCEED ····· 816
146.2 MONITOR_CONCURRENCY_BELOW ····· 817
146.3 MONITOR_CONNECTION_EXCEED ····· 817
146.4 MONITOR_CONNECTION_BELOW ····· 818
146.5 MONITOR_SECP_IPV4_EXCEED ····· 818
146.6 MONITOR_SECP_IPV4_BELOW ····· 818
146.7 MONITOR_SECP_IPV6_EXCEED ····· 819
146.8 MONITOR_SECP_IPV6_BELOW ····· 819
146.9 MONITOR_CONTEXT_EXCEED ····· 819
146.10 MONITOR_CONTEXT_BELOW ····· 820
146.11 MONITOR_NAT_EXCEED ····· 820
146.12 MONITOR_NAT_BELOW ····· 820
146.13 MONITOR_BAGG_EXCEED ····· 821
146.14 MONITOR_BAGG_BELOW ····· 821
146.15 MONITOR_RAGG_EXCEED ····· 821
146.16 MONITOR_RAGG_BELOW ····· 822
146.17 MONITOR_BLADE_THROUGHPUT_EXCEED ····· 822
146.18 MONITOR_BLADE_THROUGHPUT_BELOW ····· 823
146.19 MONITOR_QACL_EXCEED ····· 823
146.20 MONITOR_QACL_BELOW ····· 824
146.21 MONITOR_BANDWIDTH_EXCEED ····· 824
146.22 MONITOR_BANDWIDTH_BELOW ····· 824
147 SECP ····· 824
147.1 SECP_ACCELERATE_NO_RES ····· 825
147.2 SECP_ACCELERATE_NOT_SUPPORT ····· 825

147.3 SECP_ACCELERATE_UNK_ERR 825
148 SESSION 825
148.1 DENY_SESSION_IPV4_FLOW 826
148.2 DENY_SESSION_IPV6_FLOW 827
148.3 SESSION_IPV4_FLOW 828
148.4 SESSION_IPV6_FLOW 830
148.5 SESSION_IPV4_TRAFFIC 831
148.6 SESSION_IPV6_TRAFFIC 832
149 SFLOW 833
149.1 SFLOW_HARDWARE_ERROR 834
150 SHELL 834
150.1 SHELL_CMD 834
150.2 SHELL_CMD_CONFIRM 835
150.3 SHELL_CMD_EXECUTEFAIL 835
150.4 SHELL_CMD_INPUT 836
150.5 SHELL_CMD_INPUT_TIMEOUT 836
150.6 SHELL_CMD_MATCHFAIL 837
150.7 SHELL_CMDDENY 837
150.8 SHELL_CMDFAIL 837
150.9 SHELL_COMMIT 838
150.10 SHELL_COMMIT_DELAY 838
150.11 SHELL_COMMIT_REDELAY 838
150.12 SHELL_COMMIT_ROLLBACK 839
150.13 SHELL_COMMIT_ROLLBACKDONE 839
150.14 SHELL_COMMIT_ROLLBACKFAILED 839
150.15 SHELL_COMMIT_WILLROLLBACK 840
150.16 SHELL_CRITICAL_CMDFAIL 840
150.17 SHELL_LOGIN 840
150.18 SHELL_LOGOUT 841
151 SLSP 841
151.1 SLSP_LABEL_DUPLICATE 841
152 SMLK 841
152.1 SMLK_LINK_SWITCH 842
153 SNMP 842
153.1 AGENTX 842
153.2 SNMP_ACL_RESTRICTION 843

153.3 SNMP_AUTHENTICATION_FAILURE 843
153.4 SNMP_GET 843
153.5 SNMP_INFORM_LOST 844
153.6 SNMP_NOTIFY 845
153.7 SNMP_SET 846
153.8 SNMP_USM_NOTINTIMEWINDOW 846
154 SSH 846
154.1 SSH_WEAK_CIPHER_ALGORITHM 847
154.2 SSH_WEAK_MAC_ALGORITHM 847
155 SSHC 847
155.1 SSHC_ALGORITHM_MISMATCH 847
156 SSHS 848
156.1 SSHS_ACL_DENY 848
156.2 SSHS_ALGORITHM_MISMATCH 848
156.3 SSHS_AUTH_EXCEED_RETRY_TIMES 849
156.4 SSHS_AUTH_FAIL 849
156.5 SSHS_AUTH_TIMEOUT 849
156.6 SSHS_CONNECT 850
156.7 SSHS_DECRYPT_FAIL 850
156.8 SSHS_DISCONNECT 850
156.9 SSHS_ENCRYPT_FAIL 851
156.10 SSHS_LOG 851
156.11 SSHS_MAC_ERROR 851
156.12 SSHS_REACH_SESSION_LIMIT 852
156.13 SSHS_REACH_USER_LIMIT 852
156.14 SSHS_SCP_OPER 852
156.15 SSHS_SFTP_OPER 853
156.16 SSHS_SRV_UNAVAILABLE 853
156.17 SSHS_VERSION_MISMATCH 854
157 SSL VPN 854
157.1 SSLVPN_ADD_CONTENT_TYPE 854
157.2 SSLVPN_ADD_CONTENT_TYPE_FAILED 854
157.3 SSLVPN_ADD_CONTEXT 855
157.4 SSLVPN_ADD_CONTEXT_FAILED 855
157.5 SSLVPN_ADD_EXCROUTEITEM 855
157.6 SSLVPN_ADD_EXCROUTEITEM_FAILED 856

157.7 SSLVPN_ADD_FILEPOLICY ····856
157.8 SSLVPN_ADD_FILEPOLICY_FAILED ····856
157.9 SSLVPN_ADD_GATEWAY ····857
157.10 SSLVPN_ADD_GATEWAY_FAILED ····857
157.11 SSLVPN_ADD_INCROUTEITEM ····857
157.12 SSLVPN_ADD_INCROUTEITEM_FAILED ····858
157.13 SSLVPN_ADD_IPADDRESSPOOL ····858
157.14 SSLVPN_ADD_IPADDRESSPOOL_FAILED ····858
157.15 SSLVPN_ADD_IPTUNNELACIF ····859
157.16 SSLVPN_ADD_IPTUNNELACIF_FAILED ····859
157.17 SSLVPN_ADD_IPV4_RANGE ····859
157.18 SSLVPN_ADD_IPV4_RANGE_FAILED ····860
157.19 SSLVPN_ADD_IPV6_RANGE ····860
157.20 SSLVPN_ADD_IPV6_RANGE_FAILED ····860
157.21 SSLVPN_ADD_LOCALPORT ····861
157.22 SSLVPN_ADD_LOCALPORT_FAILED ····862
157.23 SSLVPN_ADD_NEWCONTENT ····862
157.24 SSLVPN_ADD_NEWCONTENT_FAILED ····863
157.25 SSLVPN_ADD_OLDCONTENT ····863
157.26 SSLVPN_ADD_OLDCONTENT_FAILED ····864
157.27 SSLVPN_ADD_PORTFWD ····864
157.28 SSLVPN_ADD_PORTFWD_FAILED ····864
157.29 SSLVPN_ADD_PORTFWD_ITEM ····865
157.30 SSLVPN_ADD_PORTFWD_ITEM_FAILED ····865
157.31 SSLVPN_ADD_PYGROUP ····865
157.32 SSLVPN_ADD_PYGROUP_FAILED ····866
157.33 SSLVPN_ADD_REFER_PFWDITEM ····866
157.34 SSLVPN_ADD_REFER_PFWDITEM_FAILED ····866
157.35 SSLVPN_ADD_REFER_SCUTLIST ····867
157.36 SSLVPN_ADD_REFERIPACL ····867
157.37 SSLVPN_ADD_REFERIPACL_FAILED ····868
157.38 SSLVPN_ADD_REFERPORTFWD ····868
157.39 SSLVPN_ADD_REFERPORTFWD_FAILED ····869
157.40 SSLVPN_ADD_REFERSCUTLIST_FAILED ····869
157.41 SSLVPN_ADD_REFERSHORTCUT ····869
157.42 SSLVPN_ADD_REFERSHORTCUT_FAILED ····870
157.43 SSLVPN_ADD_REFERSNATPOOL ····870

157.44 SSLVPN_ADD_REFERSNATPOOL_FAILED 870
157.45 SSLVPN_ADD_REFERTCPACL 871
157.46 SSLVPN_ADD_REFERTCPACL_FAILED 871
157.47 SSLVPN_ADD_REFERURIACL 872
157.48 SSLVPN_ADD_REFERURIACL_FAILED 872
157.49 SSLVPN_ADD_REFERURLLIST 873
157.50 SSLVPN_ADD_REFERURLLIST_FAILED 873
157.51 SSLVPN_ADD_REFERWEBACL 874
157.52 SSLVPN_ADD_REFERWEBACL_FAILED 874
157.53 SSLVPN_ADD_REWRITE_RULE 875
157.54 SSLVPN_ADD_REWRITE_RULE_FAILED 875
157.55 SSLVPN_ADD_ROUTELIST 875
157.56 SSLVPN_ADD_ROUTELIST_FAILED 876
157.57 SSLVPN_ADD_ROUTEREFER 876
157.58 SSLVPN_ADD_ROUTEREFER_FAILED 877
157.59 SSLVPN_ADD_SERVERURL 877
157.60 SSLVPN_ADD_SERVERURL_FAILED 878
157.61 SSLVPN_ADD_SHORTCUT 878
157.62 SSLVPN_ADD_SHORTCUT_FAILED 878
157.63 SSLVPN_ADD_SHORTCUTLIST 879
157.64 SSLVPN_ADD_SHORTCUTLIST_FAILED 879
157.65 SSLVPN_ADD_SNATPOOL 879
157.66 SSLVPN_ADD_SNATPOOL_FAILED 880
157.67 SSLVPN_ADD_URIACL 880
157.68 SSLVPN_ADD_URIACL_FAILED 880
157.69 SSLVPN_ADD_URIACL_RULE 881
157.70 SSLVPN_ADD_URIACL_RULE_FAILED 881
157.71 SSLVPN_ADD_URL 881
157.72 SSLVPN_ADD_URL_FAILED 882
157.73 SSLVPN_ADD_URLITEM 882
157.74 SSLVPN_ADD_URLITEM_FAILED 882
157.75 SSLVPN_ADD_URLLIST 883
157.76 SSLVPN_ADD_URLLIST_FAILED 883
157.77 SSLVPN_ADD_USER 883
157.78 SSLVPN_ADD_USER_FAILED 884
157.79 SSLVPN_CFG_AAADOMAIN 884
157.80 SSLVPN_CFG_AAADOMAIN_FAILED 884

157.81 SSLVPN_CFG_AUTHMODE 885
157.82 SSLVPN_CFG_AUTHMODE_FAILED 885
157.83 SSLVPN_CFG_BINDIP 885
157.84 SSLVPN_CFG_BINDIP_FAILED 886
157.85 SSLVPN_CFG_BINDIPAUTO 886
157.86 SSLVPN_CFG_BINDIPAUTO_FAILED 886
157.87 SSLVPN_CFG_CERTATTRIBUTE 887
157.88 SSLVPN_CFG_CERTATTRIBUTE_FAILED 887
157.89 SSLVPN_CFG_CTXUSERMAX 887
157.90 SSLVPN_CFG_CTXUSERMAX_FAILED 888
157.91 SSLVPN_CFG_CONTEXT_USERMAXIMUM 888
157.92 SSLVPN_CFG_CONTEXT_USERMAXIMUM_FAILED 888
157.93 SSLVPN_CFG_CONTEXTVPN 889
157.94 SSLVPN_CFG_CONTEXTVPN_FAILED 889
157.95 SSLVPN_CFG_CTX_WEBPAGECUST_FAIL 889
157.96 SSLVPN_CFG_CTX_WEBPAGECUST 890
157.97 SSLVPN_CFG_CTXGATEWAY 890
157.98 SSLVPN_CFG_CTXGATEWAY_FAILED 891
157.99 SSLVPN_CFG_DEFAULTPGROUP 891
157.100 SSLVPN_CFG_DEFAULTPGROUP_FAILED 892
157.101 SSLVPN_CFG_DNSSERVER 892
157.102 SSLVPN_CFG_DNSSERVER_FAILED 893
157.103 SSLVPN_CFG_EMOSERVER 893
157.104 SSLVPN_CFG_EMOSERVER_FAILED 894
157.105 SSLVPN_CFG_GATEWAYVPN 894
157.106 SSLVPN_CFG_GATEWAYVPN_FAILED 894
157.107 SSLVPN_CFG_GLB_WEBPAGECUST_FAIL 895
157.108 SSLVPN_CFG_GLB_WEBPAGECUST 895
157.109 SSLVPN_CFG_GWIPADDRESS 895
157.110 SSLVPN_CFG_GWIPADDRESS_FAILED 896
157.111 SSLVPN_CFG_GWIPV6ADDRESS 896
157.112 SSLVPN_CFG_GWIPV6ADDRESS_FAILED 897
157.113 SSLVPN_CFG_HTTPREDIRECT 897
157.114 SSLVPN_CFG_HTTPREDIRECT_FAILED 897
157.115 SSLVPN_CFG_IMCADDRESS 898
157.116 SSLVPN_CFG_IMCADDRESS_FAILED 898
157.117 SSLVPN_CFG_IPAC_WEBRESPUSH 898

157.118 SSLVPN_CFG_IPAC_WEBRESPUSH_FAIL ····· 899
157.119 SSLVPN_CFG_IPCLIENT_AUTOACT ····· 899
157.120 SSLVPN_CFG_IPCLIENT_AUTOACT_FAIL ····· 899
157.121 SSLVPN_CFG_IPTNL_RATE-LIMIT ····· 900
157.122 SSLVPN_CFG_IPTNL_RATE-LIMIT_FAIL ····· 900
157.123 SSLVPN_CFG_IPTUNNELPOOL ····· 901
157.124 SSLVPN_CFG_IPTUNNELPOOL_FAILED ····· 901
157.125 SSLVPN_CFG_KEEPALIVE ····· 901
157.126 SSLVPN_CFG_KEEPALIVE_FAILED ····· 902
157.127 SSLVPN_CFG_LOCALPORT ····· 902
157.128 SSLVPN_CFG_LOCALPORT_FAILED ····· 903
157.129 SSLVPN_CFG_LOGINMESSAGE ····· 903
157.130 SSLVPN_CFG_LOGINMESSAGE_FAILED ····· 904
157.131 SSLVPN_CFG_LOGO ····· 904
157.132 SSLVPN_CFG_LOGO_FAILED ····· 905
157.133 SSLVPN_CFG_MAXONLINES ····· 905
157.134 SSLVPN_CFG_MAXONLINES_FAILED ····· 905
157.135 SSLVPN_CFG_MAXUSERS ····· 906
157.136 SSLVPN_CFG_MAXUSERS_FAILED ····· 906
157.137 SSLVPN_CFG_MSGSERVER ····· 906
157.138 SSLVPN_CFG_MSGSERVER_FAILED ····· 907
157.139 SSLVPN_CFG_PFWDEXECUTION ····· 907
157.140 SSLVPN_CFG_PFWDEXECUTION_FAILED ····· 908
157.141 SSLVPN_CFG_SCUTEXECUTION ····· 908
157.142 SSLVPN_CFG_SCUTEXECUTION_FAILED ····· 908
157.143 SSLVPN_CFG_SHORTCUTDESC ····· 909
157.144 SSLVPN_CFG_SHORTCUTDESC_FAILED ····· 909
157.145 SSLVPN_CFG_SSLCLIENT ····· 909
157.146 SSLVPN_CFG_SSLCLIENT_FAILED ····· 910
157.147 SSLVPN_CFG_SSLSERVER ····· 910
157.148 SSLVPN_CFG_SSLSERVER_FAILED ····· 910
157.149 SSLVPN_CFG_TIMEOUTIDLE ····· 911
157.150 SSLVPN_CFG_TIMEOUTIDLE_FAILED ····· 911
157.151 SSLVPN_CFG_TITLE ····· 911
157.152 SSLVPN_CFG_TITLE_FAILED ····· 912
157.153 SSLVPN_CFG_TRAFFICTHRESHOLD ····· 912
157.154 SSLVPN_CFG_TRAFFICTHRESHOLD_FAIL ····· 912

157.155 SSLVPN_CFG_URLLISTHEAD 913
157.156 SSLVPN_CFG_URLLISTHEAD_FAILED 913
157.157 SSLVPN_CFG_WINSSERVER 913
157.158 SSLVPN_CFG_WINSSERVER_FAILED 914
157.159 SSLVPN_CLR_AAADOMAIN 914
157.160 SSLVPN_CLR_AAADOMAIN_FAILED 914
157.161 SSLVPN_CLR_AUTHMODE 915
157.162 SSLVPN_CLR_AUTHMODE_FAILED 915
157.163 SSLVPN_CLR_BINDIP 915
157.164 SSLVPN_CLR_BINDIP_FAILED 916
157.165 SSLVPN_CLR_CERTATTRIBUTE 916
157.166 SSLVPN_CLR_CERTATTRIBUTE_FAILED 916
157.167 SSLVPN_CLR_CONTEXT_USERMAX 917
157.168 SSLVPN_CLR_CONTEXT_USERMAX_FAILED 917
157.169 SSLVPN_CLR_CONTEXTVPN 917
157.170 SSLVPN_CLR_CONTEXTVPN_FAILED 918
157.171 SSLVPN_CLR_CTXGATEWAY 918
157.172 SSLVPN_CLR_CTXGATEWAY_FAILED 918
157.173 SSLVPN_CLR_DEFAULT_PGROUP 919
157.174 SSLVPN_CLR_DEFAULT_PGROUP_FAILED 919
157.175 SSLVPN_CLR_DNSSERVER 919
157.176 SSLVPN_CLR_DNSSERVER_FAILED 920
157.177 SSLVPN_CLR_EMOSERVER 920
157.178 SSLVPN_CLR_EMOSERVER_FAILED 920
157.179 SSLVPN_CLR_GATEWAYVPN 921
157.180 SSLVPN_CLR_GATEWAYVPN_FAILED 921
157.181 SSLVPN_CLR_GWIPADDRESS 921
157.182 SSLVPN_CLR_GWIPADDRESS_FAILED 922
157.183 SSLVPN_CLR_GWIPV6ADDRESS 922
157.184 SSLVPN_CLR_GWIPV6ADDRESS_FAILED 922
157.185 SSLVPN_CLR_HTTPREDIRECT 923
157.186 SSLVPN_CLR_HTTPREDIRECT_FAILED 923
157.187 SSLVPN_CLR_IMCADDRESS 923
157.188 SSLVPN_CLR_IMCADDRESS_FAILED 924
157.189 SSLVPN_CLR_IPAC_WEBRESPUSH 924
157.190 SSLVPN_CLR_IPAC_WEBRESPUSH_FAIL 924
157.191 SSLVPN_CLR_IPCLIENT_AUTOACT 925

157.192 SSLVPN_CLR_IPCLIENT_AUTOACT_FAIL ····925
157.193 SSLVPN_CLR_IPTNL_RATE-LIMIT ····925
157.194 SSLVPN_CLR_IPTNL_RATE-LIMIT_FAIL ····926
157.195 SSLVPN_CLR_IPTUNNELPOOL ····926
157.196 SSLVPN_CLR_IPTUNNELPOOL_FAILED ····926
157.197 SSLVPN_CLR_LOCALPORT ····927
157.198 SSLVPN_CLR_LOCALPORT_FAILED ····927
157.199 SSLVPN_CLR_LOGO ····927
157.200 SSLVPN_CLR_LOGO_FAILED ····928
157.201 SSLVPN_CLR_MSGSERVER ····928
157.202 SSLVPN_CLR_MSGSERVER_FAILED ····928
157.203 SSLVPN_CLR_PFWDEXECUTION ····929
157.204 SSLVPN_CLR_PFWDEXECUTION_FAILED ····929
157.205 SSLVPN_CLR_SCUTDESCRIPTION ····929
157.206 SSLVPN_CLR_SCUTDESCRIPTION_FAILED ····930
157.207 SSLVPN_CLR_SCUTEXECUTION ····930
157.208 SSLVPN_CLR_SCUTEXECUTION_FAILED ····930
157.209 SSLVPN_CLR_SSLCLIENT ····931
157.210 SSLVPN_CLR_SSLCLIENT_FAILED ····931
157.211 SSLVPN_CLR_SSLSERVER ····931
157.212 SSLVPN_CLR_SSLSERVER_FAILED ····932
157.213 SSLVPN_CLR_TRAFFICTHRESHOLD ····932
157.214 SSLVPN_CLR_TRAFFICTHRESHOLD_FAIL ····932
157.215 SSLVPN_CLR_WINSSERVER ····933
157.216 SSLVPN_CLR_WINSSERVER_FAILED ····933
157.217 SSLVPN_DEL_CONTENT_TYPE ····933
157.218 SSLVPN_DEL_CONTENT_TYPE_FAILED ····934
157.219 SSLVPN_DEL_CONTEXT ····934
157.220 SSLVPN_DEL_CONTEXT_FAILED ····934
157.221 SSLVPN_DEL_EXCROUTEITEM ····935
157.222 SSLVPN_DEL_EXCROUTEITEM_FAILED ····935
157.223 SSLVPN_DEL_FILEPOLICY ····935
157.224 SSLVPN_DEL_FILEPOLICY_FAILED ····936
157.225 SSLVPN_DEL_GATEWAY ····936
157.226 SSLVPN_DEL_GATEWAY_FAILED ····936
157.227 SSLVPN_DEL_INCROUTEITEM ····937
157.228 SSLVPN_DEL_INCROUTEITEM_FAILED ····937

157.229 SSLVPN_DEL_IPADDRESSPOOL ····· 937
157.230 SSLVPN_DEL_IPADDRESSPOOL_FAILED ····· 938
157.231 SSLVPN_DEL_IPTUNNELACIF ····· 938
157.232 SSLVPN_DEL_IPTUNNELACIF_FAILED ····· 938
157.233 SSLVPN_DEL_IPV4_RANGE ····· 939
157.234 SSLVPN_DEL_IPV4_RANGE_FAILED ····· 939
157.235 SSLVPN_DEL_IPV6_RANGE ····· 939
157.236 SSLVPN_DEL_IPV6_RANGE_FAILED ····· 940
157.237 SSLVPN_DEL_LOCALPORT ····· 940
157.238 SSLVPN_DEL_LOCALPORT_FAILED ····· 940
157.239 SSLVPN_DEL_NEWCONTENT ····· 941
157.240 SSLVPN_DEL_NEWCONTENT_FAILED ····· 941
157.241 SSLVPN_DEL_OLDCONTENT ····· 941
157.242 SSLVPN_DEL_OLDCONTENT_FAILED ····· 942
157.243 SSLVPN_DEL_PORTFWD ····· 942
157.244 SSLVPN_DEL_PORTFWD_FAILED ····· 942
157.245 SSLVPN_DEL_PORTFWD_ITEM ····· 943
157.246 SSLVPN_DEL_PORTFWD_ITEM_FAILED ····· 943
157.247 SSLVPN_DEL_PYGROUP ····· 943
157.248 SSLVPN_DEL_PYGROUP_FAILED ····· 944
157.249 SSLVPN_DEL_REFERIPACL ····· 944
157.250 SSLVPN_DEL_REFERIPACL_FAILED ····· 944
157.251 SSLVPN_DEL_REFERPFWDITEM ····· 945
157.252 SSLVPN_DEL_REFERPFWDITEM_FAILED ····· 945
157.253 SSLVPN_DEL_REFERPORTFWD ····· 945
157.254 SSLVPN_DEL_REFERPORTFWD_FAILED ····· 946
157.255 SSLVPN_DEL_REFERSCUTLIST ····· 946
157.256 SSLVPN_DEL_REFERSCUTLIST_FAILED ····· 946
157.257 SSLVPN_DEL_REFERSHORTCUT ····· 947
157.258 SSLVPN_DEL_REFERSHORTCUT_FAILED ····· 947
157.259 SSLVPN_DEL_REFERSNATPOOL ····· 947
157.260 SSLVPN_DEL_REFERSNATPOOL_FAILED ····· 948
157.261 SSLVPN_DEL_REFERTCPACL ····· 948
157.262 SSLVPN_DEL_REFERTCPACL_FAILED ····· 948
157.263 SSLVPN_DEL_REFERURIACL ····· 949
157.264 SSLVPN_DEL_REFERURIACL_FAILED ····· 949
157.265 SSLVPN_DEL_REFERURLITEM ····· 950

157.266 SSLVPN_DEL_REFERURLITEM_FAILED ····· 950
157.267 SSLVPN_DEL_REFERURLLIST ····· 950
157.268 SSLVPN_DEL_REFERURLLIST_FAILED ····· 951
157.269 SSLVPN_DEL_REFERWEBACL ····· 951
157.270 SSLVPN_DEL_REFERWEBACL_FAILED ····· 951
157.271 SSLVPN_DEL_REWRITE_RULE ····· 952
157.272 SSLVPN_DEL_REWRITE_RULE_FAILED ····· 952
157.273 SSLVPN_DEL_ROUTELIST ····· 952
157.274 SSLVPN_DEL_ROUTELIST_FAILED ····· 953
157.275 SSLVPN_DEL_ROUTEREFER ····· 953
157.276 SSLVPN_DEL_ROUTEREFER_FAILED ····· 953
157.277 SSLVPN_DEL_SERVERURL ····· 954
157.278 SSLVPN_DEL_SERVERURL_FAILED ····· 954
157.279 SSLVPN_DEL_SHORTCUT ····· 954
157.280 SSLVPN_DEL_SHORTCUT_FAILED ····· 955
157.281 SSLVPN_DEL_SHORTCUTLIST ····· 955
157.282 SSLVPN_DEL_SHORTCUTLIST_FAILED ····· 955
157.283 SSLVPN_DEL_SNATPOOL ····· 956
157.284 SSLVPN_DEL_SNATPOOL_FAILED ····· 956
157.285 SSLVPN_DEL_URIACL ····· 956
157.286 SSLVPN_DEL_URIACL_FAILED ····· 957
157.287 SSLVPN_DEL_URIACL_RULE ····· 957
157.288 SSLVPN_DEL_URIACL_RULE_FAILED ····· 957
157.289 SSLVPN_DEL_URL ····· 958
157.290 SSLVPN_DEL_URL_FAILED ····· 958
157.291 SSLVPN_DEL_URLITEM ····· 958
157.292 SSLVPN_DEL_URLITEM_FAILED ····· 959
157.293 SSLVPN_DEL_URLLIST ····· 959
157.294 SSLVPN_DEL_URLLIST_FAILED ····· 959
157.295 SSLVPN_DEL_URLMAPPING ····· 960
157.296 SSLVPN_DEL_URLMAPPING_FAILED ····· 960
157.297 SSLVPN_DEL_USER ····· 960
157.298 SSLVPN_DEL_USER_FAILED ····· 961
157.299 SSLVPN_DISABLE_CONTEXT ····· 961
157.300 SSLVPN_DISABLE_CONTEXT_FAILED ····· 961
157.301 SSLVPN_DISABLE_CRTAUTH ····· 962
157.302 SSLVPN_DISABLE_CRTAUTH_FAILED ····· 962

157.303 SSLVPN_DISABLE_DYNAMICPWD ····962
157.304 SSLVPN_DISABLE_DYNAMICPWD_FAILED ····963
157.305 SSLVPN_DISABLE_GATEWAY ····963
157.306 SSLVPN_DISABLE_GATEWAY_FAILED ····963
157.307 SSLVPN_DISABLE_GLOBAL_LOG ····964
157.308 SSLVPN_DISABLE_GLOBAL_LOG_FAILED ····964
157.309 SSLVPN_DISABLE_GLOBALURLMASKING ····964
157.310 SSLVPN_DISABLE_GLOBALURLMASKING_FAILED ····965
157.311 SSLVPN_DISABLE_IPTNL_LOG ····965
157.312 SSLVPN_DISABLE_IPTNL_LOG_FAIL ····965
157.313 SSLVPN_DISABLE_PWDAUTH ····966
157.314 SSLVPN_DISABLE_PWDAUTH_FAILED ····966
157.315 SSLVPN_DISABLE_SMSIMC ····966
157.316 SSLVPN_DISABLE_SMSIMC_FAILED ····967
157.317 SSLVPN_DISABLE_URLMASKING ····967
157.318 SSLVPN_DISABLE_URLMASKING_FAILED ····967
157.319 SSLVPN_DISABLE_VERIFYCODE ····968
157.320 SSLVPN_DISABLE_VERIFYCODE_FAILED ····968
157.321 SSLVPN_DOMAIN_URLMAPPING ····968
157.322 SSLVPN_DOMAIN_URLMAPPING_FAILED ····969
157.323 SSLVPN_ENABLE_CONTEXT ····969
157.324 SSLVPN_ENABLE_CONTEXT_FAILED ····969
157.325 SSLVPN_ENABLE_CRTAUTH ····970
157.326 SSLVPN_ENABLE_CRTAUTH_FAILED ····970
157.327 SSLVPN_ENABLE_DYNAMICPWD ····970
157.328 SSLVPN_ENABLE_DYNAMICPWD_FAILED ····971
157.329 SSLVPN_ENABLE_FORCELOGOUT ····971
157.330 SSLVPN_ENABLE_FORCELOGOUT_FAILED ····971
157.331 SSLVPN_ENABLE_GATEWAY ····972
157.332 SSLVPN_ENABLE_GATEWAY_FAILED ····972
157.333 SSLVPN_ENABLE_GLOBAL_LOG ····972
157.334 SSLVPN_ENABLE_GLOBAL_LOG_FAILED ····973
157.335 SSLVPN_ENABLE_GLOBALURLMASKING ····973
157.336 SSLVPN_ENABLE_GLOBALURLMASKING_FAILED ····973
157.337 SSLVPN_ENABLE_IPTNL_LOG ····974
157.338 SSLVPN_ENABLE_IPTNL_LOG_FAIL ····974
157.339 SSLVPN_ENABLE_PWDAUTH ····974

157.340 SSLVPN_ENABLE_PWDAUTH_FAILED 975
157.341 SSLVPN_ENABLE_SMSIMC 975
157.342 SSLVPN_ENABLE_SMSIMC_FAILED 975
157.343 SSLVPN_ENABLE_URLMASKING 976
157.344 SSLVPN_ENABLE_URLMASKING_FAILED 976
157.345 SSLVPN_ENABLE_VERIFYCODE 976
157.346 SSLVPN_ENABLE_VERIFYCODE_FAILED 977
157.347 SSLVPN_IP_RESOURCE_DENY 977
157.348 SSLVPN_IP_RESOURCE_FAILED 977
157.349 SSLVPN_IP_RESOURCE_PERMIT 978
157.350 SSLVPN_IPAC_ALLOC_ADDR_FAIL 978
157.351 SSLVPN_IPAC_ALLOC_ADDR_SUCCESS 979
157.352 SSLVPN_IPAC_CONN_CLOSE 980
157.353 SSLVPN_IPAC_PACKET_DROP 981
157.354 SSLVPN_IPAC_RELEASE_ADDR_SUCCESS 981
157.355 SSLVPN_PORT_URLMAPPING 982
157.356 SSLVPN_PORT_URLMAPPING_FAILED 982
157.357 SSLVPN_SERVICE_UNAVAILABLE 983
157.358 SSLVPN_TCP_RESOURCE_DENY 983
157.359 SSLVPN_TCP_RESOURCE_FAILED 984
157.360 SSLVPN_TCP_RESOURCE_PERMIT 984
157.361 SSLVPN_UNDO_FORCELOGOUT 985
157.362 SSLVPN_UNDO_FORCELOGOUT_FAILED 985
157.363 SSLVPN_URLITEM_ADD_URIACL 985
157.364 SSLVPN_URLITEM_ADD_URIACL_FAILED 986
157.365 SSLVPN_URLITEM_DEL_URIACL 986
157.366 SSLVPN_URLITEM_DEL_URIACL_FAILED 986
157.367 SSLVPN_USER_LOGIN 987
157.368 SSLVPN_USER_LOGINFAILED 987
157.369 SSLVPN_USER_LOGOUT 988
157.370 SSLVPN_USER_NUMBER 988
157.371 SSLVPN_WEB_RESOURCE_DENY 989
157.372 SSLVPN_WEB_RESOURCE_FAILED 989
157.373 SSLVPN_WEB_RESOURCE_PERMIT 990
158 STAMGR 990
158.1 STAMGR_ADD_FAILVLAN 990

158.2 STAMGR_ADDBAC_INFO 991
158.3 STAMGR_ADDSTA_INFO 991
158.4 STAMGR_AUTHORACL_FAILURE 992
158.5 STAMGR_AUTHORUSERPROFILE_FAILURE 993
158.6 STAMGR_BSS_FAILURE 993
158.7 STAMGR_CLIENT_FAILURE 994
158.8 STAMGR_CLIENT_OFFLINE 1002
158.9 STAMGR_CLIENT_ONLINE 1007
158.10 STAMGR_CLIENT_SNOOPING 1008
158.11 STAMGR_DELBAC_INFO 1008
158.12 STAMGR_DELSTA_INFO 1009
158.13 STAMGR_MACA_LOGIN_FAILURE 1010
158.14 STAMGR_MACA_LOGIN_SUCC 1011
158.15 STAMGR_MACA_LOGOFF 1012
158.16 STAMGR_ROAM_FAILED 1014
158.17 STAMGR_ROAM_SUCCESS 1015
158.18 STAMGR_SERVICE_FAILURE 1015
158.19 STAMGR_SERVICE_OFF 1021
158.20 STAMGR_STA_ADDMOB_LKUP_ENDOFIOCTL 1022
158.21 STAMGR_SERVICE_ON 1022
158.22 STAMGR_STAIPCHANGE_INFO 1023
158.23 STAMGR_TRIGGER_IP 1023
159 STM 1023
159.1 STM_AUTO_UPDATE_FAILED 1024
159.2 STM_AUTO_UPDATE_FINISHED 1025
159.3 STM_AUTO_UPDATING 1025
159.4 STM_HELLOPKT_NOTSEND 1026
159.5 STM_HELLOPKT_NOTRCV 1026
159.6 STM_LINK_UP 1026
159.7 STM_LINK_DOWN 1027
159.8 STM_LINK_TIMEOUT 1027
159.9 STM_MERGE 1027
159.10 STM_MERGE_NEED_REBOOT 1028
159.11 STM_MERGE_NOT_NEED_REBOOT 1028
159.12 STM_SAMEMAC 1028
159.13 STM_SOMER_CHECK 1029

160 STP 1029
160.1 STP_BPDU_PROTECTION 1029
160.2 STP_BPDU_RECEIVE_EXPIRY 1029
160.3 STP_CONSISTENCY_RESTORATION 1030
160.4 STP_DETECTED_TC 1030
160.5 STP_DISABLE 1030
160.6 STP_DISCARDING 1031
160.7 STP_ENABLE 1031
160.8 STP_FORWARDING 1031
160.9 STP_LOOP_PROTECTION 1032
160.10 STP_NOT_ROOT 1032
160.11 STP_NOTIFIED_TC 1032
160.12 STP_PORT_TYPE_INCONSISTENCY 1033
160.13 STP_PVID_INCONSISTENCY 1033
160.14 STP_PVST_BPDU_PROTECTION 1033
160.15 STP_ROOT_PROTECTION 1034
160.16 STP_STG_NUM_DETECTION 1034
161 SYSEVENT 1034
161.1 EVENT_TIMEOUT 1035
162 SYSLOG 1035
162.1 ENCODING 1035
162.2 SYSLOG_LOGBUFFER_FAILURE 1036
162.3 SYSLOG_LOGFILE_FULL 1036
162.4 SYSLOG_RESTART 1036
163 TAC 1036
163.1 LB_TAC_AUTH (快速日志) 1037
163.2 LB_TAC_NOTIFY_OFFLINE (快速日志) 1037
163.3 LB_TAC_NOTIFY_PERMISSIONUPDOWN (快速日志) 1038
164 TACACS 1038
164.1 TACACS_ACCT_SERVER_DOWN 1039
164.2 TACACS_ACCT_SERVER_UP 1039
164.3 TACACS_AUTH_FAILURE 1040
164.4 TACACS_AUTH_SERVER_DOWN 1040
164.5 TACACS_AUTH_SERVER_UP 1041
164.6 TACACS_AUTH_SUCCESS 1041
164.7 TACACS_AUTHOR_SERVER_DOWN 1042

164.8 TACACS_AUTHOR_SERVER_UP ····· 1042
164.9 TACACS_REMOVE_SERVER_FAIL ····· 1043
165 TCSM ····· 1043
165.1 TCSM_CERT_BROKEN ····· 1043
165.2 TCSM_KEY_BROKEN ····· 1043
165.3 TCSM_KEY_HIERARCHY_BROKEN ····· 1044
165.4 TCSM_TSS_SVC_DOWN ····· 1044
165.5 TCSM_TSS_SVC_UP ····· 1044
166 TELNETD ····· 1044
166.1 TELNETD_ACL_DENY ····· 1045
166.2 TELNETD_REACH_SESSION_LIMIT ····· 1045
167 TERMINAL ····· 1045
167.1 TERMINAL_CHANGED_LOG_IP ····· 1046
167.2 TERMINAL_CHANGED_LOG_IPV6 ····· 1047
168 TRILL ····· 1047
168.1 TRILL_DUP_SYSTEMID ····· 1048
168.2 TRILL_INTF_CAPABILITY ····· 1048
168.3 TRILL_LICENSE_EXPIRED ····· 1048
168.4 TRILL_MEM_ALERT ····· 1049
168.5 TRILL_NBR_CHG ····· 1049
168.6 TRILL_NO_LICENSE ····· 1049
169 UDPI ····· 1050
169.1 USER-NETLOG ····· 1050
170 UFLT ····· 1050
170.1 UFLT_MATCH_IPV4_LOG（系统日志） ····· 1051
170.2 UFLT_MATCH_IPV6_LOG（系统日志） ····· 1052
170.3 UFLT_NOT_MATCH_IPV4_LOG（系统日志） ····· 1053
170.4 UFLT_NOT_MATCH_IPV6_LOG（系统日志） ····· 1054
170.5 UFLT_WARNING（系统日志） ····· 1055
170.6 UFLT_WARNING（系统日志） ····· 1055
170.7 UFLT_WARNING（系统日志） ····· 1055
170.8 UFLT_WARNING（系统日志） ····· 1056
170.9 UFLT_WARNING（系统日志） ····· 1056
170.10 UFLT_WARNING（系统日志） ····· 1056
170.11 UFLT_MATCH_IPV4_LOG（快速日志） ····· 1057
170.12 UFLT_MATCH_IPV6_LOG（快速日志） ····· 1059

170.13 UFLT_NOT_MATCH_IPV4_LOG（快速日志）……1060
170.14 UFLT_NOT_MATCH_IPV6_LOG（快速日志）……1062
171 VLAN……1063
171.1 VLAN_FAILED……1063
171.2 VLAN_VLANMAPPING_FAILED……1063
171.3 VLAN_VLANSTRIP_REG_DIFF_CONFIG……1063
171.4 VLAN_VLANTRANSPARENT_FAILED……1064
172 VRRP……1064
172.1 VRRP_AUTH_FAILED……1064
172.2 VRRP_CONFIG_ERROR……1065
172.3 VRRP_PACKET_ERROR……1065
172.4 VRRP_STATUS_CHANGE……1066
172.5 VRRP_VF_STATUS_CHANGE……1067
172.6 VRRP_VMAC_INEFFECTIVE……1067
173 VSRP……1067
173.1 VSRP_BIND_FAILED……1068
174 VXLAN……1068
174.1 VXLAN_LICENSE_UNAVAILABLE……1068
175 WAF……1068
175.1 WAF_IPV4_INTERZONE（快速日志）……1069
175.2 WAF_IPV6_INTERZONE（快速日志）……1072
175.3 WAF_WARNING（系统日志）……1075
175.4 WAF_WARNING（系统日志）……1075
175.5 WAF_WARNING（系统日志）……1075
175.6 WAF_WARNING（系统日志）……1076
175.7 WAF_WARNING（系统日志）……1076
176 WEB……1076
176.1 LOGIN……1077
176.2 LOGIN_FAILED……1077
176.3 LOGOUT……1078
177 WEB……1078
177.1 LOGIN……1078
177.2 LOGIN_FAILED……1078
177.3 LOGOUT……1079
178 WEBCACHE……1079
178.1 WEBCACHE_CHECK……1079

178.2 WEBCACHE_AVAILABLE 1079
178.3 WEBCACHE_INAVAILABLE 1080
179 WFF 1080
179.1 WFF_HARDWARE_INIT_FAILED 1080
179.2 WFF_HARDWARE_IPC_FAILED 1080
179.3 WFF_HARDWARE_LOOPBACK_FAILED 1081
179.4 WFF_HARDWARE_PCIE_FAILED 1081
180 WIPS 1081
180.1 APFLOOD 1081
180.2 AP_CHANNEL_CHANGE 1082
180.3 ASSOCIATEOVERFLOW 1082
180.4 HONEYPOT 1082
180.5 HTGREENMODE 1083
180.6 MAN_IN_MIDDLE 1083
180.7 WIPS_DOS 1083
180.8 WIPS_FLOOD 1084
180.9 WIPS_MALF 1085
180.10 WIPS_ROGUE 1086
180.11 WIPS_SPOOF 1086
180.12 WIPS_UNAUTH 1087
180.13 WIPS_WEAKIV 1087
180.14 WIRELESSBRIDGE 1087
181 WLANAUD 1088
181.1 WLANAUD_CLIENT_ONLINE 1088
182 WMESH 1088
182.1 MESH_ACTIVELINK_SWITCH 1089
182.2 MESH_LINKDOWN 1090
182.3 MESH_LINKUP 1091
182.4 MESH_REVOPEN_MAC 1091
183 WRDC 1091
183.1 WRDC_USER_DELETE 1092
183.2 WRDC_USER_OFFLINE 1092
183.3 WRDC_USER_ONLINE 1093
183.4 WRDC_USER_ROAM 1093
184 WSA 1093
184.1 WSA_DEVICE 1094

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。

基于的 Uniware 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 UNIS 网络产品。

1.1 系统日志格式说明

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UNIS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

	• -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	Notice	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
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 快速日志格式说明

1. 日志头格式

快速日志的日志头格式如下：

表1-4 日志头格式表

格式类型	格式		举例
标准格式日志头	<PRI> Timestamp AppName %%10 SN:sn VsysId:id		<134> Apr 28 15:35:32 2020 UNIS %%10 SN:10056879 VsysId:1
定制格式日志头	URL过滤unicom格式	PRI Vision HostName Timestamp AppName MsgID HostName Len	142 1 100.0.0.1 2020 Apr 28 15:35:43 UNIS NAT444:SessionU 57
	NAT cmcc格式	<PRI> Vision HostName Timestamp AppName ProcID MsgID	<142> 1 100.0.0.1 2020 Apr 28 15:35:32 UNIS - NAT444:SessionA
	NAT unicom格式	<PRI> Vision HostName Timestamp AppName ProcID MsgID	<142> 1 100.0.0.1 2020 Apr 28 15:35:43 UNIS - NAT444:SessionA
	NAT telecom格式	<PRI> Vision Timestamp HostName AppName ProcID MsgID	<134> 1 2020 Apr 28 15:35:38 100.0.0.1 UNIS - NAT444:sessionbasedA

2. 字段说明

- PRI：日志类型码。标准格式和 NAT telecom 格式固定为 134；URL 过滤 unicom 格式、NAT cmcc 格式和 NAT unicom 格式固定为 142。
- Timestamp：日志信息产生的时间，方便用户查看和定位系统事件。格式为：YYYY Mon DD hh:mm:ss。
- AppName：生成该日志信息的设备名称。
- %%10：设备的厂家标志。
- SN：设备的序列号。只有执行 **customlog with-sn** 开启携带 SN 功能后才会携带该字段。设备的序列号可通过 **display device manuinfo** 命令中的 DEVICE_SERIAL_NUMBER 字段查看。
- VsysId：产生快速日志的虚拟系统 ID。
- HostName：快速日志输出时使用的源 IPv4 地址。
- MsgID：日志消息类型。

- Len：日志头总长度，单位为字节。
- ProcID：固定为-。

1.3 如何获取日志信息

业务模块将生成的日志发送给信息中心模块，由信息中心模块统一管理。

缺省情况下，设备的信息中心功能处于开启状态，并允许向控制台（console）、监视终端（monitor）、日志缓冲区（logbuffer）、日志主机（loghost）和日志文件（logfile）方向输出日志信息。

通过 **info-center source** 命令可以设置日志信息的输出规则，通过输出规则可以指定日志的输出方向以及对哪些特性模块或信息等级的日志信息进行输出。所有信息等级高于或等于设置等级的日志信息都会被输出到指定的输出方向。例如，输出规则中如果指定允许等级为 6（informational）的信息输出，则等级 0～6 的信息均会被输出到指定的输出方向。

关于信息中心的详细描述请参见“网络管理和监控配置指导”中的“信息中心”。

1.3.1 通过控制台获取日志

用户通过 Console 接口登录设备后，可以在控制台上实时看到设备输出的日志。

1.3.2 通过监视终端获取日志

监视终端是指以 AUX、VTY、TTY 类型用户线登录的用户终端。使用监视终端登录设备后，如需在当前终端上显示日志，还需要进行以下配置：

- 执行 **terminal monitor** 命令打开终端显示功能
- 通过 **terminal logging level** 命令设置在当前终端上显示日志的级别。实际能够在终端上显示的日志级别由 **info-center source** 和 **terminal logging level** 命令共同决定。

terminal monitor 命令和 **terminal logging level** 命令只对当前登录生效，用户重新登录设备后，需要重新配置。

1.3.3 通过日志缓冲区获取日志

通过 **display logbuffer** 命令可以查看日志缓冲区中记录的日志。

1.3.4 通过日志文件获取日志

系统将日志保存到日志文件缓冲区后，用户可以通过以下方式将日志文件缓冲区中的日志保存到日志文件：

- 执行 **logfile save** 命令手动将日志文件缓冲区中的内容全部保存到日志文件。
- 系统周期性将日志文件缓冲区中的内容保存到日志文件。缺省情况下，周期为 24 小时。用户可以通过 **info-center logfile frequency** 命令修改保存周期。

日志文件的缺省保存路径为 cfa0:/logfile/；如果 CF 卡已经分区，则缺省保存路径为 CF 卡第二个分区下的 logfile 目录（cfa1:/logfile/）。

通过 **more** 命令可以查看日志文件的内容。

1.3.5 通过日志主机获取日志

用户配置 **info-center loghost** 命令后，设备会向指定 IP 地址的日志主机发送日志，在日志主机上用户可以查看到设备的日志。如需指定多个日志主机，可多次执行 **info-center loghost** 命令。

请注意：设备上配置的日志主机接收日志信息的端口号必须和日志主机侧的设置一致，否则，日志主机将无法接收日志信息。这个端口号的缺省值为 514。

1.4 软件模块列表

表 1-5 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1-5 软件模块列表

模块名	模块全称
AAA	Authentication, Authorization and Accounting
ACL	Access Control List
ADVPN	Auto Discovery Virtual Private Network
AFT	Address Family Translation
ANCP	Access Node Control Protocol
ANTIVIRUS	Anti-virus
APMGR	Access Point Management
APR	Application Recognition
ARP	Address Resolution Protocol
ASPF	Advanced Stateful Packet Filter
ATK	ATK Detect and Defense
ATM	Asynchronous Transfer Mode
AUDIT	Audit
AUTOCFG	Automatic configuration
AVC	Application Visible Control
BFD	Bidirectional Forwarding Detection
BGP	Border Gateway Protocol
BLS	Blacklist
CC	Challenge Collapsar Defense
CFD	Connectivity Fault Detection
CFGLOG	Configuration log
CFGMAN	Configuration Management
CGROUP	Collaboration Group
CONNLMT	Connect Limit

模块名	模块全称
CONTEXT	Context
DAC	Data Analysis Center
DEV	Device Management
DFILTER	Data Filter
DHCP	Dynamic Host Configuration Protocol
DHCPS	IPv4 DHCP Server
DHCPS6	IPv6 DHCP Server
DHCPSP4	IPv4 DHCP snooping
DHCPSP6	IPv6 DHCP snooping
DIAG	Diagnosis
DLDP	Device Link Detection Protocol
DOT1X	802.1X
EDEV	Extender Device Management
EIGRP	Enhanced Interior Gateway Routing Protocol
ERPS	Ethernet Ring Protection Switching
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
FFILTER	File Filter
FILTER	Filter
FIPSNG	FIP Snooping
FS	File System
FTP	File Transfer Protocol
GLB	Global Load Balance
gRPC	Google Remote Procedure Call
HA	High Availability
HQOS	Hierarchical QoS
HTTPD	Hypertext Transfer Protocol Daemon
IDENTITY	IDENTITY
IFNET	Interface Net Management
IKE	Internet Key Exchange
IMA	Integrity Measurements Architecture

模块名	模块全称
IP6ADDR	IPv6 address
IPADDR	IP address
IPOE	IP Over Ethernet
IPREPUTATION	IP Reputation
IPS	Intrusion Prevention System
IPSEC	IP Security
IPSG	IP Source Guard
IRDP	ICMP Router Discovery Protocol
IRF	Intelligent Resilient Framework
ISIS	Intermediate System-to-Intermediate System
ISSU	In-Service Software Upgrade
KDNS	Kernel Domain Name System
KHTTP	Kernel Hypertext Transfer Protocol
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
LIPC	Leopard Inter-process Communication
LLDP	Link Layer Discovery Protocol
LOAD	Load Management
LOGIN	Login
LPDT	Loopback Detection
LS	Local Server
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

模块名	模块全称
MTLK	Monitor Link
NAT	Network Address Translate
NETCONF	Network Configuration Protocol
NETSHARE	Netshare Control
ND	Neighbor Discovery
NQA	Network Quality Analyzer
NTP	Network Time Protocol
OBJP	Object Policy
OFP	OpenFlow Protocol
OPTMOD	Optical Module
OPENSRC(RSYNC)	Open Source(Remote Synchronize)
OSPF	Open Shortest Path First
OSPFV3	Open Shortest Path First Version 3
PBB	Provider Backbone Bridge
PBR	Policy Based Route
PCAPWARE	Packet Capture Wireshark
PCE	Path Computation Element
PEX	Port Extender
PFILTER	Packet Filter
PHYD	Physical Detection
PIM	Protocol Independent Multicast
PING	Packet Internet Groper
PKI	Public Key Infrastructure
PKT2CPU	Packet to CPU
PKTCPT	Packet Capture
PORTAL	Portal
PORTSEC	Port Security
POSA	Point Of Sales
PPP	Point to Point Protocol
PREPROVISION	Preprovision
PTS	Platform Trust Services
PWDCTL	Password Control
QOS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RBM	Remote Backup Management

模块名	模块全称
RDDC	Redundancy
RIP	Routing Information Protocol
RIPNG	Routing Information Protocol Next Generation
RM	Routing Management
RPR	Resilient Packet Ring
RRPP	Rapid Ring Protect Protocol
RTM	Real-Time Management
SANDBOX	Sandbox
SCD	Server Connection Detection
SCMD	Service Control Manager
SCRLSP	Static CRLSP
SECDIAG	Security Diagnose
SECP	Security Policy
SESSION	Session
SFLOW	Sampler Flow
SHELL	Shell
SLSP	Static LSP
SMLK	Smart Link
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSHC	Secure Shell Client
SSHS	Secure Shell Server
SSL VPN	Secure Sockets Layer Virtual Private Network
STAMGR	Station Management
STM	Stack Topology Management
STP	Spanning Tree Protocol
SYSEVENT	System Event
SYSLOG	System Log
TAC	Trusted Access Control
TCSM	Trusted Computing Services Management
TACACS	Terminal Access Controller Access Control System
TELNETD	Telnet Daemon
TERMINAL	Terminal Identification
TRILL	Transparent Interconnect of Lots of Links
UDPI	User DPI

模块名	模块全称
UFLT	URL Filter
VLAN	Virtual Local Area Network
VRRP	Virtual Router Redundancy Protocol
VSRP	Virtual Service Redundancy Protocol
VXLAN	Virtual eXtensible LAN
WAF	Web Application Firewall
WEB	Web
WEBCACHE	Web Cache
WFF	WLAN Fast Forwarding
WIPS	Wireless Intrusion Prevention System
WLANAUD	WLAN Audit
WMESH	Wireless Mesh
WRDC	Wireless Roaming Data Center
WSA	Wireless Spectrum Analysis

1.5 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 1-6。

表1-6 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_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

3.3 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

3.4 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

3.5 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

3.6 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_DYNRULE_COMMENT

日志内容	The comment of [STRING], which was generated dynamically, can't be added or deleted manually.
参数解释	$1：ACL动态规则信息
日志等级	6
举例	ACL/6/ACL_DYNRULE_COMMENT: The comment of IPv4 ACL 3000 rule 1, which was generated dynamically, can't be added or deleted manually.
日志说明	不支持添加或删除动态规则的描述信息
处理建议	无

3.8 ACL_DYNRULE_MDF

日志内容	[STRING], which was generated dynamically, was deleted or modified manually.
参数解释	$1：ACL动态规则信息
日志等级	5
举例	ACL/5/ACL_DYNRULE_MDF: IPv4 ACL 3000 rule 1, which was generated dynamically, was deleted or modified manually.
日志说明	业务模块运行时动态添加的ACL规则被用户手动删除或者修改
处理建议	用户手动删除或者修改业务模块动态添加的规则时，可能会导致业务模功能异常。需确保删除或修改业务模块动态添加的规则后不影响现网功能

3.9 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	ACL/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

3.10 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

3.11 ACL_RULE_REACH_MAXNUM

日志内容	The maximum of rules in [STRING] ACL [UNIT32] already reached.
参数解释	$1：ACL类型 $2：ACL编号
日志等级	5
举例	ACL/5/ACL_RULE_REACH_MAXNUM:The maximum of rules in IPv4 ACL 3000 already reached.
日志说明	ACL规则数已达到上限，业务模块动态添加规则失败
处理建议	根据ACL规则实际使用情况删除部分无用的规则

3.12 ACL_RULE_SUBID_EXCEED

日志内容	The rule ID in [STRING] ACL [UNIT32] is out of range.
参数解释	$1：ACL类型 $2：ACL编号
日志等级	5
举例	ACL/5/ ACL_RULE_SUBID_EXCEED: The rule ID in IPv4 ACL 3000 is out of range.
日志说明	ACL规则索引已达到上限，业务模块动态添加规则失败
处理建议	业务模块按ACL组实际使用情况调整步长

3.13 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 ADVPN

本节介绍 ADVPN 模块输出的日志信息。

4.1 ADVPN_SESSION_DELETED

日志内容	An ADVPN tunnel was deleted: tunnel interface=[STRING], private addr=[STRING], public addr=[STRING], peer private addr=[STRING], peer public addr=[STRING], type=[STRING], last state=[STRING], last state duration=[STRING], domain name=[STRING], ADVPN group name=[STRING].
参数解释	$1：隧道接口名称 $2：ADVPN隧道的私网地址 $3：ADVPN隧道的公网地址 $4：ADVPN隧道对端的私网地址 $5：ADVPN隧道对端的公网地址 $6：ADVPN隧道类型 $7：ADVPN隧道上一个状态 $8：ADVPN隧道上一个状态的持续时间，为x小时y分z秒（xH yM zS） $9：ADVPN域的名称 $10：ADVPN隧道所使用的组名
日志等级	4
举例	ADVPN/4/ADVPN_SESSION_DELETED: An ADVPN tunnel was deleted: tunnel interface=888, private addr=112.168.60.56, public addr=192.168.60.137,peer private addr=112.168.60.18, peer public addr=192.168.60.11,type=Spoke-Hub, last state=Success, last state duration=0H 8M 8S,domain name=abc, ADVPN group name=
日志说明	ADVPN隧道被删除
处理建议	检查网络状态和配置是否改变

4.2 ADVPN_SESSION_STATE_CHANGED

日志内容	ADVPN tunnel state changed from [STRING] to [STRING]: tunnel interface=[STRING], private addr=[STRING], public addr=[STRING], peer private addr=[STRING], peer public addr=[STRING], type=[STRING], last state=[STRING], last state duration=[STRING], domain name=[STRING], ADVPN group name=[STRING].
参数解释	$1：ADVPN隧道当前状态 $2：ADVPN隧道变化后的状态 $3：隧道接口名称 $2：ADVPN隧道的私网地址 $3：ADVPN隧道的公网地址 $4：ADVPN隧道对端的私网地址 $5：ADVPN隧道对端的公网地址 $6：ADVPN隧道类型 $7：ADVPN隧道上一个状态 $8：ADVPN隧道上一个状态的持续时间，为x小时y分z秒（xH yM zS） $9：ADVPN域的名称 $10：ADVPN隧道所使用的组名
日志等级	4
举例	ADVPN/4/ADVPN_SESSION_STATE_CHANGED: ADVPN tunnel state changed from Establishing to Success: tunnel interface=888, private addr=112.168.60.56, public addr=192.168.60.137,peer private addr=112.168.60.18, peer public addr=192.168.60.11,type=Spoke-Hub, last state=Establishing, last state duration=0H 0M 5S,domain name=abc, ADVPN group name=
日志说明	ADVPN隧道状态发生了变化
处理建议	检查网络状态和配置是否改变

5 AFT

本节介绍 AFT 模块输出的日志信息。

5.1 AFT_V4TOV6_FLOW

日志内容	Protocol(1001)=[STRING];Application(1002)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];AFTSrcIPv6Addr(1005)=[IPADDR];AFTSrcPort(1006)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];AFTDstIPv6Addr(1009)=[IPADDR];AFTDstPort(1010)=[UINT16];InitPktCount(1044)=[UINT32];InitByteCount(1046)=[UINT32];RplyPktCount(1045)=[UINT32];RplyByteCount(1047)=[UINT32];SrcVPNInstance(1042)=[STRING];DstVPNInstance(1043)=[STRING];BeginTime(1013)=[STRING];EndTime(1014)=[STRING];Event(1048)=[STRING].
参数解释	$1：协议类型 $2：应用协议名称 $3：源IP地址 $4：源端口号 $5：AFT转换后的源IPv6地址 $6：AFT转换后的源端口号 $7：目的IP地址 $8：目的端口号 $9：AFT转换后的目的IPv6地址 $10：AFT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：创建会话的时间 $18：会话删除时间 $19：日志类型描述信息 ○ Session created：会话创建日志 ○ Session deleted：会话删除日志
日志等级	6
举例	aft/6/AFT_V4TOV6_FLOW: Protocol(1001)=UDP;Application(1002)=sip;SrcIPAddr(1003)=10.10.10.1;SrcPort(1004)=1024;AFTSrcIPv6Addr(1005)=100::1;AFTSrcPort(1006)=1024;DstIPAddr(1007)=20.20.20.1;DstPort(1008)=21;AFTDstIPv6Addr(1009)=100::1414:1401;AFTDstPort(1010)=21;InitPktCount(1044)=1;InitByteCount(1046)=50;RplyPktCount(1045)=0;RplyByteCount(1047)=0;SrcVPNInstance(1042)=;DstVPNInstance(1043)=;BeginTime(1013)=03182024082546;EndTime(1014)=;Event(1048)=Session created.
日志说明	创建、删除IPv4侧发起的会话时生成该日志
处理建议	无

5.2 AFT_V6TOV4_FLOW

日志内容	Protocol(1001)=[STRING];Application(1002)=[STRING];SrcIPv6Addr(1036)=[IPADDR];SrcPort(1004)=[UINT16];AFTSrcIPAddr(1005)=[IPADDR];AFTSrcPort(1006)=[UINT16];DstIPv6Addr(1037)=[IPADDR];DstPort(1008)=[UINT16];AFTDstIPAddr(1009)=[IPADDR];AFTDstPort(1010)=[UINT16];InitPktCount(1044)=[UINT32];InitByteCount(1046)=[UINT32];RplyPktCount(1045)=[UINT32];RplyByteCount(1047)=[UINT32];SrcVPNInstance(1042)=[STRING];DstVPNInstance(1043)=[STRING];BeginTime(1013)=[STRING];EndTime(1014)=[STRING];Event(1048)=[STRING].
参数解释	$1：协议类型 $2：应用协议名称 $3：源IPv6地址 $4：源端口号 $5：AFT转换后的源IP地址 $6：AFT转换后的源端口号 $7：目的IPv6地址 $8：目的端口号 $9：AFT转换后的目的IP地址 $10：AFT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：创建会话的时间 $18：会话删除时间 $19：日志类型描述信息 ○ Session created：会话创建日志 ○ Session deleted：会话删除日志
日志等级	6
举例	aft/6/AFT_V6TOV4_FLOW: Protocol(1001)=TCP;Application(1002)=general_tcp;SrcIPv6Addr(1036)=100::c613:102;SrcPort(1004)=1024;AFTSrcIPAddr(1005)=101.1.1.14;AFTIPSrcPort(1006)=1025;DstIPv6Addr(1037)=100::6;DstPort(1008)=1025;AFTDstIPAddr(1009)=101.1.1.1;AFTDstPort(1010)=1025;InitPktCount(1044)=1;InitByteCount(1046)=110;RplyPktCount(1047)=0;RplyByteCount(1047)=0;SrcVPNInstance(1042)=;DstVPNInstance(1043)=;BeginTime(1013)=03182024082901;EndTime(1014)=;Event(1048)=Session created.
日志说明	创建、删除IPv6侧发起的会话时生成该日志
处理建议	无

6 ANCP

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

6.1 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

7 ANTIVIRUS

本节介绍防病毒模块输出的日志信息。

7.1 ANTIVIRUS_IPV4_INTERZONE

日志内容	Protocol(1001)=[STRING]; Application(1002)=[STRING]; SrcIPAddr(1003)=[IPADDR]; SrcPort(1004)=[UINT16]; DstIPAddr(1007)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1042)=[STRING]; SrcZoneName(1025)=[STRING]; DstZoneName(1035)=[STRING]; UserName(1113)=[STRING]; PolicyName(1079)=[STRING]; VirusName(1085)=[STRING]; VirusID(1086)=[UINT32]; VirusCategory(1182)=[STRING]; Severity(1087)=[STRING]; MD5(1129)=[STRING]; Action(1053)=[STRING]; HitDirection(1115)=[STRING]; RealSrcIP(1100)=[STRING]; FileName(1097)=[STRING]; FileType(1096)=[STRING]; SrcMacAddr(1021)=[STRING]; DstMacAddr(1022)=[STRING]; RealSrcMacAddr(1204)=[STRING]; RealDstMacAddr(1205)=[STRING];
参数解释	$1：协议类型 $2：应用协议名称 $3：源IP地址 $4：源端口号 $5：目的IP地址 $6：目的端口号 $7：源VPN名称 $8：源安全域名称 $9：目的安全域名称 $10：身份识别用户的名称 $11：策略名称 $12：病毒名称 $13：病毒ID $14：病毒分类 $15：严重级别，包括如下取值： • LOW：低 • MEDIUM：中 • HIGH：高 • CRITICAL：严重 $16：MD5值 $17：动作名称，包括如下取值： • Reset & Logging：阻断并生成日志 • Permit & Logging：允许并生成日志 • Redirect & Logging：重定向并生成日志 $18：命中报文方向，包括如下取值： • original：请求方向 • reply：应答方向 $19：真实源IP地址 $20：文件名 $21：文件类型 $22：源MAC地址 $23：目的MAC地址 $24：真实源MAC地址（仅当开启跨三层MAC地址识别功能后显示取值）

	$25：真实目的MAC地址（仅当开启跨三层MAC地址识别功能后显示取值）
日志等级	4
举例	ANTI-VIR/4/ANTIVIRUS_IPV4_INTERZONE:-Context=1; Protocol(1001)=TCP; Application(1002)=http; SrcIPAddr(1003)=100.10.10.40; SrcPort(1004)=56690; DstIPAddr(1007)=200.10.10.40; DstPort(1008)=80; RcvVPNInstance(1042)=; SrcZoneName(1025)=spf; DstZoneName(1035)=spf; UserName(1113)=abc; PolicyName(1079)=av; VirusName(1085)=MODIFIED-EICAR-Test-File; VirusID(1086)=95; VirusCategory(1182)=Worm; Severity(1087)=MEDIUM; MD5(1129)=d41d8cd98f00b204e9800998ecf8427e; Action(1053)=Reset & Logging; HitDirection(1115)=original; RealSrcIP(1100)=10.10.10.10,20.20.20.20; FileName(1097)=123.pptx; FileType(1096)=pptx; SrcMacAddr(1021)=dc2d-cb01-0001; DstMacAddr(1022)=dc2d-cb93-02ac; RealSrcMacAddr(1204)=; RealDstMacAddr(1205)=;
日志说明	当报文与病毒特征匹配成功时输出该日志
处理建议	无

7.2 ANTIVIRUS_IPV6_INTERZONE

日志内容	Protocol(1001)=[STRING]; Application(1002)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; SrcPort(1004)=[UINT16]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1042)=-[STRING]; SrcZoneName(1025)=[STRING]; DstZoneName(1035)=[STRING]; UserName(1113)=[STRING]; PolicyName(1079)=[STRING]; VirusName(1085)=[STRING]; VirusID(1086)=[UINT32]; VirusCategory(1182)=[STRING]; Severity(1087)=[STRING]; MD5(1129)=[STRING]; Action(1053)=[STRING]; HitDirection(1115)=[STRING]; RealSrcIP(1100)=[STRING]; FileName(1097)=[STRING]; FileType(1096)=[STRING]; SrcMacAddr(1021)=[STRING]; DstMacAddr(1022)=[STRING]; RealSrcMacAddr(1204)=[STRING]; RealDstMacAddr(1205)=[STRING];
参数解释	$1：协议类型 $2：应用协议名称 $3：源IPv6地址 $4：源端口号 $5：目的IPv6地址 $6：目的端口号 $7：源VPN名称 $8：源安全域名称 $9：目的安全域名称 $10：身份识别用户的名称 $11：策略名称 $12：病毒名称 $13：病毒ID $14：病毒分类 $15：严重级别，包括如下取值： • LOW：低 • MEDIUM：中 • HIGH：高 • CRITICAL：严重 $16：MD5值 $17：动作名称，包括如下取值： • Reset & Logging：阻断并生成日志 • Permit & Logging：告警并生成日志 • Redirect & Logging：重定向并生成日志 $18：命中报文方向，包括如下取值： • original：请求方向 • reply：应答方向 $19：真实源IP地址 $20：文件名 $21：文件类型 $22：源MAC地址 $23：目的MAC地址 $24：真实源MAC地址（仅当开启跨三层MAC地址识别功能后显示取值）

	$25：真实目的MAC地址（仅当开启跨三层MAC地址识别功能后显示取值）
日志等级	4
举例	ANTI-VIR/4/ANTIVIRUS_IPV6_INTERZONE:-Context=1; Protocol(1001)=TCP; Application(1002)=http; SrcIPv6Addr(1036)=100::40; SrcPort(1004)=56690; DstIPv6Addr(1037)=200::40; DstPort(1008)=80; RcvVPNInstance(1042)=; SrcZoneName(1025)=spf; DstZoneName(1035)=spf; UserName(1113)=aaa; PolicyName(1079)=av; VirusName(1085)=MODIFIED-EICAR-Test-File; VirusID(1086)=95; VirusCategory(1182)=Worm; Severity(1087)=MEDIUM; MD5(1129)=d41d8cd98f00b204e9800998ecf8427e; Action(1053)=Reset & Logging; HitDirection(1115)=original; RealSrcIP(1100)=10::1; FileName(1097)=123.pptx; FileType(1096)=pptx; SrcMacAddr(1021)=[STRING]; DstMacAddr(1022)=[STRING]; RealSrcMacAddr(1204)=[STRING]; RealDstMacAddr(1205)=[STRING];
日志说明	当IPv6报文与病毒特征匹配成功时输出该日志
处理建议	无

7.3 ANTIVIRUS_WARNING

日志内容	Updated the antivirus signature library successfully.
参数解释	无
日志等级	4
举例	ANTI-VIR/4/ANTIVIRUS_WARNING: -Context=1; Updated the antivirus signature library successfully.
日志说明	防病毒特征库升级成功，包含如下情况： • 立即升级成功 • 本地升级成功
处理建议	无

7.4 ANTIVIRUS_WARNING

日志内容	Rolled back the antivirus signature library successfully.
参数解释	无
日志等级	4
举例	ANTI-VIR/4/ANTIVIRUS_WARNING: -Context=1; Rolled back the antivirus signature library successfully.
日志说明	防病毒特征库回滚成功，包含如下情况： • 回滚到上一个版本成功 • 回滚到出厂版本成功
处理建议	无

7.5 ANTIVIRUS_WARNING

日志内容	Failed to update the antivirus signature library because no valid license was found for the antivirus feature.
参数解释	无
日志等级	4
举例	ANTI-VIR/4/ANTIVIRUS_WARNING: -Context=1; Failed to update the antivirus signature library because no valid license was found for the antivirus feature.
日志说明	没有找到有效的License，防病毒特征库升级失败。包含如下情况： • 立即升级失败 • 本地升级失败（仅在使用 Web 方式进行升级时提示）
处理建议	无

8 APMGR

本节介绍 AP 管理模块输出的日志信息。

8.1 AP_CREATE_FAILURE

日志内容	Failed to create an AP with entity ID [UINT32] and model [STRING]. Reason: Region code is not available.
参数解释	$1：AP ID $2：AP型号
日志等级	6
举例	APMGR/6/AP_CREATE_FAILURE: Failed to create an AP with entity ID 1 and model WA2620i-AGN. Reason: Region code is not available.
日志说明	AP模板创建失败，原因：区域码不可用
处理建议	在全局视图配置区域码

8.2 AP_REBOOT_REASON

日志内容	AP in Run state is rebooting. Reason: The physical status of the radio is down.
参数解释	无
日志等级	6
举例	APMGR/6/AP_REBOOT_REASON: AP in Run state is rebooting. Reason: The physical status of the radio is down.
日志说明	AP射频物理口状态为down，导致AP重启。
处理建议	AP重启后，查看射频口下配置是否正确

8.3 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 dc2d-cb16-28cd.
日志说明	Master AC与BAS AC建立连接
处理建议	无

8.4 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/4/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

8.5 APMGR_AP_ONLINE

日志内容	The AP failed to come online in discovery stage. Reason: AP model [$1] is not supported.
参数解释	$1：AP的型号。
日志等级	6
举例	APMGR/6/APMGR_AP_ONLINE: The AP failed to come online in discovery stage. Reason: AP model wa2620i-AGN is not supported.
日志说明	当AC收到不支持型号的AP发送的上线请求时，提示上线失败，原因为该AP型号不支持。
处理建议	无

8.6 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 dc2d-cb16-28cd.
日志说明	Master AC断开与BAS AC的连接
处理建议	无

8.7 APMGR_GET_AP_MODEL_FAILURE

日志内容	Failed to get an AP model because no region code is configured globally or for AP group [STRING] .
参数解释	$1：AP组名称
日志等级	6
举例	APMGR/6/APMGR_GET_AP_MODEL_FAILURE: Failed to get an AP model because no region code is configured globally or for AP group g2.
日志说明	由于设备上未配置区域码，导致AP组中创建AP型号失败
处理建议	在全局或者当前AP组下配置可用区域码

8.8 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_LOG_ADD_AP_FAIL: AP ap1 failed to come online using serial ID 01247ef96: MAC address dc2d-cb61-5201 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

8.9 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_LOG_LACOFFLINE: 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

8.10 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_LOG_LACONLINE: 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

8.11 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_LOG_MEMALERT: 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

8.12 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

8.13 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_LOG_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

8.14 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_LOG_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

8.15 APMGR_LOG_ONLINE_FAILED

日志内容	[STRING] ([STRING]) failed to come online in join state. Reason: [STRING] ([STRING]) was offline.
参数解释	$1：被管理设备系列名称 $2：被管理设备序列号 $3：管理设备系列名称 $4：管理设备序列号
日志等级	6
举例	• APMGR/6/APMGR_AP_ONLINE_FAILED: WTU (219801A0WA916BQ12535) failed to come online in join state. Reason: WT (219801A11UC173000153) was offline. • APMGR/6/APMGR_AP_ONLINE_FAILED: WAP (219801A0VW916AG00254) failed to come online in join state. Reason: SPM (219801A13DB05B0004350) was offline.
日志说明	• 无线终结者（WT）未上线则无线终结单元（WTU）不能上线 • 智能 PoE 管理器（SPM）在集中管理模式下，SPM 未上线则 WAP 不能上线
处理建议	• 检查 WT 设备未上线原因并使之上线 • 检查 SPM 未上线原因并使之上线

8.16 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

8.17 APMGR_ERROR

日志内容	Failed to install WLAN feature package. Reason: Insufficient hardware resources.
参数解释	无
日志等级	6
举例	APMGR/6/ERROR : Failed to install WLAN feature package. Reason: Insufficient hardware resources.
日志说明	硬件资源耗尽时，无法安装WLAN Feature包
处理建议	手动卸载WLAN Feature包，查找硬件资源耗尽原因，重新安装

8.18 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

8.19 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

8.20 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： • Image was downloaded successfully：版本文件下载成功 • Reset by admin：管理员重启 AP • The radio status was incorrect：AC 和 AP 上的 Radio 状态不一致 • WT was offline：直通模式下，由于 WT 不在线导致的 WTU 重启 • 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: Reset by admin.
日志说明	AP重启及重启原因
处理建议	无

8.21 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

8.22 CWS_IMG_DOWNLOAD_FAILED

日志内容	Failedto download image file[STRING1] for [STRING2] [STRING3].
参数解释	$1：下载文件名 $2：AP或Local AC $3：AP名称或Local AC名称
日志等级	6
举例	CWS/6/CWS_IMG_DOWNLOAD_FAILED: Failed to download image file wa4300.ipe for AP ap1.
日志说明	AP或Local AC下载版本失败
处理建议	无

8.23 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

8.24 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

8.25 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_LOCALAC_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

8.26 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_LOCALAC_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

8.27 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

8.28 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

8.29 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

8.30 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 by admin：管理员重启 AP • WT was offline：直通模式下，由于 WT 不在线导致的 WTU 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 by admin.
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

8.31 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

8.32 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

8.33 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

8.34 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

8.35 CWS_IMG_ OPENFILE_FAILED

日志内容	Failed to open the image file [STRING].
参数解释	$1：AP从AC下载版本的路径
日志等级	3
举例	CWS/3/CWS_IMG_OPENFILE_FAILED: Failed to open the image file slot1#cfa0:/wa5600.ipe.
日志说明	AP打开AC上的版本文件失败
处理建议	无

8.36 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_LOCALAC_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

8.37 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_LOCALAC_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

8.38 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

8.39 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

8.40 RADIO

日志内容	APMGR/6/RADIO: Current channel usage [UINT32] of radio [CHAR] on AP [STRING] exceeded the threshold.
参数解释	$1：当前信道使用率 $2：射频ID $3：AP名称
日志等级	6
举例	APMGR/6/RADIO: Current channel usage 63% of radio 2 on AP ap1 exceeded the threshold.
日志说明	当前信道使用率高于设置的使用率门限值
处理建议	通过channel命令切换低使用率信道

9 APR

本节介绍应用识别模块输出的日志信息。

9.1 NBAR_WARNING

日志内容	Updated the APR signature library successfully.
参数解释	无
日志等级	4
举例	NBAR/4/NBAR_WARNING: -Context=1; Updated the APR signature library successfully..
日志说明	应用识别特征库升级成功，包含如下情况： • 立即升级成功 • 本地升级成功
处理建议	无

9.2 NBAR_WARNING

日志内容	Rolled back the APR signature library successfully.
参数解释	无
日志等级	4
举例	NBAR/4/NBAR_WARNING: -Context=1; Rolled back the APR signature library successfully.
日志说明	应用识别特征库回滚成功，包含如下情况： • 回滚到上一个版本成功 • 回滚到出厂版本成功
处理建议	无

9.3 NBAR_WARNING

日志内容	Failed to update the APR signature library because no valid license was found for the NBAR feature.
参数解释	无
日志等级	4
举例	NBAR/4/NBAR_WARNING: -Context=1; Failed to update the APR signature library because no valid license was found for the NBAR feature.
日志说明	没有找到有效的License，应用识别特征库升级失败。包含如下情况： • 立即升级失败 • 本地升级失败（仅在使用 Web 方式进行升级时提示）
处理建议	无

9.4 NBAR_WARNING

日志内容	Failed to update the APR signature library because the target signature library failed to be downloaded.
参数解释	无
日志等级	4
举例	NBAR/4/NBAR_WARNING: -Context=1; Failed to update the APR signature library because the target signature library failed to be downloaded.
日志说明	未能成功从官网下载特征库，导致特征库升级失败
处理建议	无

10 ARP

本节介绍 ARP 模块输出的日志信息。

10.1 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

10.2 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 GigabitEthernet1/0/1 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

10.3 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 DC2D-CB44-A947, VLAN 1, Gateway MAC DC2D-CB12-1108.
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

10.4 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	6
举例	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	不需处理

10.5 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	6
举例	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

10.6 ARP_DYNAMIC_SLOT

日志内容	The maximum number of dynamic ARP entries for [STRING] reached.
参数解释	$1：槽位号或者成员编号、槽位号
日志等级	6
举例	The maximum number of dynamic ARP entries for slot 2 reached. The maximum number of dynamic ARP entries for chassis 1 slot 2 reached.
日志说明	某槽位上板卡学到的ARP表项总数到达最大值(设备堆叠情况，打印成员编号)，打印该提示信息
处理建议	无需处理

10.7 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

10.8 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 GigabitEthernet1/0/1 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

10.9 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

10.10 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 DC2D-CB14-0E00 was not identical to Ethernet source MAC DC2D-CB14-0E00 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

10.11 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 DC2D-CB14-0E00 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

10.12 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 GigabitEthernet1/0/1.
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

10.13 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 DC2D-CB44-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

10.14 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 DC2D-CB00-0001.
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

10.15 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 DC2D-CB44-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

11 ASPF

本节介绍 ASPF 模块输出的日志信息。

11.1 ASPF_IPV4_DNS

日志内容	SrcIPAddr(1003)=[IPADDR];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];RcvDSLiteTunnelPeer(1040)=[STRING];DomainName(1099)=[STRING];Action(1053)=[STRING];Reason(1056)=[STRING].
参数解释	$1：源IP地址 $2：目的IP地址 $3：VPN实例的名称 $4：DS-Lite隧道本端地址 $5：域名 $6：对检测到的非法协议报文的处理行为，取值包括： o drop：丢弃报文 o logging：生成日志信息 o none：不做处理，放行 $7：日志产生原因，取值包括： o Invalid DNS RR：检测 DNS RR 无效 o Failed to check DNS header flag：检测 DNS 报文头的标志失败 o Failed to check DNS header ID：检测 DNS 报文头的 ID 失败
日志等级	6
举例	ASPF/6/ASPF_IPV4_DNS:SrcIPAddr(1003)=1.1.1.3;DstIPAddr(1007)=2.1.1.2;RcvVPNInstance(1042)=vpn;RcvDSLiteTunnelPeer(1040)=dstunnel1;DomainName(1099)=www.unisyue.com;Action(1053)=drop,logging;Reason(1056)=Check DNS RR invalid.
日志说明	开启DNS协议的ASPF检测，DNS报文格式非法时，丢弃报文并生成日志信息
处理建议	无

11.2 ASPF_IPV6_DNS

日志内容	SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];DomainName(1099)=[STRING];Action(1053)=[STRING];Reason(1056)=[STRING].
参数解释	$1：源IP地址 $2：目的IP地址 $3：VPN实例的名称 $4：域名 $5：对检测到的非法协议报文的处理行为，取值包括： o drop：丢弃报文 o logging：生成日志信息 o none：不做处理，放行 $7：日志产生原因，取值包括： o Invalid DNS RR：检测 DNS RR 无效 o Failed to check DNS header flag：检测 DNS 报文头的标志失败 o Failed to check DNS header ID：检测 DNS 报文头的 ID 失败
日志等级	6
举例	ASPF/6/ASPF_IPV6_DNS:SrcIPv6Addr(1036)=2001::1;DstIPv6Addr(1037)=3001::1;RcvVPNInstance(1042)=vpn;DomainName(1099)=www.unisyue.com;Action(1053)=drop,logging;Reason(1056)=Check DNS RR invalid.
日志说明	开启DNS协议的ASPF检测，DNS报文格式非法时，丢弃报文并生成日志信息
处理建议	无

12 ATK

本节介绍 ATK 模块输出的日志信息。

12.1 ATK_ICMP_ADDRMASK_REQ

日志内容	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：ICMP类型 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $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_ICMP_ADDRMASK_REQ:SubModule(1127)=SINGLE;IcmpType(1062)=17;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=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

12.2 ATK_ICMP_ADDRMASK_REQ_RAW

日志内容	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：ICMP类型 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_ADDRMASK_REQ_RAW:SubModule(1127)=SINGLE;IcmpType(1062)=17;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=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

12.3 ATK_ICMP_ADDRMASK_REQ_RAW_SZ

日志内容	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：ICMP类型 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_ADDRMASK_REQ_RAW_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=17;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=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

12.4 ATK_ICMP_ADDRMASK_REQ_SZ

日志内容	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：ICMP类型 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $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_ICMP_ADDRMASK_REQ_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=17;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=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

12.5 ATK_ICMP_ADDRMASK_RPL

日志内容	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：ICMP类型 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $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_ICMP_ADDRMASK_RPL:SubModule(1127)=SINGLE;IcmpType(1062)=18;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=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

12.6 ATK_ICMP_ADDRMASK_RPL_RAW

日志内容	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：ICMP类型 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_ADDRMASK_RPL_RAW:SubModule(1127)=SINGLE;IcmpType(1062)=18;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=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

12.7 ATK_ICMP_ADDRMASK_RPL_RAW_SZ

日志内容	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：ICMP类型 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_ADDRMASK_RPL_RAW_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=18;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=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

12.8 ATK_ICMP_ADDRMASK_RPL_SZ

日志内容	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：ICMP类型 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $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_ICMP_ADDRMASK_RPL_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=18;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=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

12.9 ATK_ICMP_ECHO_REQ

日志内容	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：ICMP类型 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $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_ICMP_ECHO_REQ:SubModule(1127)=SINGLE;IcmpType(1062)=8;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=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

12.10 ATK_ICMP_ECHO_REQ_RAW

日志内容	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：ICMP类型 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_ECHO_REQ_RAW:SubModule(1127)=SINGLE;IcmpType(1062)=8;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=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

12.11 ATK_ICMP_ECHO_REQ_RAW_SZ

日志内容	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：ICMP类型 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_ECHO_REQ_RAW_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=8;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=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

12.12 ATK_ICMP_ECHO_REQ_SZ

日志内容	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：ICMP类型 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $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_ICMP_ECHO_REQ_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=8;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=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

12.13 ATK_ICMP_ECHO_RPL

日志内容	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：ICMP类型 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $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_ICMP_ECHO_RPL:SubModule(1127)=SINGLE;IcmpType(1062)=0;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=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

12.14 ATK_ICMP_ECHO_RPL_RAW

日志内容	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：ICMP类型 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_ECHO_RPL_RAW:SubModule(1127)=SINGLE;IcmpType(1062)=0;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=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

12.15 ATK_ICMP_ECHO_RPL_RAW_SZ

日志内容	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：ICMP类型 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_ECHO_RPL_RAW_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=0;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=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

12.16 ATK_ICMP_ECHO_RPL_SZ

日志内容	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：ICMP类型 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $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_ICMP_ECHO_RPL_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=0;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=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

12.17 ATK_ICMP_FLOOD

日志内容	RcvIfName(1023)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $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_ICMP_FLOOD:RcvIfName(1023)=GigabitEthernet0/0/2;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=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

12.18 ATK_ICMP_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[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_ICMP_FLOOD_SZ:SrcZoneName(1025)=Trust;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=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

12.19 ATK_ICMP_INFO_REQ

日志内容	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：ICMP类型 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $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_ICMP_INFO_REQ:SubModule(1127)=SINGLE;IcmpType(1062)=15;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=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

12.20 ATK_ICMP_INFO_REQ_RAW

日志内容	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：ICMP类型 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_INFO_REQ_RAW:SubModule(1127)=SINGLE;IcmpType(1062)=15;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=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

12.21 ATK_ICMP_INFO_REQ_RAW_SZ

日志内容	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：ICMP类型 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_INFO_REQ_RAW_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=15;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=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

12.22 ATK_ICMP_INFO_REQ_SZ

日志内容	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：ICMP类型 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $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_ICMP_INFO_REQ_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=15;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=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

12.23 ATK_ICMP_INFO_RPL

日志内容	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：ICMP类型 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $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_ICMP_INFO_RPL:SubModule(1127)=SINGLE;IcmpType(1062)=16;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=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

12.24 ATK_ICMP_INFO_RPL_RAW

日志内容	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：ICMP类型 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_INFO_RPL_RAW:SubModule(1127)=SINGLE;IcmpType(1062)=16;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=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

12.25 ATK_ICMP_INFO_RPL_RAW_SZ

日志内容	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：ICMP类型 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_INFO_RPL_RAW_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=16;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=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

12.26 ATK_ICMP_INFO_RPL_SZ

日志内容	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：ICMP类型 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $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_ICMP_INFO_RPL_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=16;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=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

12.27 ATK_ICMP_LARGE

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel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/3/ATK_ICMP_LARGE:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=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

12.28 ATK_ICMP_LARGE_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel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/3/ATK_ICMP_LARGE_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=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

12.29 ATK_ICMP_LARGE_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel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_LARGE_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=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

12.30 ATK_ICMP_LARGE_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel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/3/ATK_ICMP_LARGE_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=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

12.31 ATK_ICMP_PARAPROBLEM

日志内容	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：ICMP类型 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $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_ICMP_PARAPROBLEM:SubModule(1127)=SINGLE;IcmpType(1062)=12;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=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

12.32 ATK_ICMP_PARAPROBLEM_RAW

日志内容	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：ICMP类型 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_PARAPROBLEM_RAW:SubModule(1127)=SINGLE;IcmpType(1062)=12;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=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

12.33 ATK_ICMP_PARAPROBLEM_RAW_SZ

日志内容	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：ICMP类型 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_PARAPROBLEM_RAW_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=12;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=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

12.34 ATK_ICMP_PARAPROBLEM_SZ

日志内容	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：ICMP类型 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $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_ICMP_PARAPROBLEM_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=12;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=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

12.35 ATK_ICMP_PINGOFDEATH

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel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	3
举例	ATK/3/ATK_ICMP_PINGOFDEATH:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=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(IPoffset*8)+(IPdatalenth)>65535的ICMP报文数超过1，聚合后触发日志
处理建议	无

12.36 ATK_ICMP_PINGOFDEATH_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	3
举例	ATK/3/ATK_ICMP_PINGOFDEATH_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=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(IPoffset*8)+(IPdatalenth)>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(IPoffset*8)+(IPdatalenth)>65535的ICMP报文触发一个日志
处理建议	无

12.37 ATK_ICMP_PINGOFDEATH_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	3
举例	ATK/3/ATK_ICMP_PINGOFDEATH_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=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(IPoffset*8)+(IPdatalenth)>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(IPoffset*8)+(IPdatalenth)>65535的ICMP报文触发一个日志
处理建议	无

12.38 ATK_ICMP_PINGOFDEATH_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel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	3
举例	ATK/3/ATK_ICMP_PINGOFDEATH_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=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(IPoffset*8)+(IPdatalenth)>65535的ICMP报文数超过1，聚合后触发日志
处理建议	无

12.39 ATK_ICMP_REDIRECT

日志内容	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：ICMP类型 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $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_ICMP_REDIRECT:SubModule(1127)=SINGLE;IcmpType(1062)=5;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=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

12.40 ATK_ICMP_REDIRECT_RAW

日志内容	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：ICMP类型 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_REDIRECT_RAW:SubModule(1127)=SINGLE;IcmpType(1062)=5;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=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

12.41 ATK_ICMP_REDIRECT_RAW_SZ

日志内容	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：ICMP类型 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_REDIRECT_RAW_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=5;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=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

12.42 ATK_ICMP_REDIRECT_SZ

日志内容	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：ICMP类型 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $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_ICMP_REDIRECT_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=5;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=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

12.43 ATK_ICMP_SMURF

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel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	3
举例	ATK/3/ATK_ICMP_SMURF:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=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

12.44 ATK_ICMP_SMURF_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	3
举例	ATK/3/ATK_ICMP_SMURF_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=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

12.45 ATK_ICMP_SMURF_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	3
举例	ATK/3/ATK_ICMP_SMURF_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=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

12.46 ATK_ICMP_SMURF_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel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	3
举例	ATK/3/ATK_ICMP_SMURF_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=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

12.47 ATK_ICMP_SOURCEQUENCH

日志内容	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：ICMP类型 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $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_ICMP_SOURCEQUENCH:SubModule(1127)=SINGLE;IcmpType(1062)=4;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=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

12.48 ATK_ICMP_SOURCEQUENCH_RAW

日志内容	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：ICMP类型 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_SOURCEQUENCH_RAW:SubModule(1127)=SINGLE;IcmpType(1062)=4;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=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

12.49 ATK_ICMP_SOURCEQUENCH_RAW_SZ

日志内容	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：ICMP类型 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_SOURCEQUENCH_RAW_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=4;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=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

12.50 ATK_ICMP_SOURCEQUENCH_SZ

日志内容	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：ICMP类型 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $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_ICMP_SOURCEQUENCH_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=4;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=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

12.51 ATK_ICMP_TIMEEXCEED

日志内容	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：ICMP类型 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $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_ICMP_TIMEEXCEED:SubModule(1127)=SINGLE;IcmpType(1062)=11;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=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

12.52 ATK_ICMP_TIMEEXCEED_RAW

日志内容	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：ICMP类型 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_TIMEEXCEED_RAW:SubModule(1127)=SINGLE;IcmpType(1062)=11;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=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

12.53 ATK_ICMP_TIMEEXCEED_RAW_SZ

日志内容	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：ICMP类型 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_TIMEEXCEED_RAW_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=11;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=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

12.54 ATK_ICMP_TIMEEXCEED_SZ

日志内容	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：ICMP类型 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $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_ICMP_TIMEEXCEED_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=11;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=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

12.55 ATK_ICMP_TRACEROUTE

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel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	4
举例	ATK/3/ATK_ICMP_TRACEROUTE:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=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

12.56 ATK_ICMP_TRACEROUTE_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	4
举例	ATK/3/ATK_ICMP_TRACEROUTE_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=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

12.57 ATK_ICMP_TRACEROUTE_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	4
举例	ATK/3/ATK_ICMP_TRACEROUTE_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=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

12.58 ATK_ICMP_TRACEROUTE_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel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	4
举例	ATK/3/ATK_ICMP_TRACEROUTE_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=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

12.59 ATK_ICMP_TSTAMP_REQ

日志内容	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：ICMP类型 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $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_ICMP_TSTAMP_REQ:SubModule(1127)=SINGLE;IcmpType(1062)=13;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=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

12.60 ATK_ICMP_TSTAMP_REQ_RAW

日志内容	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：ICMP类型 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_TSTAMP_REQ_RAW:SubModule(1127)=SINGLE;IcmpType(1062)=13;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=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

12.61 ATK_ICMP_TSTAMP_REQ_RAW_SZ

日志内容	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：ICMP类型 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_TSTAMP_REQ_RAW_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=13;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=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

12.62 ATK_ICMP_TSTAMP_REQ_SZ

日志内容	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：ICMP类型 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $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_ICMP_TSTAMP_REQ_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=13;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=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

12.63 ATK_ICMP_TSTAMP_RPL

日志内容	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：ICMP类型 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $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_ICMP_TSTAMP_RPL:SubModule(1127)=SINGLE;IcmpType(1062)=14;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=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

12.64 ATK_ICMP_TSTAMP_RPL_RAW

日志内容	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：ICMP类型 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_TSTAMP_RPL_RAW:SubModule(1127)=SINGLE;IcmpType(1062)=14;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=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

12.65 ATK_ICMP_TSTAMP_RPL_RAW_SZ

日志内容	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：ICMP类型 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_TSTAMP_RPL_RAW_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=14;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=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

12.66 ATK_ICMP_TSTAMP_RPL_SZ

日志内容	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：ICMP类型 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $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_ICMP_TSTAMP_RPL_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=14;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=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

12.67 ATK_ICMP_TYPE

日志内容	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：ICMP类型 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $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_ICMP_TYPE:SubModule(1127)=SINGLE;IcmpType(1062)=38;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=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

12.68 ATK_ICMP_TYPE_RAW

日志内容	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：ICMP类型 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_TYPE_RAW:SubModule(1127)=SINGLE;IcmpType(1062)=38;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=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

12.69 ATK_ICMP_TYPE_RAW_SZ

日志内容	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：ICMP类型 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_TYPE_RAW_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=38;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=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

12.70 ATK_ICMP_TYPE_SZ

日志内容	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：ICMP类型 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $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_ICMP_TYPE_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=38;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=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

12.71 ATK_ICMP_UNREACHABLE

日志内容	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：ICMP类型 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $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_ICMP_UNREACHABLE:SubModule(1127)=SINGLE;IcmpType(1062)=3;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=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

12.72 ATK_ICMP_UNREACHABLE_RAW

日志内容	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：ICMP类型 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_UNREACHABLE_RAW:SubModule(1127)=SINGLE;IcmpType(1062)=3;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=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

12.73 ATK_ICMP_UNREACHABLE_RAW_SZ

日志内容	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：ICMP类型 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_UNREACHABLE_RAW_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=3;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=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

12.74 ATK_ICMP_UNREACHABLE_SZ

日志内容	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：ICMP类型 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $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_ICMP_UNREACHABLE_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=3;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=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

12.75 ATK_ICMPV6_DEST_UNREACH

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];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：子模块名称 $2：ICMPv6类型 $3：入接口名称 $4：源IPv6地址 $5：目的IPv6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_ICMPV6_DEST_UNREACH:SubModule(1127)=SINGLE;Icmpv6Type(1064)=133;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=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

12.76 ATK_ICMPV6_DEST_UNREACH_RAW

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入接口名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_DEST_UNREACH_RAW:SubModule(1127)=SINGLE;Icmpv6Type(1064)=133;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=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

12.77 ATK_ICMPV6_DEST_UNREACH_RAW_SZ

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入域名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_DEST_UNREACH_RAW_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=133;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=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

12.78 ATK_ICMPV6_DEST_UNREACH_SZ

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];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：子模块名称 $2：ICMPv6类型 $3：入域名称 $4：源IPv6地址 $5：目的IPv6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_ICMPV6_DEST_UNREACH_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=133;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=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

12.79 ATK_ICMPV6_ECHO_REQ

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];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：子模块名称 $2：ICMPv6类型 $3：入接口名称 $4：源IPv6地址 $5：目的IPv6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_ICMPV6_ECHO_REQ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=128;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=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

12.80 ATK_ICMPV6_ECHO_REQ_RAW

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入接口名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_ECHO_REQ_RAW:SubModule(1127)=SINGLE;Icmpv6Type(1064)=128;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=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

12.81 ATK_ICMPV6_ECHO_REQ_RAW_SZ

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入域名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_ECHO_REQ_RAW_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=128;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=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

12.82 ATK_ICMPV6_ECHO_REQ_SZ

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];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：子模块名称 $2：ICMPv6类型 $3：入域名称 $4：源IPv6地址 $5：目的IPv6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_ICMPV6_ECHO_REQ_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=128;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=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

12.83 ATK_ICMPV6_ECHO_RPL

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];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：子模块名称 $2：ICMPv6类型 $3：入接口名称 $4：源IPv6地址 $5：目的IPv6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_ICMPV6_ECHO_RPL:SubModule(1127)=SINGLE;Icmpv6Type(1064)=129;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=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

12.84 ATK_ICMPV6_ECHO_RPL_RAW

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入接口名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_ECHO_RPL_RAW:SubModule(1127)=SINGLE;Icmpv6Type(1064)=129;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=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

12.85 ATK_ICMPV6_ECHO_RPL_RAW_SZ

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入域名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_ECHO_RPL_RAW_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=129;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=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

12.86 ATK_ICMPV6_ECHO_RPL_SZ

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];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：子模块名称 $2：ICMPv6类型 $3：入域名称 $4：源IPv6地址 $5：目的IPv6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_ICMPV6_ECHO_RPL_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=129;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=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

12.87 ATK_ICMPV6_FLOOD

日志内容	RcvIfName(1023)=[STRING];DstIPv6Addr(1037)=[IPADDR];DstPort(1008)=[UINT16];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[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)=GigabitEthernet0/0/2;DstIPv6Addr(1007)=2002::2;DstPort(1008)=22;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=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

12.88 ATK_ICMPV6_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING];DstIPv6Addr(1037)=[IPADDR];DstPort(1008)=[UINT16];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[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(1042)=;UpperLimit(1049)=10;Action(1053)=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

12.89 ATK_ICMPV6_GROUPQUERY

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];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：子模块名称 $2：ICMPv6类型 $3：入接口名称 $4：源IPv6地址 $5：目的IPv6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_ICMPV6_GROUPQUERY:SubModule(1127)=SINGLE;Icmpv6Type(1064)=130;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=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

12.90 ATK_ICMPV6_GROUPQUERY_RAW

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入接口名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_GROUPQUERY_RAW:SubModule(1127)=SINGLE;Icmpv6Type(1064)=130;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=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ICMPV6组播侦听者查询的报文触发一个日志
处理建议	无

12.91 ATK_ICMPV6_GROUPQUERY_RAW_SZ

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入域名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_GROUPQUERY_RAW_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=130;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=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ICMPV6组播侦听者查询的报文触发一个日志
处理建议	无

12.92 ATK_ICMPV6_GROUPQUERY_SZ

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];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：子模块名称 $2：ICMPv6类型 $3：入域名称 $4：源IPv6地址 $5：目的IPv6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_ICMPV6_GROUPQUERY_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=130;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=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

12.93 ATK_ICMPV6_GROUPREDUCTION

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];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：子模块名称 $2：ICMPv6类型 $3：入接口名称 $4：源IPv6地址 $5：目的IPv6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_ICMPV6_GROUPREDUCTION:SubModule(1127)=SINGLE;Icmpv6Type(1064)=132;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=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

12.94 ATK_ICMPV6_GROUPREDUCTION_RAW

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入接口名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_GROUPREDUCTION_RAW:SubModule(1127)=SINGLE;Icmpv6Type(1064)=132;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=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ICMPV6组播侦听者Done的报文触发一个日志
处理建议	无

12.95 ATK_ICMPV6_GROUPREDUCTION_RAW_SZ

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入域名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_GROUPREDUCTION_RAW_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=132;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=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ICMPV6组播侦听者Done的报文触发一个日志
处理建议	无

12.96 ATK_ICMPV6_GROUPREDUCTION_SZ

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];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：子模块名称 $2：ICMPv6类型 $3：入域名称 $4：源IPv6地址 $5：目的IPv6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_ICMPV6_GROUPREDUCTION_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=132;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=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

12.97 ATK_ICMPV6_GROUPREPORT

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];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：子模块名称 $2：ICMPv6类型 $3：入接口名称 $4：源IPv6地址 $5：目的IPv6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_ICMPV6_GROUPREPORT:SubModule(1127)=SINGLE;Icmpv6Type(1064)=131;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=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

12.98 ATK_ICMPV6_GROUPREPORT_RAW

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入接口名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_GROUPREPORT_RAW:SubModule(1127)=SINGLE;Icmpv6Type(1064)=131;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=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ICMPV6组播侦听者报告的报文触发一个日志
处理建议	无

12.99 ATK_ICMPV6_GROUPREPORT_RAW_SZ

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入域名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_GROUPREPORT_RAW_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=131;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=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ICMPV6组播侦听者报告的报文触发一个日志
处理建议	无

12.100 ATK_ICMPV6_GROUPREPORT_SZ

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];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：子模块名称 $2：ICMPv6类型 $3：入域名称 $4：源IPv6地址 $5：目的IPv6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_ICMPV6_GROUPREPORT_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=131;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=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

12.101 ATK_ICMPV6_LARGE

日志内容	SubModule(1127)=SINGLE;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：子模块名称 $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/3/ATK_ICMPV6_LARGE:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=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

12.102 ATK_ICMPV6_LARGE_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $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/3/ATK_ICMPV6_LARGE_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=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ICMPV6超长报文触发一个日志
处理建议	无

12.103 ATK_ICMPV6_LARGE_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $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/3/ATK_ICMPV6_LARGE_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=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ICMPV6超长报文触发一个日志
处理建议	无

12.104 ATK_ICMPV6_LARGE_SZ

日志内容	SubModule(1127)=SINGLE;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：子模块名称 $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/3/ATK_ICMPV6_LARGE_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=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

12.105 ATK_ICMPV6_PACKETTOOBIG

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];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：子模块名称 $2：ICMPv6类型 $3：入接口名称 $4：源IPv6地址 $5：目的IPv6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_ICMPV6_PACKETTOOBIG:SubModule(1127)=SINGLE;Icmpv6Type(1064)=136;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=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

12.106 ATK_ICMPV6_PACKETTOOBIG_RAW

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入接口名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_PACKETTOOBIG_RAW:SubModule(1127)=SINGLE;Icmpv6Type(1064)=136;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=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

12.107 ATK_ICMPV6_PACKETTOOBIG_RAW_SZ

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入域名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_PACKETTOOBIG_RAW_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=136;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=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

12.108 ATK_ICMPV6_PACKETTOOBIG_SZ

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];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：子模块名称 $2：ICMPv6类型 $3：入域名称 $4：源IPv6地址 $5：目的IPv6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_ICMPV6_PACKETTOOBIG_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=136;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=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

12.109 ATK_ICMPV6_PARAPROBLEM

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];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：子模块名称 $2：ICMPv6类型 $3：入接口名称 $4：源IPv6地址 $5：目的IPv6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_ICMPV6_PARAPROBLEM:SubModule(1127)=SINGLE;Icmpv6Type(1064)=135;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=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

12.110 ATK_ICMPV6_PARAPROBLEM_RAW

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入接口名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_PARAPROBLEM_RAW:SubModule(1127)=SINGLE;Icmpv6Type(1064)=135;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=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

12.111 ATK_ICMPV6_PARAPROBLEM_RAW_SZ

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入域名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_PARAPROBLEM_RAW_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=135;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=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

12.112 ATK_ICMPV6_PARAPROBLEM_SZ

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];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：子模块名称 $2：ICMPv6类型 $3：入域名称 $4：源IPv6地址 $5：目的IPv6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_ICMPV6_PARAPROBLEM_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=135;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=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

12.113 ATK_ICMPV6_TIMEEXCEED

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];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：子模块名称 $2：ICMPv6类型 $3：入接口名称 $4：源IPv6地址 $5：目的IPv6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_ICMPV6_TIMEEXCEED:SubModule(1127)=SINGLE;Icmpv6Type(1064)=134;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=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

12.114 ATK_ICMPV6_TIMEEXCEED_RAW

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入接口名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_TIMEEXCEED_RAW:SubModule(1127)=SINGLE;Icmpv6Type(1064)=134;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=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

12.115 ATK_ICMPV6_TIMEEXCEED_RAW_SZ

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入域名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_TIMEEXCEED_RAW_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=134;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=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

12.116 ATK_ICMPV6_TIMEEXCEED_SZ

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];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：子模块名称 $2：ICMPv6类型 $3：入域名称 $4：源IPv6地址 $5：目的IPv6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_ICMPV6_TIMEEXCEED_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=134;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=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

12.117 ATK_ICMPV6_TRACEROUTE

日志内容	SubModule(1127)=SINGLE;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：子模块名称 $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	4
举例	ATK/3/ATK_ICMPV6_TRACEROUTE:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=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

12.118 ATK_ICMPV6_TRACEROUTE_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING].
参数解释	$1：子模块名称 $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	4
举例	ATK/3/ATK_ICMPV6_TRACEROUTE_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=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

12.119 ATK_ICMPV6_TRACEROUTE_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING].
参数解释	$1：子模块名称 $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	4
举例	ATK/3/ATK_ICMPV6_TRACEROUTE_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=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

12.120 ATK_ICMPV6_TRACEROUTE_SZ

日志内容	SubModule(1127)=SINGLE;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：子模块名称 $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	4
举例	ATK/3/ATK_ICMPV6_TRACEROUTE_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=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

12.121 ATK_ICMPV6_TYPE

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];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：子模块名称 $2：ICMPv6类型 $3：入接口名称 $4：源IPv6地址 $5：目的IPv6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_ICMPV6_TYPE:SubModule(1127)=SINGLE;Icmpv6Type(1064)=38;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=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

12.122 ATK_ICMPV6_TYPE_RAW

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入接口名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_TYPE_RAW:SubModule(1127)=SINGLE;Icmpv6Type(1064)=38;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=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

12.123 ATK_ICMPV6_TYPE_RAW_SZ

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：ICMPv6类型 $3：入域名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_TYPE_RAW_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=38;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=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

12.124 ATK_ICMPV6_TYPE_SZ

日志内容	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];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：子模块名称 $2：ICMPv6类型 $3：入域名称 $4：源IPv6地址 $5：目的IPv6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_ICMPV6_TYPE_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=38;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=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

12.125 ATK_IP_OPTION

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：IP选项值 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型 $10：攻击开始时间 $11：攻击结束时间 $12：攻击次数
日志等级	5
举例	ATK/5/ATK_IP_OPTION:SubModule(1127)=SINGLE;IPOptValue(1061)=38;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging;BeginTime_c(1011)=20131011063123;EndTime_c(1012)=20131011063623;AtkTimes(1054)=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

12.126 ATK_IP_OPTION_RAW

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：IP选项值 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型
日志等级	5
举例	ATK/5/ATK_IP_OPTION_RAW:SubModule(1127)=SINGLE;IPOptValue(1061)=38;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=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

12.127 ATK_IP_OPTION_RAW_SZ

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：IP选项值 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型
日志等级	5
举例	ATK/5/ATK_IP_OPTION_RAW_SZ:SubModule(1127)=SINGLE;IPOptValue(1061)=38;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=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

12.128 ATK_IP_OPTION_SZ

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：IP选项值 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型 $10：攻击开始时间 $11：攻击结束时间 $12：攻击次数
日志等级	5
举例	ATK/5/ATK_IP_OPTION_SZ:SubModule(1127)=SINGLE;IPOptValue(1061)=38;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging;BeginTime_c(1011)=20131011063123;EndTime_c(1012)=20131011063623;AtkTimes(1054)=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

12.129 ATK_IP4_ACK_FLOOD

日志内容	RcvIfName(1023)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $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_ACK_FLOOD:RcvIfName(1023)=GigabitEthernet0/0/2;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=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

12.130 ATK_IP4_ACK_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[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_ACK_FLOOD_SZ:SrcZoneName(1025)=Trust;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=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

12.131 ATK_IP4_DIS_PORTSCAN

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];Protocol(1001)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
参数解释	$1：子模块名称 $2：入接口名称 $3：协议名称 $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:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;Protocol(1001)=UDP;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=vpn1;Action(1053)=logging,block-source;BeginTime_c(1011)=20131009052955.
日志说明	报文满足分布式portscan时触发日志
处理建议	无

12.132 ATK_IP4_DIS_PORTSCAN_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];Protocol(1001)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
参数解释	$1：子模块名称 $2：入域名称 $3：协议名称 $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_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;Protocol(1001)=TCP;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=vpn1;Action(1053)=logging,block-source;BeginTime_c(1011)=20131009052955.
日志说明	报文满足分布式portscan时触发日志
处理建议	无

12.133 ATK_IP4_DNS_FLOOD

日志内容	RcvIfName(1023)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $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_DNS_FLOOD:RcvIfName(1023)=GigabitEthernet0/0/2;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009093351.
日志说明	单位时间内向指定目的IP发送DNSQuery的报文数超过阈值，触发日志发送
处理建议	无

12.134 ATK_IP4_DNS_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[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_DNS_FLOOD_SZ:SrcZoneName(1025)=Trust;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009093351.
日志说明	单位时间内向指定目的IP发送DNSQuery的报文数超过阈值，触发日志发送
处理建议	无

12.135 ATK_IP4_FIN_FLOOD

日志内容	RcvIfName(1023)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $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_FIN_FLOOD:RcvIfName(1023)=GigabitEthernet0/0/2;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=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

12.136 ATK_IP4_FIN_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[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_FIN_FLOOD_SZ:SrcZoneName(1025)=Trust;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=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

12.137 ATK_IP4_FRAGMENT

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel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	4
举例	ATK/3/ATK_IP4_FRAGMENT:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=TCP;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=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

12.138 ATK_IP4_FRAGMENT_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel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	4
举例	ATK/3/ATK_IP4_FRAGMENT_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=TCP;Action(1053)=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

12.139 ATK_IP4_FRAGMENT_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel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	4
举例	ATK/3/ATK_IP4_FRAGMENT_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=TCP;Action(1053)=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

12.140 ATK_IP4_FRAGMENT_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel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	4
举例	ATK/3/ATK_IP4_FRAGMENT_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=TCP;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=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

12.141 ATK_IP4_HTTP_FLOOD

日志内容	RcvIfName(1023)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $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_HTTP_FLOOD:RcvIfName(1023)=GigabitEthernet0/0/2;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=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

12.142 ATK_IP4_HTTP_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[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_HTTP_FLOOD_SZ:SrcZoneName(1025)=Trust;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=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

12.143 ATK_IP4_IMPOSSIBLE

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel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	3
举例	ATK/3/ATK_IP4_IMPOSSIBLE:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=TCP;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=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

12.144 ATK_IP4_IMPOSSIBLE_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel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	3
举例	ATK/3/ATK_IP4_IMPOSSIBLE_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=TCP;Action(1053)=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

12.145 ATK_IP4_IMPOSSIBLE_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel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	3
举例	ATK/3/ATK_IP4_IMPOSSIBLE_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=TCP;Action(1053)=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

12.146 ATK_IP4_IMPOSSIBLE_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel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	3
举例	ATK/3/ATK_IP4_IMPOSSIBLE_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=TCP;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=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

12.147 ATK_IP4_IPSWEEP

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];Protocol(1001)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
参数解释	$1：子模块名称 $2：入接口名称 $3：协议名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP4_IPSWEEP:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;Protocol(1001)=TCP;SrcIPAddr(1003)=9.1.1.5;SndDSLiteTunnelPeer(1041)=--;RcvVPNInstance(1042)=vpn1;Action(1053)=logging,block-source;BeginTime_c(1011)=20131009060657.
日志说明	报文满足ipsweep时触发日志
处理建议	无

12.148 ATK_IP4_IPSWEEP_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];Protocol(1001)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
参数解释	$1：子模块名称 $2：入域名称 $3：协议名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP4_IPSWEEP_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;Protocol(1001)=TCP;SrcIPAddr(1003)=9.1.1.5;SndDSLiteTunnelPeer(1041)=--;RcvVPNInstance(1042)=vpn1;Action(1053)=logging,block-source;BeginTime_c(1011)=20131009060657.
日志说明	报文满足ipsweep时触发日志
处理建议	无

12.149 ATK_IP4_PORTSCAN

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];Protocol(1001)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];RcvVPNInstance(1042)=[STRING];DstIPAddr(1007)=[IPADDR];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
参数解释	$1：子模块名称 $2：入接口名称 $3：协议名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：VPN名称 $7：目的IP地址 $8：动作类型 $9：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP4_PORTSCAN:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;Protocol(1001)=TCP;SrcIPAddr(1003)=9.1.1.5;SndDSLiteTunnelPeer(1041)=--;RcvVPNInstance(1042)=vpn1;DstIPAddr(1007)=6.1.1.5;Action(1053)=logging,block-source;BeginTime_c(1011)=20131009052955.
日志说明	报文满足portscan时触发日志
处理建议	无

12.150 ATK_IP4_PORTSCAN_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];Protocol(1001)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];RcvVPNInstance(1042)=[STRING];DstIPAddr(1007)=[IPADDR];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
参数解释	$1：子模块名称 $2：入域名称 $3：协议名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：VPN名称 $7：目的IP地址 $8：动作类型 $9：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP4_PORTSCAN_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;Protocol(1001)=TCP;SrcIPAddr(1003)=9.1.1.5;SndDSLiteTunnelPeer(1041)=--;RcvVPNInstance(1042)=vpn1;DstIPAddr(1007)=6.1.1.5;Action(1053)=logging,block-source;BeginTime_c(1011)=20131009052955.
日志说明	报文满足portscan时触发日志
处理建议	无

12.151 ATK_IP4_RST_FLOOD

日志内容	RcvIfName(1023)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $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_RST_FLOOD:RcvIfName(1023)=GigabitEthernet0/0/2;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=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

12.152 ATK_IP4_RST_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[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_RST_FLOOD_SZ:SrcZoneName(1025)=Trust;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=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

12.153 ATK_IP4_SLOW_ATTACK

日志内容	RcvIfName(1023)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $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_SLOW_ATTACK:RcvIfName(1023)=GigabitEthernet0/0/2;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009093351.
日志说明	检测周期内指定目的地址的慢速攻击IPv4报文数超过阈值，触发日志
处理建议	无

12.154 ATK_IP4_SLOW_ATTACK_SZ

日志内容	SrcZoneName(1025)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[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_SLOW_ATTACK_SZ:SrcZoneName(1025)=Trust;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009093351.
日志说明	检测周期内指定目的地址的慢速攻击IPv4报文数超过阈值，触发日志
处理建议	无

12.155 ATK_IP4_SYN_FLOOD

日志内容	RcvIfName(1023)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $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:RcvIfName(1023)=GigabitEthernet0/0/2;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=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

12.156 ATK_IP4_SYN_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：目的IP地址 $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_SZ:SrcZoneName(1025)=Trust;SrcIPAddr(1003)=2.3.3.1;DstIPAddr(1007)=6.1.1.5;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=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

12.157 ATK_IP4_SYNACK_FLOOD

日志内容	RcvIfName(1023)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $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_SYNACK_FLOOD:RcvIfName(1023)=GigabitEthernet0/0/2;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=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

12.158 ATK_IP4_SYNACK_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[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_SYNACK_FLOOD_SZ:SrcZoneName(1025)=Trust;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=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

12.159 ATK_IP4_TCP_ALLFLAGS

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel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	3
举例	ATK/3/ATK_IP4_TCP_ALLFLAGS:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=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

12.160 ATK_IP4_TCP_ALLFLAGS_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TCP_ALLFLAGS_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=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

12.161 ATK_IP4_TCP_ALLFLAGS_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TCP_ALLFLAGS_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=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

12.162 ATK_IP4_TCP_ALLFLAGS_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel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	3
举例	ATK/3/ATK_IP4_TCP_ALLFLAGS_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=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

12.163 ATK_IP4_TCP_FINONLY

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel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	3
举例	ATK/3/ATK_IP4_TCP_FINONLY:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=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

12.164 ATK_IP4_TCP_FINONLY_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TCP_FINONLY_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=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

12.165 ATK_IP4_TCP_FINONLY_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TCP_FINONLY_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=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

12.166 ATK_IP4_TCP_FINONLY_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel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	3
举例	ATK/3/ATK_IP4_TCP_FINONLY_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=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

12.167 ATK_IP4_TCP_INVALIDFLAGS

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel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	3
举例	ATK/3/ATK_IP4_TCP_INVALIDFLAGS:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20130111074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=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

12.168 ATK_IP4_TCP_INVALIDFLAGS_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TCP_INVALIDFLAGS_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=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IPV4TCP报文触发日志 日志聚合开关关闭，每个TCP标志位无效的IPv4TCP报文触发一个日志
处理建议	无

12.169 ATK_IP4_TCP_INVALIDFLAGS_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TCP_INVALIDFLAGS_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=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IPV4TCP报文触发日志 日志聚合开关关闭，每个TCP标志位无效的IPv4TCP报文触发一个日志
处理建议	无

12.170 ATK_IP4_TCP_INVALIDFLAGS_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel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	3
举例	ATK/3/ATK_IP4_TCP_INVALIDFLAGS_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=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

12.171 ATK_IP4_TCP_LAND

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel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	3
举例	ATK/3/ATK_IP4_TCP_LAND:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=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

12.172 ATK_IP4_TCP_LAND_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TCP_LAND_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=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

12.173 ATK_IP4_TCP_LAND_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TCP_LAND_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=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

12.174 ATK_IP4_TCP_LAND_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel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	3
举例	ATK/3/ATK_IP4_TCP_LAND_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=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

12.175 ATK_IP4_TCP_NULLFLAG

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel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	3
举例	ATK/3/ATK_IP4_TCP_NULLFLAG:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=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

12.176 ATK_IP4_TCP_NULLFLAG_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TCP_NULLFLAG_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=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

12.177 ATK_IP4_TCP_NULLFLAG_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TCP_NULLFLAG_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=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

12.178 ATK_IP4_TCP_NULLFLAG_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel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	3
举例	ATK/3/ATK_IP4_TCP_NULLFLAG_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=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

12.179 ATK_IP4_TCP_SYNFIN

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel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	3
举例	ATK/3/ATK_IP4_TCP_SYNFIN:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=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

12.180 ATK_IP4_TCP_SYNFIN_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TCP_SYNFIN_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=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

12.181 ATK_IP4_TCP_SYNFIN_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TCP_SYNFIN_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=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

12.182 ATK_IP4_TCP_SYNFIN_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel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	3
举例	ATK/3/ATK_IP4_TCP_SYNFIN_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=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

12.183 ATK_IP4_TCP_WINNUKE

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel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	3
举例	ATK/3/ATK_IP4_TCP_WINNUKE:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=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

12.184 ATK_IP4_TCP_WINNUKE_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TCP_WINNUKE_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=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

12.185 ATK_IP4_TCP_WINNUKE_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TCP_WINNUKE_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=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

12.186 ATK_IP4_TCP_WINNUKE_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel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	3
举例	ATK/3/ATK_IP4_TCP_WINNUKE_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=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

12.187 ATK_IP4_TEARDROP

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel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	3
举例	ATK/3/ATK_IP4_TEARDROP:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=TCP;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=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

12.188 ATK_IP4_TEARDROP_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel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	3
举例	ATK/3/ATK_IP4_TEARDROP_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=TCP;Action(1053)=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

12.189 ATK_IP4_TEARDROP_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel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	3
举例	ATK/3/ATK_IP4_TEARDROP_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=TCP;Action(1053)=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

12.190 ATK_IP4_TEARDROP_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel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	3
举例	ATK/3/ATK_IP4_TEARDROP_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=TCP;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=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

12.191 ATK_IP4_TINY_FRAGMENT

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel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	4
举例	ATK/3/ATK_IP4_TINY_FRAGMENT:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=TCP;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=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

12.192 ATK_IP4_TINY_FRAGMENT_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel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	4
举例	ATK/3/ATK_IP4_TINY_FRAGMENT_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=TCP;Action(1053)=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

12.193 ATK_IP4_TINY_FRAGMENT_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel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	4
举例	ATK/3/ATK_IP4_TINY_FRAGMENT_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=TCP;Action(1053)=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

12.194 ATK_IP4_TINY_FRAGMENT_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel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	4
举例	ATK/3/ATK_IP4_TINY_FRAGMENT_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=TCP;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=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

12.195 ATK_IP4_UDP_BOMB

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel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	3
举例	ATK/3/ATK_IP4_UDP_BOMB:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=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

12.196 ATK_IP4_UDP_BOMB_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_UDP_BOMB_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=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

12.197 ATK_IP4_UDP_BOMB_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_UDP_BOMB_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=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

12.198 ATK_IP4_UDP_BOMB_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel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	3
举例	ATK/3/ATK_IP4_UDP_BOMB_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=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

12.199 ATK_IP4_UDP_FLOOD

日志内容	RcvIfName(1023)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $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_UDP_FLOOD:RcvIfName(1023)=GigabitEthernet0/0/2;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=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

12.200 ATK_IP4_UDP_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：目的IP地址 $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;SrcIPAddr(1003)=2.3.3.1;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=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

12.201 ATK_IP4_UDP_FRAGGLE

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel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	3
举例	ATK/3/ATK_IP4_UDP_FRAGGLE:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=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

12.202 ATK_IP4_UDP_FRAGGLE_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_UDP_FRAGGLE_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=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

12.203 ATK_IP4_UDP_FRAGGLE_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_UDP_FRAGGLE_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=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

12.204 ATK_IP4_UDP_FRAGGLE_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel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	3
举例	ATK/3/ATK_IP4_UDP_FRAGGLE_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=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

12.205 ATK_IP4_UDP_SNORK

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel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	3
举例	ATK/3/ATK_IP4_UDP_SNORK:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=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

12.206 ATK_IP4_UDP_SNORK_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_UDP_SNORK_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=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

12.207 ATK_IP4_UDP_SNORK_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_UDP_SNORK_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=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

12.208 ATK_IP4_UDP_SNORK_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel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	3
举例	ATK/3/ATK_IP4_UDP_SNORK_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=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

12.209 ATK_IP6_ACK_FLOOD

日志内容	RcvIfName(1023)=[STRING];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：目的IPv6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_IP6_ACK_FLOOD:RcvIfName(1023)=GigabitEthernet0/0/2;DstIPv6Addr(1037)=2::2;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=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

12.210 ATK_IP6_ACK_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：目的IPv6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_IP6_ACK_FLOOD_SZ:SrcZoneName(1025)=Trust;DstIPv6Addr(1037)=2::2;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=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

12.211 ATK_IP6_DIS_PORTSCAN

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];Protocol(1001)=[STRING];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
参数解释	$1：子模块名称 $2：入接口名称 $3：协议名称 $4：目的IPv6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_IP6_DIS_PORTSCAN:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;Protocol(1001)=UDP;DstIPv6Addr(1037)=2::2;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131009100928.
日志说明	IPV6报文满足分布式portscan时触发日志
处理建议	无

12.212 ATK_IP6_DIS_PORTSCAN_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];Protocol(1001)=[STRING];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
参数解释	$1：子模块名称 $2：入域名称 $3：协议名称 $4：目的IPv6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_IP6_DIS_PORTSCAN_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;Protocol(1001)=TCP;DstIPv6Addr(1037)=2::2;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131009100928.
日志说明	IPV6报文满足分布式portscan时触发日志
处理建议	无

12.213 ATK_IP6_DNS_FLOOD

日志内容	RcvIfName(1023)=[STRING];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：目的IPv6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_IP6_DNS_FLOOD:RcvIfName(1023)=GigabitEthernet0/0/2;DstIPv6Addr(1037)=2::2;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009100434.
日志说明	单位时间内向指定目的IP发送DNSQuery的IPV6报文数超过阈值，触发日志发送
处理建议	无

12.214 ATK_IP6_DNS_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：目的IPv6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_IP6_DNS_FLOOD_SZ:SrcZoneName(1025)=Trust;DstIPv6Addr(1037)=2::2;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009100434.
日志说明	单位时间内向指定目的IP发送DNSQuery的IPV6报文数超过阈值，触发日志发送
处理建议	无

12.215 ATK_IP6_EXHEADER_ABNORMAL

日志内容	SubModule(1127)=[STRING];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：子模块名称 $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_IP6_EXHEADER_ABNORMAL:SubModule(1127)=SINGLE;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，扩展头异常的IPv6报文数超过1，聚合后触发日志
处理建议	无

12.216 ATK_IP6_EXHEADER_ABNORMAL_RAW

日志内容	SubModule(1127)=[STRING];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $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_IP6_EXHEADER_ABNORMAL_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=Ethernet0/0/2;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=--;Action(1053)=logging.
日志说明	日志聚合开关开启，扩展头异常的IPv6报文首包触发日志；日志聚合开关关闭，每个扩展头异常的IPv6报文触发一个日志
处理建议	无

12.217 ATK_IP6_EXHEADER_ABNORMAL_RAW_SZ

日志内容	SubModule(1127)=[STRING];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $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_IP6_EXHEADER_ABNORMAL_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=--;Action(1053)=logging.
日志说明	日志聚合开关开启，扩展头异常的IPv6报文首包触发日志；日志聚合开关关闭，每个扩展头异常的IPv6报文触发一个日志
处理建议	无

12.218 ATK_IP6_EXHEADER_ABNORMAL_SZ

日志内容	SubModule(1127)=[STRING];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：子模块名称 $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_IP6_EXHEADER_ABNORMAL_SZ:SubModule(1127)=SINGLE;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	日志聚合开关打开，扩展头异常的IPv6报文数超过1，聚合后触发日志
处理建议	无

12.219 ATK_IP6_EXHEADER_EXCEED

日志内容	SubModule(1127)=[STRING];IPv6ExtHdrLimitValue(1142)=[UINT32];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：子模块名称 $2：IPv6扩展头限制数目 $3：入接口名称 $4：源IPv6地址 $5：目的IPv6地址 $6：入接口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_IP6_EXHEADER_EXCEED:SubModule(1127)=SINGLE;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	日志聚合开关打开，扩展头数目超限的IPv6报文数超过1，聚合后触发日志
处理建议	无

12.220 ATK_IP6_EXHEADER_EXCEED_RAW

日志内容	SubModule(1127)=[STRING];IPv6ExtHdrLimitValue(1142)=[UINT32];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：IPv6扩展头限制数目 $3：入接口名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_IP6_EXHEADER_EXCEED_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=Ethernet0/0/2;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=--;Action(1053)=logging.
日志说明	日志聚合开关开启，扩展头数目超限的IPv6报文首包触发日志；日志聚合开关关闭，每个扩展头数目超限的IPv6报文触发一个日志
处理建议	无

12.221 ATK_IP6_EXHEADER_EXCEED_RAW_SZ

日志内容	SubModule(1127)=[STRING];IPv6ExtHdrLimitValue(1142)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：IPv6扩展头限制数目 $3：入域名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_IP6_EXHEADER_EXCEED_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=--;Action(1053)=logging.
日志说明	日志聚合开关开启，扩展头数目超限的IPv6报文首包触发日志；日志聚合开关关闭，每个扩展头数目超限的IPv6报文触发一个日志
处理建议	无

12.222 ATK_IP6_EXHEADER_EXCEED_SZ

日志内容	SubModule(1127)=[STRING];IPv6ExtHdrLimitValue(1142)=[UINT32];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：子模块名称 $2：IPv6扩展头限制数目 $3：入域名称 $4：源IPv6地址 $5：目的IPv6地址 $6：入接口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_IP6_EXHEADER_EXCEED_SZ:SubModule(1127)=SINGLE;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	日志聚合开关打开，扩展头数目超限的IPv6报文数超过1，聚合后触发日志
处理建议	无

12.223 ATK_IP6_FIN_FLOOD

日志内容	RcvIfName(1023)=[STRING];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：目的IPv6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_IP6_FIN_FLOOD:RcvIfName(1023)=GigabitEthernet0/0/2;DstIPv6Addr(1037)=2::2;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=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

12.224 ATK_IP6_FIN_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：目的IPv6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_IP6_FIN_FLOOD_SZ:SrcZoneName(1025)=Trust;DstIPv6Addr(1037)=2::2;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=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

12.225 ATK_IP6_FRAGMENT

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6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	4
举例	ATK/3/ATK_IP6_FRAGMENT:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=1::1;RcvVPNInstance(1042)=;Protocol(1001)=IPv6-ICMP;Action(1053)=logging;BeginTime_c(1011)=20131011103335;EndTime_c(1012)=20131011103835;AtkTimes(1054)=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

12.226 ATK_IP6_FRAGMENT_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：协议名称 $7：动作类型
日志等级	4
举例	ATK/3/ATK_IP6_FRAGMENT_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=1::1;RcvVPNInstance(1042)=;Protocol(1001)=IPv6-ICMP;Action(1053)=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

12.227 ATK_IP6_FRAGMENT_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：协议名称 $7：动作类型
日志等级	4
举例	ATK/3/ATK_IP6_FRAGMENT_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=1::1;RcvVPNInstance(1042)=;Protocol(1001)=IPv6-ICMP;Action(1053)=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

12.228 ATK_IP6_FRAGMENT_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：入域名称 $3：源IPv6地址 $4：目的IPv6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	4
举例	ATK/3/ATK_IP6_FRAGMENT_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=1::1;RcvVPNInstance(1042)=;Protocol(1001)=IPv6-ICMP;Action(1053)=logging;BeginTime_c(1011)=20131011103335;EndTime_c(1012)=20131011103835;AtkTimes(1054)=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

12.229 ATK_IP6_HTTP_FLOOD

日志内容	RcvIfName(1023)=[STRING];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：目的IPv6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_IP6_HTTP_FLOOD:RcvIfName(1023)=GigabitEthernet0/0/2;DstIPv6Addr(1037)=2::2;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=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IPV6Get报文数超过阈值，触发日志发送
处理建议	无

12.230 ATK_IP6_HTTP_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：目的IPv6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_IP6_HTTP_FLOOD_SZ:SrcZoneName(1025)=Trust;DstIPv6Addr(1037)=2::2;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=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IPV6Get报文数超过阈值，触发日志发送
处理建议	无

12.231 ATK_IP6_IMPOSSIBLE

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6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_IP6_IMPOSSIBLE:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=1::1;RcvVPNInstance(1042)=;Protocol(1001)=IPv6-ICMP;Action(1053)=logging;BeginTime_c(1011)=20131011103335;EndTime_c(1012)=20131011103835;AtkTimes(1054)=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

12.232 ATK_IP6_IMPOSSIBLE_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：协议名称 $7：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_IMPOSSIBLE_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=1::1;RcvVPNInstance(1042)=;Protocol(1001)=IPv6-ICMP;Action(1053)=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

12.233 ATK_IP6_IMPOSSIBLE_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：协议名称 $7：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_IMPOSSIBLE_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=1::1;RcvVPNInstance(1042)=;Protocol(1001)=IPv6-ICMP;Action(1053)=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

12.234 ATK_IP6_IMPOSSIBLE_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：入域名称 $3：源IPv6地址 $4：目的IPv6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_IP6_IMPOSSIBLE_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=1::1;RcvVPNInstance(1042)=;Protocol(1001)=IPv6-ICMP;Action(1053)=logging;BeginTime_c(1011)=20131011103335;EndTime_c(1012)=20131011103835;AtkTimes(1054)=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

12.235 ATK_IP6_IPSWEEP

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];Protocol(1001)=[STRING];SrcIPv6Addr(1036)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
参数解释	$1：子模块名称 $2：入接口名称 $3：协议名称 $4：源IPv6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_IP6_IPSWEEP:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;Protocol(1001)=UDP;SrcIPv6Addr(1036)=1::5;RcvVPNInstance(1042)=;Action(1053)=logging,block-source;BeginTime_c(1011)=20131009100639.
日志说明	IPV6报文满足ipsweep时触发日志
处理建议	无

12.236 ATK_IP6_IPSWEEP_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];Protocol(1001)=[STRING];SrcIPv6Addr(1036)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
参数解释	$1：子模块名称 $2：入域名称 $3：协议名称 $4：源IPv6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_IP6_IPSWEEP_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;Protocol(1001)=TCP;SrcIPv6Addr(1036)=1::5;RcvVPNInstance(1042)=;Action(1053)=logging,block-source;BeginTime_c(1011)=20131009100639.
日志说明	IPV6报文满足ipsweep时触发日志
处理建议	无

12.237 ATK_IP6_PORTSCAN

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];Protocol(1001)=[STRING];SrcIPv6Addr(1036)=[IPADDR];RcvVPNInstance(1042)=[STRING];DstIPv6Addr(1037)=[IPADDR];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
参数解释	$1：子模块名称 $2：入接口名称 $3：协议名称 $4：源IPv6地址 $5：VPN名称 $6：目的IPv6地址 $7：动作类型 $8：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP6_PORTSCAN:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;Protocol(1001)=UDP;SrcIPv6Addr(1036)=1::5;RcvVPNInstance(1042)=;DstIPv6Addr(1037)=2::2;Action(1053)=logging,block-source;BeginTime_c(1011)=20131009100455.
日志说明	IPV6报文满足portscan时触发日志
处理建议	无

12.238 ATK_IP6_PORTSCAN_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];Protocol(1001)=[STRING];SrcIPv6Addr(1036)=[IPADDR];RcvVPNInstance(1042)=[STRING];DstIPv6Addr(1037)=[IPADDR];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
参数解释	$1：子模块名称 $2：入域名称 $3：协议名称 $4：源IPv6地址 $5：VPN名称 $6：目的IPv6地址 $7：动作类型 $8：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP6_PORTSCAN_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;Protocol(1001)=TCP;SrcIPv6Addr(1036)=1::5;RcvVPNInstance(1042)=;DstIPv6Addr(1037)=2::2;Action(1053)=logging,block-source;BeginTime_c(1011)=20131009100455.
日志说明	IPV6报文满足portscan时触发日志
处理建议	无

12.239 ATK_IP6_RST_FLOOD

日志内容	RcvIfName(1023)=[STRING];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：目的IPv6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_IP6_RST_FLOOD:RcvIfName(1023)=GigabitEthernet0/0/2;DstIPv6Addr(1037)=2::2;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=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

12.240 ATK_IP6_RST_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：目的IPv6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_IP6_RST_FLOOD_SZ:SrcZoneName(1025)=Trust;DstIPv6Addr(1037)=2::2;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=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

12.241 ATK_IP6_SLOW_ATTACK

日志内容	RcvIfName(1023)=[STRING];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：目的IPv6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_IP6_SLOW_ATTACK:RcvIfName(1023)=GigabitEthernet0/0/2;DstIPv6Addr(1037)=2::2;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009093351.
日志说明	检测周期内指定目的地址的慢速攻击IPv6报文数超过阈值，触发日志
处理建议	无

12.242 ATK_IP6_SLOW_ATTACK_SZ

日志内容	SrcZoneName(1025)=[STRING];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：目的IPv6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_IP6_SLOW_ATTACK_SZ:SrcZoneName(1025)=Trust;DstIPv6Addr(1037)=2::2;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009093351.
日志说明	检测周期内指定目的地址的慢速攻击IPv6报文数超过阈值，触发日志
处理建议	无

12.243 ATK_IP6_SYN_FLOOD

日志内容	RcvIfName(1023)=[STRING];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：目的IPv6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_IP6_SYN_FLOOD:RcvIfName(1023)=GigabitEthernet0/0/2;DstIPv6Addr(1037)=2::2;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=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

12.244 ATK_IP6_SYN_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：目的IPv6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_IP6_SYN_FLOOD_SZ:SrcZoneName(1025)=Trust;DstIPv6Addr(1037)=2::2;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=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

12.245 ATK_IP6_SYNACK_FLOOD

日志内容	RcvIfName(1023)=[STRING];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：目的IPv6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_IP6_SYNACK_FLOOD:RcvIfName(1023)=GigabitEthernet0/0/2;DstIPv6Addr(1037)=2::2;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=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

12.246 ATK_IP6_SYNACK_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：目的IPv6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_IP6_SYNACK_FLOOD_SZ:SrcZoneName(1025)=Trust;DstIPv6Addr(1037)=2::2;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=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

12.247 ATK_IP6_TCP_ALLFLAGS

日志内容	SubModule(1127)=SINGLE;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：子模块名称 $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	3
举例	ATK/3/ATK_IP6_TCP_ALLFLAGS:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;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，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

12.248 ATK_IP6_TCP_ALLFLAGS_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $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
日志等级	3
举例	ATK/3/ATK_IP6_TCP_ALLFLAGS_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=2000::1;DstIPv6Addr(1037)=2003::200;RcvVPNInstance(1042)=;Action(1053)=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

12.249 ATK_IP6_TCP_ALLFLAGS_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $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
日志等级	3
举例	ATK/3/ATK_IP6_TCP_ALLFLAGS_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=2000::1;DstIPv6Addr(1037)=2003::200;RcvVPNInstance(1042)=;Action(1053)=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

12.250 ATK_IP6_TCP_ALLFLAGS_SZ

日志内容	SubModule(1127)=SINGLE;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：子模块名称 $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	3
举例	ATK/3/ATK_IP6_TCP_ALLFLAGS_SZ:SubModule(1127)=SINGLE;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，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

12.251 ATK_IP6_TCP_FINONLY

日志内容	SubModule(1127)=SINGLE;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：子模块名称 $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	3
举例	ATK/3/ATK_IP6_TCP_FINONLY:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;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，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

12.252 ATK_IP6_TCP_FINONLY_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $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
日志等级	3
举例	ATK/3/ATK_IP6_TCP_FINONLY_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=2000::1;DstIPv6Addr(1037)=2003::200;RcvVPNInstance(1042)=;Action(1053)=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

12.253 ATK_IP6_TCP_FINONLY_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $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
日志等级	3
举例	ATK/3/ATK_IP6_TCP_FINONLY_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=2000::1;DstIPv6Addr(1037)=2003::200;RcvVPNInstance(1042)=;Action(1053)=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

12.254 ATK_IP6_TCP_FINONLY_SZ

日志内容	SubModule(1127)=SINGLE;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：子模块名称 $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	3
举例	ATK/3/ATK_IP6_TCP_FINONLY_SZ:SubModule(1127)=SINGLE;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，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

12.255 ATK_IP6_TCP_INVALIDFLAGS

日志内容	SubModule(1127)=SINGLE;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：子模块名称 $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	3
举例	ATK/3/ATK_IP6_TCP_INVALIDFLAGS:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;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，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

12.256 ATK_IP6_TCP_INVALIDFLAGS_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $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
日志等级	3
举例	ATK/3/ATK_IP6_TCP_INVALIDFLAGS_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=2000::1;DstIPv6Addr(1037)=2003::200;RcvVPNInstance(1042)=;Action(1053)=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IPV6TCP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IPV6TCP报文触发一个日志
处理建议	无

12.257 ATK_IP6_TCP_INVALIDFLAGS_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $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
日志等级	3
举例	ATK/3/ATK_IP6_TCP_INVALIDFLAGS_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=2000::1;DstIPv6Addr(1037)=2003::200;RcvVPNInstance(1042)=;Action(1053)=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IPV6TCP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IPV6TCP报文触发一个日志
处理建议	无

12.258 ATK_IP6_TCP_INVALIDFLAGS_SZ

日志内容	SubModule(1127)=SINGLE;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：子模块名称 $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	3
举例	ATK/3/ATK_IP6_TCP_INVALIDFLAGS_SZ:SubModule(1127)=SINGLE;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，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

12.259 ATK_IP6_TCP_LAND

日志内容	SubModule(1127)=SINGLE;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：子模块名称 $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	3
举例	ATK/3/ATK_IP6_TCP_LAND:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;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，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

12.260 ATK_IP6_TCP_LAND_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $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
日志等级	3
举例	ATK/3/ATK_IP6_TCP_LAND_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=2000::1;DstIPv6Addr(1037)=2003::200;RcvVPNInstance(1042)=;Action(1053)=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

12.261 ATK_IP6_TCP_LAND_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $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
日志等级	3
举例	ATK/3/ATK_IP6_TCP_LAND_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=2000::1;DstIPv6Addr(1037)=2003::200;RcvVPNInstance(1042)=;Action(1053)=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

12.262 ATK_IP6_TCP_LAND_SZ

日志内容	SubModule(1127)=SINGLE;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：子模块名称 $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	3
举例	ATK/3/ATK_IP6_TCP_LAND_SZ:SubModule(1127)=SINGLE;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，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

12.263 ATK_IP6_TCP_NULLFLAG

日志内容	SubModule(1127)=SINGLE;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：子模块名称 $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	3
举例	ATK/3/ATK_IP6_TCP_NULLFLAG:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;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，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

12.264 ATK_IP6_TCP_NULLFLAG_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $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
日志等级	3
举例	ATK/3/ATK_IP6_TCP_NULLFLAG_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=2000::1;DstIPv6Addr(1037)=2003::200;RcvVPNInstance(1042)=;Action(1053)=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

12.265 ATK_IP6_TCP_NULLFLAG_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $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
日志等级	3
举例	ATK/3/ATK_IP6_TCP_NULLFLAG_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=2000::1;DstIPv6Addr(1037)=2003::200;RcvVPNInstance(1042)=;Action(1053)=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

12.266 ATK_IP6_TCP_NULLFLAG_SZ

日志内容	SubModule(1127)=SINGLE;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：子模块名称 $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	3
举例	ATK/3/ATK_IP6_TCP_NULLFLAG_SZ:SubModule(1127)=SINGLE;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，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

12.267 ATK_IP6_TCP_SYNFIN

日志内容	SubModule(1127)=SINGLE;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：子模块名称 $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	3
举例	ATK/3/ATK_IP6_TCP_SYNFIN:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;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，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

12.268 ATK_IP6_TCP_SYNFIN_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $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
日志等级	3
举例	ATK/3/ATK_IP6_TCP_SYNFIN_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=2000::1;DstIPv6Addr(1037)=2003::200;RcvVPNInstance(1042)=;Action(1053)=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

12.269 ATK_IP6_TCP_SYNFIN_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $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
日志等级	3
举例	ATK/3/ATK_IP6_TCP_SYNFIN_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=2000::1;DstIPv6Addr(1037)=2003::200;RcvVPNInstance(1042)=;Action(1053)=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

12.270 ATK_IP6_TCP_SYNFIN_SZ

日志内容	SubModule(1127)=SINGLE;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：子模块名称 $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	3
举例	ATK/3/ATK_IP6_TCP_SYNFIN_SZ:SubModule(1127)=SINGLE;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，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

12.271 ATK_IP6_TCP_WINNUKE

日志内容	SubModule(1127)=SINGLE;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：子模块名称 $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	3
举例	ATK/3/ATK_IP6_TCP_WINNUKE:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;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，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

12.272 ATK_IP6_TCP_WINNUKE_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $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	3
举例	ATK/3/ATK_IP6_TCP_WINNUKE_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;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

12.273 ATK_IP6_TCP_WINNUKE_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $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	3
举例	ATK/3/ATK_IP6_TCP_WINNUKE_RAW_SZ:SubModule(1127)=SINGLE;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

12.274 ATK_IP6_TCP_WINNUKE_SZ

日志内容	SubModule(1127)=SINGLE;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：子模块名称 $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	3
举例	ATK/3/ATK_IP6_TCP_WINNUKE_SZ:SubModule(1127)=SINGLE;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，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

12.275 ATK_IP6_UDP_FLOOD

日志内容	RcvIfName(1023)=[STRING];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：目的IPv6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_IP6_UDP_FLOOD:RcvIfName(1023)=GigabitEthernet0/0/2;DstIPv6Addr(1037)=2::2;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=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

12.276 ATK_IP6_UDP_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：目的IPv6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_IP6_UDP_FLOOD_SZ:SrcZoneName(1025)=Trust;DstIPv6Addr(1037)=2::2;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=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

12.277 ATK_IP6_UDP_FRAGGLE

日志内容	SubModule(1127)=SINGLE;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：子模块名称 $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	3
举例	ATK/3/ATK_IP6_UDP_FRAGGLE:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;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，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

12.278 ATK_IP6_UDP_FRAGGLE_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $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	3
举例	ATK/3/ATK_IP6_UDP_FRAGGLE_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;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

12.279 ATK_IP6_UDP_FRAGGLE_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $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	3
举例	ATK/3/ATK_IP6_UDP_FRAGGLE_RAW_SZ:SubModule(1127)=SINGLE;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

12.280 ATK_IP6_UDP_FRAGGLE_SZ

日志内容	SubModule(1127)=SINGLE;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：子模块名称 $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	3
举例	ATK/3/ATK_IP6_UDP_FRAGGLE_SZ:SubModule(1127)=SINGLE;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，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

12.281 ATK_IP6_UDP_SNORK

日志内容	SubModule(1127)=SINGLE;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：子模块名称 $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	3
举例	ATK/3/ATK_IP6_UDP_SNORK:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;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，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

12.282 ATK_IP6_UDP_SNORK_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $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	3
举例	ATK/3/ATK_IP6_UDP_SNORK_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;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

12.283 ATK_IP6_UDP_SNORK_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $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	3
举例	ATK/3/ATK_IP6_UDP_SNORK_RAW_SZ:SubModule(1127)=SINGLE;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

12.284 ATK_IP6_UDP_SNORK_SZ

日志内容	SubModule(1127)=SINGLE;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：子模块名称 $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	3
举例	ATK/3/ATK_IP6_UDP_SNORK_SZ:SubModule(1127)=SINGLE;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，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

12.285 ATK_IPOPT_ABNORMAL

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel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	3
举例	ATK/3/ATK_IPOPT_ABNORMAL:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging;BeginTime_c(1011)=20131011072002;EndTime_c(1012)=20131011072502;AtkTimes(1054)=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

12.286 ATK_IPOPT_ABNORMAL_RAW

日志内容	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：入接口名称 $3：源IP地址 $4：DS-LiteTunnel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	3
举例	ATK/3/ATK_IPOPT_ABNORMAL_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=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

12.287 ATK_IPOPT_ABNORMAL_RAW_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel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	3
举例	ATK/3/ATK_IPOPT_ABNORMAL_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=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

12.288 ATK_IPOPT_ABNORMAL_SZ

日志内容	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：入域名称 $3：源IP地址 $4：DS-LiteTunnel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	3
举例	ATK/3/ATK_IPOPT_ABNORMAL_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging;BeginTime_c(1011)=20131011072002;EndTime_c(1012)=20131011072502;AtkTimes(1054)=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

12.289 ATK_IPOPT_LOOSESRCROUTE

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：IP选项值 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型 $10：攻击开始时间 $11：攻击结束时间 $12：攻击次数
日志等级	5
举例	ATK/5/ATK_IPOPT_LOOSESRCROUTE:SubModule(1127)=SINGLE;IPOptValue(1061)=131;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging;BeginTime_c(1011)=20131011063123;EndTime_c(1012)=20131011063623;AtkTimes(1054)=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

12.290 ATK_IPOPT_LOOSESRCROUTE_RAW

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：IP选项值 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型
日志等级	5
举例	ATK/5/ATK_IPOPT_LOOSESRCROUTE_RAW:SubModule(1127)=SINGLE;IPOptValue(1061)=131;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=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

12.291 ATK_IPOPT_LOOSESRCROUTE_RAW_SZ

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：IP选项值 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型
日志等级	5
举例	ATK/5/ATK_IPOPT_LOOSESRCROUTE_RAW_SZ:SubModule(1127)=SINGLE;IPOptValue(1061)=131;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=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

12.292 ATK_IPOPT_LOOSESRCROUTE_SZ

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：IP选项值 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型 $10：攻击开始时间 $11：攻击结束时间 $12：攻击次数
日志等级	5
举例	ATK/5/ATK_IPOPT_LOOSESRCROUTE_SZ:SubModule(1127)=SINGLE;IPOptValue(1061)=131;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging;BeginTime_c(1011)=20131011063123;EndTime_c(1012)=20131011063623;AtkTimes(1054)=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

12.293 ATK_IPOPT_RECORDROUTE

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：IP选项值 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型 $10：攻击开始时间 $11：攻击结束时间 $12：攻击次数
日志等级	5
举例	ATK/5/ATK_IPOPT_RECORDROUTE:SubModule(1127)=SINGLE;IPOptValue(1061)=7;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging;BeginTime_c(1011)=20131011063123;EndTime_c(1012)=20131011063623;AtkTimes(1054)=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

12.294 ATK_IPOPT_RECORDROUTE_RAW

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：IP选项值 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型
日志等级	5
举例	ATK/5/ATK_IPOPT_RECORDROUTE_RAW:SubModule(1127)=SINGLE;IPOptValue(1061)=7;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=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

12.295 ATK_IPOPT_RECORDROUTE_RAW_SZ

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：IP选项值 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型
日志等级	5
举例	ATK/5/ATK_IPOPT_RECORDROUTE_RAW_SZ:SubModule(1127)=SINGLE;IPOptValue(1061)=7;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=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

12.296 ATK_IPOPT_RECORDROUTE_SZ

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：IP选项值 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型 $10：攻击开始时间 $11：攻击结束时间 $12：攻击次数
日志等级	5
举例	ATK/5/ATK_IPOPT_RECORDROUTE_SZ:SubModule(1127)=SINGLE;IPOptValue(1061)=7;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging;BeginTime_c(1011)=20131011063123;EndTime_c(1012)=20131011063623;AtkTimes(1054)=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

12.297 ATK_IPOPT_ROUTEALERT

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：IP选项值 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型 $10：攻击开始时间 $11：攻击结束时间 $12：攻击次数
日志等级	5
举例	ATK/5/ATK_IPOPT_ROUTEALERT:SubModule(1127)=SINGLE;IPOptValue(1061)=148;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging;BeginTime_c(1011)=20131011063123;EndTime_c(1012)=20131011063623;AtkTimes(1054)=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

12.298 ATK_IPOPT_ROUTEALERT_RAW

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：IP选项值 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型
日志等级	5
举例	ATK/5/ATK_IPOPT_ROUTEALERT_RAW:SubModule(1127)=SINGLE;IPOptValue(1061)=148;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=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

12.299 ATK_IPOPT_ROUTEALERT_RAW_SZ

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：IP选项值 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型
日志等级	5
举例	ATK/5/ATK_IPOPT_ROUTEALERT_RAW_SZ:SubModule(1127)=SINGLE;IPOptValue(1061)=148;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=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

12.300 ATK_IPOPT_ROUTEALERT_SZ

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：IP选项值 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型 $10：攻击开始时间 $11：攻击结束时间 $12：攻击次数
日志等级	5
举例	ATK/5/ATK_IPOPT_ROUTEALERT_SZ:SubModule(1127)=SINGLE;IPOptValue(1061)=148;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging;BeginTime_c(1011)=20131011063123;EndTime_c(1012)=20131011063623;AtkTimes(1054)=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

12.301 ATK_IPOPT_SECURITY

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：IP选项值 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型 $10：攻击开始时间 $11：攻击结束时间 $12：攻击次数
日志等级	5
举例	ATK/5/ATK_IPOPT_SECURITY:SubModule(1127)=SINGLE;IPOptValue(1061)=130;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging;BeginTime_c(1011)=20131009091022;EndTime_c(1012)=20131009091522;AtkTimes(1054)=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

12.302 ATK_IPOPT_SECURITY_RAW

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：IP选项值 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型
日志等级	5
举例	ATK/5/ATK_IPOPT_SECURITY_RAW:SubModule(1127)=SINGLE;IPOptValue(1061)=130;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=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

12.303 ATK_IPOPT_SECURITY_RAW_SZ

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：IP选项值 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型
日志等级	5
举例	ATK/5/ATK_IPOPT_SECURITY_RAW_SZ:SubModule(1127)=SINGLE;IPOptValue(1061)=130;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=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

12.304 ATK_IPOPT_SECURITY_SZ

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：IP选项值 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型 $10：攻击开始时间 $11：攻击结束时间 $12：攻击次数
日志等级	5
举例	ATK/5/ATK_IPOPT_SECURITY_SZ:SubModule(1127)=SINGLE;IPOptValue(1061)=130;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging;BeginTime_c(1011)=20131009091022;EndTime_c(1012)=20131009091522;AtkTimes(1054)=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

12.305 ATK_IPOPT_STREAMID

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：IP选项值 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型 $10：攻击开始时间 $11：攻击结束时间 $11：攻击次数
日志等级	5
举例	ATK/5/ATK_IPOPT_STREAMID:SubModule(1127)=SINGLE;IPOptValue(1061)=136;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging;BeginTime_c(1011)=20131011063123;EndTime_c(1012)=20131011063623;AtkTimes(1054)=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

12.306 ATK_IPOPT_STREAMID_RAW

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：IP选项值 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型
日志等级	5
举例	ATK/5/ATK_IPOPT_STREAMID_RAW:SubModule(1127)=SINGLE;IPOptValue(1061)=136;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=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

12.307 ATK_IPOPT_STREAMID_RAW_SZ

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：IP选项值 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型
日志等级	5
举例	ATK/5/ATK_IPOPT_STREAMID_RAW_SZ:SubModule(1127)=SINGLE;IPOptValue(1061)=136;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=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

12.308 ATK_IPOPT_STREAMID_SZ

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：IP选项值 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型 $10：攻击开始时间 $11：攻击结束时间 $12：攻击次数
日志等级	5
举例	ATK/5/ATK_IPOPT_STREAMID_SZ:SubModule(1127)=SINGLE;IPOptValue(1061)=136;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging;BeginTime_c(1011)=20131011063123;EndTime_c(1012)=20131011063623;AtkTimes(1054)=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

12.309 ATK_IPOPT_STRICTSRCROUTE

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：IP选项值 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型 $10：攻击开始时间 $11：攻击结束时间 $12：攻击次数
日志等级	5
举例	ATK/5/ATK_IPOPT_STRICTSRCROUTE:SubModule(1127)=SINGLE;IPOptValue(1061)=137;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging;BeginTime_c(1011)=20131011063123;EndTime_c(1012)=20131011063623;AtkTimes(1054)=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

12.310 ATK_IPOPT_STRICTSRCROUTE_RAW

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：IP选项值 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型
日志等级	5
举例	ATK/5/ATK_IPOPT_STRICTSRCROUTE_RAW:SubModule(1127)=SINGLE;IPOptValue(1061)=137;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=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

12.311 ATK_IPOPT_STRICTSRCROUTE_RAW_SZ

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：IP选项值 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型
日志等级	5
举例	ATK/5/ATK_IPOPT_STRICTSRCROUTE_RAW_SZ:SubModule(1127)=SINGLE;IPOptValue(1061)=137;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=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

12.312 ATK_IPOPT_STRICTSRCROUTE_SZ

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：IP选项值 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型 $10：攻击开始时间 $11：攻击结束时间 $12：攻击次数
日志等级	5
举例	ATK/5/ATK_IPOPT_STRICTSRCROUTE_SZ:SubModule(1127)=SINGLE;IPOptValue(1061)=137;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging;BeginTime_c(1011)=20131011063123;EndTime_c(1012)=20131011063623;AtkTimes(1054)=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

12.313 ATK_IPOPT_TIMESTAMP

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：IP选项值 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型 $10：攻击开始时间 $11：攻击结束时间 $12：攻击次数
日志等级	5
举例	ATK/5/ATK_IPOPT_TIMESTAMP:SubModule(1127)=SINGLE;IPOptValue(1061)=68;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging;BeginTime_c(1011)=20131011063123;EndTime_c(1012)=20131011063623;AtkTimes(1054)=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

12.314 ATK_IPOPT_TIMESTAMP_RAW

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：IP选项值 $3：入接口名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型
日志等级	5
举例	ATK/5/ATK_IPOPT_TIMESTAMP_RAW:SubModule(1127)=SINGLE;IPOptValue(1061)=68;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=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

12.315 ATK_IPOPT_TIMESTAMP_RAW_SZ

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：IP选项值 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型
日志等级	5
举例	ATK/5/ATK_IPOPT_TIMESTAMP_RAW_SZ:SubModule(1127)=SINGLE;IPOptValue(1061)=68;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=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

12.316 ATK_IPOPT_TIMESTAMP_SZ

日志内容	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：子模块名称 $2：IP选项值 $3：入域名称 $4：源IP地址 $5：DS-LiteTunnel对端地址 $6：目的IP地址 $7：VPN名称 $8：协议类型 $9：动作类型 $10：攻击开始时间 $11：攻击结束时间 $12：攻击次数
日志等级	5
举例	ATK/5/ATK_IPOPT_TIMESTAMP_SZ:SubModule(1127)=SINGLE;IPOptValue(1061)=68;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging;BeginTime_c(1011)=20131011063123;EndTime_c(1012)=20131011063623;AtkTimes(1054)=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

12.317 ATK_IPV6_EXT_HEADER

日志内容	SubModule(1127)=SINGLE;IPv6ExtHeader(1066)=[UINT32];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：子模块名称 $2：IPv6扩展头 $3：入接口名称 $4：源IPv6地址 $5：目的IPv6地址 $6：入接口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_IPV6_EXT_HEADER:SubModule(1127)=SINGLE;IPv6ExtHeader(1066)=43;RcvIfName(1023)=GigabitEthernet0/0/2;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

12.318 ATK_IPV6_EXT_HEADER_RAW

日志内容	SubModule(1127)=SINGLE;IPv6ExtHeader(1066)=[UINT32];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：IPv6扩展头 $3：入接口名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_IPV6_EXT_HEADER_RAW:SubModule(1127)=SINGLE;IPv6ExtHeader(1066)=43;RcvIfName(1023)=GigabitEthernet0/0/2;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

12.319 ATK_IPV6_EXT_HEADER_RAW_SZ

日志内容	SubModule(1127)=SINGLE;IPv6ExtHeader(1066)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：子模块名称 $2：IPv6扩展头 $3：入域名称 $4：源IPv6地址 $5：目的IPv6地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_IPV6_EXT_HEADER_RAW_SZ:SubModule(1127)=SINGLE;IPv6ExtHeader(1066)=43;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

12.320 ATK_IPV6_EXT_HEADER_SZ

日志内容	SubModule(1127)=SINGLE;IPv6ExtHeader(1066)=[UINT32];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：子模块名称 $2：IPv6扩展头 $3：入域名称 $4：源IPv6地址 $5：目的IPv6地址 $6：入接口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_IPV6_EXT_HEADER_SZ:SubModule(1127)=SINGLE;IPv6ExtHeader(1066)=43;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

13 ATM

本节介绍 ATM 模块输出的日志信息。

13.1 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	**4.** 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：
	5. 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
	6. 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
	7. 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

13.2 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	**8.** 无需处理

14 AUDIT

本节介绍应用审计与管理模块输出的日志信息。

14.1 AUDIT_RULE_MATCH_AS_IPV4_LOG（系统日志）

日志内容	Protocol(1001)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];UserName(1113)=[STRING];PolicyName(1079)=[STRING];Application(1002)=[STRING];Behavior(1101)=[STRING];BehaviorContent(1102)={Account(1103)=[STRING],Content(1104)=[STRING]};Client(1110)=[STRING];SoftVersion(1111)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
参数解释	$1：协议类型 $2：源IPv4地址 $3：源端口号 $4：目的IPv4地址 $5：目的端口号 $6：源安全域名称 $7：目的安全域名称 $8：用户名称 $9：应用审计与管理策略名称 $10：应用协议名称 $11：应用行为 $12：应用行为内容 $13：账号 $14：内容 $15：客户端类型 $16：应用软件版本 $17：动作名称，包括如下取值： • Permit：允许 • Deny：阻断 $18：VLAN ID $19：VXLAN ID $20：源地区 $21：目的地区
日志等级	6
举例	AUDIT/6/AUDIT_RULE_MATCH_AS_IPV4_LOG:Protocol(1001)=TCP;SrcIPAddr(1003)=1.2.3.4;SrcPort(1004)=8080;DstIPAddr(1007)=6.1.1.1;DstPort(1008)=8080;SrcZoneName(1025)=spf;DstZoneName(1035)=spf;UserName(1113)=hjp;PolicyName(1079)=policy1;Application(1002)=tonghuashun;Behavior(1101)=Login;BehaviorContent(1102)={Account(1103)=hjk123456,Content(1104)=hello};Client(1110)=PC;SoftVersion(1111)=;Action(1053)=Deny;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
日志说明	当报文与娱乐股票类应用的审计规则匹配成功，输出该日志
处理建议	无

14.2 AUDIT_RULE_MATCH_FILE_IPV4_LOG（系统日志）

日志内容	Protocol(1001)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];UserName(1113)=[STRING];PolicyName(1079)=[STRING];Application(1002)=[STRING];Behavior(1101)=[STRING];BehaviorContent(1102)={Account(1103)=[STRING],FileName(1097)=[STRING]};Client(1110)=[STRING];SoftVersion(1111)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
参数解释	$1：协议类型 $2：源IPv4地址 $3：源端口号 $4：目的IPv4地址 $5：目的端口号 $6：源安全域名称 $7：目的安全域名称 $8：用户名称 $9：应用审计与管理策略名称 $10：应用协议名称 $11：应用行为 $12：应用行为内容 $13：账号 $14：文件名 $15：客户端类型 $16：应用软件版本 $17：动作名称，包括如下取值： • Permit：允许 • Deny：阻断 $18：VLAN ID $19：VXLAN ID $20：源地区 $21：目的地区
日志等级	6
举例	AUDIT/6/AUDIT_RULE_MATCH_FILE_IPV4_LOG:Protocol(1001)=TCP;SrcIPAddr(1003)=1.2.3.4;SrcPort(1004)=8080;DstIPAddr(1007)=6.1.1.1;DstPort(1008)=8080;SrcZoneName(1025)=spf;DstZoneName(1035)=spf;UserName(1113)=hjp;PolicyName(1079)=policy1;Application(1002)=ftp;Behavior(1101)=UploadFile;BehaviorContent(1102)={Account(1103)=ghj123,FileName(1097)=abc.txt};Client(1110)=PC;SoftVersion(1111)=;Action(1053)=Deny;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
日志说明	当报文与文件传输类应用的审计规则匹配成功，输出该日志
处理建议	无

14.3 AUDIT_RULE_MATCH_FORUM_IPV4_LOG（系统日志）

日志内容	Protocol(1001)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];UserName(1113)=[STRING];PolicyName(1079)=[STRING];Application(1002)=[STRING];Behavior(1101)=[STRING];BehaviorContent(1102)={Account(1103)=[STRING],Content(1104)=[STRING]};Client(1110)=[STRING];SoftVersion(1111)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
参数解释	$1：协议类型 $2：源IPv4地址 $3：源端口号 $4：目的IPv4地址 $5：目的端口号 $6：源安全域名称 $7：目的安全域名称 $8：用户名称 $9：应用审计与管理策略名称 $10：应用协议名称 $11：应用行为 $12：应用行为内容 $13：账号 $14：内容 $15：客户端类型 $16：应用软件版本 $17：动作名称，包括如下取值： • Permit：允许 • Deny：阻断 $18：VLAN ID $19：VXLAN ID $20：源地区 $21：目的地区
日志等级	6
举例	AUDIT/6/AUDIT_RULE_MATCH_FORUM_IPV4_LOG:Protocol(1001)=TCP;SrcIPAddr(1003)=1.2.3.4;SrcPort(1004)=8080;DstIPAddr(1007)=6.1.1.1;DstPort(1008)=8080;SrcZoneName(1025)=spf;DstZoneName(1035)=spf;UserName(1113)=hjp;PolicyName(1079)=policy1;Application(1002)=SinaWeibo;Behavior(1101)=Comment;BehaviorContent(1102)={Account(1103)=hjk123456,Content(1104)=hello};Client(1110)=PC;SoftVersion(1111)=;Action(1053)=Deny;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
日志说明	当报文与社区类应用的审计规则匹配成功，输出该日志
处理建议	无

14.4 AUDIT_RULE_MATCH_IM_IPV4_LOG（系统日志）

日志内容	Protocol(1001)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];UserName(1113)=[STRING];PolicyName(1079)=[STRING];Application(1002)=[STRING];Behavior(1101)=[STRING];BehaviorContent(1102)={Account(1103)=[STRING],Content(1104)=[STRING],FileName(1097)=[STRING],FileSize(1105)=[STRING]};Client(1110)=[STRING];SoftVersion(1111)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
参数解释	$1：协议类型 $2：源IPv4地址 $3：源端口号 $4：目的IPv4地址 $5：目的端口号 $6：源安全域名称 $7：目的安全域名称 $8：用户名称 $9：应用审计与管理策略名称 $10：应用协议名称 $11：应用行为 $12：应用行为内容 $13：账号 $14：内容 $15：文件名 $16：文件大小 $17：客户端类型 $18：应用软件版本 $19：动作名称，包括如下取值： • Permit：允许 • Deny：阻断 $20：VLAN ID $21：VXLAN ID $22：源地区 $23：目的地区
日志等级	6
举例	AUDIT/6/AUDIT_RULE_MATCH_IM_IPV4_LOG:Protocol(1001)=TCP;SrcIPAddr(1003)=1.2.3.4;SrcPort(1004)=8080;DstIPAddr(1007)=6.1.1.1;DstPort(1008)=8080;SrcZoneName(1025)=spf;DstZoneName(1035)=spf;UserName(1113)=hjp;PolicyName(1079)=policy1;Application(1002)=qq;Behavior(1101)=Login;BehaviorContent(1102)={Account(1103)=12345678,Content(1104)=test,FileName(1097)=text,FileSize(1105)=152389};Client(1110)=PC;SoftVersion(1111)=;Action(1053)=Deny;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
日志说明	当报文与即时通讯类应用的审计规则匹配成功，输出该日志
处理建议	无

14.5 AUDIT_RULE_MATCH_MAIL_IPV4_LOG（系统日志）

日志内容	Protocol(1001)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];UserName(1113)=[STRING];PolicyName(1079)=[STRING];Application(1002)=[STRING];Behavior(1101)=[STRING];BehaviorContent(1102)={Sender_addr(1106)=[STRING],Receiver_addr(1107)=[STRING],Subject(1108)=[STRING],Body(1109)=[STRING]};Client(1110)=[STRING];SoftVersion(1111)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
参数解释	$1：协议类型 $2：源IPv4地址 $3：源端口号 $4：目的IPv4地址 $5：目的端口号 $6：源安全域名称 $7：目的安全域名称 $8：用户名称 $9：应用审计与管理策略名称 $10：应用协议名称 $11：应用行为 $12：应用行为内容 $13：发件人 $14：收件人 $15：主题 $16：正文 $17：客户端类型 $18：应用软件版本 $19：动作名称，包括如下取值： • Permit：允许 • Deny：阻断 $20：VLAN ID $21：VXLAN ID $22：源地区 $23：目的地区
日志等级	6
举例	AUDIT/6/AUDIT_RULE_MATCH_MAIL_IPV4_LOG:Protocol(1001)=TCP;SrcIPAddr(1003)=1.2.3.4;SrcPort(1004)=8080;DstIPAddr(1007)=6.1.1.1;DstPort(1008)=8080;SrcZoneName(1025)=spf;DstZoneName(1035)=spf;UserName(1113)=hjp;PolicyName(1079)=policy1;Application(1002)=smtp;Behavior(1101)=SendMail;BehaviorContent(1102)={Sender_addr(1106)="wb"<wb@ubuntu.wb>,Receiver_addr(1107)=<wb@ubuntu.wb>,Subject(1108)=test,Body(1109)=abc};Client(1110)=PC;SoftVersion(1111)=;Action(1053)=Deny;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
日志说明	当报文与邮件类应用的审计规则匹配成功，输出该日志
处理建议	无

14.6 AUDIT_RULE_MATCH_OTHER_IPV4_LOG（系统日志）

日志内容	Protocol(1001)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];UserName(1113)=[STRING];PolicyName(1079)=[STRING];Application(1002)=[STRING];Behavior(1101)=[STRING];BehaviorContent(1102)={Account(1103)=[STRING],Password(1112)=[STRING],Content(1104)=[STRING]};Client(1110)=[STRING];SoftVersion(1111)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)= [STRING];
参数解释	$1：协议类型 $2：源IPv4地址 $3：源端口号 $4：目的IPv4地址 $5：目的端口号 $6：源安全域名称 $7：目的安全域名称 $8：用户名称 $9：应用审计与管理策略名称 $10：应用协议名称 $11：应用行为 $12：应用行为内容 $13：账号 $14：密码 $15：内容 $16：客户端类型 $17：应用软件版本 $18：动作名称，包括如下取值： • Permit：允许 • Deny：阻断 $19：VLAN ID $20：VXLAN ID $21：源地区 $22：目的地区
日志等级	6
举例	AUDIT/6/AUDIT_RULE_MATCH_OTHER_IPV4_LOG:Protocol(1001)=TCP;SrcIPAddr(1003)=1.2.3.4;SrcPort(1004)=8080;DstIPAddr(1007)=6.1.1.1;DstPort(1008)=8080;SrcZoneName(1025)=spf;DstZoneName(1035)=spf;UserName(1113)=hjp;PolicyName(1079)=policy1;Application(1002)=Telnet;Behavior(1101)=Download;BehaviorContent(1102)={Account(1103)=hjk123456,Password(1112)=hhh123,Content(1104)=hello};Client(1110)=PC;SoftVersion(1111)=;Action(1053)=Deny;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
日志说明	当报文与其它类应用的审计规则匹配成功，输出该日志
处理建议	无

14.7 AUDIT_RULE_MATCH_SEARCH_IPV4_LOG（系统日志）

日志内容	Protocol(1001)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];UserName(1113)=[STRING];PolicyName(1079)=[STRING];Application(1002)=[STRING];Behavior(1101)=[STRING];BehaviorContent(1102)={Keyword(1095)=[STRING]};Client(1110)=[STRING];SoftVersion(1111)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
参数解释	$1：协议类型 $2：源IPv4地址 $3：源端口号 $4：目的IPv4地址 $5：目的端口号 $6：源安全域名称 $7：目的安全域名称 $8：用户名称 $9：应用审计与管理策略名称 $10：应用协议名称 $11：应用行为 $12：应用行为内容 $13：关键字 $14：客户端类型 $15：应用软件版本 $16：动作名称，包括如下取值： • Permit：允许 • Deny：阻断 $17：VLAN ID $18：VXLAN ID $19：源地区 $20：目的地区
日志等级	6
举例	AUDIT/6/AUDIT_RULE_MATCH_SEARCH_IPV4_LOG:Protocol(1001)=TCP;SrcIPAddr(1003)=1.2.3.4;SrcPort(1004)=8080;DstIPAddr(1007)=6.1.1.1;DstPort(1008)=8080;SrcZoneName(1025)=spf;DstZoneName(1035)=spf;UserName(1113)=hjp;PolicyName(1079)=policy1;Application(1002)=BaiduSearch;Behavior(1101)=Search;BehaviorContent(1102)={Keyword(1095)=12345678};Client(1110)=PC;SoftVersion(1111)=;Action(1053)=Deny;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
日志说明	当报文与搜索引擎类应用的审计规则匹配成功，输出该日志
处理建议	无

14.8 AUDIT_RULE_MATCH_AS_IPV4_LOG（快速日志）

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];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];UserName(1113)=[STRING];PolicyName(1079)=[STRING];Application(1002)=[STRING];Behavior(1101)=[STRING];BehaviorContent(1102)={Account(1103)=[STRING],Content(1104)=[STRING]};Client(1110)=[STRING];SoftVersion(1111)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
参数解释	$1：协议类型 $2：源IPv4地址 $3：源端口号 $4：NAT地址转换后的源IPv4地址 $5：NAT地址转换后的源端口号 $6：目的IPv4地址 $7：目的端口号 $8：NAT地址转换后的目的IPv4地址 $9：NAT地址转换后的目的端口号 $10：源安全域名称 $11：目的安全域名称 $12：用户名称 $13：应用审计与管理策略名称 $14：应用协议名称 $15：应用行为 $16：应用行为内容 $17：账号 $18：内容 $19：客户端类型 $20：应用软件版本 $21：动作名称，包括如下取值： • Permit：允许 • Deny：阻断 $22：VLAN ID $23：VXLAN ID $24：源地区 $25：目的地区
日志等级	6
举例	AUDIT/6/AUDIT_RULE_MATCH_AS_IPV4_LOG:Protocol(1001)=TCP;SrcIPAddr(1003)=1.2.3.4;SrcPort(1004)=8080;NATSrcIPAddr(1005)=200.20.20.2;NATSrcPort(1006)=50753;DstIPAddr(1007)=6.1.1.1;DstPort(1008)=8080;NATDstIPAddr(1009)=192.168.56.2;NATDstPort(1010)=80;SrcZoneName(1025)=spf;DstZoneName(1035)=spf;UserName(1113)=hjp;PolicyName(1079)=policy1;Application(1002)=tonghuashun;Behavior(1101)=Login;BehaviorContent(1102)={Account(1103)=hjk123456,Content(1104)=hello};Client(1110)=PC;SoftVersion(1111)=;Action(1053)=Deny;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;

日志说明	当报文与娱乐股票类应用的审计规则匹配成功，输出该日志
处理建议	无

14.9 AUDIT_RULE_MATCH_FILE_IPV4_LOG（快速日志）

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];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];UserName(1113)=[STRING];PolicyName(1079)=[STRING];Application(1002)=[STRING];Behavior(1101)=[STRING];BehaviorContent(1102)={Account(1103)=[STRING],FileName(1097)=[STRING]};Client(1110)=[STRING];SoftVersion(1111)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
参数解释	$1：协议类型 $2：源IPv4地址 $3：源端口号 $4：NAT地址转换后的源IPv4地址 $5：NAT地址转换后的源端口号 $6：目的IPv4地址 $7：目的端口号 $8：NAT地址转换后的目的IPv4地址 $9：NAT地址转换后的目的端口号 $10：源安全域名称 $11：目的安全域名称 $12：用户名称 $13：应用审计与管理策略名称 $14：应用协议名称 $15：应用行为 $16：应用行为内容 $17：账号 $18：文件名 $19：客户端类型 $20：应用软件版本 $21：动作名称，包括如下取值： • Permit：允许 • Deny：阻断 $22：VLAN ID $23：VXLAN ID $24：源地区 $25：目的地区
日志等级	6
举例	AUDIT/6/AUDIT_RULE_MATCH_FILE_IPV4_LOG:Protocol(1001)=TCP;SrcIPAddr(1003)=1.2.3.4;SrcPort(1004)=8080;NATSrcIPAddr(1005)=200.20.20.2;NATSrcPort(1006)=50753;DstIPAddr(1007)=6.1.1.1;DstPort(1008)=8080;NATDstIPAddr(1009)=192.168.56.2;NATDstPort(1010)=80;SrcZoneName(1025)=spf;DstZoneName(1035)=spf;UserName(1113)=hjp;PolicyName(1079)=policy1;Application(1002)=ftp;Behavior(1101)=UploadFile;BehaviorContent(1102)={Account(1103)=ghj123,FileName(1097)=abc.txt};Client(1110)=PC;SoftVersion(1111)=;Action(1053)=Deny;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;

日志说明	当报文与文件传输类应用的审计规则匹配成功，输出该日志
处理建议	无

14.10 AUDIT_RULE_MATCH_FORUM_IPV4_LOG（快速日志）

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];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];UserName(1113)=[STRING];PolicyName(1079)=[STRING];Application(1002)=[STRING];Behavior(1101)=[STRING];BehaviorContent(1102)={Account(1103)=[STRING],Content(1104)=[STRING]};Client(1110)=[STRING];SoftVersion(1111)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
参数解释	$1：协议类型 $2：源IPv4地址 $3：源端口号 $4：NAT地址转换后的源IPv4地址 $5：NAT地址转换后的源端口号 $6：目的IPv4地址 $7：目的端口号 $8：NAT地址转换后的目的IPv4地址 $9：NAT地址转换后的目的端口号 $10：源安全域名称 $11：目的安全域名称 $12：用户名称 $13：应用审计与管理策略名称 $14：应用协议名称 $15：应用行为 $16：应用行为内容 $17：账号 $18：内容 $19：客户端类型 $20：应用软件版本 $21：动作名称，包括如下取值： • Permit：允许 • Deny：阻断 $22：VLAN ID $23：VXLAN ID $24：源地区 $25：目的地区
日志等级	6
举例	AUDIT/6/AUDIT_RULE_MATCH_FORUM_IPV4_LOG:Protocol(1001)=TCP;SrcIPAddr(1003)=1.2.3.4;SrcPort(1004)=8080;NATSrcIPAddr(1005)=200.20.20.2;NATSrcPort(1006)=50753;DstIPAddr(1007)=6.1.1.1;DstPort(1008)=8080;NATDstIPAddr(1009)=192.168.56.2;NATDstPort(1010)=80;SrcZoneName(1025)=spf;DstZoneName(1035)=spf;UserName(1113)=hjp;PolicyName(1079)=policy1;Application(1002)=SinaWeibo;Behavior(1101)=Comment;BehaviorContent(1102)={Account(1103)=hjk123456,Content(1104)=hello};Client(1110)=PC;SoftVersion(1111)=;Action(1053)=Deny;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;

日志说明	当报文与社区类应用的审计规则匹配成功，输出该日志
处理建议	无

14.11 AUDIT_RULE_MATCH_IM_IPV4_LOG（快速日志）

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];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];UserName(1113)=[STRING];PolicyName(1079)=[STRING];Application(1002)=[STRING];Behavior(1101)=[STRING];BehaviorContent(1102)={Account(1103)=[STRING],Content(1104)=[STRING],FileName(1097)=[STRING],FileSize(1105)=[STRING]};Client(1110)=[STRING];SoftVersion(1111)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
参数解释	$1：协议类型 $2：源IPv4地址 $3：源端口号 $4：NAT地址转换后的源IPv4地址 $5：NAT地址转换后的源端口号 $6：目的IPv4地址 $7：目的端口号 $8：NAT地址转换后的目的IPv4地址 $9：NAT地址转换后的目的端口号 $10：源安全域名称 $11：目的安全域名称 $12：用户名称 $13：应用审计与管理策略名称 $14：应用协议名称 $15：应用行为 $16：应用行为内容 $17：账号 $18：内容 $19：文件名 $20：文件大小 $21：客户端类型 $22：应用软件版本 $23：动作名称，包括如下取值： • Permit：允许 • Deny：阻断 $24：VLAN ID $25：VXLAN ID $26：源地区 $27：目的地区
日志等级	6
举例	AUDIT/6/AUDIT_RULE_MATCH_IM_IPV4_LOG:Protocol(1001)=TCP;SrcIPAddr(1003)=1.2.3.4;SrcPort(1004)=8080;NATSrcIPAddr(1005)=200.20.20.2;NATSrcPort(1006)=50753;DstIPAddr(1007)=6.1.1.1;DstPort(1008)=8080;NATDstIPAddr(1009)=192.168.56.2;NATDstPort(1010)=80;SrcZoneName(1025)=spf;DstZoneName(1035)=spf;UserName(1113)=hjp;PolicyName(1079)=policy1;Application(1002)=qq;Behavior(1101)=Login;BehaviorContent(1102)={Account(1103)=12345678,Content(1104)=test,FileName(1097)=tex

	t,FileSize(1105)=152389};Client(1110)=PC;SoftVersion(1111)=;Action(1053)=Deny;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
日志说明	当报文与即时通讯类应用的审计规则匹配成功，输出该日志
处理建议	无

14.12 AUDIT_RULE_MATCH_MAIL_IPV4_LOG（快速日志）

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];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];UserName(1113)=[STRING];PolicyName(1079)=[STRING];Application(1002)=[STRING];Behavior(1101)=[STRING];BehaviorContent(1102)={Sender_addr(1106)=[STRING],Receiver_addr(1107)=[STRING],Subject(1108)=[STRING],Body(1109)=[STRING]};Client(1110)=[STRING];SoftVersion(1111)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
参数解释	$1：协议类型 $2：源IPv4地址 $3：源端口号 $4：NAT地址转换后的源IPv4地址 $5：NAT地址转换后的源端口号 $6：目的IPv4地址 $7：目的端口号 $8：NAT地址转换后的目的IPv4地址 $9：NAT地址转换后的目的端口号 $10：源安全域名称 $11：目的安全域名称 $12：用户名称 $13：应用审计与管理策略名称 $14：应用协议名称 $15：应用行为 $16：应用行为内容 $17：发件人 $18：收件人 $19：主题 $20：正文 $21：客户端类型 $22：应用软件版本 $23：动作名称，包括如下取值： • Permit：允许 • Deny：阻断 $24：VLAN ID $25：VXLAN ID $26：源地区 $27：目的地区
日志等级	6
举例	AUDIT/6/AUDIT_RULE_MATCH_MAIL_IPV4_LOG:Protocol(1001)=TCP;SrcIPAddr(1003)=1.2.3.4;SrcPort(1004)=8080;NATSrcIPAddr(1005)=200.20.20.2;NATSrcPort(1006)=50753;DstIPAddr(1007)=6.1.1.1;DstPort(1008)=8080;NATDstIPAddr(1009)=192.168.56.2;NATDstPort(1010)=80;SrcZoneName(1025)=spf;DstZoneName(1035)=spf;UserName(1113)=hjp;PolicyName(1079)=policy1;Application(1002)=smtp;Behavior(1101)=SendMail;BehaviorContent(1102)={Sender_addr(1106)="wb"<wb@ubuntu.wb>,Receiver_addr(1

	107)=<wb@ubuntu.wb>,Subject(1108)=test,Body(1109)=abc};Client(1110)=PC;SoftVersion(1111)=;Action(1053)=Deny;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
日志说明	当报文与邮件类应用的审计规则匹配成功，输出该日志
处理建议	无

14.13 AUDIT_RULE_MATCH_OTHER_IPV4_LOG（快速日志）

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];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];UserName(1113)=[STRING];PolicyName(1079)=[STRING];Application(1002)=[STRING];Behavior(1101)=[STRING];BehaviorContent(1102)={Account(1103)=[STRING],Password(1112)=[STRING],Content(1104)=[STRING]};Client(1110)=[STRING];SoftVersion(1111)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
参数解释	$1：协议类型 $2：源IPv4地址 $3：源端口号 $4：NAT地址转换后的源IPv4地址 $5：NAT地址转换后的源端口号 $6：目的IPv4地址 $7：目的端口号 $8：NAT地址转换后的目的IPv4地址 $9：NAT地址转换后的目的端口号 $10：源安全域名称 $11：目的安全域名称 $12：用户名称 $13：应用审计与管理策略名称 $14：应用协议名称 $15：应用行为 $16：应用行为内容 $17：账号 $18：密码 $19：内容 $20：客户端类型 $21：应用软件版本 $22：动作名称，包括如下取值： • Permit：允许 • Deny：阻断 $23：VLAN ID $24：VXLAN ID $25：源地区 $26：目的地区
日志等级	6
举例	AUDIT/6/AUDIT_RULE_MATCH_OTHER_IPV4_LOG:Protocol(1001)=TCP;SrcIPAddr(1003)=1.2.3.4;SrcPort(1004)=8080;NATSrcIPAddr(1005)=200.20.20.2;NATSrcPort(1006)=50753;DstIPAddr(1007)=6.1.1.1;DstPort(1008)=8080;NATDstIPAddr(1009)=192.168.56.2;NATDstPort(1010)=80;SrcZoneName(1025)=spf;DstZoneName(1035)=spf;UserName(1113)=hjp;PolicyName(1079)=policy1;Application(1002)=Telnet;Behavior(1101)=Download;BehaviorContent(1102)={Account(1103)=hjk123456,Password(1112)=hhh123,Content(1104)=hello};Client(1110)=PC;SoftVersion(1111)=;Action(1053)=Deny;VlanID(11

	75)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
日志说明	当报文与其它类应用的审计规则匹配成功，输出该日志
处理建议	无

14.14 AUDIT_RULE_MATCH_SEARCH_IPV4_LOG（快速日志）

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];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];UserName(1113)=[STRING];PolicyName(1079)=[STRING];Application(1002)=[STRING];Behavior(1101)=[STRING];BehaviorContent(1102)={Keyword(1095)=[STRING]};Client(1110)=[STRING];SoftVersion(1111)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
参数解释	$1：协议类型 $2：源IPv4地址 $3：源端口号 $4：NAT地址转换后的源IPv4地址 $5：NAT地址转换后的源端口号 $6：目的IPv4地址 $7：目的端口号 $8：NAT地址转换后的目的IPv4地址 $9：NAT地址转换后的目的端口号 $10：源安全域名称 $11：目的安全域名称 $12：用户名称 $13：应用审计与管理策略名称 $14：应用协议名称 $15：应用行为 $16：应用行为内容 $17：关键字 $18：客户端类型 $19：应用软件版本 $20：动作名称，包括如下取值： • Permit：允许 • Deny：阻断 $21：VLAN ID $22：VXLAN ID $23：源地区 $24：目的地区
日志等级	6
举例	AUDIT/6/AUDIT_RULE_MATCH_SEARCH_IPV4_LOG:Protocol(1001)=TCP;SrcIPAddr(1003)=1.2.3.4;SrcPort(1004)=8080;NATSrcIPAddr(1005)=200.20.20.2;NATSrcPort(1006)=50753;DstIPAddr(1007)=6.1.1.1;DstPort(1008)=8080;NATDstIPAddr(1009)=192.168.56.2;NATDstPort(1010)=80;SrcZoneName(1025)=spf;DstZoneName(1035)=spf;UserName(1113)=hjp;PolicyName(1079)=policy1;Application(1002)=BaiduSearch;Behavior(1101)=Search;BehaviorContent(1102)={Keyword(1095)=12345678};Client(1110)=PC;SoftVersion(1111)=;Action(1053)=Deny;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
日志说明	当报文与搜索引擎类应用的审计规则匹配成功，输出该日志

处理建议	无

14.15 AUDIT_RULE_MATCH_AS_IPV6_LOG（系统日志）（快速日志）

日志内容	Protocol(1001)=[STRING];SrcIPv6Addr(1036)=[IPADDR];SrcPort(1004)=[UINT16];DstIPv6Addr(1037)=[IPADDR];DstPort(1008)=[UINT16];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];UserName(1113)=[STRING];PolicyName(1079)=[STRING];Application(1002)=[STRING];Behavior(1101)=[STRING];BehaviorContent(1102)={Account(1103)=[STRING],Content(1104)=[STRING]};Client(1110)=[STRING];SoftVersion(1111)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
参数解释	$1：协议类型 $2：源IPv6地址 $3：源端口号 $4：目的IPv6地址 $5：目的端口号 $6：源安全域名称 $7：目的安全域名称 $8：用户名称 $9：应用审计与管理策略名称 $10：应用协议名称 $11：应用行为 $12：应用行为内容 $13：账号 $14：内容 $15：客户端类型 $16：应用软件版本 $17：动作名称，包括如下取值： • Permit：允许 • Deny：阻断 $18：VLAN ID $19：VXLAN ID $20：源地区 $21：目的地区
日志等级	6
举例	AUDIT/6/AUDIT_RULE_MATCH_AS_IPV6_LOG:Protocol(1001)=TCP;SrcIPv6Addr(1036)=2001::2;SrcPort(1004)=51396;DstIPv6Addr(1037)=3001::2;DstPort(1008)=25;SrcZoneName(1025)=spf;DstZoneName(1035)=spf;UserName(1113)=hjp;PolicyName(1079)=policy1;Application(1002)=tonghuashun;Behavior(1101)=Login;BehaviorContent(1102)={Account(1103)=hjk123456,Content(1104)=hello};Client(1110)=PC;SoftVersion(1111)=;Action(1053)=Deny;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
日志说明	当报文与娱乐股票类应用的审计规则匹配成功，输出该日志
处理建议	无

14.16 AUDIT_RULE_MATCH_FILE_IPV6_LOG（系统日志）（快速日志）

日志内容	Protocol(1001)=[STRING];SrcIPv6Addr(1036)=[IPADDR];SrcPort(1004)=[UINT16];DstIPv6Addr(1037)=[IPADDR];DstPort(1008)=[UINT16];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];UserName(1113)=[STRING];PolicyName(1079)=[STRING];Application(1002)=[STRING];Behavior(1101)=[STRING];BehaviorContent(1102)={Account(1103)=[STRING],FileName(1097)=[STRING]};Client(1110)=[STRING];SoftVersion(1111)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
参数解释	$1：协议类型 $2：源IPv6地址 $3：源端口号 $4：目的IPv6地址 $5：目的端口号 $6：源安全域名称 $7：目的安全域名称 $8：用户名称 $9：应用审计与管理策略名称 $10：应用协议名称 $11：应用行为 $12：应用行为内容 $13：账号 $14：文件名 $15：客户端类型 $16：应用软件版本 $17：动作名称，包括如下取值： • Permit：允许 • Deny：阻断 $18：VLAN ID $19：VXLAN ID $20：源地区 $21：目的地区
日志等级	6
举例	AUDIT/6/AUDIT_RULE_MATCH_FILE_IPV6_LOG:Protocol(1001)=TCP;SrcIPv6Addr(1036)=2001::2;SrcPort(1004)=51396;DstIPv6Addr(1037)=3001::2;DstPort(1008)=25;SrcZoneName(1025)=spf;DstZoneName(1035)=spf;UserName(1113)=hjp;PolicyName(1079)=policy1;Application(1002)=ftp;Behavior(1101)=UploadFile;BehaviorContent(1102)={Account(1103)=ghj123,FileName(1097)=abc.txt};Client(1110)=PC;SoftVersion(1111)=;Action(1053)=Deny;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
日志说明	当报文与文件传输类应用的审计规则匹配成功，输出该日志
处理建议	无

14.17 AUDIT_RULE_MATCH_FORUM_IPV6_LOG（系统日志）（快速日志）

日志内容	Protocol(1001)=[STRING];SrcIPv6Addr(1036)=[IPADDR];SrcPort(1004)=[UINT16];DstIPv6Addr(1037)=[IPADDR];DstPort(1008)=[UINT16];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];UserName(1113)=[STRING];PolicyName(1079)=[STRING];Application(1002)=[STRING];Behavior(1101)=[STRING];BehaviorContent(1102)={Account(1103)=[STRING],Content(1104)=[STRING]};Client(1110)=[STRING];SoftVersion(1111)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
参数解释	$1：协议类型 $2：源IPv6地址 $3：源端口号 $4：目的IPv6地址 $5：目的端口号 $6：源安全域名称 $7：目的安全域名称 $8：用户名称 $9：应用审计与管理策略名称 $10：应用协议名称 $11：应用行为 $12：应用行为内容 $13：账号 $14：内容 $15：客户端类型 $16：应用软件版本 $17：动作名称，包括如下取值： • Permit：允许 • Deny：阻断 $18：VLAN ID $19：VXLAN ID $20：源地区 $21：目的地区
日志等级	6
举例	AUDIT/6/AUDIT_RULE_MATCH_FORUM_IPV6_LOG:Protocol(1001)=TCP;SrcIPv6Addr(1036)=2001::2;SrcPort(1004)=51396;DstIPv6Addr(1037)=3001::2;DstPort(1008)=25;SrcZoneName(1025)=spf;DstZoneName(1035)=spf;UserName(1113)=hjp;PolicyName(1079)=policy1;Application(1002)=SinaWeibo;Behavior(1101)=Comment;BehaviorContent(1102)={Account(1103)=hjk123456,Content(1104)=hello};Client(1110)=PC;SoftVersion(1111)=;Action(1053)=Deny;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
日志说明	当报文与社区类应用的审计规则匹配成功，输出该日志
处理建议	无

14.18 AUDIT_RULE_MATCH_IM_IPV6_LOG（系统日志）（快速日志）

日志内容	Protocol(1001)=[STRING];SrcIPv6Addr(1036)=[IPADDR];SrcPort(1004)=[UINT16];DstIPv6Addr(1037)=[IPADDR];DstPort(1008)=[UINT16];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];UserName(1113)=[STRING];PolicyName(1079)=[STRING];Application(1002)=[STRING];Behavior(1101)=[STRING];BehaviorContent(1102)={Account(1103)=[STRING],Content(1104)=[STRING],FileName(1097)=[STRING],FileSize(1105)=[STRING]};Client(1110)=[STRING];SoftVersion(1111)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
参数解释	$1：协议类型 $2：源IPv6地址 $3：源端口号 $4：目的IPv6地址 $5：目的端口号 $6：源安全域名称 $7：目的安全域名称 $8：用户名称 $9：应用审计与管理策略名称 $10：应用协议名称 $11：应用行为 $12：应用行为内容 $13：账号 $14：内容 $15：文件名 $16：文件大小 $17：客户端类型 $18：应用软件版本 $19：动作名称，包括如下取值： • Permit：允许 • Deny：阻断 $20：VLAN ID $21：VXLAN ID $22：源地区 $23：目的地区
日志等级	6
举例	AUDIT/6/AUDIT_RULE_MATCH_IM_IPV6_LOG:Protocol(1001)=TCP;SrcIPv6Addr(1036)=2001::2;SrcPort(1004)=51396;DstIPv6Addr(1037)=3001::2;DstPort(1008)=25;SrcZoneName(1025)=spf;DstZoneName(1035)=spf;UserName(1113)=hjp;PolicyName(1079)=policy1;Application(1002)=qq;Behavior(1101)=Login;BehaviorContent(1102)={Account(1103)=12345678,Content(1104)=test,FileName(1097)=text,FileSize(1105)=152389};Client(1110)=PC;SoftVersion(1111)=;Action(1053)=Deny;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
日志说明	当报文与即时通讯类应用的审计规则匹配成功，输出该日志
处理建议	无

14.19 AUDIT_RULE_MATCH_MAIL_IPV6_LOG（系统日志）（快速日志）

日志内容	Protocol(1001)=[STRING];SrcIPv6Addr(1036)=[IPADDR];SrcPort(1004)=[UINT16];DstIPv6Addr(1037)=[IPADDR];DstPort(1008)=[UINT16];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];UserName(1113)=[STRING];PolicyName(1079)=[STRING];Application(1002)=[STRING];Behavior(1101)=[STRING];BehaviorContent(1102)={Sender_addr(1106)=[STRING],Receiver_addr(1107)=[STRING],Subject(1108)=[STRING],Body(1109)=[STRING]};Client(1110)=[STRING];SoftVersion(1111)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
参数解释	$1：协议类型 $2：源IPv6地址 $3：源端口号 $4：目的IPv6地址 $5：目的端口号 $6：源安全域名称 $7：目的安全域名称 $8：用户名称 $9：应用审计与管理策略名称 $10：应用协议名称 $11：应用行为 $12：应用行为内容 $13：发件人 $14：收件人 $15：主题 $16：正文 $17：客户端类型 $18：应用软件版本 $19：动作名称，包括如下取值： • Permit：允许 • Deny：阻断 $20：VLAN ID $21：VXLAN ID $22：源地区 $23：目的地区
日志等级	6
举例	AUDIT/6/AUDIT_RULE_MATCH_MAIL_IPV6_LOG:Protocol(1001)=TCP;SrcIPv6Addr(1036)=2001::2;SrcPort(1004)=51396;DstIPv6Addr(1037)=3001::2;DstPort(1008)=25;SrcZoneName(1025)=spf;DstZoneName(1035)=spf;UserName(1113)=hjp;PolicyName(1079)=policy1;Application(1002)=smtp;Behavior(1101)=SendMail;BehaviorContent(1102)={Sender_addr(1106)="wb"<wb@ubuntu.wb>,Receiver_addr(1107)=<wb@ubuntu.wb>,Subject(1108)=test,Body(1109)=abc};Client(1110)=PC;SoftVersion(1111)=;Action(1053)=Deny;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
日志说明	当报文与邮件类应用的审计规则匹配成功，输出该日志

处理建议	无

14.20 AUDIT_RULE_MATCH_OTHER_IPV6_LOG（系统日志）（快速日志）

日志内容	Protocol(1001)=[STRING];SrcIPv6Addr(1036)=[IPADDR];SrcPort(1004)=[UINT16];DstIPv6Addr(1037)=[IPADDR];DstPort(1008)=[UINT16];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];UserName(1113)=[STRING];PolicyName(1079)=[STRING];Application(1002)=[STRING];Behavior(1101)=[STRING];BehaviorContent(1102)={Account(1103)=[STRING],Password(1112)=[STRING],Content(1104)=[STRING]};Client(1110)=[STRING];SoftVersion(1111)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
参数解释	$1：协议类型 $2：源IPv6地址 $3：源端口号 $4：目的IPv6地址 $5：目的端口号 $6：源安全域名称 $7：目的安全域名称 $8：用户名称 $9：应用审计与管理策略名称 $10：应用协议名称 $11：应用行为 $12：应用行为内容 $13：账号 $14：密码 $15：内容 $16：客户端类型 $17：应用软件版本 $18：动作名称，包括如下取值： • Permit：允许 • Deny：阻断 $19：VLAN ID $20：VLAN ID $21：源地区 $22：目的地区
日志等级	6
举例	AUDIT/6/AUDIT_RULE_MATCH_OTHER_IPV6_LOG:Protocol(1001)=TCP;SrcIPv6Addr(1036)=2001::2;SrcPort(1004)=51396;DstIPv6Addr(1037)=3001::2;DstPort(1008)=25;SrcZoneName(1025)=spf;DstZoneName(1035)=spf;UserName(1113)=hjp;PolicyName(1079)=policy1;Application(1002)=Telnet;Behavior(1101)=Download;BehaviorContent(1102)={Account(1103)=hjk123456,Password(1112)=hhh123,Content(1104)=hello};Client(1110)=PC;SoftVersion(1111)=;Action(1053)=Deny;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
日志说明	当报文与其它类应用的审计规则匹配成功，输出该日志
处理建议	无

14.21 AUDIT_RULE_MATCH_SEARCH_IPV6_LOG（系统日志）（快速日志）

日志内容	Protocol(1001)=[STRING];SrcIPv6Addr(1036)=[IPADDR];SrcPort(1004)=[UINT16];DstIPv6Addr(1037)=[IPADDR];DstPort(1008)=[UINT16];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];UserName(1113)=[STRING];PolicyName(1079)=[STRING];Application(1002)=[STRING];Behavior(1101)=[STRING];BehaviorContent(1102)={Keyword(1095)=[STRING]};Client(1110)=[STRING];SoftVersion(1111)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
参数解释	$1：协议类型 $2：源IPv6地址 $3：源端口号 $4：目的IPv6地址 $5：目的端口号 $6：源安全域名称 $7：目的安全域名称 $8：用户名称 $9：应用审计与管理策略名称 $10：应用协议名称 $11：应用行为 $12：应用行为内容 $13：关键字 $14：客户端类型 $15：应用软件版本 $16：动作名称，包括如下取值： • Permit：允许 • Deny：阻断 $17：VLAN ID $18：VXLAN ID $19：源地区 $20：目的地区
日志等级	6
举例	AUDIT/6/AUDIT_RULE_MATCH_SEARCH_IPV6_LOG:Protocol(1001)=TCP;SrcIPv6Addr(1036)=2001::2;SrcPort(1004)=51396;DstIPv6Addr(1037)=3001::2;DstPort(1008)=25;SrcZoneName(1025)=spf;DstZoneName(1035)=spf;UserName(1113)=hjp;PolicyName(1079)=policy1;Application(1002)=BaiduSearch;Behavior(1101)=Search;BehaviorContent(1102)={Keyword(1095)=12345678};Client(1110)=PC;SoftVersion(1111)=;Action(1053)=Deny;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
日志说明	当报文与搜索引擎类应用的审计规则匹配成功，输出该日志
处理建议	无

15 AUTOCFG

本节介绍自动配置模块输出的日志信息。

15.1 AUTOCFG_URL_START_SUCCESS

日志内容	URL-based automatic configuration started by [STRING] from [STRING].
参数解释	$1：用户名称 $1：IP地址
日志等级	6
举例	AUTOCFG/6/AUTOCFG_URL_START_SUCCESS: URL-based automatic configuration started by admin from 192.168.111.250.
日志说明	来自某个IP地址的用户开始使用URL方式进行自动配置
处理建议	无

15.2 AUTOCFG_URL_EXECUTE_SUCCESS

日志内容	URL-based automatic configuration finished successfully.
参数解释	无
日志等级	6
举例	AUTOCFG/6/AUTOCFG_URL_EXECUTE_SUCCESS: URL-based automatic configuration finished successfully.
日志说明	使用URL方式进行自动配置成功
处理建议	无

15.3 AUTOCFG_URL_EXECUTE_FAILURE

日志内容	URL-based automatic configuration failed at command line [STRING] and stopped.
参数解释	$1：执行失败的命令行
日志等级	4
举例	AUTOCFG/4/AUTOCFG_URL_EXECUTE_FAILURE: URL-based automatic configuration failed at command line "system-view" and stopped.
日志说明	使用URL方式进行自动配置，执行某条命令行失败，后续命令不再执行
处理建议	收集日志信息并联系技术支持处理

15.4 AUTOCFG_URL_START_FAILED

日志内容	URL-based automatic configuration service by [STRING] from [STRING] failed.
参数解释	$1：用户名称 $1：IP地址
日志等级	5
举例	AUTOCFG/6/AUTOCFG_URL_START_FAILED: URL-based automatic configuration service by admin from 192.168.111.250 failed.
日志说明	来自某个IP地址的用户启动URL自动配置失败
处理建议	检查用户名密码是否配置错误

16 AVC

本节介绍带宽管理模块输出的快速日志信息。

16.1 AVC_MATCH_IPV4_LOG

日志内容	Application(1002)=[STRING];UserName(1113)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[USHORT];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[USHORT];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];PolicyName(1079)=[STRING];VistTime(1114)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
参数解释	$1：应用名称 $2：用户名称 $3：源地址 $4：源端口 $5：目的地址 $6：目的端口 $7：源安全域 $8：目的安全域 $9：策略名称 $10：命中时间 $11：规则动作 $12：VLAN ID $13：VXLAN ID $14：源地区 $15：目的地区
日志等级	6
举例	AVC/6/AVC_MATCH_IPV4_LOG:Application(1002)=App;UserName(1113)=User1;SrcIPAddr(1003)=12.2.2.2;SrcPort(1004)=5141;DstIPAddr(1007)=13.1.1.14;DstPort(1008)=5784;SrcZoneName(1025)=whx;DstZoneName(1035)=hea;PolicyName(1079)=aaa;VistTime(1114)=Wed, 22 May 2019 16:43:47;Action(1053)=drop;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
日志说明	当报文命中带宽管理规则时会以快速日志的方式向日志主机发送日志
处理建议	无

16.2 AVC_MATCH_IPV6_LOG

日志内容	Application(1002)=[STRING];UserName(1113)=[STRING];SrcIPv6Addr(1036)=[IPADDR];SrcPort(1004)=[USHORT];DstIPv6Addr(1037)=[IPADDR];DstPort(1008)=[USHORT];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];PolicyName(1079)=[STRING];VistTime(1114)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
参数解释	$1：应用名称 $2：用户名称 $3：源地址 $4：源端口 $5：目的地址 $6：目的端口 $7：源安全域 $8：目的安全域 $9：策略名称 $10：命中时间 $11：规则动作 $12：VLAN ID $13：VXLAN ID $14：源地区 $15：目的地区
日志等级	6
举例	AVC/6/AVC_MATCH_IPV6_LOG:Application(1002)=App;UserName(1113)=User1;SrcIPv6Addr(1036)=12::2;SrcPort(1004)=5141;DstIPv6Addr(1037)=13::4;DstPort(1008)=5784;SrcZoneName(1025)=whx;DstZoneName(1035)=hea;PolicyName(1079)=aaa;VistTime(1114)=Wed, 22 May 2019 16:52:08;Action(1053)=drop;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
日志说明	当报文命中带宽管理规则时会以快速日志的方式向日志主机发送日志
处理建议	无

16.3 AVC_THRESHOLDWARNING_FASTLOGGING_FMT

日志内容	SrcIPAddr(1003)=[IPADDR];PolicyName(1079)=[STRING];ProfileName(1158)=[STRING];DeviceInfo(1159)=[STRING];BandwidthUpperLimit(1160)=[UINT32];BandwidthLowerLimit(1161)=[UINT32];UpperWarningValue(1162)=[UINT32];LowerWarningValue(1163)=[UINT32];CurRateValue(1164)=[UINT32];WarningTime(1165)=[STRING];WarningDuration(1166)=[UINT32];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];
参数解释	$1：源IP地址 $2：带宽策略名称 $3：带宽通道名称 $4：设备信息 $5：带宽阈值上限值，单位为kbps $6：带宽阈值下限值，单位为kbps $7：达到阈值上限后最高带宽值，单位为kbps $8：达到阈值下限后最低带宽值，单位为kbps $9：实时带宽速率值，单位为kbps $10：告警时间（即设备检测到带宽超过阈值的时间） $11：告警持续时间（即设备检测到带宽超过阈值的持续时间），单位为分钟 $12：VLAN ID $13：VXLAN ID $14：源地区
日志等级	6
举例	AVC/6/AVC_THRESHOLDWARNING_FASTLOGGING_FMT:SrcIPAddr(1003)=192.168.1.8;PolicyName(1079)=a;ProfileName(1158)=p;DeviceInfo(1159)=YuShi;BandwidthUpperLimit(1160)=8366;BandwidthLowerLimit(1161)=2091;UpperWarningValue(1162)=6;LowerWarningValue(1163)=6;CurRateValue(1164)=6;WarningTime(1165)=Fri, 8 Oct 2019 17:38:32;WarningDuration(1166)=7;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;
日志说明	需要同时满足以下条件后，带宽管理模块才会以快速日志的方式向日志主机发送日志： • 有流量触发 • 流量速率超过带宽阈值 • 距离最新一次告警超过一分钟
处理建议	无

16.4 AVC_THRESHOLDWARNING_FASTLOGGING_IPV6FMT

日志内容	SrcIPv6Addr(1036)=[IPADDR];PolicyName(1079)=[STRING];ProfileName(1158)=[STRING];DeviceInfo(1159)=[STRING];BandwidthUpperLimit(1160)=[UINT32];BandwidthLowerLimit(1161)=[UINT32];UpperWarningValue(1162)=[UINT32];LowerWarningValue(1163)=[UINT32];CurRateValue(1164)=[UINT32];WarningTime(1165)=[STRING];WarningDuration(1166)=[UINT32];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];Location(1209)=[STRING];
参数解释	$1：源IPv6地址 $2：带宽策略名称 $3：带宽通道名称 $4：设备信息 $5：带宽阈值上限值，单位为kbps $6：带宽阈值下限值，单位为kbps $7：达到阈值上限后最高带宽值，单位为kbps $8：达到阈值下限后最低带宽值，单位为kbps $9：实时带宽速率值，单位为kbps $10：告警时间（即设备检测到带宽超过阈值的时间） $11：告警持续时间（即设备检测到带宽超过阈值的持续时间），单位为分钟 $12：VLAN ID $13：VXLAN ID $14：地区
日志等级	6
举例	AVC/6/AVC_THRESHOLDWARNING_FASTLOGGING_IPV6FMT:SrcIPv6Addr(1036)=2001::1;PolicyName(1079)=a;ProfileName(1158)=p;DeviceInfo(1159)=YuShi;BandwidthUpperLimit(1160)=8366;BandwidthLowerLimit(1161)=2091;UpperWarningValue(1162)=6;LowerWarningValue(1163)=6;CurRateValue(1164)=6;WarningTime(1165)=Fri, 8 Oct 2019 17:38:32;WarningDuration(1166)=7;VlanID(1175)=400;VNI(1213)=--;Location(1209)=China Macao;
日志说明	需要同时满足以下条件后，带宽管理模块才会以快速日志的方式向日志主机发送日志： • 有流量触发 • 流量速率超过带宽阈值 • 距离最新一次告警超过一分钟
处理建议	无

17 BFD

本节介绍 BFD 模块输出的日志信息。

17.1 BFD_CHANGE_FSM

日志内容	Sess[STRING], Ver, Sta: [STRING]->[STRING], Diag: [STRING]
参数解释	$1：BFD会话的源地址、目的地址、接口和消息类型 $2：变化前状态机的名称 $3：变化后状态机的名称 $4：诊断信息，包括 • 0 (No Diagnostic)：表示 BFD 会话处于 up 状态或未收到 BFD 报文 • 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)：表示本端主动进入会话 down 状态
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: INIT->UP, Diag: 0 (No Diagnostic).
日志说明	BFD会话的状态机发生变化。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

17.2 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	5
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

18 BGP

本节介绍 BGP 模块输出的日志信息。

18.1 BGP_EXCEED_ROUTE_LIMIT

日志内容	BGP.[STRING]: The number of routes from peer [STRING] ([STRING]) exceeds the limit [UINT32].
参数解释	$1：VPN实例名称。如果是公网内的日志信息，则显示为空 $2：BGP对等体的IP地址 $3：BGP对等体的地址族 $4：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.vpn1: The number of routes 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

18.2 BGP_REACHED_THRESHOLD

日志内容	BGP.[STRING]: The proportion of prefixes received from peer [STRING] ([STRING]) to maximum allowed prefixes reached the threshold value ([UINT32]%).
参数解释	$1：VPN实例名称。如果是公网内的日志信息，则显示为空 $2：BGP对等体的IP地址 $3：BGP对等体的地址族 $4：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	5
举例	BGP/5/BGP_REACHED_THRESHOLD: BGP.vpn1: The proportion of prefixes received from peer 1.1.1.1 (IPv4-UNC) to maximum allowed prefixes reached the threshold value (60%).
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

18.3 BGP_MEM_ALERT

日志内容	BGP process received system memory alert [STRING] event.
参数解释	$1：内存告警的类型，包括stop、start
日志等级	5
举例	BGP/5/BGP_MEM_ALERT: BGP process 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

18.4 BGP_PEER_LICENSE_REACHED

日志内容	Number of peers in Established state reached the license limit.
参数解释	无
日志等级	5
举例	BGP/5/BGP_PEER_LICENSE_REACHED: 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

18.5 BGP_ROUTE_LICENSE_REACHED

日志内容	Number of [STRING] routes reached the license limit.
参数解释	$1：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	5
举例	BGP/5/BGP_ROUTE_LICENSE_REACHED: 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

18.6 BGP_STATE_CHANGED

日志内容	形式一： BGP.[STRING]: [STRING] state has changed from [STRING] to [STRING]. 形式二： BGP.[STRING]: [STRING] state has changed from [STRING] to [STRING] for [STRING].
参数解释	形式一： $1：VPN实例名称。如果是公网内的日志信息，则显示为空 $2：BGP对等体的IP地址 $3：变化前的状态名称 $4：变化后的状态名称 形式二： $1：VPN实例名称。如果是公网内的日志信息，则显示为空 $2：BGP对等体的IP地址 $3：变化前的状态名称 $4：变化后的状态名称 $5：状态变化的原因
日志等级	5
举例	BGP/5/BGP_STATE_CHANGED: BGP.vpn1: 192.99.0.2 state has changed from OPENCONFIRM to ESTABLISHED.
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

19 BLS

本节介绍 BLS 模块输出的日志信息。

19.1 BLS_DIP_BLOCK

日志内容	DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];SndDSLiteTunnelPeer(1041)=[STRING].
参数解释	$1：黑名单目的IPv4地址 $2：VPN名称 $3：DS-Lite Tunnel 对端地址
日志等级	3
举例	BLS/3/BLS_DIP_BLOCK:DstIPAddr(1007)=1.1.1.5;RcvVPNInstance(1042)=;SndDSLiteTunnelPeer(1041)=--.
日志说明	流量命中IPv4目的黑名单时，触发日志发送；日志发送时间间隔为30秒
处理建议	无

19.2 BLS_DIPV6_BLOCK

日志内容	DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING].
参数解释	$1：黑名单目的IPv6地址 $2：VPN名称
日志等级	3
举例	BLS/3/BLS_DIPV6_BLOCK: DstIPv6Addr(1037)=200::3;RcvVPNInstance(1042)=.
日志说明	流量命中IPv6目的黑名单时，触发日志发送；日志发送时间间隔为30秒
处理建议	无

19.3 BLS_ENTRY_ADD

日志内容	SrcIPAddr(1003)=[IPADDR]; SndDSLiteTunnelPeer(1041)=[STRING]; RcvVPNInstance(1042)=[STRING]; TTL(1055)=[STRING]; Reason(1056)=[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: -Context=1; SrcIPAddr(1003)=1.1.1.6; SndDSLiteTunnelPeer(1041)=--; RcvVPNInstance(1042)=; TTL(1055)=; Reason(1056)=Configuration. BLS/5/BLS_ENTRY_ADD: -Context=1; SrcIPAddr(1003)=9.1.1.5; SndDSLiteTunnelPeer(1041)=--; RcvVPNInstance(1042)=vpn1; TTL(1055)=10; Reason(1056)=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

19.4 BLS_ENTRY_DEL

日志内容	SrcIPAddr(1003)=[IPADDR]; SndDSLiteTunnelPeer(1041)=[STRING]; RcvVPNInstance(1042)=[STRING]; Reason(1056)=[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: -Context=1; SrcIPAddr(1003)=1.1.1.3; SndDSLiteTunnelPeer(1041)=--; RcvVPNInstance(1042)=; Reason(1056)=Configuration. BLS/5/BLS_ENTRY_DEL: -Context=1; SrcIPAddr(1003)=9.1.1.5; SndDSLiteTunnelPeer(1041)=--; RcvVPNInstance(1042)=vpn1; Reason(1056)=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

19.5 BLS_IP_BLOCK

日志内容	SrcIPAddr(1003)=[IPADDR];RcvVPNInstance(1042)=[STRING];SndDSLiteTunnelPeer(1041)=[STRING].
参数解释	$1：黑名单源IPv4地址 $2：VPN名称 $3：DS-Lite Tunnel 对端地址
日志等级	3
举例	BLS/3/BLS_IP_BLOCK:SrcIPAddr(1003)=1.1.1.3;RcvVPNInstance(1042)=;SndDSLiteTunnelPeer(1041)=--.
日志说明	流量命中IPv4源黑名单或地址对象组黑名单时，触发日志发送；日志发送时间间隔为30秒
处理建议	无

19.6 BLS_IPV6_BLOCK

日志内容	SrcIPv6Addr(1036)=[IPADDR];RcvVPNInstance(1042)=[STRING].
参数解释	$1：黑名单源IPv6地址 $2：VPN名称
日志等级	3
举例	BLS/3/BLS_IPV6_BLOCK: SrcIPv6Addr(1036)=200::2;RcvVPNInstance(1042)=.
日志说明	流量命中IPv6源黑名单时，触发日志发送；日志发送时间间隔为30秒
处理建议	无

19.7 BLS_IPV6_ENTRY_ADD

日志内容	SrcIPv6Addr(1036)=[IPADDR]; RcvVPNInstance(1042)=[STRING]; TTL(1055)=[STRING]; Reason(1056)=[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: -Context=1; SrcIPv6Addr(1036)=2::2; RcvVPNInstance(1042)=; TTL(1055)=; Reason(1056)=Configuration. BLS/5/BLS_IPV6_ENTRY_ADD: -Context=1; SrcIPv6Addr(1036)=1::5; RcvVPNInstance(1042)=; TTL(1055)=10; Reason(1056)=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

19.8 BLS_IPV6_ENTRY_DEL

日志内容	SrcIPv6Addr(1036)=[IPADDR]; RcvVPNInstance(1042)=[STRING]; Reason(1056)=[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: -Context=1; SrcIPv6Addr(1036)=2::2; RcvVPNInstance(1042)=; Reason(1056)=Configuration. BLS/5/BLS_IPV6_ENTRY_DEL: -Context=1; SrcIPv6Addr(1036)=1::5; RcvVPNInstance(1042)=; Reason(1056)= 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

19.9 BLS_ENTRY_USER_ADD

日志内容	User(1098)=[STRING]; TTL(1055)=[STRING]; Reason(1056)=[STRING]; DomainName(1099) =[STRING].
参数解释	$1：黑名单用户名称 $2：老化时间 $3：添加原因 $4：用户所属身份识别域的名称
日志等级	5
举例	BLS/5/BLS_ENTRY_USER_ADD: User(1098)=user1; TTL(1055)=10; Reason(1056)=Configuration; DomainName(1099)=domain1.
日志说明	手动添加一个用户黑名单，触发日志发送
处理建议	无

19.10 BLS_ENTRY_USER_DEL

日志内容	User(1098)=[STRING]; Reason(1056)=[STRING]; DomainName(1099) =[STRING].
参数解释	$1：黑名单用户名称 $2：删除原因，包括： • 手动删除 • 老化删除 $3：用户所属身份识别域的名称
日志等级	5
举例	BLS/5/BLS_ENTRY_USER_DEL: User(1098)=user1; Reason(1056)=Configuration; DomainName(1099)=domain1. BLS/5/BLS_ENTRY_USER_DEL: User(1098)=user1; Reason(1056)=Aging; DomainName(1099)=domain1.
日志说明	删除一个用户黑名单，触发日志发送；老化删除一个黑名单；触发日志发送
处理建议	无

19.11 BLS_USER_IP_BLOCK

日志内容	User(1098)=[STRING];SrcIPAddr(1003)=[IPADDR];DomainName(1099)=[STRING]; RcvVPNInstance(1042)=[STRING];SrcMacAddr(1021)=[STRING].
参数解释	$1：黑名单用户名称 $2：用户IPv4地址 $3：用户所属身份识别域的名称 $4：VPN名称 $5：用户MAC地址
日志等级	3
举例	BLS/3/BLS_USER_IP_BLOCK: User(1098)=user1;SrcIPAddr(1003)=1.1.1.6;DomainName(1099)=; RcvVPNInstance(1042)=;SrcMacAddr(1021)=dc2d-cba7-829a.
日志说明	流量命中IPv4用户黑名单时，触发日志发送；日志发送时间间隔为30秒
处理建议	无

19.12 BLS_USER_IPV6_BLOCK

日志内容	User(1098)=[STRING];SrcIPAddr(1003)=[IPADDR];DomainName(1099)=[STRING];RcvVPNInstance(1042)=[STRING];SrcMacAddr(1021)=[STRING].
参数解释	$1：黑名单用户名称 $2：用户IPv6地址 $3：用户所属身份识别域的名称 $4：VPN名称 $5：用户MAC地址
日志等级	3
举例	BLS/3/BLS_USER_IPV6_BLOCK:User(1098)=user2;SrcIPAddr(1003)=1.1.1.7;DomainName(1099)=;RcvVPNInstance(1042)=;SrcMacAddr(1021)=dc2d-cba7-829b.
日志说明	流量命中IPv6用户黑名单时，触发日志发送；日志发送时间间隔为30秒
处理建议	无

20 CC

本节介绍 CC 攻击防护模块输出的快速日志信息。

20.1 CC_MATCH_IPV4_LOG

日志内容	Protocol(1001)=[STRING];Application(1002)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];PolicyName(1079)=[STRING];RuleName(1080)=[STRING];ProtectedURL(1136)=[STRING];HitSrcIPAddr(1137)=[IPADDR];HitTime(1138)=[STRING];RequestRate(1139)=[UINT32];RequestConcentration(1140)=[UINT32];Action(1053)=[STRING];BlockTime(1141)=[UINT32];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
参数解释	$1：协议类型 $2：应用协议名称 $3：源IP地址 $4：源端口号 $5：目的IP地址 $6：目的端口号 $7：CC策略名称 $8：CC规则名称 $9：命中的防护路径 $10：命中的源IP地址 $11：命中防护路径的时间 $12：请求速率 $13：请求集中度 $14：动作名称，包括如下取值： • Block：源地址阻断 • Permit：允许 $15：阻断时间 $16：VLAN ID $17：VXLAN ID $18：源地区 $19：目的地区
日志等级	6
举例	CC-DEFENSE/6/CC_MATCH_IPV4_LOG:Protocol(1001)=TCP;Application(1002)=SouhuNews;SrcIPAddr(1003)=112.1.1.2;SrcPort(1004)=3887;DstIPAddr(1007)=114.1.1.2;DstPort(1008)=80;PolicyName(1079)=1;RuleName(1080)=test;ProtectedURL(1136)=news.sohu.com/upload/itoolbar/itoolbar.index.loader.20140923.js;HitSrcIPAddr(1137)=112.1.1.2;HitTime(1138)=1480691551;RequestRate(1139)=10;RequestConcentration(1140)=150;Action(1053)=Block;BlockTime(1141)=300;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
日志说明	报文命中CC攻击防护规则且达到检测项阈值时，则生成日志
处理建议	无

20.2 CC_MATCH_IPV6_LOG

日志内容	Protocol(1001)=[STRING];Application(1002)=[STRING];SrcIPv6Addr(1036)=[IPADDR];SrcPort(1004)=[UINT16];DstIPv6Addr(1037)=[IPADDR];DstPort(1008)=[UINT16];PolicyName(1079)=[STRING];RuleName(1080)=[STRING];ProtectedURL(1136)=[STRING];HitSrcIPv6Addr(1037)=[IPADDR];HitTime(1138)=[STRING];RequestRate(1139)=[UINT32];RequestConcentration(1140)=[UINT32];Action(1053)=[STRING];BlockTime(1141)=[UINT32];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
参数解释	$1：协议类型 $2：应用协议名称 $3：源IPV6地址 $4：源端口号 $5：目的IPV6地址 $6：目的端口号 $7：CC策略名称 $8：CC规则名称 $9：命中的防护路径 $10：命中源IPv6地址 $11：命中防护路径的时间 $12：请求速率 $13：请求集中度 $14：动作名称，包括如下取值： • Block：源地址阻断 • Permit：允许 $15：阻断时间 $16：VLAN ID $17：VXLAN ID $18：源地区 $19：目的地区
日志等级	6
举例	CC-DEFENSE/6/CC_MATCH_IPV6_LOG:Protocol(1001)=TCP;Application(1002)=SouhuNews;SrcIPv6Addr(1036)=2001::2;SrcPort(1004)=51396;DstIPv6Addr(1037)=3001::2;DstPort(1008)=25;PolicyName(1079)=1;RuleName(1080)=test;ProtectedURL(1136)=news.sohu.com/upload/itoolbar/itoolbar.index.loader.20140923.js;HitSrcIPv6Addr(1137)=1:2:3:4:5:6:7:8;HitTime(1138)=1480691551;RequestRate(1139)=150;RequestConcentration(1140)=20;Action(1053)=Block;BlockTime(1141)=300;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
日志说明	报文命中CC攻击防护规则达到检测项阈值时，则生成日志
处理建议	无

21 CFD

本节介绍 CFD 模块输出的日志信息。

21.1 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 DC2D-CB33-4401, 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

21.2 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 DC2D-CB33-4401, 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

21.3 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

21.4 CFD_REACH_LOWERLIMIT

日志内容	[STRING] reached or fell below the lower limit [STRING] on MEP [UINT16] in service instance [INT32].
参数解释	$1：检测事件： ○ Bit error ratio：表示比特错误率 ○ Far-end frame loss ratio：表示目标 MEP 的帧丢失率 ○ Near-end frame loss ratio：表示源 MEP 的帧丢失率 ○ Frame delay：表示帧时延 $2：阈值 $3：本地MEP的ID $4：服务实例ID
日志等级	6
举例	CFD/6/ CFD_REACH_LOWERLIMIT: Bit error ratio reached or fell below the lower limit 4% on MEP 2 in service instance 3.
日志说明	检测结果达到或低于下限
处理建议	无

21.5 CFD_REACH_UPPERLIMIT

日志内容	[STRING] reached or exceeded the upper limit [STRING] on MEP [UINT16] in service instance [INT32].
参数解释	$1：检测事件： ○ Bit error ratio：表示比特错误率 ○ Far-end frame loss ratio：表示目标 MEP 的帧丢失率 ○ Near-end frame loss ratio：表示源 MEP 的帧丢失率 ○ Frame delay：表示帧时延 $2：阈值 $3：本地MEP的ID $4：服务实例ID
日志等级	6
举例	CFD/6/ CFD_REACH_UPPERLIMIT: Bit error ratio reached or exceeded the upper limit 80% on MEP in service instance 3.
日志说明	检测结果达到或超过上限
处理建议	无

21.6 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

22 CFGLOG

本节介绍 CFGLOG 模块输出的日志信息。

22.1.1 CFGLOG_CFGOPERATE

日志内容	-Client=[STRING]-User=[STRING]-IPAddr=[STRING]-Role=[STRING];Config in [STRING] changed: -Old setting=[STRING]; -New setting=[STRING];
参数解释	$1：配置方式，包括CLI、NETCONF、SNMP、CWMP、Web配置方式 $2：执行该配置的用户使用的用户名。如果用户登录时未进行用户名认证，则显示为** $3：执行该配置的用户的登录IP地址。如果用户使用Console口登录，则显示为** $4：执行该配置的用户的用户角色 $5：配置路径 $6：修改前的配置 $7：修改后的配置 如果一次配置操作导致了多个配置的变化，$5、$6、$7字段可能出现多次
日志等级	6
举例	CFGLOG/6/CFGLOG_CFGOPERATE: -Client=CLI-User=**-IPAddr=**-Role=network-admin; Config in system changed: -Old setting=sysname Device -New setting=sysname Test.
日志说明	用户修改了设备上的配置
处理建议	无

23 CFGMAN

本节介绍配置管理模块输出的日志信息。

23.1 CFGMAN_ARCHIVE_FAIL

日志内容	Failed to archive the running configuration to a remote server: Location=[STRING]
参数解释	$1：配置文件备份服务器的URL地址。如果是FTP服务器，地址格式为ftp://用户名@服务器地址[:端口号]/文件路径。服务器地址为IPv6地址时，必须用中括号“[]”将IPv6地址括起来。如果是TFTP服务器，则URL地址中不带用户名
日志等级	4
举例	CFGMAN/4/CFGMAN_ARCHIVE_FAIL: Failed to archive the running configuration to a remote server: Location=ftp://admin@192.168.21.21[:21]/test/
日志说明	设备向备份服务器保存配置文件失败时，打印此日志信息
处理建议	1. 确认配置文件是否在本地保存成功 2. 确认服务器能否成功登录 3. 确认服务器的存储空间是否充足

23.2 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 SNMP 或者 SNMP 监控到配置数据库发生变化 • 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

23.3 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

23.4 CFGMAN_REPLACE_CANCEL

日志内容	Configuration rollback from remote server was canceled: Replacement file=[STRING]
参数解释	$1：配置回滚服务器上配置文件的URL地址，如果是FTP服务器，格式为ftp://用户名@服务器地址[:端口号]/文件路径。服务器地址为IPv6地址时，必须用中括号“[]”将IPv6地址括起来。如果是TFTP服务器，则URL地址中不带用户名
日志等级	5
举例	CFGMAN/5/CFGMAN_REPLACE_CANCEL: Configuration rollback from remote server was canceled: Replacement file=ftp://admin@192.168.21.21[:21]/test/startup.cfg
日志说明	使用configuration replace server file命令指定了从远程回滚服务器下载配置文件进行配置回滚的时间，但是，由于系统时间改变导致当前系统时间超过了指定的时间，则取消配置回滚操作。此时打印此日志信息，提示用户本次配置回滚操作被取消
处理建议	请根据需要，重新配置远程配置回滚功能

23.5 CFGMAN_REPLACE_FAIL

日志内容	Failed to replace running configuration with a remote configuration file: File=[STRING]
参数解释	$1：配置回滚服务器上配置文件的URL地址。如果是FTP服务器，格式为ftp://用户名@服务器地址[:端口号]/文件路径。服务器地址为IPv6地址时，必须用中括号“[]”将IPv6地址括起来。如果是TFTP服务器，则URL地址中不带用户名
日志等级	4
举例	CFGMAN/4/CFGMAN_REPLACE_FAIL: Failed to replace running configuration with a remote configuration file: File=ftp://admin@192.168.21.21[:21]/test/startup.cfg
日志说明	设备从配置回滚服务器下载配置文件执行配置回滚失败时，打印此日志信息
处理建议	**1.** 确认服务器能否成功登录 **2.** 确认服务器上是否存在指定的配置文件 **3.** 确认本地磁盘空间是否足够 **4.** 确认配置文件内容、格式是否正确

23.6 CFGMAN_REPLACE_SOON

日志内容	The system will replace running configuration with a remote file in 1 minute: File=[STRING]
参数解释	$1：配置回滚服务器上配置文件的URL地址，如果是FTP服务器，格式为ftp://用户名@服务器地址[:端口号]/文件路径。服务器地址为IPv6地址时，必须用中括号“[]”将IPv6地址括起来。如果是TFTP服务器，则URL地址中不带用户名
日志等级	5
举例	CFGMAN/5/CFGMAN_REPLACE_SOON: The system will replace running configuration with a remote file in 1 minute: File=ftp://admin@192.168.21.21[:21]/test/startup.cfg
日志说明	设备指定时间从配置回滚服务器下载配置文件进行配置回滚，在指定时间的前一分钟打印此日志信息
处理建议	如需取消远程配置回滚操作，请执行undo configuration replace server file命令

24 CGROUP

本节介绍 CGROUP（接口组联动）模块输出的日志信息。

24.1 CGROUP_STATUS_CHANGE

日志内容	The status of collaboration group [UINT32] is [STRING].
参数解释	$1：接口组联动ID $2：接口组联动状态 ○ down：故障 ○ up：正常
日志等级	6
举例	CGROUP/6/CGROUP_STATUS_CHANGE: The status of collaboration group 1 is up.
日志说明	接口组联动链路up或down
处理建议	检查故障链路

25 CONNLMT

本节介绍连接数限制模块输出的日志信息。

25.1 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];Action(1053)=[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 $12：允许/禁止新建连接
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;Action(1053)=Permit new connections;
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

25.2 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

25.3 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];Action(1053)=[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 $12：允许/禁止新建连接
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;Action(1053)=Permit new connections;
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

25.4 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

25.5 CONNLMT_IPV4_RATELIMIT

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];LimitRate(1073)=[UINT32];LimitRuleNum(1051)=[UINT16];Event(1048)=[STRING];Action(1053)=[STRING];
参数解释	$1：全局或接口名称 $2：传输层协议类型 $3：源IPv4地址 $4：目的IPv4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：新建速率的最大值 $10：规则ID $11：Event信息 $12：允许/禁止新建连接
日志等级	6
举例	CONNLMT/6/CONNLMT_IPV4_RATELIMIT: -MDC=1; RcvIfName(1023)=M-GigabitEthernet0/0/0;Protocol(1001)=;SrcIPAddr(1003)=;DstIPAddr(1007)=;ServicePort(1071)=; RcvVPNInstance(1042)=;SndVPNInstance(1043)=;SndDSLiteTunnelPeer(1041)=;LimitRate(1073)=10;LimitRuleNum(1051)=1;Event(1048)=Exceeded rate limit;Action(1053)=Permit new connections;
日志说明	当连接数的新建速率超过最大值时触发日志输出，连续触发时，仅第一次触发时输出日志
处理建议	无

25.6 CONNLMT_IPV6_RATELIMIT

日志内容	RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];ServicePort(1071)=[UINT16];RcvVPNInstance(1042)=[STRING];SndVPNInstance(1043)=[STRING];SndDSLiteTunnelPeer(1041)=[STRING];LimitRate(1073)=[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：新建速率的最大值 $10：规则ID $11：Event信息
日志等级	6
举例	CONNLMT/6/CONNLMT_IPV6_RATELIMIT: -MDC=1; RcvIfName(1023)=M-GigabitEthernet0/0/0;Protocol(1001)=;SrcIPAddr(1036)=;DstIPAddr(1037)=;ServicePort(1071)=; RcvVPNInstance(1042)=;SndVPNInstance(1043)=;SndDSLiteTunnelPeer(1041)=;LimitRate(1073)=10;LimitRuleNum(1051)=1;Event(1048)=Exceeded rate limit;
日志说明	当连接数的新建速率超过最大值时触发日志输出，连续触发时，仅第一次触发时输出日志
处理建议	无

26 CONTEXT

本节介绍 CONTEXT 模块输出的日志信息。

26.1 CAR_DESTROY

日志内容	-Context=[UINT]; The throughput of context [STRING]([UINT]) is changed to default.
参数解释	$1：Context的ID $2：Context的名称 $3：Context的ID
日志等级	6
举例	缺省Context：CAR/6/CAR_DESTROY: The throughput of context slb128(128) is changed to default. 非缺省Context：CAR/6/CAR_ DESTROY:-Context=128; The throughput of context slb128(128) is changed to default.
日志说明	Context的吞吐量恢复到阈值
处理建议	无

26.2 CAR_MODIFY

日志内容	-Context=[UINT]; The throughput of context [STRING]([UINT]) is changed to [UINT] kbps/pps.
参数解释	$1：Context的ID $2：Context的名称 $3：Context的ID $4：Context的吞吐阈值
日志等级	6
举例	缺省Context：CAR/6/CAR_MODIFY: The throughput of context slb128(128) is changed to 66666 pps. 非缺省Context：CAR/6/CAR_MODIFY: -Context=128; The throughput of context slb128(128) is changed to 66666 pps.
日志说明	Context的吞吐阈值发生变化
处理建议	无

26.3 SIB_BROADCAST_DROP

日志内容	Dropped [UINT] broadcast packets of context [UINT].
参数解释	$1：Context的广播报文丢包数 $2：Context的ID
日志等级	6
举例	SIB/6/SIB_BROADCAST_DROP: Dropped 65478 broadcast packets of context 1.
日志说明	Context的广播报文出现丢包
处理建议	无

26.4 SIB_CORE_ATTACK_DROP

日志内容	Dropped [UINT] packets because of core attack.
参数解释	$1：设备的单播报文丢包数
日志等级	6
举例	SIB/6/ SIB_CORE_ATTACK_DROP: Dropped 65478 packets because of core attack.
日志说明	设备的报文出现丢包
处理建议	无

26.5 SIB_MAC_DUPLICATE

日志内容	The new MAC address ([STRING]) of interface [STRING] is already used as the VRRP group MAC address on interface [STRING] of context = [UINT].
参数解释	$1：MAC地址 $2：接口名称 $3：接口名称 $4：Context的ID
日志等级	3
举例	SIB/3/SIB_MAC_DUPLICATE: The new mac address（dc2d-cb45-0902） of interface GigabitEthernet1/0/0 duplicate with virtual MAC address of interface GigabitEthernet1/0/1, context = 2.
日志说明	接口XXX的新实MAC地址与Context xx中接口XXX上的VRRP虚拟MAC地址重复
处理建议	请更改相应接口的实MAC地址

26.6 SIB_MAC_DUPLICATE

日志内容	The VRRP group MAC address ([STRING]) is already used as the MAC address of interface [STRING] on context = [UINT].
参数解释	$1：MAC地址 $2：接口名称 $3：接口名称 $4：Context的ID
日志等级	3
举例	SIB/3/SIB_MAC_DUPLICATE: The vrrp mac address(dc2d-cb45-0902) and mac address of interface GigabitEthernet1/0/0 is duplication, context = 2.
日志说明	Context xxx上接口XXX的VRRP虚mac地址和实mac地址重复
处理建议	请更改相应接口的VRRP虚拟MAC地址

26.7 SIB_MULTICAST_DROP

日志内容	Dropped [UINT] multicast packets of context [UINT].
参数解释	$1：Context的组播报文丢包数 $2：Context的ID
日志等级	6
举例	SIB/6/SIB_MULTICAST_DROP: Dropped 750036 multicast packets of context 1.
日志说明	Context的组播报文出现丢包
处理建议	无

27 DAC

本节介绍数据分析中心模块输出的日志信息。

27.1 DAC_STORE_STATE_STOREFULL

日志内容	DPI/4/DAC_STORE_STATE_STOREFULL: The total storage usage reached 98%.
日志等级	4
举例	DPI/4/DAC_STORE_STATE_STOREFULL: The total storage usage reached 98%.
日志说明	DAC业务的总存储空间使用率已达到98%
处理建议	无

27.2 DAC_STORE_STATE_FULL

日志内容	DPI/4/DAC_STORE_STATE_FULL: The [STRING] alarm threshold (AlarmThreshold(1121)=[STRING]) for StoreName(1119)=[STRING] was reached.
参数解释	$1：门限类型，其取值如下： • storage time-based：数据存储时间上限 • storage space-based：数据存储空间上限 $2：门限值 $3：业务名称
日志等级	4
举例	DPI/4/DAC_STORE_STATE_FULL: The storage space-based alarm threshold (AlarmThreshold(1121)=80%) for StoreName(1119)=audit was reached. DPI/4/DAC_STORE_STATE_FULL: The storage time-based alarm threshold (AlarmThreshold(1121)=30 days) for StoreName(1119)=audit was reached.
日志说明	DAC中指定业务存储空间达到告警门限。设备每隔5分钟对存储空间进行采样，如果达到或超过门限值，则发送一次告警提示
处理建议	无

27.3 DAC_STORE_DELETE_FILE

日志内容	DPI/4/DAC_STORE_DELETE_FILE: Deleted data from the storage space of the [STRING] service because the [STRING] alarm threshold was reached.
参数解释	$1：业务名称 $2：门限类型，其取值如下： • storage time-based：数据保存周期 • storage space-based：存储空间上限
日志等级	4
举例	DPI/4/DAC_STORE_DELETE_FILE: Deleted data from the storage space of the audit service because the storage time-based alarm threshold was reached.
日志说明	指定业务达到数据保存周期，删除保存周期之外的数据 指定业务达到存储空间上限，删除保存时间最长的数据
处理建议	无

27.4 DAC_HDD_FULL

日志内容	DPI/4/DAC_HDD_FULL: New logs will be saved in [STRING] because less than 1 GB of free space is left in the disk.
参数解释	$1：存储介质文件系统名称，取值如下： • hda0: • hda1: • hdb0: • hdb1: • usba0: • usbb0: • usbc0: • memory
日志等级	4
举例	DPI/4/DAC_HDD_FULL: New logs will be saved in memory because less than 1 GB of free space is left in the disk.
日志说明	磁盘空间不足1个G，新的日志将保存到内存中
处理建议	无

28 DEV

本节介绍 DEV（设备管理）模块输出的日志信息。

28.1 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	用户在重启单板，或者单板因为异常而重启
处理建议	1. 检查是否有用户在重启单板 2. 如果没有用户重启，等待单板重新启动后，通过 display version 命令、对应单板信息中的 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

28.2 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

28.3 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

28.4 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	对于单CPU的单板，此日志表示一块新插入的LPU或者备用MPU完成了初始化； 对于多CPU的单板，此日志专指主用CPU完成了初始化，其他CPU完成初始化另有日志信息
处理建议	无

28.5 CFCARD_INSERTED

日志内容	CF card was inserted in [STRING] CF card slot [INT32].
参数解释	$1：chassis编号+slot编号或slot编号 $2：CF卡槽位号
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	一块CF卡安装到了指定槽位
处理建议	无

28.6 CFCARD_REMOVED

日志内容	CF card was removed from [STRING] CF card slot [INT32].
参数解释	$1：chassis编号+slot编号或slot编号 $2：CF卡所在的槽位号
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	一块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

28.7 CHASSIS_REBOOT

日志内容	Chassis [INT32] 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

28.8 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

28.9 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

28.10 FAN_ABSENT

日志内容	形式一： Fan [INT32] is absent. 形式二： Chassis [INT32] 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者风扇被拔出
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，建议安装风扇框 **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

28.11 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

28.12 FAN_FAILED

日志内容	形式一： Fan [INT32] failed. 形式二： Chassis [INT32] 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

28.13 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	5
举例	DEV/5/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

28.14 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

28.15 MAD_PROC

日志内容	[STRING] protocol detected MAD conflict: Local health value=[UINT32], Peer health value=[UINT32].
参数解释	$1：检测到MAD冲突的协议名称，取值为ARP、ND、LACP、BFD $2：本端堆叠的健康值 $3：检测到MAD冲突时对端堆叠的检查值
日志等级	6
举例	DEV/6/MAD_PROC: ARP protocol detected MAD conflict: Local health value=1, Peer health value=0.
日志说明	在IRF组网环境中，ARP、ND、LACP或BFD协议检测到MAD冲突。冲突发生时，记录本端堆叠和对端堆叠的健康值。取值为0时表示健康，取值越大越不健康
处理建议	无

28.16 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

28.17 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

28.18 POWER_FAILED_SHUTDOWN

日志内容	形式一： Power [INT32] shutdown. Reason: temperature of the power is too high. 形式二： Chassis [INT32] power [INT32] shutdown. Reason: temperature of the power is too high.
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_SHUTDOWN: Power 1 shutdown. Reason: temperature of the power is too high.
日志说明	电源模块断电，电源状态为FAILED，原因为电源温度太高
处理建议	请加强电源模块的通风散热，避免电源模块温度过高

28.19 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

28.20 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

28.21 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	5
举例	DEV/5/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

28.22 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	5
举例	DEV/5/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

28.23 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	RPS被拔出
处理建议	**1.** 检查 RPS 电源是否插紧 **2.** 检查 RPS 电源是否损坏 **3.** 重新安装 RPS 电源或更换 RPS 电源

28.24 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	RPS插入后，状态正常
处理建议	无

28.25 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

28.26 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

28.27 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

28.28 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

28.29 SYSTEM_REBOOT

日志内容	System is rebooting now.
参数解释	无
日志等级	5
举例	DEV/5/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

28.30 TEMPERATURE_ALARM

日志内容	形式一： Temperature is greater than the high-temperature alarming threshold on sensor [STRING] [USHOT]. Current temperature is [INT32] degrees centigrade. 形式二： Temperature is greater than the high-temperature alarming threshold on [STRING] sensor [STRING] [USHOT]. Current temperature is [INT32] degrees centigrade. 形式三： Temperature is greater than the high-temperature alarming threshold on [STRING] [STRING] sensor [STRING] [USHOT]. Current temperature is [INT32] degrees centigrade.
参数解释	形式一： $1：传感器类型 $2：传感器ID $3：当前温度，单位为摄氏度 形式二： $1：slot编号 $2：传感器类型 $3：传感器ID $4：当前温度，单位为摄氏度 形式三： $1：chassis编号 $2：slot编号 $3：传感器类型 $4：传感器ID $5：当前温度，单位为摄氏度
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. Current temperature is 80 degrees centigrade.
日志说明	传感器温度超过了严重级（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

28.31 TEMPERATURE_LOW

日志内容	形式一： Temperature is less than the low-temperature threshold on sensor [STRING] [INT32]. Current temperature is [INT32] degrees centigrade. 形式二： Temperature is less than the low-temperature threshold on [STRING] sensor [STRING] [INT32]. Current temperature is [INT32] degrees centigrade. 形式三： Temperature is less than the low-temperature threshold on [STRING] [STRING] sensor [STRING] [INT32]. Current temperature is [INT32] degrees centigrade.
参数解释	形式一： $1：传感器类型 $2：传感器ID $3：当前温度，单位为摄氏度 形式二： $1：slot编号 $2：传感器类型 $3：传感器ID $4：当前温度，单位为摄氏度 形式三： $1：chassis编号 $2：slot编号 $3：传感器类型 $4：传感器ID $5：当前温度，单位为摄氏度
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. Current temperature is -10 degrees centigrade.
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

28.32 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	5
举例	DEV/5/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

28.33 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. Current temperature is [INT32] degrees centigrade. 形式二： Temperature is greater than the high-temperature shutdown threshold on [STRING] sensor [STRING] [INT32]. The slot will be powered off automatically. Current temperature is [INT32] degrees centigrade. 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. Current temperature is [INT32] degrees centigrade.
参数解释	形式一： $1：传感器类型 $2：传感器ID $3：当前温度，单位为摄氏度 形式二： $1：slot编号 $2：传感器类型 $3：传感器ID $4：当前温度，单位为摄氏度 形式三： $1：chassis编号 $2：slot编号 $3：传感器类型 $4：传感器ID $5：当前温度，单位为摄氏度
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. Current temperature is 60 degrees centigrade.
日志说明	传感器温度高过了关断级高温告警门限，设备将自动关闭。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

28.34 TEMPERATURE_WARNING

日志内容	形式一： Temperature is greater than the high-temperature warning threshold on sensor [STRING] [INT32]. Current temperature is [INT32] degrees centigrade. 形式二： Temperature is greater than the high-temperature warning threshold on [STRING] sensor [STRING] [INT32]. Current temperature is [INT32] degrees centigrade. 形式三： Temperature is greater than the high-temperature warning threshold on [STRING] [STRING] sensor [STRING] [INT32]. Current temperature is [INT32] degrees centigrade.
参数解释	形式一： $1：传感器类型 $2：传感器ID $3：当前温度，单位为摄氏度 形式二： $1：slot编号 $2：传感器类型 $3：传感器ID $4：当前温度，单位为摄氏度 形式三： $1：chassis编号 $2：slot编号 $3：传感器类型 $4：传感器ID $5：当前温度，单位为摄氏度
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. Current temperature is 50 degrees centigrade.
日志说明	传感器温度高过了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

28.35 TIMER_CREATE_FAILED_FIRST

日志内容	The process with PID [UINT] failed to create a timer.Reason for the failure:[STRING]
参数解释	$1：创建定时器的进程的PID $2：最近一次创建定时器失败的原因，取值为： Maximum number of timers already reached：设备允许创建的定时器个数达到最大值
日志等级	4
举例	DEV/4/TIMER_CREATE_FAILED_FIRST: The process with PID 70 failed to creadte a timer.Reason for the failure: Maximum number of timers already reached.
日志说明	进程第一次创建定时器失败以及失败的原因。为避免异常情况下，频繁打印该日志，系统对该日志采取抑制输出机制： • 进程第一次创建定时器失败时立即输出 TIMER_CREATE_FAILED_FIRST 日志 • 超过 15 分钟后，如果该进程创建定时器再次失败，则输出日志 TIMER_CREATE_FAILED_MORE，TIMER_CREATE_FAILED_MORE 中会包含上次输出定时器创建失败日志的时间，以及上次输出定时器创建失败日志到本次输出定时器创建失败日志期间创建定时器失败的次数。15 分钟内创建失败的日志会被抑制，不会输出
处理建议	如果进程对应的业务模块的功能受到影响，可重启设备尝试修复或者联系技术支持

28.36 TIMER_CREATE_FAILED_MORE

日志内容	The process with PID [UINT] failed to create a timer:[UINT] consecutive failures since [STRING].Reason for the failure:[STRING]
参数解释	$1：创建定时器的进程的PID $2：距离上次打印日志到当前时间内创建定时器失败的次数 $3：上次打印日志的时间 $4：最近一次创建定时器失败的原因，取值为： Maximum number of timers already reached：设备允许创建的定时器个数达到最大值
日志等级	4
举例	DEV/4/TIMER_CREATE_FAILED_MORE: The process with PID 70 failed to create a timer:2 consecutive failures since 2019/11/21 16:00:00.Reason for the failure: Maximum number of timers already reached.
日志说明	进程第一次创建定时器失败以及失败的原因。为避免异常情况下，频繁打印该日志，系统对该日志采取抑制输出机制： • 进程第一次创建定时器失败时立即输出 TIMER_CREATE_FAILED_FIRST 日志 • 超过 15 分钟后，如果该进程创建定时器再次失败，则输出日志 TIMER_CREATE_FAILED_MORE，TIMER_CREATE_FAILED_MORE 中会包含上次输出定时器创建失败日志的时间，以及上次输出定时器创建失败日志到本次输出定时器创建失败日志期间创建定时器失败的次数。15 分钟内创建失败的日志会被抑制，不会输出
处理建议	如果进程对应的业务模块的功能受到影响，可重启设备尝试修复或者联系技术支持

28.37 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

29 DFILTER

本节介绍数据过滤模块输出的系统日志和快速日志信息。

29.1 DFILTER_IPV4_LOG（系统日志）

日志内容	Protocol(1001)=[STRING];Application(1002)=[STRING];DataDirection(1081)=[STRING];RuleName(1080)=[STRING];PolicyName(1079)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];SrcZone(1025)=[STRING];DstZone(1035)=[STRING];UserName(1113)=[STRING];Action(1053)=[STRING];FileName(1097)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
参数解释	$1：协议类型 $2：应用协议名称 $3：数据方向，包括如下取值： • Upload：上传方向 • Download：下载方向 • Both：双向 $4：配置的规则名称 $5：配置的策略名称 $6：源IP地址 $7：源端口号 $8：目的IP地址 $9：目的端口号 $10：源安全域 $11：目的安全域 $12：身份识别用户的名称 $13：动作名称，包括如下取值： • Permit：允许 • Drop：丢弃 $14：文件名 $15：VLAN ID $16：VXLAN ID $17：源地区 $18：目的地区
日志等级	6
举例	DFILTER/6/DFILTER_IPV4_LOG: Protocol(1001)=TCP;Application(1002)=SMTP;DataDirection(1081)=upload;RuleName(1080)=ruletest;PolicyName(1079)=policytest;SrcIPAddr(1003)=21.22.23.20;SrcPort(1004)=51396;DstIPAddr(1007)=25.26.27.20;DstPort(1008)=25;SrcZone(1025)=in;DstZone(1035)=in;UserName(1113)=abc;Action(1053)=drop;FileName(1097)=123.txt;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
日志说明	报文与配置的数据过滤规则匹配成功时输出该日志
处理建议	无

29.2 DFILTER_IPV6_LOG（系统日志）

日志内容	Protocol(1001)=[STRING];Application(1002)=[STRING];DataDirection(1081)=[STRING];RuleName(1080)=[STRING];PolicyName(1079)=[STRING];SrcIPv6Addr(1036)=[IPADDR];SrcPort(1004)=[UINT16];DstIPv6Addr(1037)=[IPADDR];DstPort(1008)=[UINT16];SrcZone(1025)=[STRING];DstZone(1035)=[STRING];UserName(1113)=[STRING];Action(1053)=[STRING];FileName(1097)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
参数解释	$1：协议类型 $2：应用协议名称 $3：数据方向，包括如下取值： • Upload：上传方向 • Download：下载方向 • Both：双向 $4：配置的规则名称 $5：配置的策略名称 $6：源IPv6地址 $7：源端口号 $8：目的IPv6地址 $9：目的端口号 $10：源安全域 $11：目的安全域 $12：身份识别用户的名称 $13：动作名称，包括如下取值： • Permit：允许 • Drop：丢弃 $14：文件名 $15：VLAN ID $16：VXLAN ID $17：源地区 $18：目的地区
日志等级	6
举例	DFILTER/6/DFILTER_IPV6_LOG: Protocol(1001)=TCP;Application(1002)=SMTP;DataDirection(1081)=upload;RuleName(1080)=ruletest;PolicyName(1079)=policytest;SrcIPv6Addr(1036)=2001::2;SrcPort(1004)=51396;DstIPv6Addr(1037)=3001::2;DstPort(1008)=25;SrcZone(1025)=in;DstZone(1035)=in;UserName(1113)=aaa;Action(1053)=drop;FileName(1097)=123.txt;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
日志说明	IPv6报文与配置的数据过滤规则匹配成功时输出该日志
处理建议	无

29.3 DFILTER_MATCH_IPV4_LOG（快速日志）

日志内容	Protocol(1001)=[STRING];Application(1002)=[STRING];DataDirection(1081)=[STRING];RuleName(1080)=[STRING];PolicyName(1079)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];SrcZone(1025)=[STRING];DstZone(1035)=[STRING];UserName(1113)=[STRING];Action(1053)=[STRING];KeywordGroup(1179)=[STRING];KeywordContent(1181)=[STRING];FileName(1097)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
参数解释	$1：协议类型 $2：应用协议名称 $3：数据方向，包括如下取值： • Upload：上传方向 • Download：下载方向 • Both：双向 $4：配置的规则名称 $5：配置的策略名称 $6：源IP地址 $7：源端口号 $8：目的IP地址 $9：目的端口号 $10：源安全域 $11：目的安全域 $12：身份识别用户的名称 $13：动作名称，包括如下取值： • Permit：允许 • Drop：丢弃 $14：关键字组名称 $15：关键字内容，预定义关键字和自定义关键字显示内容如下： • 预定义关键字显示格式为“关键字名称：关键字内容”，其中部分内容会使用星号*隐藏 • 自定义关键字则直接显示具体的关键字内容 $16：文件名 $17：VLAN ID $18：VXLAN ID $19：源地区 $20：目的地区
日志等级	6
举例	DFILTER/6/DFILTER_MATCH_IPV4_LOG: Protocol(1001)=TCP;Application(1002)=SMTP;DataDirection(1081)=upload;RuleName(1080)=ruletest;PolicyName(1079)=policytest;SrcIPAddr(1003)=21.22.23.20;SrcPort(1004)=51396;DstIPAddr(1007)=25.26.27.20;DstPort(1008)=25;SrcZone(1025)=in;DstZone(1035)=in;UserName(1113)=abc;Action(1053)=drop;KeywordGroup(1179)=3;KeywordContent(1181)=id-card-number:1101***,1501***,phone-number:1353***;FileName(1097)=123.txt;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;

日志说明	报文与配置的数据过滤规则匹配成功时输出该日志
处理建议	无

29.4 DFILTER_MATCH_IPV6_LOG（快速日志）

日志内容	Protocol(1001)=[STRING];Application(1002)=[STRING];DataDirection(1081)=[STRING];RuleName(1080)=[STRING];PolicyName(1079)=[STRING];SrcIPv6Addr(1036)=[IPADDR];SrcPort(1004)=[UINT16];DstIPv6Addr(1037)=[IPADDR];DstPort(1008)=[UINT16];SrcZone(1025)=[STRING];DstZone(1035)=[STRING];UserName(1113)=[STRING];Action(1053)=[STRING];KeywordGroup(1179)=[STRING];KeywordContent(1181)=[STRING];FileName(1097)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
参数解释	$1：协议类型 $2：应用协议名称 $3：数据方向，包括如下取值： • Upload：上传方向 • Download：下载方向 • Both：双向 $4：配置的规则名称 $5：配置的策略名称 $6：源IP地址 $7：源端口号 $8：目的IP地址 $9：目的端口号 $10：源安全域 $11：目的安全域 $12：身份识别用户的名称 $13：动作名称，包括如下取值： • Permit：允许 • Drop：丢弃 $14：关键字组名称 $15：关键字内容，预定义关键字和自定义关键字显示内容如下： • 预定义关键字显示格式为“关键字名称：关键字内容”，其中部分内容会使用星号*隐藏 • 自定义关键字则直接显示具体的关键字内容 $16：文件名 $17：VLAN ID $18：VXLAN ID $19：源地区 $20：目的地区
日志等级	6
举例	DFILTER/6/DFILTER_MATCH_IPV6_LOG: Protocol(1001)=TCP;Application(1002)=SMTP;DataDirection(1081)=upload;RuleName(1080)=ruletest;PolicyName(1079)=policytest;SrcIPv6Addr(1036)=2001::2;SrcPort(1004)=51396;DstIPv6Addr(1037)=3001::2;DstPort(1008)=25;SrcZone(1025)=in;DstZone(1035)=in;UserName(1113)=aaa;Action(1053)=drop;KeywordGroup(1179)=3;KeywordContent(1181)=id-card-number:1101***,1501***,phone-number:1353***;FileName(1097)=123.txt;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;

日志说明	报文与配置的数据过滤规则匹配成功时输出该日志
处理建议	无

30 DHCP

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

30.1 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

30.2 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

31 DHCPS

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

31.1 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 Ethernet0/2, and allocated an IP address 1.0.0.91(lease 86400 seconds) for the DHCP client(MAC dc2d-cb00-905a) 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

31.2 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 Ethernet0/2.
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

31.3 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 Ethernet0/2, and extended lease from p1 pool for the DHCP client (IP 1.0.0.91, MAC dc2d-cb00-905a).
日志说明	IPv4 DHCP服务器为IPv4 DHCP客户端续约
处理建议	无

31.4 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

31.5 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 dc2d-cb00-905a).
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

31.6 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=dc2d-cb01-0104;
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

32 DHCPS6

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

32.1 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

32.2 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

32.3 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

32.4 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

32.5 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

32.6 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

32.7 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

32.8 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

33 DHCPSP4

本节介绍 DHCPSP4 模块输出的 日志信息。

33.1 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

34 DHCPSP6

本节介绍 DHCPSP6 模块输出的 日志信息。

34.1 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

35 DIAG

本节介绍 diagnostic 模块输出的日志信息。

35.1 CORE_EXCEED_THRESHOLD

日志内容	Usage of CPU [int]core [int] exceeded the threshold ([string]).
参数解释	$1：CPU号 $2：CPU核的编号 $2：CPU核利用率告警门限
日志等级	1
举例	DIAG/1/CORE_EXCEED_THRESHOLD: Usage of CPU 0 core 2 exceeded the threshold (1%).
日志说明	系统按周期对CPU核的利用率进行采样，当采样值大于该CPU核的利用率阈值时，产生该日志
处理建议	• 使用 display process 命令查看进程对 CPU 核的占用率，再进一步定位进程是否异常 • 请使用 display cpu-usage configuration 命令查看 CPU 核的利用率阈值，并使用 monitor cpu-usage threshold 命令为不同作用的 CPU 核设置合理阈值，以防日志告警信息频繁输出

35.2 CORE_RECOVERY

日志内容	Core usage alarm CPU [int]core [int]removed.
参数解释	$1：CPU号 $2：CPU核的编号
日志等级	5
举例	DIAG/5/CORE_RECOVERY: Core usage alarm CPU 0 core 1 removed.
日志说明	CPU核利用率低于告警门限值，CPU核从告警状态恢复到正常状态
处理建议	无

35.3 CPU_EXCEED_THRESHOLD

日志内容	CPU usage threshold has been exceeded.
参数解释	无
日志等级	1
举例	DIAG/1/CPU_EXCEED_THRESHOLD: CPU usage threshold has been exceeded.
日志说明	CPU利用率告警。当CPU利用率从小于等于CPU告警阈值变成大于CPU告警阈值时，输出该信息
处理建议	请使用display current-configuration | include "monitor cpu-usage threshold"命令查看CPU的利用率告警门限，如果门限设置不合适，请使用monitor cpu-usage threshold命令修改

35.4 CPU_RECOVER_THRESHOLD

日志内容	CPU usage has dropped down to normal levels.
参数解释	无
日志等级	1
举例	DIAG/1/CPU_RECOVER_THRESHOLD: CPU usage has dropped down to normal levels.
日志说明	CPU利用率告警解除。当CPU利用率从大于等于CPU恢复阈值变成小于CPU恢复阈值时，输出该信息
处理建议	无

35.5 CPU_USAGE_LASTMINUTE

日志内容	CPU usage was [STRING] in last minute.
参数解释	$1：CPU的利用率，为百分比格式
日志等级	5
举例	DIAG/5/CPU_USAGE_LASTMINUTE: CPU usage was 10% in last minute.
日志说明	CPU最近1分钟的平均利用率
处理建议	无

35.6 DIAG_DEADLOOP_DETECT

日志内容	Dead loop detected on [string] cpu [int] core [int].
参数解释	$1：chassis编号+slot编号或slot编号 $2：CPU编号 $3：CPU核编号
日志等级	0
举例	DIAG/0/ DIAG_DEADLOOP_DETECT: Deadloop detected on slot 1 cpu 0 core 0.
日志说明	系统检测到某个内核线程发生了死循环
处理建议	跟踪相关进程检查原因

35.7 DIAG_STORAGE_BELOW_THRESHOLD

日志内容	The usage of [STRING] ([UINT32]%) has dropped below the threshold of [UINT32]%.
参数解释	$1：存储设备的名称，比如flash: $2：存储设备当前的使用率 $3：存储设备使用率阈值
日志等级	1
举例	DIAG/1/DIAG_STORAGE_BELOW_THRESHOLD: The usage of flash (90%) has dropped below the threshold of 95%.
日志说明	存储设备磁盘空间使用率小于或等于阈值
处理建议	无

35.8 DIAG_STORAGE_EXCEED_THRESHOLD

日志内容	The usage of [STRING] ([UINT32]%) exceeded the threshold of [UINT32]%.
参数解释	$1：存储设备的名称，比如flash: $2：存储设备当前的使用率 $3：存储设备使用率的阈值
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	存储设备磁盘空间使用率大于阈值
处理建议	对长期不使用的文件直接删除或者备份到PC后再删除。例如日志文件和旧版本的软件包文件占用存储空间较大，可根据需要选择直接删除或者备份到PC后再删除

35.9 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

35.10 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

35.11 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

35.12 MEM_USAGE_EXCEED_THRESHOLD

日志内容	Memory usage threshold has been exceeded.
参数解释	无
日志等级	1
举例	DIAG/1/MEM_USAGE_EXCEED_THRESHOLD: Memory usage threshold has been exceeded.
日志说明	内存利用率告警。当内存利用率从小于等于内存利用率告警阈值变成大于内存利用率告警阈值时，输出该信息
处理建议	1. 请使用 display memory-threshold 命令查看内存利用率阈值。如果门限设置不合适，请使用 memory-threshold usage 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

35.13 MEM_USAGE_RECOVER_THRESHOLD

日志内容	Memory usage has dropped down to normal levels.
参数解释	无
日志等级	1
举例	DIAG/1/MEM_USAGE_RECOVER_THRESHOLD: Memory usage has dropped down to normal levels.
日志说明	内存利用率告警解除。当内存利用率从大于等于内存利用率恢复阈值变成小于内存利用率恢复阈值时，输出该信息
处理建议	无

35.14 MEM_USAGE

日志内容	Current memory usage is [STRING].
参数解释	$1：内存的利用率，为百分比格式
日志等级	5
举例	DIAG/5/MEM_USAGE: Current memory usage is 10%.
日志说明	设备当前内存利用率
处理建议	无

36 DLDP

本节介绍 DLDP 模块输出的日志信息。

36.1 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 o AUTHENTICATION PASSWORD：表示验证字不匹配 o AUTHENTICATION TYPE：表示验证类型不匹配 o 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

36.2 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

36.3 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 o DLDP automatically blocked the interface：表示 DLDP 自动关闭了端口 o 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

36.4 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 dc2d-cb69-5f21, 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

36.5 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 dc2d-cb69-5f21, 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

36.6 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 dc2d-cb69-5f21, 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

37 DNS

本节介绍 DNS（Domain Name System）模块输出的日志信息。

37.1 DNS_SNOOPING_LOG

日志内容	UserName=[STRING], UserGroup=[STRING], SrcDeviceType=[STRING], SrcOs=[STRING], SrcMAC=[UINT64], SrcIPAddr=[UINT32], SrcPort=[UINT16], DstIPAddr=[UINT32], DstPort=[UINT16], Domain=[STRING], ResponseContent=[UINT32], Protocol=[UINT16], ReqByteCount=[UINT64], ResByteCount=[UINT64], ReqPktCount=[UINT64], ResPktCount=[UINT64], ResponseCode=[UINT4], ResquestID=[UINT16], ResponseID=[UINT16], ReqType=[UINT16], Direction=[UINT16], ResFirstAnswerTTL=[UINT32].
参数解释	$1：用户名称 $2：用户组名称 $3：终端类型 $4：终端操作系统 $5：源MAC地址 $6：源IP地址 $7：源端口号 $8：目的IP地址 $9：目的端口 $10：要解析的域名 $11：返回内容 $12：协议号 $13：请求流量 $14：响应流量 $15：请求报文数 $16：响应报文数 $17：应答的RCODE字段，取值包括： • 0：成功的响应 • 1：格式错误 • 2：服务器错误 • 3：名字错误 • 4：域名服务器不支持请求的类型 • 5：域名服务器因为策略的原因拒绝执行请求的操作。例如域名服务器不会为特定的请求者返回查询结果 $18：请求标识 $19：应答标识 $20：请求报文查询问题的类型 $21：报文方向标识，取值包括： • 0：请求方向 • 1：应答方向 • 2：双向 $22：应答报文中Answer域里的第一个TTL取值
日志等级	6
举例	DNS/6/DNS_SNOOPING_LOG: UserName=, UserGroup=, SrcDeviceType=, SrcOs=, SrcMAC= DC2D-CB00-0000, SrcIPAddr=3.3.3.1, SrcPort=9931, DstIPAddr=3.3.3.2, DstPort=53, Domain=tt, ResponseContent=1.1.1.1, Protocol=17, ReqByteCount=20,

	ResByteCount=36, ReqPktCount=1, ResPktCount=1, ResponseCode=0, ResquestID=44569, ResponseID=44569, ReqType=1, Direction=2, ResFirstAnswerTTL=3600.
日志说明	设备每隔5秒或者完成一次DNS会话（收到请求报文，并收到对应的响应报文）后，会将本日志输出到快速日志功能模块，快速日志功能模块会将本日志发送给日志主机。其它功能模块可以根据本日志内容，对网络的DNS流量进行分析 为了输出本日志，需要执行**dns snooping log enable**命令开启DNS Snooping日志功能 为了成功的将本日志发送给日志主机，需要执行**customlog host**命令配置日志主机的相关参数、执行**customlog format dns**命令开启DNS快速日志输出功能
处理建议	无

38 DOT1X

本节介绍 802.1X（DOT1X）模块输出的日志信息。

38.1 DOT1X_LOGIN_FAILURE

日志内容	-IfName=[STRING]-MACAddr=[STRING]-VLANId=[STRING]-UserName=[STRING] -ErrCode=[STRING]; The user failed the 802.1X authentication. Reason: [STRING].
参数解释	$1：接口名 $2：MAC地址 $3：VLAN ID $4：用户名 $5：错误码 o 1：客户端主动下线 o 2：端口状态错误 o 3：客户端重启（暂不支持） o 4：重认证失败 o 5：设备强制取消授权 o 6：端口重启 o 7：授权数据与服务器下发不一致，强制用户下线 o 8：用户名、密码错误或者服务器端没有配置设备信息 o 9：握手失联，设备收不到客户端的握手报文 o 10：闲置切断 o 11：服务器下发的用户时长用尽 o 12：服务器强制用户下线 o 13：实时计费失败 o 14：其它错误 o 15：端口事件导致用户下线 $6：用户802.1X认证失败的原因： o Authorization Mac-Address process failed：授权 MAC 地址失败 o Authorization VLAN process failed：授权 VLAN 失败 o Authorization ACL process failed：授权 ACL 失败 o Authorization UserProfile process failed：授权 User Profile 失败
日志等级	6
举例	DOT1X/6/DOT1X_LOGIN_FAILURE: -IfName=GigabitEthernet1/0/1-MACAddr=DC2D-CB01-0020-VLANId=2-Username=aaa-ErrCode=5; The user failed the 802.1X authentication. Reason: Authorization ACL process failed.
日志说明	用户802.1X认证失败
处理建议	根据失败原因修改相关配置

38.2 DOT1X_LOGIN_SUCC

日志内容	-IfName=[STRING]-MACAddr=[STRING]-AccessVLANId=[STRING]-AuthorizationVLANId=[STRING]-Username=[STRING]; The user passed 802.1X authentication and got online successfully.
参数解释	$1：接口名 $2：MAC地址 $3：接入VLAN ID $4：授权VLAN ID $5：用户名
日志等级	6
举例	DOT1X/6/DOT1X_LOGIN_SUCC:-IfName=GigabitEthernet1/0/4-MACAddr=dc2d-cb00-22b9-AccessVLANId=444-AuthorizationVLANId=444-Username=aaa; The user passed 802.1X authentication and got online successfully.
日志说明	802.1X用户认证成功
处理建议	无

38.3 DOT1X_LOGOFF

日志内容	-IfName=[STRING]-MACAddr=[STRING]-VLANId=[STRING]-Username=[STRING]-ErrCode=[STRING]; Session of the 802.1X user was terminated.
参数解释	$1：接口名 $2：MAC地址 $3：VLAN ID $4：用户名 $5：错误码 ○ 1：客户端主动下线 ○ 2：端口状态错误 ○ 3：客户端重启（暂不支持） ○ 4：重认证失败 ○ 5：设备强制取消授权 ○ 6：端口重启 ○ 7：授权数据与服务器下发不一致，强制用户下线 ○ 8：用户名、密码错误或者服务器端没有配置设备信息 ○ 9：握手失联，设备收不到客户端的握手报文 ○ 10：闲置切断 ○ 11：服务器下发的用户时长用尽 ○ 12：服务器强制用户下线 ○ 13：实时计费失败 ○ 14：其它错误 ○ 15：端口事件导致用户下线
日志等级	6
举例	DOT1X/6/DOT1X_LOGOFF:-IfName=GigabitEthernet1/0/4-MACAddr=dc2d-cb00-22b9-VLANId=444-Username=aaa-ErrCode=11; Session of the 802.1X user was terminated.
日志说明	802.1X用户下线
处理建议	• 若 802.1X 用户主动下线，则不用排查问题 • 若 802.1X 用户异常下线，则需要根据调试信息定位并解决问题

38.4 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

38.5 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

38.6 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

38.7 DOT1X_NOTENOUGH_EADMACREDIR_RES

日志内容	Failed to issue 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 issue a rule for redirecting HTTP packets with source MAC address dc2d-cb00-5915 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

38.8 DOT1X_NOTENOUGH_ENABLEDOT1X_RES

日志内容	Failed to enable 802.1X feature 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 feature 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

38.9 DOT1X_NOTSUPPORT_EADFREEIP_RES

日志内容	Failed to assign a rule for free IP [IPADDR] on interface [STRING]: EAD assistant was not supported.
参数解释	$1：IP地址 $2：接口名
日志等级	3
举例	DOT1X/3/DOT1X_NOTSUPPORT_EADFREEIP_RES: Failed to assign a rule for free IP 1.1.1.0 on interface Ethernet3/1/2: EAD assistant was not supported.
日志说明	当在接口上使能802.1X特性时，由于板卡不支持EAD相关功能，设备在接口上下发Free IP失败
处理建议	无

38.10 DOT1X_NOTSUPPORT_EADFREERULE_RES

日志内容	Failed to assign a rule for permitting DHCP and DNS packets on interface [STRING]: EAD assistant was not supported.
参数解释	$1：接口名
日志等级	3
举例	DOT1X/3/DOT1X_NOTSUPPORT_EADFREERULE_RES: Failed to assign a rule for permitting DHCP and DNS packets on interface Ethernet3/1/2: EAD assistant was not supported.
日志说明	当在接口上使能802.1X特性时，由于板卡不支持EAD相关功能，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	无

38.11 DOT1X_NOTSUPPORT_EADMACREDIR_RES

日志内容	Failed to assign a rule for redirecting HTTP packets with source MAC address [MAC] on interface [STRING]: EAD assistant was not supported.
参数解释	$1：接口名
日志等级	3
举例	DOT1X/3/DOT1X_NOTSUPPORT_EADMACREDIR_RES: Failed to assign a rule for redirecting HTTP packets with source MAC address dc2d-cb00-5915 on interface Ethernet3/1/2: EAD assistant was not supported.
日志说明	当在接口上使能802.1X特性时，由于板卡不支持EAD相关功能，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	无

38.12 DOT1X_NOTSUPPORT_EADPORTREDIR_RES

日志内容	Failed to assign a rule for redirecting HTTP packets on interface [STRING]: EAD assistant was not supported.
参数解释	$1：接口名
日志等级	3
举例	DOT1X/3/DOT1X_NOTSUPPORT_EADPORTREDIR_RES: Failed to assign a rule for redirecting HTTP packets on interface Ethernet3/1/2: EAD assistant was not supported.
日志说明	当在接口上使能802.1X特性时，由于板卡不支持EAD相关功能，设备不能下发规则允许该接口重定向HTTP报文
处理建议	无

38.13 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

38.14 DOT1X_WLAN_LOGIN_FAILURE

日志内容	-Username=[STRING]-UserMAC=[STRING]-SSID=[STRING]-APName=[STRING]-RadioID=[STRING]-VLANID=[STRING]; A user failed 802.1X authentication. Reason: [STRING].

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AP
	$5：用户上线的Radio ID
	$6：用户上线的VLAN ID
	$7：用户802.1X认证失败的原因：
	• AAA processed authentication request and returned error code *code*：AAA 处理认证请求并返回错误码 *code*，*code* 取值如下：
	  ○ 4：认证域不存在
	  ○ 8：认证域下的配置错误/服务器上配置的共享密钥与设备配置的共享密钥不一致/认证端口 1812 没有开启/服务器与设备网络不可达
	  ○ 26：用户名或密码错误/认证类型错误/服务器上没有添加设备 IP 地址/服务模板下认证域配置错误
	• AAA processed authorization request and returned error code *code*：AAA 处理授权请求并返回错误码 *code*，*code* 取值如下：
	  ○ 8：服务器与设备网络不可达
	• AAA processed accounting-start request and returned error code *code*：AAA 处理计费开始请求并返回错误码 *code*，*code* 取值如下：
	  ○ 8：服务器与设备网络不可达
	• AAA processed accounting-update request and returned error code code：AAA 处理计费更新请求并返回错误码 code，code 取值如下：
	  ○ 8：服务器与设备网络不可达
	• Received logoff request from the client：收到用户主动下线报文
	• Client timeout timer expired：用户定时器超时
	• Server timeout timer expired：服务器定时器超时
	• Received logoff request while authenticating the client：当用户正在认证时收到用户主动下线请求报文
	• Received user security information and kicked off the client：收到用户安全信息，删除用户
	• Accounting-update timer expired, and no responses were received from the server：计费更新定时器超时，没有收到服务器的回应
	• Kicked off the client when the idle timeout timer expired：Idle-cut 定时器超时，强制用户下线
	• Authentication method error：认证模式错误
	• Kicked off the client because the server-assigned session timeout timer is 0：服务器下发的会话时长为 0，强制用户下线
	• Received session disconnection event：收到服务器断开会话连接事件
	• Received nonexistent authorization VLAN group：收到不存在的授权 vlan 组
	• Client kicked out on expiration of the idle-cut timer because its total traffic had not reached the required minimum amount of traffic：在更新计费流量时，客户端使用流

	量低于 idle-cut 流量 • Had failed to obtain the client IP address before the accounting delay timer expired：计费延迟定时器超时且客户端没有获取到 IP 地址 • Unknown reason：其它未知原因
日志等级	5
举例	DOT1X/5/DOT1X_WLAN_LOGIN_FAILURE:-Username=Dot1X-UserMAC=dc2d-cb16-28cd-SSID=text-wifi-APName=ap1-RadioID=2-VLANID=11; A user failed 802.1X authentication. Reason: AAA processed authentication request and returned error code 26.
日志说明	AAA处理认证请求并且返回错误码26，用户802.1X认证失败
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 • 在认证过程中返回的错误码可能对应多种情况，请逐一排查

38.15 DOT1X_WLAN_LOGIN_SUCC

日志内容	-Username=[STRING]-UserMAC=[STRING]-SSID=[STRING]-APName=[STRING]-RadioID=[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AP $5：用户上线的Radio ID $6：用户上线的VLAN ID
日志等级	6
举例	DOT1X/6/DOT1X_WLAN_LOGIN_SUCC:-Username=Dot1X-UserMAC=dc2d-cb16-28cd-SSID=text-wifi-APName=ap1-RadioID=2-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

38.16 DOT1X_WLAN_LOGOFF

日志内容	Username=[STRING]-UserMAC=[STRING]-SSID=[STRING]-APName=[STRING]-Radio ID=[STRING]-VLANID=[STRING]; Session for an 802.1X user was terminated. Reason: [STRING].

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AP
	$5：用户上线的Radio ID
	$6：用户上线的VLAN ID
	$7：用户的下线原因：
	• AAA processed authentication request and returned error code code. Server reason: reason：AAA 处理认证请求，设备返回错误码 code，服务器返回失败原因 reason，当服务器未返回失败原因时，不显示此字段。code 取值如下：
	  ○ 4：认证域不存在
	  ○ 8：认证域下的配置错误/服务器上配置的共享密钥和用户配置的共享密钥不一致/认证端口 1812 没有开启/服务器与设备网络不可达
	  ○ 26：用户名或密码错误/认证类型错误/服务器上没有添加设备 IP 地址/服务模板下认证域配置错误
	• AAA processed authorization request and returned error code code. Server reason: reason：AAA 处理认证请求，设备返回错误码 code，服务器返回失败原因 reason，当服务器未返回失败原因时，不显示此字段。code 取值如下：
	  ○ 8：服务器与设备网络不可达
	• AAA processed accounting-start request and returned error code code. Server reason: reason：AAA 处理认证请求，设备返回错误码 code，服务器返回失败原因 reason，当服务器未返回失败原因时，不显示此字段。code 取值如下：
	  ○ 8：服务器与设备网络不可达
	• AAA processed accounting-update request and returned error code code. Server reason: reason：AAA 处理认证请求，设备返回错误码 code，服务器返回失败原因 reason，当服务器未返回失败原因时，不显示此字段。code 取值如下：
	  ○ 8：服务器与设备网络不可达
	• Received logoff request from the client：收到用户主动下线报文
	• User timer expired：用户定时器超时
	• Server timer expired：服务器定时器超时
	• Received logoff request while authenticating the client：当用户认证时收到用户主动下线报文
	• Received user security information and kicked off the client：收到用户安全信息，删除用户
	• Lost in shaking hands：握手失联
	• Accounting-update timer expired, and no responses were received from the server：计费更新定时器超时，没有收到服务器的回应
	• Kicked off the client when the idle timeout timer expired：Idle-cut 定时器超时，强制用户下线
	• Authentication method error：认证模式错误
	• Kicked off the client because the server-assigned session timeout timer is 0：服务器下发的会话时长为 0，强制用户下线

	• Received session disconnection event：收到服务器断开会话连接事件 • Received disassociation frame in Run state: reason code=code：在线状态收到终端去关联报文 • Received deauthentication frame in Run state: reason code=code：在线状态收到终端去认证报文 • Received disassociation packet in Userauth state：用户认证状态收到去关联报文 • Received deauthentication packet in Userauth state：用户认证状态收到去认证报文 • Received client failure message with reason code=code：其他场景收到用户上线失败消息 • Received client offline message with reason code=code：其他场景收到用户下线消息 • Unknown reason：其它未知原因
日志等级	6
举例	DOT1X/6/DOT1X_WLAN_LOGOFF:-Username=Dot1X-UserMAC=dc2d-cb16-28cd-SSID=text-wifi-APName=ap1-RadioID=2-VLANID=11; Session for an 802.1X user was terminated. Reason: Received logoff request from the client.
日志说明	收到用户主动下线报文，802.1X用户下线
处理建议	• 若 802.1X 用户主动下线，则不用排查问题 • 若 802.1X 用户异常下线，则需要根据调试信息定位并解决问题

39 EDEV

本节介绍扩展设备管理模块输出的日志信息。

39.1 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： o primary 表示备份组中 primary 节点处理业务 o 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: 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

40 EIGRP

本节介绍 EIGRP 模块输出的日志信息。

40.1 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

40.2 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40-1
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40-1进行处理

表40-1 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

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

41 ERPS

本节介绍 ERPS 模块输出的日志信息。

41.1 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

42 ETHOAM

本节介绍 ETHOAM 模块输出的日志信息。

42.1 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

42.2 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

42.3 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

42.4 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

42.5 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

42.6 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

42.7 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

42.8 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

42.9 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

42.10 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

42.11 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

42.12 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

42.13 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

42.14 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

42.15 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

42.16 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

42.17 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

42.18 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

42.19 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

42.20 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

42.21 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

42.22 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

42.23 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

42.24 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

42.25 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

42.26 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

42.27 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

42.28 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

42.29 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

42.30 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

42.31 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

43 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。

43.1 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

43.2 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

43.3 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

43.4 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

44 EVIISIS

本节介绍 EVI IS-IS 模块输出的日志信息。

44.1 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

44.2 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

45 FCLINK

本节介绍 FCLINK 模块输出的日志信息。

45.1 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

45.2 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

46 FCOE

本节介绍 FCOE 模块输出的日志信息。

46.1 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

47 FCZONE

本节介绍 FCZONE 模块输出的日志信息。

47.1 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

47.2 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

47.3 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

47.4 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

47.5 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=Fc0/2/7; 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

47.6 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=Fc0/2/7-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

47.7 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

48 FFILTER

本节介绍文件过滤模块输出的系统日志和快速日志信息。

48.1 FFILTER_IPV4_LOG

日志内容	Protocol(1001)=[STRING];Application(1002)=[STRING];DataDirection(1081)=[STRING];RuleName(1080)=[STRING];PolicyName(1079)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];SrcZone(1025)=[STRING];DstZone(1035)=[STRING];UserName(1113)=[STRING];Action(1053)=[STRING];Filetype(1096)=[STRING];FileName(1097)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
参数解释	$1：协议类型 $2：应用协议名称 $3：数据方向，包括如下取值： • Upload：上传方向 • Download：下载方向 • Both：双向 $4：配置的规则名称 $5：配置的策略名称 $6：源IP地址 $7：源端口号 $8：目的IP地址 $9：目的端口号 $10：源安全域 $11：目的安全域 $12：身份识别用户的名称 $13：动作名称，包括如下取值： • Permit：允许 • Drop：丢弃 $14：文件类型 $15：文件名 $16：Vlan ID $17：Vxlan ID $18：源地区 $19：目的地区
日志等级	6
举例	FFILTER/6/FFILTER_IPV4_LOG:-MDC=1;Protocol(1001)=TCP;Application(1002)=SMTP;DataDirection(1081)=upload;RuleName(1080)=ruletest;PolicyName(1079)=policytest;SrcIPAddr(1003)=21.22.23.20;SrcPort(1004)=51396;DstIPAddr(1007)=25.26.27.20;DstPort(1008)=25;SrcZone(1025)=in;DstZone(1035)=in;UserName(1113)=abc;Action(1053)=drop;Filetype(1096)=txt;FileName(1097)=abc.txt;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
日志说明	报文与配置的文件过滤规则匹配成功时输出该日志
处理建议	无

48.2 FFILTER_IPV6_LOG

日志内容	Protocol(1001)=[STRING];Application(1002)=[STRING];DataDirection(1081)=[STRING];RuleName(1080)=[STRING];PolicyName(1079)=[STRING];SrcIPv6Addr(1036)=[IPADDR];SrcPort(1004)=[UINT16];DstIPv6Addr(1037)=[IPADDR];DstPort(1008)=[UINT16];SrcZone(1025)=[STRING];DstZone(1035)=[STRING];UserName(1113)=[STRING];action(1053)=[STRING];Filetype(1096)=[STRING];FileName(1097)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
参数解释	$1：协议类型 $2：应用协议名称 $3：数据方向，包括如下取值： • Upload：上传方向 • Download：下载方向 • Both：双向 $4：配置的规则名称 $5：配置的策略名称 $6：源IPv6地址 $7：源端口号 $8：目的IPv6地址 $9：目的端口号 $10：源安全域 $11：目的安全域 $12：身份识别用户的名称 $13：动作名称，包括如下取值： • Permit：允许 • Drop：丢弃 $14：文件类型 $15：文件名 $16：Vlan ID $17：Vxlan ID $18：源地区 $19：目的地区
日志等级	6
举例	FFILTER/6/FFILTER_IPV6_LOG:-MDC=1;Protocol(1001)=TCP;Application(1002)=SMTP;DataDirection(1081)=upload;RuleName(1080)=ruletest;PolicyName(1079)=policytest;SrcIPv6Addr(1036)=2001::2;SrcPort(1004)=51396;DstIPv6Addr(1037)=3001::2;DstPort(1008)=25;SrcZone(1025)=in;DstZone(1035)=in;UserName(1113)=aaa;Action(1053)=drop;Filetype(1096)=txt;FileName(1097)=abc.txt;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
日志说明	IPv6报文与配置的文件过滤规则匹配成功时输出该日志
处理建议	无

49 FILTER

本节介绍 FILTER 模块输出的日志信息。

49.1 FILTER_EXECUTION_ICMP

日志内容	RcvIfName(1023)=[STRING];Direction(1070)=[STRING];Type(1067)=[STRING];Acl(1068)=[STRING];RuleID(1078)=[UINT32];Protocol(1001)=[STRING];SrcIPAddr(1003)=[IPADDR];DstIPAddr(1007)=[IPADDR];IcmpType(1062)=[STRING]([UINT16]);IcmpCode(1063)=[UINT16];MatchCount(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：ACL规则编号 $6：四层协议名称 $7：源IP地址 $8：目的IP地址 $9：ICMP类型 $10：ICMP代码 $11：命中次数 $12：事件信息
日志等级	6
举例	FILTER/6/FILTER_EXECUTION_ICMP: RcvIfName(1023)=GigabitEthernet2/0/2;Direction(1070)=inbound;Type(1067)=IPv4;Acl(1068)=3000;RuleID(1078)=0;Protocol(1001)=ICMP;SrcIPAddr(1003)=100.1.1.1;DstIPAddr(1007)=200.1.1.1;IcmpType(1062)=Echo(8);IcmpCode(1063)=0;MatchCount(1069)=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

49.2 FILTER_EXECUTION_ICMPV6

日志内容	RcvIfName(1023)=[STRING];Direction(1070)=[STRING];Type(1067)=[STRING];Acl(1068)=[STRING];RuleID(1078)=[UINT32];Protocol(1001)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];Icmpv6Type(1064)=[STRING]([UINT16]);Icmpv6Code(1065)=[UINT16];MatchCount(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：ACL规则编号 $6：四层协议名称 $7：源IPv6地址 $8：目的IPv6地址 $9：ICMPV6类型 $10：ICMPV6代码 $11：命中次数 $12：事件信息
日志等级	6
举例	FILTER/6/FILTER_EXECUTION_ICMPV6: RcvIfName(1023)=GigabitEthernet2/0/2;Direction(1070)=inbound;Type(1067)=IPv6;Acl(1068)=3000;RuleID(1078)=0;Protocol(1001)=ICMPV6;SrcIPv6Addr(1036)=2001::1;DstIPv6Addr(1037)=3001::1;Icmpv6Type(1064)=Echo(128);Icmpv6Code(1065)=0;MatchCount(1069)=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

49.3 FILTER_IPV4_EXECUTION

日志内容	RcvIfName(1023)=[STRING];Direction(1070)=[STRING];Type(1067)=[STRING];Acl(1068)=[STRING];RuleID(1078)=[UINT32];Protocol(1001)=[STRING];Application(1002)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];MatchCount(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：ACL规则编号 $6：四层协议名称 $7：应用名称 $8：源IP地址 $9：源端口号 $10：目的IP地址 $11：目的端口号 $12：命中次数 $13：事件信息
日志等级	6
举例	FILTER/6/FILTER_IPV4_EXECUTION: RcvIfName(1023)=GigabitEthernet2/0/2;Direction(1070)=inbound;Type(1067)=IPv4;Acl(1068)=3000;RuleID(1078)=0;Protocol(1001)=TCP;Application(1002)=ftp;SrcIPAddr(1003)=100.1.1.1;SrcPort(1004)=1025;DstIPAddr(1007)=200.1.1.1;DstPort(1008)=1026;MatchCount(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

49.4 FILTER_IPV6_EXECUTION

日志内容	RcvIfName(1023)=[STRING];Direction(1070)=[STRING];Type(1067)=[STRING];Acl(1068)=[STRING];RuleID(1078)=[UINT32];Protocol(1001)=[STRING];Application(1002)=[STRING];SrcIPv6Addr(1036)=[IPADDR];SrcPort(1004)=[UINT16];DstIPv6Addr(1037)=[IPADDR];DstPort(1008)=[UINT16];MatchCount(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：ACL规则编号 $6：四层协议名称 $7：应用名称 $8：源IPv6地址 $9：源端口号 $10：目的IPv6地址 $11：目的端口号 $12：命中次数 $13：事件信息
日志等级	6
举例	FILTER/6/FILTER_IPV6_EXECUTION: RcvIfName(1023)=GigabitEthernet2/0/2;Direction(1070)=inbound;Type(1067)=IPv6;Acl(1068)=3000;RuleID(1078)=0;Protocol(1001)=TCP;Application(1002)=ftp;SrcIPv6Addr(1036)=2001::1;SrcPort(1004)=1025;DstIPv6Addr(1037)=3001::1;DstPort(1008)=1026;MatchCount(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

49.5 FILTER_ZONE_IPV4_EXECUTION

日志内容	SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];Type(1067)=[STRING];ObjectPolicy(1072)=[STRING];RuleID(1078)=[UINT32];Protocol(1001)=[STRING];Application(1002)=[STRING];SrcIPAddr(1003)=[STRING];SrcPort(1004)=[UINT16];DstIPAddr(1007)=[STRING];DstPort(1008)=[UINT16];MatchCount(1069)=[UINT32];Event(1048)=[STRING];
参数解释	$1：源安全域 $2：目的安全域 $3：对象策略类型 $4：对象策略名称 $5：对象策略规则编号 $6：四层协议名称 $7：应用名称 $8：源IP地址 $9：源端口号 $10：目的IP地址 $11：目的端口号 $12：命中次数 $13：事件信息
日志等级	6
举例	FILTER/6/FILTER_ZONE_IPV4_EXECUTION: SrcZoneName(1025)=zone1;DstZoneName(1035)=zone2;Type(1067)=IPv4;ObjectPolicy(1072)=policy1;RuleID(1078)=0;Protocol(1001)=TCP;Application(1002)=ftp;SrcIPAddr(1003)=100.1.1.1;SrcPort(1004)=1025;DstIPAddr(1007)=200.1.1.1;DstPort(1008)=1026;MatchCount(1069)=1000;Event(1048)=permit;
日志说明	首次命中对象策略时发送报文过滤日志，之后定时发送该日志
处理建议	无

49.6 FILTER_ZONE_IPV4_EXECUTION

日志内容	SrcZoneName(1025)=zone1;DstZoneName(1035)=[STRING];Type(1067)=[STRING];Acl(1068)=[UINT16];RuleID(1078)=[UINT32];Protocol(1001)=[STRING];Application(1002)=[STRING];SrcIPAddr(1003)=[STRING];SrcPort(1004)=[UINT16];DstIPAddr(1007)=[STRING];DstPort(1008)=[UINT16];MatchCount(1069)=[UINT32];Event(1048)=[STRING];
参数解释	$1：源安全域 $2：目的安全域 $3：ACL类型 $4：ACL编号或者名称 $5：ACL规则编号 $6：四层协议名称 $7：应用名称 $8：源IP地址 $9：源端口号 $10：目的IP地址 $11：目的端口号 $12：命中次数 $13：事件信息
日志等级	6
举例	FILTER/6/FILTER_ZONE_IPV4_EXECUTION: SrcZoneName(1025)=zone1;DstZoneName(1035)=zone2;Type(1067)=IPv4;Acl(1068)=3000;RuleID(1078)=0;Protocol(1001)=TCP;Application(1002)=ftp;SrcIPAddr(1003)=100.1.1.1;SrcPort(1004)=1025;DstIPAddr(1007)=200.1.1.1;DstPort(1008)=1026;MatchCount(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

49.7 FILTER_ZONE_IPV4_EXECUTION

日志内容	SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];Type(1067)=[STRING];SecurityPolicy(1072)=[STRING];RuleID(1078)=[UINT32];Protocol(1001)=[STRING];Application(1002)=[STRING];SrcIPAddr(1003)=[STRING];SrcPort(1004)=[UINT16];SrcMacAddr(1021)=[STRING];DstIPAddr(1007)=[STRING];DstPort(1008)=[UINT16];DstMacAddr(1022)=[STRING];VlanID(1175)=[UINT16];VNI(1211)=[UINT32];MatchCount(1069)=[UINT32];Event(1048)=[STRING] ;
参数解释	$1：源安全域 $2：目的安全域 $3：安全策略类型 $4：安全策略名称 $5：安全策略规则编号 $6：四层协议名称 $7：应用名称 $8：源IP地址 $9：源端口号 $10：源MAC地址 $11：目的IP地址 $12：目的端口号 $13：目的MAC地址 $14：Vlan ID $15：VXLAN ID $16：命中次数 $17：事件信息
日志等级	6
举例	FILTER/6/FILTER_ZONE_IPV4_EXECUTION: SrcZoneName(1025)=zone1;DstZoneName(1035)=zone2;Type(1067)=IPv4;SecurityPolicy(1072)=policy1;RuleID(1078)=0;Protocol(1001)=TCP;Application(1002)=ftp;SrcIPAddr(1003)=100.1.1.1;SrcPort(1004)=1025;SrcMacAddr(1021)=dc2d-cb67-76eb;DstIPAddr(1007)=200.1.1.1;DstPort(1008)=1026;DstMacAddr(1022)=dc2d-cb7d-91b2;VlanID(1175)=10;VNI(1211)=--;MatchCount(1069)=1000;Event(1048)=permit;
日志说明	首次命中安全策略时发送报文过滤日志，之后定时发送该日志
处理建议	无

49.8 FILTER_ZONE_IPV6_EXECUTION

日志内容	SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];Type(1067)=[STRING];ObjectPolicy(1072)=[STRING];RuleID(1078)=[UINT32];Protocol(1001)=[STRING];Application(1002)=[STRING];SrcIPv6Addr(1036)=[STRING];SrcPort(1004)=[UINT16];DstIPv6Addr(1037)=[STRING];DstPort(1008)=[UINT16];MatchCount(1069)=[UINT32];Event(1048)=[STRING];
参数解释	$1：源安全域 $2：目的安全域 $3：对象策略类型 $4：对象策略名称 $5：对象策略规则编号 $6：四层协议名称 $7：应用名称 $8：源IPv6地址 $9：源端口号 $10：目的IPv6地址 $11：目的端口号 $12：命中次数 $13：事件信息
日志等级	6
举例	FILTER/6/FILTER_ZONE_IPV6_EXECUTION: SrcZoneName(1025)=zone1;DstZoneName(1035)=zone2;Type(1067)=IPv6;ObjectPolicy(1072)=policy1;RuleID(1078)=0;Protocol(1001)=TCP;Application(1002)=ftp;SrcIPv6Addr(1036)=2001::1;SrcPort(1004)=1025;DstIPv6Addr(1037)=3000::1;DstPort(1008)=1026;MatchCount(1069)=1000;Event(1048)=permit;
日志说明	首次命中对象策略时发送报文过滤日志，之后定时发送该日志
处理建议	无

49.9 FILTER_ZONE_IPV6_EXECUTION

日志内容	SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];Type(1067)=[STRING];Acl(1068)=[UINT16];RuleID(1078)=[UINT32];Protocol(1001)=[STRING];Application(1002)=[STRING];SrcIPv6Addr(1036)=[STRING];SrcPort(1004)=[UINT16];DstIPv6Addr(1037)=[STRING];DstPort(1008)=[UINT16];MatchCount(1069)=[UINT32];Event(1048)=[STRING];
参数解释	$1：源安全域 $2：目的安全域 $3：ACL类型 $4：ACL编号或者名称 $5：ACL规则编号 $6：四层协议名称 $7：应用名称 $8：源IPv6地址 $9：源端口号 $10：目的IPv6地址 $11：目的端口号 $12：命中次数 $13：事件信息
日志等级	6
举例	FILTER/6/FILTER_ZONE_IPV6_EXECUTION: SrcZoneName(1025)=zone1;DstZoneName(1035)=zone2;Type(1067)=IPv6;Acl(1068)=3000;RuleID(1078)=0;Protocol(1001)=TCP;Application(1002)=ftp;SrcIPv6Addr(1036)=2001::1;SrcPort(1004)=1025;DstIPv6Addr(1037)=3000::1;DstPort(1008)=1026;MatchCount(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

49.10 FILTER_ZONE_IPV6_EXECUTION

日志内容	SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];Type(1067)=[STRING];SecurityPolicy(1072)=[STRING];RuleID(1078)=[UINT32];Protocol(1001)=[STRING];Application(1002)=[STRING];SrcIPv6Addr(1036)=[STRING];SrcPort(1004)=[UINT16];SrcMacAddr(1021)=[STRING];DstIPv6Addr(1037)=[STRING];DstPort(1008)=[UINT16];DstMacAddr(1022)=[STRING];VlanID(1175)=[UINT16];VNI(1211)=[UINT32];MatchCount(1069)=[UINT32];Event(1048)=[STRING]
参数解释	$1：源安全域 $2：目的安全域 $3：安全策略类型 $4：安全策略名称 $5：安全策略规则编号 $6：四层协议名称 $7：应用名称 $8：源IPv6地址 $9：源端口号 $10：源MAC地址 $11：目的IPv6地址 $12：目的端口号 $13：目的MAC地址 $14：Vlan ID $15：VXLAN ID $16：命中次数 $17：事件信息
日志等级	6
举例	FILTER/6/FILTER_ZONE_IPV6_EXECUTION: SrcZoneName(1025)=zone1;DstZoneName(1035)=zone2;Type(1067)=IPv6;SecurityPolicy(1072)=policy1;RuleID(1078)=0;Protocol(1001)=TCP;Application(1002)=ftp;SrcIPv6Addr(1036)=2001::1;SrcPort(1004)=1025;SrcMacAddr(1021)=dc2d-cb67-76eb;DstIPv6Addr(1037)=3000::1;DstPort(1008)=1026;DstMacAddr(1022)=dc2d-cb67-76ea;VlanID(1175)=10;VNI(1211)=--;MatchCount(1069)=1000;Event(1048)=permit;
日志说明	首次命中安全策略时发送报文过滤日志，之后定时发送该日志
处理建议	无

49.11 FILTER_ZONE_EXECUTION_ICMP

日志内容	SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];Type(1067)=[STRING];ObjectPolicy(1072)=[STRING];RuleID(1078)=[UINT32];Protocol(1001)=[STRING];SrcIPAddr(1003)=[STRING];SrcPort(1004)=[UINT16];DstIPAddr(1007)=[STRING];DstPort(1008)=[UINT16];MatchCount(1069)=[UINT32];Event(1048)=[STRING];
参数解释	$1：源安全域 $2：目的安全域 $3：对象策略类型 $4：对象策略名称 $5：对象策略规则编号 $6：四层协议名称 $7：源IP地址 $8：源端口号 $9：目的IP地址 $10：目的端口号 $11：命中次数 $12：事件信息
日志等级	6
举例	FILTER/6/FILTER_ZONE_EXECUTION_ICMP: SrcZoneName(1025)=zone1;DstZoneName(1035)=zone2;Type(1067)=IPv4;ObjectPolicy(1072)=policy1;RuleID(1078)=0;Protocol(1001)=ICMP;SrcIPAddr(1003)=100.1.1.1;SrcPort(1004)=1025;DstIPAddr(1007)=200.1.1.1;DstPort(1008)=1026;MatchCount(1069)=1000;Event(1048)=permit;
日志说明	ICMP报文首次命中对象策略时发送报文过滤日志，之后定时发送该日志
处理建议	无

49.12 FILTER_ZONE_EXECUTION_ICMP

日志内容	SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];Type(1067)=[STRING];Acl(1068)=[UINT16];RuleID(1078)=[UINT32];Protocol(1001)=[STRING];SrcIPAddr(1003)=[STRING];SrcPort(1004)=[UINT16];DstIPAddr(1007)=[STRING];DstPort(1008)=[UINT16];MatchCount(1069)=[UINT32];Event(1048)=[STRING];
参数解释	$1：源安全域 $2：目的安全域 $3：ACL类型 $4：ACL编号或者名称 $5：ACL规则编号 $6：四层协议名称 $7：源IP地址 $8：源端口号 $9：目的IP地址 $10：目的端口号 $11：命中次数 $12：事件信息
日志等级	6
举例	FILTER/6/FILTER_ZONE_EXECUTION_ICMP: SrcZoneName(1025)=zone1;DstZoneName(1035)=zone2;Type(1067)=IPv4;Acl(1068)=3000;RuleID(1078)=0;Protocol(1001)=ICMP;SrcIPAddr(1003)=100.1.1.1;SrcPort(1004)=1025;DstIPAddr(1007)=200.1.1.1;DstPort(1008)=1026;MatchCount(1069)=1000;Event(1048)=permit;
日志说明	ICMP报文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

49.13 FILTER_ZONE_EXECUTION_ICMP

日志内容	SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];Type(1067)=[STRING];SecurityPolicy(1072)=[STRING];RuleID(1078)=[UINT32];Protocol(1001)=[STRING];SrcIPAddr(1003)=[STRING];SrcPort(1004)=[UINT16];SrcMacAddr(1021)=[STRING];DstIPAddr(1007)=[STRING];DstPort(1008)=[UINT16];DstMacAddr(1022)=[STRING];VlanID(1175)=[UINT16];VNI(1211)=[UINT32];MatchCount(1069)=[UINT32];Event(1048)=[STRING]
参数解释	$1：源安全域 $2：目的安全域 $3：安全策略类型 $4：安全策略名称 $5：安全策略规则编号 $6：四层协议名称 $7：源IP地址 $8：源端口号 $9：源MAC地址 $10：目的IP地址 $11：目的端口号 $12：目的MAC地址 $13：Vlan ID $14：VXLAN ID $15：命中次数 $16：事件信息
日志等级	6
举例	FILTER/6/FILTER_ZONE_EXECUTION_ICMP: SrcZoneName(1025)=zone1;DstZoneName(1035)=zone2;Type(1067)=IPv4;SecurityPolicy(1072)=policy1;RuleID(1078)=0;Protocol(1001)=ICMP;SrcIPAddr(1003)=100.1.1.1;SrcPort(1004)=1025;SrcMacAddr(1021)=dc2d-cb7d-91b1;DstIPAddr(1007) =200.1.1.1;DstPort(1008)=1026;DstMacAddr(1022)=dc2d-cb7d-91b2; VlanID(1175)=10;VNI(1211)=--;MatchCount(1069)=1000;Event(1048)=permit;
日志说明	ICMP报文首次命中安全策略时发送报文过滤日志，之后定时发送该日志
处理建议	无

49.14 FILTER_ZONE_EXECUTION_ICMPV6

日志内容	SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];Type(1067)=[STRING];ObjectPolicy(1072)=[STRING];RuleID(1078)=[UINT32];Protocol(1001)=[STRING];SrcIPv6Addr(1036)=[STRING];SrcPort(1004)=[UINT16];DstIPv6Addr(1037)=[STRING];DstPort(1008)=[UINT16];MatchCount(1069)=[UINT32];Event(1048)=[STRING];
参数解释	$1：源安全域 $2：目的安全域 $3：对象策略类型 $4：对象组策略名称 $5：对象组策略规则编号 $6：四层协议名称 $7：源IPv6地址 $8：源端口号 $9：目的IPv6地址 $10：目的端口号 $11：命中次数 $12：事件信息
日志等级	6
举例	FILTER/6/FILTER_ZONE_EXECUTION_ICMPV6: SrcZoneName(1025)=zone1;DstZoneName(1035)=zone2;Type(1067)=IPv6;ObjectPolicy(1072)=policy1;RuleID(1078)=0;Protocol(1001)=ICMPV6;SrcIPv6Addr(1036)=2001::1;SrcPort(1004)=1025;DstIPv6Addr(1037)=3000::1;DstPort(1008)=1026;MatchCount(1069)=1000;Event(1048)=permit;
日志说明	ICMPv6报文首次命中对象策略时发送报文过滤日志，之后定时发送该日志
处理建议	无

49.15 FILTER_ZONE_EXECUTION_ICMPV6

日志内容	SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];Type(1067)=[STRING];Acl(1068)=[UINT16];RuleID(1078)=[UINT32];Protocol(1001)=[STRING];SrcIPv6Addr(1036)=[STRING];SrcPort(1004)=[UINT16];DstIPv6Addr(1037)=[STRING];DstPort(1008)=[UINT16];MatchCount(1069)=[UINT32];Event(1048)=[STRING];
参数解释	$1：源安全域 $2：目的安全域 $3：ACL类型 $4：ACL编号或者名称 $5：ACL规则编号 $6：四层协议名称 $7：源IPv6地址 $8：源端口号 $9：目的IPv6地址 $10：目的端口号 $11：命中次数 $12：事件信息
日志等级	6
举例	FILTER/6/FILTER_ZONE_EXECUTION_ICMPV6: SrcZoneName(1025)=zone1;DstZoneName(1035)=zone2;Type(1067)=IPv6;Acl(1068)=3000;RuleID(1078)=0;Protocol(1001)=ICMPV6;SrcIPv6Addr(1036)=2001::1;SrcPort(1004)=1025;DstIPv6Addr(1037)=3000::1;DstPort(1008)=1026; MatchCount(1069)=1000;Event(1048)=permit;
日志说明	ICMPv6报文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

49.16 FILTER_ZONE_EXECUTION_ICMPV6

日志内容	SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];Type(1067)=[STRING];SecurityPolicy(1072)=[STRING];RuleID(1078)=[UINT32];Protocol(1001)=[STRING];SrcIPv6Addr(1036)=[STRING];SrcPort(1004)=[UINT16];SrcMacAddr(1021)=[STRING];DstIPv6Addr(1037)=[STRING];DstPort(1008)=[UINT16];DstMacAddr(1022)=[STRING];VlanID(1175)=[UINT16];VNI(1211)=[UINT32];MatchCount(1069)=[UINT32];Event(1048)=[STRING];
参数解释	$1：源安全域 $2：目的安全域 $3：安全策略类型 $4：安全策略名称 $5：安全策略规则编号 $6：四层协议名称 $7：源IPv6地址 $8：源端口号 $9：源MAC地址 $10：目的IPv6地址 $11：目的端口号 $12：目的MAC地址 $13：Vlan ID $14：VXLAN ID $15：命中次数 $16：事件信息
日志等级	6
举例	FILTER/6/FILTER_ZONE_EXECUTION_ICMPV6: SrcZoneName(1025)=zone1;DstZoneName(1035)=zone2;Type(1067)=IPv6;SecurityPolicy(1072)=policy1;RuleID(1078)=0;Protocol(1001)=ICMPV6;SrcIPv6Addr(1036)=2001::1;SrcPort(1004)=1025;SrcMacAddr(1021)=dc2d-cb7d-91b1;DstIPv6Addr(1037)=3000::1;DstPort(1008)=1026;DstMacAddr(1022)=dc2d-cb7d-91b2;VlanID(1175)=10;VNI(1211)=--;MatchCount(1069)=1000;Event(1048)=permit;
日志说明	ICMPv6报文首次命中安全策略时发送报文过滤日志，之后定时发送该日志
处理建议	无

50 FIPSNG

本节介绍 FIP Snooping 模块输出的日志信息。

50.1 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

50.2 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

51 FS

本节介绍 FS（File System）模块输出的日志信息。

51.1 FS_UNFORMATTED_PARTITION

日志内容	Partition [%s] is not formatted yet. Please format the partition first.
参数解释	$1：分区名
日志等级	4
举例	FS/4/FS_UNFORMATED_PARTITION: Partition usba0: is not formatted yet. Please format the partition first.
日志说明	分区未格式化，请先执行格式化操作
处理建议	格式化该分区

52 FTP

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

52.1 FTP_ACL_DENY

日志内容	The FTP Connection request from [IPADDR]([STRING]) was denied by ACL rule (rule ID=[INT32])
参数解释	$1：FTP客户端IP地址 $2：FTP客户端IP地址所在VPN $3：FTP客户端匹配ACL deny规则编号，如果未匹配已创建的ACL规则，则匹配缺省的ACL规则（deny）
日志等级	5
举例	FTP/5/FTP_ACL_DENY: The FTP connection request from 181.1.1.10 was denied by ACL rule (rule ID=20). FTP/5/FTP_ACL_DENY: The FTP connection request from 181.1.1.10 was denied by ACL rule (default rule).
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

52.2 FTP_REACH_SESSION_LIMIT

日志内容	FTP client $1 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 (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

53 GLB

本节介绍 GLB（Global Load Balancing）模块输出的日志信息。

53.1 GLB_SCHED (快速日志)

日志内容	DNS request: SrcIPAddr=[STRING], SrcPort=[UINT16], DestIPAddr=[STRING], DestPort=[UINT16], VPN=[STRING]; queried domain name: [STRING] (packet type=[STRING]); global DNS mapping: name= [STRING], predictor=[STRING] (priority=[STRING]); global virtual server pool: name=[STRING], predictor=[STRING] (priority=[STRING]); DNS response: IPAddr=[STRING].
参数解释	$1：DNS请求报文源IP地址 $2：DNS请求报文源端口 $3：DNS请求报文目的IP地址 $4：DNS请求报文目的端口 $5：VPN名称 $6：DNS请求报文请求域名 $7：DNS请求报文类型 $8：全局DNS映射名称 $9：全局DNS映射的调度算法 $10：全局DNS映射调度算法的优先级 $11：全局虚服务池名称 $12：全局虚服务池的调度算法 $13：全局虚服务池调度算法的优先级 $14：DNS应答IP地址
日志等级	6
举例	UNIS GLB/6/GLB_SCHED: DNS request: SrcIPAddr=190.44.0.60, SrcPort=61701, DestIPAddr=191.44.0.1, DestPort=53, VPN=; queried domain name:2.com (packet type=A); global DNS mapping: name= dmap, predictor=RR (priority=Preferred); global virtual server pool: name=gvsp, predictor=RR (priority=Preferred); DNS response: IPAddr=[1.2.2.2].
日志说明	全局负载均衡调度过程相关信息
处理建议	无

53.2 GLB_SHCED_FAILURE (快速日志)

日志内容	[STRING] a DNS request: SrcIPAddr= [STRING], SrcPort=[UINT16], DestIPAddr= [STRING], DestPort=[UINT16], VPN= [STRING]; queried domain name: [STRING] (packet type=[STRING]).
参数解释	$1：调度失败报文处理动作，包括： • Dropped：丢弃 • Rejected：拒绝，即回应 DNS 拒绝报文 $2：DNS请求报文源IP地址 $3：DNS请求报文源端口 $4：DNS请求报文目的IP地址 $5：DNS请求报文目的端口 $6：VPN名称 $7：DNS请求报文请求域名 $8：DNS请求报文类型
日志等级	6
举例	UNIS GLB/6/GLB_SCHED_FAILURE: Rejected a DNS request: SrcIPAddr=190.44.0.60, SrcPort=61701, DestIPAddr=191.44.0.1, DestPort=53, VPN=; queried domain name: [2.com] (packet type=[A]).
日志说明	全局负载均衡调度失败报文相关信息
处理建议	无

53.3 GLB_SYNCGROUP_CMD_DENY

日志内容	Configuration deployment is not allowed because of configuration conflicts on default synchronization group member devices. Please choose one device to execute the command: loadbalance default-syncgroup sync config.
参数解释	
日志等级	5
举例	UNIS GLB/5/GLB_SYNCGROUP_CMD_DENY: Configuration deployment is not allowed because of configuration conflicts on default synchronization group member devices. Please choose one device to execute the command: loadbalance default-syncgroup sync config.
日志说明	目前缺省同步组成员设备存在配置冲突，不允许下发配置。
处理建议	选择其中一台设备执行**`loadbalance default-syncgroup sync config`**命令

53.4 GLB_SYNCGROUP_MEM_CONNECT

日志内容	The default synchronization group member [STRING] connected to [STRING] successfully.
参数解释	$1：默认同步组成员名称 $2：默认同步组成员名称
日志等级	5
举例	GLB/5/GLB_SYNCGROUP_MEM_CONNECT: The default synchronization group member %s connected to %s successfully.
日志说明	默认同步组之间连接成功。
处理建议	无

53.5 GLB_SYNCGROUP_MEM_DISCONNECT

日志内容	The default synchronization group member [STRING] disconnected from [STRING] due to configuration changes.
参数解释	$1：默认同步组成员名称 $2：默认同步组成员名称
日志等级	5
举例	GLB/5/GLB_SYNCGROUP_MEM_DISCONNECT:The default synchronization group member site1 disconnected from site2 due to configuration changes.
日志说明	修改配置导致默认同步组成员之间的连接断开。
处理建议	查看默认同步组成员功能是否开启、IP地址等配置是否正确。

53.6 GLB_SYNCGROUP_MEM_DISCONNECT

日志内容	The default synchronization group member [STRING] disconnected from [STRING] due to timeout.
参数解释	$1：默认同步组成员名称 $2：默认同步组成员名称
日志等级	5
举例	GLB/5/GLB_SYNCGROUP_MEM_DISCONNECT:The default synchronization group member site1 disconnected from site2 due to timeout.
日志说明	默认同步组成员之间由于连接超时导致断开。
处理建议	检查默认同步组配置，检测网络环境（检测对端IP地址是否能ping通）。

53.7 GLB_SYNCGROUP_MEM_DISCONNECT

日志内容	The default synchronization group member [STRING] disconnected from [STRING] due to a disconnect message.
参数解释	$1：默认同步组成员名称 $2：默认同步组成员名称
日志等级	5
举例	GLB/5/GLB_SYNCGROUP_MEM_DISCONNECT:The default synchronization group member site1 disconnected from site2 due to a disconnect message.
日志说明	默认同步组成员由于收到对端设备发送的连接断开消息而主动断开连接。
处理建议	连接断开无法再次连接成功时，查看连接的对端设备配置修改是否正确。

53.8 GLB_SYNCGROUP_MEM_DISCONNECT

日志内容	The default synchronization group member [STRING] disconnected from [STRING] due to receiving an EPOLLHUP/EPOLLERR signal.
参数解释	$1：默认同步组成员名称 $2：默认同步组成员名称
日志等级	5
举例	GLB/5/GLB_SYNCGROUP_MEM_DISCONNECT:The default synchronization group member site1 disconnected from site2 due to receiving an EPOLLHUP/EPOLLERR signal.
日志说明	接收到EPOLL挂起、EPOLL错误信号导致连接断开
处理建议	断开连接后，若无法自动恢复正常，检查链路等网络环境是否正常。

53.9 GLB_SYNCGROUP_MEM_DISCONNECT

日志内容	The default synchronization group member [STRING] disconnected from [STRING] due to disconnection of the TCP connection by the peer.
参数解释	$1：默认同步组成员名称 $2：默认同步组成员名称
日志等级	5
举例	GLB/5/GLB_SYNCGROUP_MEM_DISCONNECT:The default synchronization group member site1 disconnected from site2 due to disconnection of the TCP connection by the peer.
日志说明	对端关闭连接导致连接断开
处理建议	检查对端配置的默认同步组成员的IP地址与本端是否一致。

53.10 GLB_SYNCGROUP_MEM_DISCONNECT

日志内容	The default synchronization group member [STRING] failed to connect to [STRING] due to different member names.
参数解释	$1：默认同步组成员名称 $2：默认同步组成员名称
日志等级	5
举例	GLB/5/GLB_SYNCGROUP_MEM_DISCONNECT: The default synchronization group member %s failed to connect to %s due to different member names.
日志说明	默认同步组成员之间由于名称不一致导致连接建立失败
处理建议	检查建立连接的默认同步组成员名称是否配置一致。

53.11 GLB_SYNCGROUP_MEM_DOMAINCONFLICT

日志内容	Failed to configure the domain name ([STRING]), because it had been used by the remote end.
参数解释	$1：默认同步组成员名称
日志等级	5
举例	UNISGLB/5/GLB_SYNCGROUP_MEM_DOMAINCONFLICT: Failed to configure the domain name (site1), because it had been used by the remote end.
日志说明	由于该域名已被远端默认同步组成员使用，导致配置域名失败。
处理建议	重新配置合法的域名

53.12 GLB_SYNCGROUP_SYNC_CONFLICT

日志内容	Inconsistent ([STRING]) configuration exists on the default synchronization group member devices during connection establishment. Please choose one device to execute the command: loadbalance default-syncgroup sync config. The value some indicates that the remote end detects inconsistent configurations.
参数解释	默认同步组成员中配置不一致的对象，包括： • data-center：数据中心 • global-dns-map：全局 DNS 映射 • global-isp：全局 ISP • global-proximity：全局动态就近性 • global-region：全局区域 • global-reverse-zone：全局 DNS 反向区域 • global-topology：全局静态就近性 • global-vsp：全局虚服务器池 • global-zone：全局 DNS 争相区域 • 若显示为 some，则表示配置不一致的通知来自远端默认同步组成员
日志等级	5
举例	UNIS GLB/5/GLB_SYNCGROUP_SYNC_CONFLICT: Inconsistent configuration exists on the default synchronization group member devices during connection establishment. Please choose one device to execute the command: loadbalance default-syncgroup sync config.
日志说明	缺省同步组成员设备建立连接时配置不完全一致，请选择其中一台设备执行loadbalance default-syncgroup sync config命令。
处理建议	选择其中一台设备执行loadbalance default-syncgroup sync config命令

54 gRPC

本节介绍 gRPC 模块输出的日志信息。

54.1 GRPC_ENABLE_WITHOUT_TLS

日志内容	PKI domain [STRING] isn't associated with a valid local certificate. The gRPC process will start without the PKI domain.
参数解释	$1：PKI域名
日志等级	4
举例	GRPC/4/GRPC_ENABLE_WITHOUT_TLS: PKI domain xxx isn't associated with a valid local certificate. The gRPC process will start without the PKI domain.
日志说明	由于PKI域中没有包含有效的本地证书，gRPC功能不会使用该PKI域进行加密通信，将以普通方式启动
处理建议	如果要使用gRPC的加密连接功能，请先创建gRPC引用的PKI域并确保该域中包含有效的证书和密钥，然后依次执行**undo grpc enable**、**grpc pki domain**、**grpc enable**命令使gRPC引用的PKI域生效

55 HA

本节介绍 HA 模块输出的日志信息。

55.1 HA_BATCHBACKUP_FINISHED

日志内容	Batch backup of standby board in [STRING] has finished.
参数解释	$1：chassis编号+slot编号或slot编号。如果slot支持多CPU，该参数还会包含CPU的编号
日志等级	5
举例	HA/5/HA_BATCHBACKUP_FINISHED: Batch backup of standby board in slot 1 has finished.
日志说明	指定slot/CPU和主用slot/CPU之间的批量备份完成
处理建议	无

55.2 HA_BATCHBACKUP_STARTED

日志内容	Batch backup of standby board in [STRING] started.
参数解释	$1：chassis编号+slot编号或slot编号。如果slot支持多CPU，该参数还会包含CPU的编号
日志等级	5
举例	HA/5/HA_BATCHBACKUP_STARTED: Batch backup of standby board in slot 1 started.
日志说明	指定slot/CPU和主用slot/CPU之间的批量备份开始
处理建议	无

55.3 HA_STANDBY_NOT_READY

日志内容	Standby board in [STRING] is not ready, reboot ...
参数解释	$1：chassis编号+slot编号或slot编号。如果slot支持多CPU，该参数还会包含CPU的编号
日志等级	4
举例	HA/4/HA_STANDBY_NOT_READY: Standby board in slot 1 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	建议备用主控板批量备份完成前不要进行主备倒换

55.4 HA_STANDBY_TO_MASTER

日志内容	Standby board in [STRING] changed to the master.
参数解释	$1：chassis编号+slot编号或slot编号。如果slot支持多CPU，该参数还会包含CPU的编号
日志等级	5
举例	HA/5/HA_STANDBY_TO_MASTER: Standby board in slot 1 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

56 HLTH

本节介绍 HLTH（健康检测）模块输出的日志信息。

56.1 LIPC_COMM_FAULTY

日志内容	LIPC [STRING] between [STRING] and [STRING] might be faulty.
参数解释	$1：通信类型，取值包括： • unicast：表示单播 • broadcast：表示广播 • topo：表示拓扑 $2：chassis编号+slot编号+CPU编号或slot编号+CPU编号，仅支持多CPU的slot后面会携带CPU编号 $3：chassis编号+slot编号+CPU编号或slot编号+CPU编号，仅支持多CPU的slot后面会携带CPU编号
日志等级	4
举例	HLTH/4/LIPC_COMM_FAULTY: LIPC unicast between slot 1 and slot 2 might be faulty.
日志说明	LIPC通信异常
处理建议	使用display system health命令查看设备的健康状态，如果30分钟后设备仍处于故障状态，请联系技术支持

56.2 LIPC_COMM_RECOVER

日志内容	LIPC [STRING] between [STRING] and [STRING] recovered.
参数解释	$1：通信类型，取值包括： • unicast：表示单播 • broadcast：表示广播 • topo：表示拓扑 $2：chassis编号+slot编号+CPU编号或slot编号+CPU编号，仅支持多CPU的slot后面会携带CPU编号 $3：chassis编号+slot编号+CPU编号或slot编号+CPU编号，仅支持多CPU的slot后面会携带CPU编号
日志等级	6
举例	HLTH/6/LIPC_COMM_NORMAL: LIPC unicast between slot 1 and slot 2 recovered.
日志说明	LIPC通信恢复正常
处理建议	无

57 HQOS

本节介绍 HQOS（Hierarchical QoS）模块输出的日志信息。

57.1 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

57.2 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

57.3 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

57.4 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

58 HTTPD

本节介绍 HTTPD（HTTP daemon）模块输出的日志信息。

58.1 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

58.2 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

58.3 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

58.4 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

58.5 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

58.6 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

59 IDENTITY

本节介绍 IDENTITY（用户身份识别与管理）模块输出的日志信息。

59.1 IDENTITY_AUTO_IMPORT_FINISHED

日志内容	Finished importing identity user accounts and groups automatically.
参数解释	无
日志等级	5
举例	IDENTITY/5/IDENTITY_AUTO_IMPORT_FINISHED: Finished importing identity user accounts and groups automatically.
日志说明	本次自动导入身份识别账户和身份识别用户组结束
处理建议	无

59.2 IDENTITY_AUTO_IMPORT_START

日志内容	Started to import identity user accounts and groups automatically.
参数解释	无
日志等级	5
举例	IDENTITY/5/IDENTITY_AUTO_IMPORT_START: Started to import identity user accounts and groups automatically.
日志说明	本次自动导入身份识别账户和身份识别用户组开始
处理建议	无

59.3 IDENTITY_CSV_IMPORT_FAILED

日志内容	Failed to import identity user [STRING] to domain [STRING] from the .csv file.
参数解释	$1：用户名 $2：用户所属身份识别域名
日志等级	5
举例	IDENTITY/5/IDENTITY_CSV_IMPORT_FAILED: Failed to import identity user network-us?er1 to domain system-domain from the .csv file.
日志说明	通过CSV文件向设备中导入身份识别用户账户失败，且停止导入身份识别账户
处理建议	• 检查设备上是否有同名身份识别用户 • 检查域名或用户名中是否包含非法字符

59.4 IDENTITY_IMC_IMPORT_FAILED_NO_MEMORY

日志内容	Failed to obtain data from IMC. Reason: Not enough memory.
参数解释	无
日志等级	5
举例	IDENTITY/5/IDENTITY_IMC_IMPORT_FAILED_NO_MEMORY: Failed to obtain data from IMC. Reason: Not enough memory.
日志说明	从iMC服务器导入身份识别用户账户和身份识别在线用户失败，内存不足
处理建议	无

59.5 IDENTITY_LDAP_IMPORT_FAILED_NO_MEMORY

日志内容	Failed to obtain data from the LDAP server specified in scheme [STRING]. Reason: Not enough memory.
参数解释	$1：LDAP方案名称
日志等级	5
举例	IDENTITY/5/IDENTITY_LDAP_IMPORT_FAILED_NO_MEMORY: Failed to obtain data from the LDAP server specified in scheme test. Reason: Not enough memory.
日志说明	从LDAP服务器导入用户和用户组失败，内存不足
处理建议	无

59.6 IDENTITY_LDAP_IMPORT_GROUP_FAILED

日志内容	Failed to import identity group [STRING] to domain [STRING] from the LDAP server specified in scheme [STRING].
参数解释	$1：用户组名 $2：用户所属身份识别域名 $3：LDAP方案名称
日志等级	5
举例	IDENTITY/5/IDENTITY_LDAP_IMPORT_GROUP_FAILED: Failed to import identity group group-na?me1 to domain system-domain from the LDAP server specified in scheme ldap-scheme1.
日志说明	从LDAP方案中指定的LDAP服务器上导入身份识别用户组失败
处理建议	• 检查设备上是否存在同名身份识别用户组 • 检查域名或用户组名中是否包含有非法字符

59.7 IDENTITY_LDAP_IMPORT_USER_FAILED

日志内容	Failed to import identity user [STRING] to domain [STRING] from the LDAP server specified in scheme [STRING].
参数解释	$1：用户名 $2：用户所属身份识别域名 $3：LDAP方案名称
日志等级	5
举例	IDENTITY/5/IDENTITY_LDAP_IMPORT_USER_FAILED: Failed to import identity user user-na?me1 to domain system-domain from the LDAP server specified in scheme ldap-scheme1.
日志说明	从LDAP方案中指定的LDAP服务器上导入身份识别用户失败
处理建议	• 检查设备上是否存在同名身份识别用户 • 检查域名或用户名中是否包含非法字符

60 IFNET

本节介绍接口管理模块输出的日志信息。

60.1 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

60.2 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

60.3 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

60.4 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	5
举例	IFNET/5/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

60.5 PFC_WARNING

日志内容	On interface [STRING], the rate of [STRING] PFC packets of 802.1p priority [INTEGER] exceeded the PFC early-warning threshold [INTEGER] pps. The current rate is [INTEGER].
参数解释	$1：接口名称 $2：告警方向，input、output $3：指定的802.1p优先级 $4：指定接口每秒接收的PFC帧数量，单位为pps $5：当前接口接收PFC报文的速率，单位为pps
日志等级	4
举例	IFNET/4/PFC_WARNING: On interface GigabitEthernet1/0/1, the rate of input PFC packets of 802.1p priority 1 exceeded the PFC early-warning threshold 50 pps. The current rate is 60.
日志说明	接口接收或者发送PFC报文的速率达到预警门限
处理建议	无

60.6 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 interface 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

60.7 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

60.8 STORM_CONSTRAIN_BELOW

日志内容	[STRING] is in controlled status, [STRING] flux falls below its lower threshold [STRING].
参数解释	$1：接口名称 $2：报文类型，BC、MC、UC $3：抑制下限 • lowerlimit% • lowerlimit pps • lowerlimit kbps
日志等级	1
举例	IFNET/1/STORM_CONSTRAIN_BELOW: GigabitEthernet1/0/1 is in controlled status, BC flux falls below its lower threshold 90%.
日志说明	端口处于受控状态，该端口下任意类型的流量从超上限回落到小于下限阈值
处理建议	无

60.9 STORM_CONSTRAIN_CONTROLLED

日志内容	[STRING] turned into controlled status, port status is controlled, packet type is [STRING], upper threshold is [STRING].
参数解释	$1：接口名称 $2：报文类型，BC、MC、UC $3：抑制上限 • upperlimit% • upperlimit pps • upperlimit kbps
日志等级	1
举例	IFNET/1/STORM_CONSTRAIN_CONTROLLED: GigabitEthernet1/0/1 turned into controlled status, port status is controlled, packet type is BC, upper threshold is 90%.
日志说明	端口处于受控状态，该端口下任意类型的流量超过配置的上限阈值
处理建议	无

60.10 STORM_CONSTRAIN_EXCEED

日志内容	[STRING] is in controlled status, [STRING] flux exceeds its upper threshold [STRING].
参数解释	$1：接口名称 $2：报文类型，BC、MC、UC $3：抑制上限 • *upperlimit*% • *upperlimit* pps • *upperlimit* kbps
日志等级	1
举例	IFNET/1/STORM_CONSTRAIN_EXCEED: GigabitEthernet1/0/1 is in controlled status, BC flux exceeds its upper threshold 90%.
日志说明	端口处于受控状态，该端口下任意类型的流量超过配置的上限阈值
处理建议	无

60.11 STORM_CONSTRAIN_NORMAL

日志内容	[STRING] returned to normal status, port status is [STRING], packet type is [STRING], lower threshold is [STRING].
参数解释	$1：接口名称 $2：报文类型，BC、MC、UC $3：抑制下限 • *lowerlimit*% • *lowerlimit* pps • *lowerlimit* kbps
日志等级	1
举例	IFNET/1/STORM_CONSTRAIN_NORMAL: GigabitEthernet1/0/1 returned to normal status, port status is normal, packet type is BC, lower threshold is 10%.
日志说明	端口处于正常状态，该端口下任意类型的流量从超上限回落到小于下限阈值
处理建议	无

60.12 TUNNEL_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	5
举例	IFNET/5/TUNNEL_LINK_UPDOWN: Line protocol state on the interface Tunnel1 changed to down.
日志说明	Tunnel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

60.13 TUNNEL_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/TUNNEL_PHY_UPDOWN: Physical state on the interface Tunnel1 changed to down.
日志说明	Tunnel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

60.14 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接口导致动态VLAN转换成静态VLAN
处理建议	无

61 IKE

本节介绍 IKE 模块输出的日志信息。

61.1 IKE_P1_SA_ESTABLISH_FAIL

日志内容	Failed to establish phase 1 SA in [STRING] mode [STRING] state. Reason: [STRING]. SA information: • Role: [STRING] • Local IP: [STRING] • Local ID type: [STRING] • Local ID: [STRING] • Local port: [UINT32] • Retransmissions: [UINT32] • Remote IP: [STRING] • Remote ID type: [STRING] • Remote ID: [STRING] • Remote port: [UINT32] • Recived retransmissions: [UINT32] • Inside VPN instance: [STRING] • Outside VPN instance: [STRING] • Initiator Cookie: [STRING] • Responder Cookie: [STRING] • Connection ID: [UINT32] • Tunnel ID: [UINT32] • IKE profile name: [STRING]
参数解释	$1：协商模式，主模式或者野蛮模式 $2：协商状态机状态 $3：失败原因： • 认证对端签名失败，显示为：Failed to verify the peer signature • 缺少 HASH 载荷，显示为：HASH payload is missing • 认证对端 HASH 失败，显示为：Failed to verify the peer HASH. Local HASH is %s. Peer HASH is %s • 缺少签名载荷，显示为：Signature payload is missing • 从证书中获取摘要名称失败，显示为：Failed to get subject name from certificate • 获取证书失败，显示为：Failed to get certificate • 获取本地证书失败，显示为：Failed to get local certificate • 获取私钥失败，显示为：Failed to get private key • 认证对端证书失败，显示为：Failed to verify the peer certificate (%s) • 从 ID 载荷中获取 ID 数据失败，显示为：Failed to get ID data for constructing ID payload • 无效的 ID 载荷长度，显示为：Invalid ID payload length: %d • 无效的 ID 载荷协议和端口号，显示为：Invalid ID payload with protocol %u and port %u • 无效的 ID 类型，显示为：Invalid ID type (%u) • 不支持的属性，显示为：Unsupported attribute %u

	• 属性重复，显示为：Attribute %s is repeated • 不支持的 DOI，显示为：Unsupported DOI %s • 不支持的 DOI 场景，显示为：Unsupported IPsec DOI situation (%u) • KE（KEY EXCHANGE）载荷不存在，显示为：KE payload is missing • 无效的 KE 载荷长度，显示为：Invalid KE payload length (%lu) • 无效的 Nonce 载荷长度，显示为：Invalid nonce payload length (%lu) • 无可用的提议，显示为：No available proposal • 解析证书请求载荷失败，显示为：Failed to parse the Cert Request payload • 提议载荷必须为 SA 载荷中的最后一个载荷，但提议载荷后有载荷，显示为：The proposal payload must be the last payload in the SA payload, but it is found followed by the %s payload • 提议载荷中出现非预期的协议 ID，显示为：Unexpected protocol ID (%u) found in proposal payload • 提议载荷中缺少变换载荷，显示为：No transform payload in proposal payload • 变换载荷编号非递增，显示为：Transform number is not monotonically increasing • 无效的变换载荷 ID，显示为：Invalid transform ID (%s) • 没有找到匹配的变换载荷，显示为：No acceptable transform • 提议载荷中出现非预期的载荷，显示为：Unexpected %s payload in proposal • 提议载荷中存在无效的 SPI 长度，显示为：Invalid SPI length (%d) in proposal payload • 一个提议载荷中只能存在一个变换载荷，当前存在多个变换载荷，显示为：Only one transform is permitted in one proposal, but %u transforms are found • 在 profile 下未找到匹配的提议，显示为：Failed to find matching proposal in profile %s • 在 profile 下没有找到提议，显示为：Failed to find proposal %u in profile %s • 在 profile 下没有找到 keychain，显示为：Failed to find keychain %s in profile %s • 重传超时，显示为：Retransmission timeout • 配置错误，显示为：Incorrect configuration • 构造证书请求载荷失败，显示为：Failed to construct certificate request payload • 收到错误通知，显示为：An error notification is received • 添加 Tunnel 失败，显示为：Failed to add tunnel $4：建立IPsec SA的角色，发起者或者响应者 $5-$9：本端信息 $10-$14: 远端信息 $15: 内部VPN实例 $16: 外部VPN实例 $17-$18: 发起者Cookie和响应者Cookie $19: 连接号 $20: IKE Tunnel编号，默认值为4294967295 $21: IKE profile名称

日志等级	6
举例	IKE/6/IKE_P1_SA_ESTABLISH_FAIL: Failed to establish phase 1 SA in main mode IKE_P1_STATE_SEND1 state. Reason: Failed to get certificate. SA information: • Role: Initiator • Local IP: 4.4.4.4 • Local ID type: IPV4_ADDR • Local ID: 4.4.4.4 • Local port: 500 • Retransmissions: 0 • Remote IP: 4.4.4.5 • Remote ID type: IPV4_ADDR • Remote ID: 4.4.4.5 • Remote port: 500 • Recived retransmissions: 0 • Inside VPN instance: aaa • Outside VPN instance : bbb • Initiator Cookie: 4a42af47dbf0b2b1 • Responder Cookie: 8f8c1ff6645efbaf • Connection ID: 1 • Tunnel ID: 1 • IKE profile name: abc
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

61.2 IKE_P1_SA_TERMINATE

日志内容	The IKE phase 1 SA was deleted. Reason: [STRING]. SA information: • Role: [STRING] • Local IP: [STRING] • Local ID type: [STRING] • Local ID: [STRING] • Local port: [UINT32] • Retransmissions: [UINT32] • Remote IP: [STRING] • Remote ID type: [STRING] • Remote ID: [STRING] • Remote port: [UINT32] • Recived retransmissions: [UINT32] • Inside VPN instance: [STRING] • Outside VPN instance: [STRING] • Initiator Cookie: [STRING] • Responder Cookie: [STRING] • Connection ID: [UINT32] • Tunnel ID: [UINT32] • IKE profile name: [STRING]
参数解释	$1：删除原因： • DPD 超时，显示为：DPD timeout • 新的 IKE SA 已经协商，旧的 SA 将要被删除，显示为：New IKE SA had been negotiated, and the old one was deleted • 删除冗余的 SA，显示为：The IKE SA was redundant • 收到对端的 IKE SA 删除报文，显示为：An IKE SA deletion message was received from peer • IKE keepalive 超时，显示为：IKE keepalive timed out • IKE SA 已经老化，即将被删除，显示为：The IKE SA expired • 执行了 reset ike sa [connection-id connection-id]命令，显示为：Delete IKE SA by connection-id • 所有的 IKE SA 被删除，显示为：All IKE SAs were deleted • GDOI 组的 IKE SA 被删除，显示为：The IKE SA in the GDOI group was deleted $2：建立IPsec SA的角色，发起者或者响应者 $3-$7：本端信息 $8-$12: 远端信息 $13: 内部VPN实例 $14: 外部VPN实例 $15-$16: 发起者Cookie和响应者Cookie $17: 连接号.

	$18: IKE Tunnel编号，默认值为4294967295 $19: IKE profile名称
日志等级	6
举例	IKE/6/IKE_P1_SA_TERMINATE: The IKE phase 1 SA was deleted. Reason: DPD timeout. SA information: • Role: Responder • Local IP: 4.4.4.4 • Local ID type: IPV4_ADDR • Local ID: 4.4.4.4 • Local port: 500 • Retransmissions: 0 • Remote IP: 4.4.4.5 • Remote ID type: IPV4_ADDR • Remote ID: 4.4.4.5 • Remote port: 500 • Recived retransmissions: 0 • Inside VPN instance: aaa • Outside VPN instance: bbb • Initiator Cookie: 4a42af47dbf0b2b1 • Responder Cookie: 8f8c1ff6645efbaf • Connection ID: 1 • Tunnel ID: 1 • IKE profile name: abc
日志说明	第一阶段SA删除
处理建议	无

61.3 IKE_P2_SA_ESTABLISH_FAIL

日志内容	Failed to establish phase 2 SA in [STRING] state. Reason: [STRING]. SA information: • Role: [STRING]. • Local address: [STRING]. • Remote address: [STRING]. • Sour addr: [STRING] Port: [UINT32] Protocol: [STRING] • Dest addr: Protocol:[STRING] Port: [UINT32] Protocol: [STRING] • Inside VPN instance: [STRING]. • Outside VPN instance: [STRING]. • Inbound AH SPI: [STRING] • Outbound AH SPI: [STRING] • Inbound ESP SPI: [STRING] • Outbound ESP SPI: [STRING] • Initiator Cookie: [STRING] • Responder Cookie: [STRING]. • Message ID: [STRING]. • Connection ID: [UINT32]. • Tunnel ID: [UINT32].
参数解释	$1：协商状态机状态 $2：失败原因： • 构造 ID 载荷失败，显示为：Failed to construct ID payload • 计算 HASH 算法失败，显示为：Failed to calculate %s • 验证 HASH 算法失败，显示为：Failed to validate %s • 计算密钥材料失败，显示为：Failed to compute key material • 配置错误，显示为：Incorrect configuration • 转换 IPsec SA 失败，显示为：Failed to switch IPsec SA • Nonce 载荷不存在，显示为：The nonce payload doesn't exist • 无效的 Nonce 载荷长度，显示为：Invalid nonce payload length (%lu) • SA 载荷中没有有效的 DH group 描述，显示为：No valid DH group description in SA payload • KE 载荷不存在，显示为：The KE payload doesn't exist • 存在多个 KE 载荷，显示为：Too many KE payloads • KE 载荷长度与 DH group 描述不匹配，显示为：The length of the KE payload doesn't match the DH group description • 获取 SP 时与 IPsec 通信失败，显示为：Failed to send message to IPsec when getting SP • 获取 SPI 时与 IPsec 通信失败，显示为 Failed to send message to IPsec when getting SPI • 添加 IPsec SA 失败，显示为：Failed to add phase 2 SA • 二阶段报文重传超时，显示为：Retransmission of phase 2 packet timed out

	• 二阶段双方同时发起协商冲突，显示为：Collision detected in phase 2 negotiation • 未找到匹配的提议，显示为：No matching proposal found between the local and remote ends • 变换载荷编号非递增，显示为：Transform number is not monotonically increasing • 提议载荷存在的变换载荷比指定变换载荷多，显示为：Proposal payload has more transforms than specified in the proposal payload • 提议载荷存在的变换载荷比指定变换载荷少，显示为：Proposal payload has less transforms than specified in the proposal payload • IPsec 变换载荷中属性重复，显示为：Attribute %d is repeated in IPsec transform %d • 报文中 SA_LIFE_TYPE 属性重复，显示为：SA_LIFE_TYPE attribute is repeated in packet • 消息中的 SA_LIFE_TYPE 属性必须在 SA_LIFE_DURATION 属性前，显示为 The SA_LIFE_TYPE attribute must be in front of the SA_LIFE_DURATION attribute • 不支持的 IPsec 属性，显示为：Unsupported IPsec attribute %s • IPsec 安全提议必须指定封装模式，显示为：The encapsulation mode must be specified in the IPsec transform set • IPsec 提议的 SPI 长度超出范围，显示为：Invalid SPI length (%u) in IPsec proposal • IPsec 提议中的 SPI 无效，显示为：Invalid SPI (%u) in IPsec proposal • 变换载荷中的变换 ID 与认证算法不匹配，显示为：The Transform ID (%d) in transform %d doesn't match authentication algorithm %s (%u) • 从提议中获取 SPI 失败，显示为：Failed to get SPI from proposal • IPsec 提议中没有变换载荷，显示为：No transform in IPsec proposal • 同一个提议中存在多个 AH 提议，显示为：A proposal payload contains more than one AH proposal • 提议中存在无效的下一个载荷，显示为：Invalid next payload (%u) in proposal • 没有 ESP 或 AH 提议，显示为：No ESP or AH proposal • 不支持的 DOI，显示为：Unsupported DOI • 不支持的 DOI 场景，显示为：Unsupported IPsec DOI situation (%u) • 无效的 IPsec 提议，显示为：Invalid IPsec proposal %u • 重协商 IPsec SA 时获取 IPsec 策略失败，显示为：Failed to get IPsec policy when renegotiating IPsec SA • P2 阶段响应方获取 IPsec 策略失败，显示为：Failed to get IPsec policy as phase 2 responder $3：建立IPsec SA的角色，发起者或者响应者 $4：本端IP地址 $5：远端IP地址 $6-$11: 数据流 $12: 内部VPN实例 $13: 外部VPN实例 $14: 入方向AH SPI $15: 出方向AH SPI $16: 入方向ESP SPI $17: 出方向ESP SPI $18-$19: 发起者Cookie和响应者Cookie

	$20: 消息ID $21: 连接号 $22: IKE Tunnel编号，默认值为4294967295
日志等级	6
举例	IKE/6/IKE_P2_SA_ESTABLISH_FAIL: Failed to establish phase 2 SA in IKE_P2_STATE_GETSPI state. Reason: Failed to get SPI from proposal. SA information: • Role: Responder • Local address: 2.2.2.2 • Remote address: 1.1.1.1 • Sour addr: 192.168.2.0/255.255.255.0 Port: 0 Protocol: IP • Dest addr: 192.168.1.0/255.255.255.0 Port: 0 Protocol: IP • Inside VPN instance: aaa • Outside VPN instance: bbb • Inbound AH SPI: 192365458 • Outbound AH SPI: 13654581 • Inbound ESP SPI: 292334583 • Outbound ESP SPI: 5923654586 • Initiator Cookie: 4a42af47dbf0b2b1 • Responder Cookie: 8f8c1ff6645efbaf • Message ID: 0xa2b11c8e • Connection ID: 1 • Tunnel ID: 1
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

61.4 IKE_P2_SA_TERMINATE

日志内容	The IKE phase 2 SA was deleted. Reason: [STRING]. SA information: • Role: [STRING] • Local address: [STRING] • Remote address: [STRING] • Sour addr: [STRING] Port: [UINT32] Protocol: [STRING] • Dest addr: [STRING] Port: [UINT32] Protocol: [STRING] • Inside VPN instance: [STRING] • Outside VPN instance: [STRING] • Inbound AH SPI: [STRING] • Outbound AH SPI: [STRING] • Inbound ESP SPI: [STRING] • Outbound ESP SPI: [STRING] • Initiator Cookie: [STRING] • Responder Cookie: [STRING] • Message ID: [STRING] • Connection ID: [UINT32] • Tunnel ID: [UINT32]
参数解释	$1：删除原因： • 硬超时，显示为：The SA expired • 收到 IPsec SA 删除消息，显示为：An IPsec SA deletion message was received from peer • 新的 P2 SA 已协商，旧的删除，显示为：New P2 SA had been negotiated, and the old one was deleted • 删除所有 SA，显示为：All P2 SAs were deleted • 按 SPID 删除 SA，显示为：The P2 SA was deleted by SPID • 按接口删除 SA，显示为：The P2 SA was deleted by IFIndex • 按 SA 索引删除 SA，显示为：The P2 SA was deleted by SA index $2：建立IPsec SA的角色，发起者或者响应者 $3：本端IP地址 $4：远端IP地址 $5-$10: 数据流 $11: 内部VPN实例 $12: 外部VPN实例 $13: 入方向AH SPI $14: 出方向AH SPI $15: 入方向ESP SPI $16: 出方向ESP SPI $17-$18: 发起者Cookie和响应者Cookie $19: 消息ID.

	$20: 连接号 $21: IKE Tunnel编号，默认值为4294967295
日志等级	6
举例	IKE/6/IKE_P2_SA_TERMINATE: The IKE phase 2 SA was deleted. Reason: An IPsec SA deletion message was received. SA information: • Role: Responder • Local address: 2.2.2.2 • Remote address: 1.1.1.1 • Sour addr: 192.168.2.0/255.255.255.0 Port: 0 Protocol: IP • Dest addr: 192.168.1.0/255.255.255.0 Port: 0 Protocol: IP • Inside VPN instance: aaa • Outside VPN instance: bbb • Inbound AH SPI: 192365458 • Outbound AH SPI: 13654581 • Inbound ESP SPI: 292334583 • Outbound ESP SPI: 5923654586 • Initiator Cookie: 4a42af47dbf0b2b1 • Responder Cookie: 8f8c1ff6645efbaf • Message ID: 0xa2b11c8e • Connection ID: 1 • Tunnel ID: 1
日志说明	第二阶段SA删除
处理建议	无

61.5 IKE_XAUTH_FAILE

日志内容	Failed to pass extended authentication in [STRING] mode [STRING] state. Reason: [STRING]. SA information: • Role: [STRING]. • Local IP: [STRING]. • Local ID type: [STRING]. • Local ID: [STRING]. • Local port: [UINT32]. • Retransmissions: [UINT32] • Remote IP: [STRING]. • Remote ID type: [STRING]. • Remote ID: [STRING]. • Remote port: [UINT32]. • Recived retransmissions: [UINT32] • Inside VPN instance: [STRING]. • Outside VPN instance: [STRING]. • Initiator Cookie: [STRING] • Responder Cookie: [STRING]. • Message ID: [STRING]. • Connection ID: [UINT32].
参数解释	$1：协商模式，主模式或者野蛮模式 $2：协商状态机状态 $3：失败原因： • 认证 HASH 失败，显示为：Failed to verify the HASH payload • 解析属性失败，显示为：Failed to parse the attribute payload $4：建立IPsec SA的角色，发起者或者响应者 $5-$9：本端信息 $10-$14: 远端信息 $15: 内部VPN实例 $16: 外部VPN实例 $17-$18: 发起者Cookie和响应者Cookie $19: 消息ID $20: 连接号
日志等级	6
举例	IKE/6/IKE_XAUTU_FAILE: Failed to pass extended authentication, in main mode IKE_XAUTH_STATE_SET state. Reason: Failed to parse the attribute payload. SA information: • Role: Initiator • Local IP: 4.4.4.4

	• Local ID type: IPV4_ADDR • Local ID: 4.4.4.4 • Local port: 500 • Retransmissions: 0 • Remote IP: 4.4.4.5 • Remote ID type: IPV4_ADDR • Remote ID: 4.4.4.5 • Remote port: 500 • Recived retransmissions: 0 • Inside VPN instance: aaa • Outside VPN instance: bbb • Initiator Cookie: 4a42af47dbf0b2b1 • Responder Cookie: 8f8c1ff6645efbaf • Message ID: 0xa2b11c8e • Connection ID: 1
日志说明	xauth协商失败信息及原因
处理建议	无

62 IMA

本节介绍 IMA（Integrity Measurements Architecture，完整性度量架构）模块输出的日志信息。

62.1 IMA_ALLOCATE_FAILED

日志内容	Failed to allocate resource for file [STRING].
参数解释	$1：可信度量的目标文件名称
日志等级	4
举例	IMA/4/IMA_ALLOCATE_FAILED: Failed to allocate resource for file /sbin/tcsmd.
日志说明	IMA给度量目标文件分配资源失败
处理建议	请联系技术支持

62.2 IMA_DATA_ERROR

日志内容	Can't collect data of file [STRING].
参数解释	$1：可信度量的目标文件名称
日志等级	4
举例	IMA/4/IMA_DATA_ERROR: Can't collect data of file /sbin/tcsmd.
日志说明	收集目标文件的数据失败，可能是打开或读取文件失败，或计算文件Hash值出错
处理建议	请联系技术支持

62.3 IMA_FILE_HASH_FAILED

日志内容	Hash value of file [STRING] is not consistent with that in the RM file.
参数解释	$1：可信度量的目标文件名称
日志等级	4
举例	IMA/4/IMA_FILE_HASH_FAILED: Hash value of file /sbin/tcsmd is not consistent with that in the RM file.
日志说明	目标文件的Hash值与RM文件中该文件的Hash值不匹配，此时该文件不可信
处理建议	请联系技术支持

62.4 IMA_RM_FILE_MISS

日志内容	File [STRING] is missing in the RM file.
参数解释	$1：可信度量的目标文件名称
日志等级	4
举例	IMA/4/IMA_RM_FILE_MISS: File /sbin/tcsmd is missing in the RM file.
日志说明	RM文件中未找到目标文件的信息
处理建议	请联系技术支持

62.5 IMA_RM_HASH_MISS

日志内容	Hash value of file [STRING] is missing in the RM file.
参数解释	$1：可信度量的目标文件名称
日志等级	4
举例	IMA/4/IMA_RM_HASH_MISS: Hash value of file /sbin/tcsmd is missing in the RM file.
日志说明	RM文件中没有目标文件的Hash值，可能目标文件在度量时使用的Hash算法在RM中不支持
处理建议	请联系技术支持

62.6 IMA_TEMPLATE_ERROR

日志内容	Failed to extend template hash value of file [STRING] to the PCR.
参数解释	$1：可信度量的目标文件名称
日志等级	4
举例	IMA/4/IMA_TEMPLATE_ERROR: Failed to extend template hash value of file /sbin/tcsmd to the PCR.
日志说明	将目标文件的模板Hash值扩展到PCR失败
处理建议	请联系技术支持

63 IP6ADDR

本节介绍 IPv6 地址模块输出的日志信息。

63.1 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

64 IPADDR

本节介绍 IP 地址模块输出的日志信息。

64.1 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

64.2 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

65 IPOE

本节介绍 IPoE 模块输出的日志信息。

65.1 IPOE_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：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=user1-IPAddr=1.1.0.1-IfName=Bas-interface0-OuterVLAN=N/A-InnerVLAN=N/A-MACAddr=FFFF-FFFF-FFFF; The user came online successfully.
日志说明	用户上线成功
处理建议	无

65.2 IPOE_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65-1
日志等级	6
举例	IPOE/6/IPOE_USER_LOGON_FAILED: -UserName=user1-IPAddr=N/A-IfName=Bas-interface0-OuterVLAN=N/A-InnerVLAN=N/A-MACAddr=FFFF-FFFF-FFFF-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65-1

表65-1 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 • 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

65.3 IPOE_USER_LOGOFF_NORMAL

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65-2
日志等级	6
举例	IPOE/6/IPOE_USER_LOGOFF_NORMAL: -UserName=user1-IPAddr=1.1.0.1-IfName=Bas-interface0-OuterVLAN=N/A-InnerVLAN=N/A-MACAddr=FFFF-FFFF-FFFF-Reason=DHCP user request; The user logged off.
日志说明	用户正常下线
处理建议	具体处理意见请见表65-2

表65-2 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

65.4 IPOE_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1-3
日志等级	6
举例	IPOE/6/IPOE_USER_LOGOFF_ABNORMAL: -UserName=user1-IPAddr=1.1.0.1-IfName=Bas-interface0-OuterVLAN=N/A-InnerVLAN=N/A-MACAddr=FFFF-FFFF-Reason= Session timeout; 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65-3

表65-3 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
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
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UNIS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**
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
BRAS errors	设备内部软件处理异常造成的用户下线	1. 请依次执行如下命令收集用户上线过程的调试信息 o terminal monitor o terminal debugging o debugging ip subscriber 2. 将相关日志信息和调试信息保存到本地，并联系UNIS 技术支持

66 IPS

本节介绍 IPS 模块输出的系统日志和快速日志信息。

66.1 IPS_IPV4_INTERZONE（系统日志）（快速日志）

日志内容	Protocol(1001)=[STRING]; Application(1002)=[STRING]; SrcIPAddr(1003)=[IPADDR]; SrcPort(1004)=[UINT16]; DstIPAddr(1007)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1042)=[STRING]; SrcZoneName(1025)=[STRING]; DstZoneName(1035)=[STRING]; UserName(1113)=[STRING]; PolicyName(1079)=[STRING]; AttackName(1088)=[STRING]; AttackID(1089)=[UINT32]; Category(1090)=[STRING]; Protection(1091)=[STRING]; SubProtection(1092)=[STRING]; Severity(1087)=[STRING]; Action(1053)=[STRING]; CVE(1075)=[STRING]; BID(1076)=[STRING]; MSB(1077)=[STRING]; HitDirection(1115)=[STRING]; RealSrcIP(1100)=[STRING]; SubCategory(1124)=[STRING]; LoginUserName(1177)=[STRING]; LoginPwd(1178)=[STRING]; CapturePktName(1116)=[STRING]; DomainName(1099)=[STRING]; HttpHost(1117)=[STRING]; HttpFirstLine(1118)=[STRING]; FileName(1097)=[STRING]; SrcMacAddr(1021)=[STRING]; DstMacAddr(1022)=[STRING]; RealSrcMacAddr(1204)=[STRING]; RealDstMacAddr(1205)=[STRING]; PayLoad(1135)=[STRING]; CWE(1174)=[STRING]; VlanID(1175)=[UINT32]; VNI(1213)=[UINT32]; SrcLocation(1209)=[STRING]; DstLocation(1214)=[STRING];
参数解释	$1：协议类型 $2：应用协议名称 $3：源IP地址 $4：源端口号 $5：目的IP地址 $6：目的端口号 $7：源VPN名称 $8：源安全域名称 $9：目的安全域名称 $10：身份识别用户的名称 $11：策略名称 $12：威胁名称 $13：威胁ID $14：攻击分类 $15：保护对象 $16：保护子对象 $17：严重级别，包括如下取值： • INVALID：未指定 • LOW：低 • MEDIUM：中 • HIGH：高 • CRITICAL：严重 $18：动作名称，包括如下取值： • Block-Source ：阻断源 • Drop ：丢包 • Reset：重置 • Permit：告警 • Redirect：重定向

	• Capture：捕获 • Logging：生成日志 $19：CVE（公共漏洞和暴露编号） $20：BID（软件漏洞跟踪编号） $21：MSB（微软安全公告编号） $22：命中报文方向，包括如下取值： • original：请求方向 • reply：应答方向 $23：真实源IP地址 $24：攻击子分类 $25：登录用户名 $26：登录用户密码（本字段的支持情况与设备型号有关，请以设备实际情况为准） $27：捕获文件名称 $28：域名（设备从DNS协议请求报文中提取到的） $29：主机名（设备从HTTP协议请求报文中提取到的） $30：报文首行 $31：文件名 $32：源MAC地址 $33：目的MAC地址 $34：真实源MAC地址（仅当开启跨三层MAC地址识别功能后显示取值） $35：真实目的MAC地址（仅当开启跨三层MAC地址识别功能后显示取值） $36：事件返回参数 $37：CWE（公共漏洞和暴露编号） $38：VLAN ID $39：VXLAN ID $40：源地区 $41：目的地区

日志等级	4
举例	IPS/4/IPS_IPV4_INTERZONE:-Context=1; Protocol(1001)=TCP; Application(1002)=http; SrcIPAddr(1003)=100.10.10.40; SrcPort(1004)=2999; DstIPAddr(1007)=200.10.10.40; DstPort(1008)=80; RcvVPNInstance(1042)=; SrcZoneName(1025)=spf; DstZoneName(1035)=spf; UserName(1113)=abc; PolicyName(1079)=ips; AttackName(1088)=WEB_CLIENT_Windows_Media_ASF_File_Download_SET; AttackID(1089)=5707; Category(1090)=Other; Protection(1091)=Other; SubProtection(1092)=Other; Severity(1087)=CRITICAL; Action(1053)=Reset & Logging; CVE(1075)=CVE-2014-6277 | CVE-2014-6278; BID(1076)=BID-22559; MSB(1077)=MS10-017; HitDirection(1115)=original; RealSrcIP(1100)=10.10.10.10,20.20.20.20; SubCategory(1124)=Other; LoginUserName(1177)=admin; LoginPwd(1178)=YW5nc2MxMDA2Vw==; CapturePktName(1116)=ips_100.10.10.40_20171205_101112_5707.pcap; DomainName(1099)=; HttpHost(1117)=www.shr.com; HttpFirstLine(1118)=/file/show.cgi%7cecho%20HSC/http_pic_300k.jpg; FileName(1097)=123.txt; SrcMacAddr(1021)=dc2d-cb01-0001; DstMacAddr(1022)=dc2d-cb93-02ac; RealSrcMacAddr(1204)=; RealDstMacAddr(1205)=; PayLoad(1135)=/file/show.cgi; CWE(1174)=CWE-94; VlanID(1175)=400; VNI(1213)=--; SrcLocation(1209)=China Macao; DstLocation(1214)=SaintKittsandNevis;
日志说明	当报文与IPS特征匹配成功时输出该日志
处理建议	无

66.2 IPS_IPV6_INTERZONE（系统日志）（快速日志）

日志内容	Protocol(1001)=[STRING]; Application(1002)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; SrcPort(1004)=[UINT16]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1042)=-[STRING]; SrcZoneName(1025)=[STRING]; DstZoneName(1035)=[STRING]; UserName(1113)=[STRING]; PolicyName(1079)=[STRING]; AttackName(1088)=[STRING]; AttackID(1089)=[UINT32]; Category(1090)=[STRING]; Protection(1091)=[STRING]; SubProtection(1092)=[STRING]; Severity(1087)=[STRING]; Action(1053)=[STRING]; CVE(1075)=[STRING]; BID(1076)=[STRING]; MSB(1077)=[STRING]; HitDirection(1115)=[STRING]; RealSrcIP(1100)=[STRING]; SubCategory(1124)=[STRING]; LoginUserName(1177)=[STRING]; LoginPwd(1178)=[STRING]; CapturePktName(1116)=[STRING]; DomainName(1099)=[STRING]; HttpHost(1117)=[STRING]; HttpFirstLine(1118)=[STRING]; FileName(1097)=[STRING]; SrcMacAddr(1021)=[STRING]; DstMacAddr(1022)=[STRING]; RealSrcMacAddr(1204)=[STRING]; RealDstMacAddr(1205)=[STRING]; PayLoad(1135)=[STRING]; CWE(1174)=[STRING]; VlanID(1175)=[UINT32]; VNI(1213)=[UINT32]; SrcLocation(1209)=[STRING]; DstLocation(1214)= [STRING];
参数解释	$1：协议类型 $2：应用协议名称 $3：源IPv6地址 $4：源端口号 $5：目的IPv6地址 $6：目的端口号 $7：源VPN名称 $8：源安全域名称 $9：目的安全域名称 $10：身份识别用户的名称 $11：策略名称 $12：威胁名称 $13：威胁ID $14：攻击分类 $15：保护对象 $16：保护子对象 $17：严重级别，包括如下取值： • INVALID：未指定 • LOW：低 • MEDIUM：中 • HIGH：高 • CRITICAL：严重 $18：动作名称，包括如下取值： • Block-Source ：阻断源 • Drop ：丢包 • Reset：重置 • Permit：告警 • Redirect：重定向

	• Capture：捕获 • Logging：生成日志 $19：CVE（公共漏洞和暴露编号） $20：BID（软件漏洞跟踪编号） $21：MSB（微软安全公告编号） $22：命中报文方向，包括如下取值： • original：请求方向 • reply：应答方向 $23：真实源IP地址 $24：攻击子分类 25：登录用户名 $26：登录用户密码（本字段的支持情况与设备型号有关，请以设备实际情况为准） $27：捕获文件名称（动作配置为抓包） $28：域名（设备从DNS协议请求报文中提取到的） $29：主机名（设备从HTTP协议请求报文中提取到的） $30：报文首行 $31：文件名 $32：源MAC地址 $33：目的MAC地址 $34：真实源MAC地址（仅当开启跨三层MAC地址识别功能后显示取值） $35：真实目的MAC地址（仅当开启跨三层MAC地址识别功能后显示取值） $36：事件返回参数 $37：CWE（公共漏洞和暴露编号） $38：VLAN ID $39：VXLAN ID $40：源地区 $41：目的地区

日志等级	4
举例	IPS/4/IPS_IPV6_INTERZONE:-Context=1; Protocol(1001)=TCP; Application(1002)=http; SrcIPv6Addr(1036)=100::40; SrcPort(1004)=2999; DstIPv6Addr(1037)=200::40; DstPort(1008)=80; RcvVPNInstance(1042)=; SrcZoneName(1025)=spf; DstZoneName(1035)=spf; UserName(1113)=aaa; PolicyName(1079)=ips; AttackName(1088)=WEB_CLIENT_Windows_Media_ASF_File_Download_SET; AttackID(1089)=5707; Category(1090)=Other; Protection(1091)=Other; SubProtection(1092)=Other; Severity(1087)=CRITICAL; Action(1053)=Reset & Logging; CVE(1075)=CVE-2014-6277 | CVE-2014-6278; BID(1076)=BID-22559; MSB(1077)=MS10-017; HitDirection(1115)=reply; RealSrcIP(1100)=10::1; SubCategory(1124)=Other; LoginUserName(1177)=admin; LoginPwd(1178)=YW5nc2MxMDA2Vw==; CapturePktName(1116)=ips_100::40_20171205_101112_5707.pcap; DomainName(1099)=; HttpHost(1117)=www.shr.com; HttpFirstLine(1118)=/file/show.cgi%7cecho%20HSC/http_pic_300k.jpg; FileName(1097)=123.txt; SrcMacAddr(1021)=dc2d-cb01-0001; DstMacAddr(1022)=dc2d-cb93-02ac; RealSrcMacAddr(1204)=; RealDstMacAddr(1205)=; PayLoad(1135)=/file/show.cgi; CWE(1174)=CWE-94; VlanID(1175)=400; VNI(1213)=--; SrcLocation(1209)=China Macao; DstLocation(1214)=SaintKittsandNevis;
日志说明	当IPv6报文与IPS特征匹配成功时输出该日志
处理建议	无

66.3 IPS_WARNING（系统日志）

日志内容	Updated the IPS signature library successfully.
参数解释	无
日志等级	4
举例	IPS/4/IPS_WARNING: -Context=1; Updated the IPS signature library successfully.
日志说明	入侵防御特征库升级成功，包含如下情况： • 立即升级成功 • 本地升级成功
处理建议	无

66.4 IPS_WARNING（系统日志）

日志内容	Rolled back the IPS signature library successfully.
参数解释	无
日志等级	4
举例	IPS/4/IPS_WARNING: -Context=1; Rolled back the IPS signature library successfully.
日志说明	入侵防御特征库回滚成功，包含如下情况： • 回滚到上一个版本成功 • 回滚到出厂版本成功
处理建议	无

66.5 IPS_WARNING（系统日志）

日志内容	Failed to update the IPS signature library because no valid license was found for the IPS feature.
参数解释	无
日志等级	4
举例	IPS/4/IPS_WARNING: -Context=1; Failed to update the IPS signature library because no valid license was found for the IPS feature.
日志说明	没有找到有效的License，入侵防御特征库升级失败。包含如下情况： • 立即升级失败 • 本地升级失败（仅在使用 Web 方式进行升级时提示） • 定时升级失败
处理建议	无

66.6 IPS_WARNING（系统日志）

日志内容	SNORT rule may lost because lock failed during recover!
参数解释	无
日志等级	4
举例	IPS/4/IPS_WARNING: -Context=1; SNORT rule may lost because lock failed during recover!
日志说明	当配置恢复期间加锁失败时，提示用户这样可能会导致部分Snort规则丢失
处理建议	无

66.7 IPS_WARNING（系统日志）

日志内容	The max of snort rule count is 1024.
参数解释	无
日志等级	4
举例	IPS/4/IPS_WARNING: -Context=1; The max of snort rule count is 1024.
日志说明	最多可以导入1024条Snort规则
处理建议	无

66.8 IPS_WARNING（系统日志）

日志内容	Import snort rule successfully.
参数解释	无
日志等级	4
举例	IPS/4/IPS_WARNING: -Context=1; Import snort rule successfully.
日志说明	导入Snort规则成功
处理建议	无

66.9 IPS_WARNING（系统日志）

日志内容	Import snort rule completely,the total error rules [UINT32].
参数解释	$1：导入失败的自定义规则总数
日志等级	4
举例	IPS/4/IPS_WARNING: -Context=1; Import snort rule completely,the total error rules 10.
日志说明	Snort规则已完成导入，提示用户导入失败的Snort规则总数为XXX
处理建议	无

66.10 IPS_WARNING（系统日志）

日志内容	Unload the user-defined snort rules successfully.
参数解释	无
日志等级	4
举例	IPS/4/IPS_WARNING: -Context=1; Unload the user-defined snort rules successfully.
日志说明	删除Snort规则成功
处理建议	无

66.11 IPS_WARNING（系统日志）

日志内容	Copy SigPack file failed because flash is not enough.
参数解释	无
日志等级	4
举例	IPS/4/IPS_WARNING: -Context=1; Copy SigPack file failed because flash is not enough.
日志说明	Flash存储空间不足，IPS特征库升级失败
处理建议	无

66.12 IPS_WARNING（系统日志）

日志内容	Failed to update signature package in phase [STRING].
参数解释	$1：升级阶段，包括如下取值： • DOWNLOAD：下载特征库阶段 • GETURLFILE：获取特征库文件下载路径阶段 • PREPARE：特征库准备阶段 • PARSE：特征库解析阶段 • UNKNOWN：未知
日志等级	4
举例	IPS/4/IPS_WARNING: -Context=1; Failed to update signature package in phase PARSE.
日志说明	特征库升级失败时，提示用户失败发生在特征库升级的某个阶段
处理建议	无

67 IPSEC

本节介绍 IPsec 模块输出的日志信息。

67.1 IPSEC_DEBUG_LOG

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/log: 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

67.2 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
处理建议	对于硬件资源不足情况，请联系技术支持

67.3 IPSEC_KD3P_LOGINFO

日志内容	Anti-replay dropped a packet: src=[STRING]; time-sent=[STRING], [UINT32] [STRING] [UINT32] [UINT32]:[UINT32]:[UINT32] [UINT32]us; time-received=[STRING], [UINT32] [STRING] [UINT32] [UINT32]:[UINT32]:[UINT32] [UINT32]us; time-diff=[UINT32]us; window-size= +-[FLOAT]ms.
参数解释	$1：被丢弃报文的源IP地址 $2：发送报文的星期 $3：发送报文的日期 $4：发送报文的月份 $5：发送报文的年份 $6：发送报文的小时 $7：发送报文的分钟 $8：发送报文的秒数 $9：发送报文的微妙数 $10：接收报文的星期 $11：接收报文的日期 $12：接收报文的月份 $13：接收报文的年份 $14：接收报文的小时 $15：接收报文的分钟 $16：接收报文的秒数 $17：接收报文的微妙数 $18：发送接收之间的时间差，微秒数 $19：时间窗口的一半，毫秒数
日志等级	6
举例	IPSEC/6/log:Anti-replay dropped a packet: src=192.168.58.178;time-sent=Sat, 23 Apr 2016 11:17:29 594565us; time-received =Sat, 23 Apr 2016 11:17:26 707866us; time-diff=2886699us; window-size =+-2500ms.
日志说明	报文被丢弃。触发该日志的原因可能有如下几种： • 报文发送和接收之间的时间差超出窗口大小 • 接收端抗重放使能而收到的报文没有抗重放头 • 隧道模式下，抗重放未使能但是收到带有抗重放头的报文
处理建议	无

67.4 IPSEC_SA_ESTABLISH

日志内容	IPsec SA was established. SA information: Role: [STRING] Local address: [STRING] Remote address: [STRING] Sour addr: [STRING] Port: [UINT32] Protocol: [STRING] Dest addr: [STRING] Port: [UINT32] Protocol: [STRING] Inside VPN instance: [STRING] Outside VPN instance: [STRING] Inbound AH SPI: [STRING] Outbound AH SPI: [STRING] Inbound ESP SPI: [STRING] Outbound ESP SPI: [STRING] ACL number: [UINT32] ACL name: [STRING]
参数解释	$1：建立IPsec SA的角色，发起者或者响应者 $2：本端IP地址 $3：远端IP地址 $4-$9：数据流 $10: 内部VPN实例 $11: 外部VPN实例 $12: 入方向AH SPI $13: 出方向AH SPI $14: 入方向ESP SPI $15: 出方向ESP SPI $16: ACL编号，默认值为4294967295 $17: ACL名称，ACL编号与ACL名称只会显示其中一种
日志等级	6
举例	IPSEC/6/IPSEC_SA_ESTABLISH: IPsec SA was established. Role: Responder Local address: 2.2.2.2 Remote address: 1.1.1.1 Sour addr: 192.168.2.0/255.255.255.0 Port: 0 Protocol: IP Dest addr: 192.168.1.0/255.255.255.0 Port: 0 Protocol: IP Inside VPN instance: aaa Outside VPN instance: bbb Inbound AH SPI: 192365458 Outbound AH SPI: 13654581 Inbound ESP SPI: 292334583 Outbound ESP SPI: 5923654586 ACL number: 3101
日志说明	IPsec SA创建成功

处理建议	无

67.5 IPSEC_SA_ESTABLISH_FAIL

日志内容	Failed to establish IPsec SA. Reason: [STRING]. SA information: Role: [STRING] Local address: [STRING] Remote address: [STRING] Sour addr: [STRING] Port: [UINT32] Protocol: [STRING] Dest addr: [STRING] Port: [UINT32] Protocol: [STRING] Inside VPN instance: [STRING] Outside VPN instance: [STRING] Inbound AH SPI: [STRING] Outbound AH SPI: [STRING] Inbound ESP SPI: [STRING] Outbound ESP SPI: [STRING] ACL number: [UINT32] ACL name: [STRING]
参数解释	$1：IPsec SA创建失败的原因： • 获取 SP 时 SP 配置不完整，显示为：Get SP: Required configuration is missing in the SP. SP ID=%u. • 获取 SP 时本地地址不匹配，显示为：Get SP: The SP's local address doesn't match the local address configured in the IKE profile. SP ID=%u, SP's local address=%s, p2policy's local address=%s. • 获取 SP 时远端地址不存在，显示为：Get SP: The remote address doesn't exist. SP ID=%u, hostname=%s. • 远端地址不匹配，显示为：Get SP: The SP's remote address doesn't match the remote address configured in the IKE profile. SP ID=%u, SP's remote address=%s, p2policy's remote address=%s. • ACL 或 profile 配置错误，显示为：The policy contains incorrect ACL or IKE profile configuration. PolicyName=%s, Seqnum=%d. • 获取 SP 时在 SP 中未找到 IPsec 安全提议，显示为：Get SP: The SP doesn't have an IPsec transform set. • 创建临时 SA 失败，显示为：Get SP: Failed to create larval SA. • 填充 SA 数据失败，显示为：Create SA: Failed to fill the SA. • 添加 IKE SA 失败，显示为：Create SA: Failed to create SA. • 添加 IKE SA 时未找到 SP，显示为：Create SA: Can't find SP. • Tunnel 已存在，显示为：Failed to create tunnel because a tunnel with the same index and sequence number already exists. Tunnel index=%d, tunnel seq=%d. • 切换 SA 未找到入方向 SA，显示为：Failed to switch SA because the inbound SA can't be found. SPI=%u. • 切换 SA 时 SA 状态错误，显示为：Failed to switch SA because the SA state is incorrect. • 切换 SA，未找到出方向 SA，显示为：Failed to switch SA because the outbound SA can't be found. • 切换 SA 时未找到使用另一种安全协议的 SA，显示为：Failed to switch SA because the outbound SA using another security protocol can't be found.

	• 内核态切换 SA 失败，显示为：Failed to switch SA in kernel. • 通知内核链路层变化失败，显示为：Failed to notify kernel of the link state change. • Tunnel 数达到能力上限，显示为：Number of IPsec tunnels reached the crypto capacity of the device. • Tunnel 个数达到上限，显示为：Maximum number of IPsec tunnels already reached. • 内核态添加 SA 失败，显示为：Failed to add IPsec tunnel to kernel. • 获取 SP 时 IPsec 正在平滑，显示为：Getting SP: IPsec is smoothing. • 获取 SP 时 IPsec 进程未运行，显示为：Getting SP: IPsec is not running. • 获取 SP 时，通过 index 和 SeqNum 查找 SP 失败，显示为：Getting SP: Failed to find SP by index and sequence number. • 获取 SP 时生成 SA 超时，显示为：Getting SP: Creating SA timed out. • 获取 SP 时，通过普通接口获取 SP 时，目标板不在线，显示为：Getting SP by interface: Target node not online. • 获取 SP 时，按照 mGRE 方式获取 SP，获取接口失败，显示为：Getting SP by mGRE: Failed to get interface. • 获取 SP 时，尝试按照 mGRE 方式获取 SP 失败，无效的接口类型，显示为：Getting SP: Failed to get SP by mGRE because interface type was invalid. • 获取 SP 时，尝试按照 mGRE 方式获取 SP 失败，缺少相关配置，显示为：Getting SP: Failed to get SP by mGRE because of no tunnel protection configuration. • 获取 SP 时，尝试按照 mGRE 方式获取 SP 失败，未找到 profile，显示为：Getting SP: Failed to get SP by mGRE because profile %s was not found. • 获取 SP 时，尝试按照 mGRE 方式获取 SP 失败，profile 类型错误，显示为：Getting SP: Failed to get SP by mGRE because of wrong profile type. • 获取 SP 时，按照 mGRE 方式获取 SP，通过 profile 查找 SP 失败，显示为：Getting SP by mGRE: Failed to find profile SP by profile %s. • 尝试按照 mGRE 方式获取 SP 失败，显示为：Getting SP: Failed to get SP by mgre. • 尝试按照 SVTI 方式获取 SP 失败，无效的接口类型，显示为：Getting SP: Failed to get SP by SVTI because of invalid interface type. • 尝试按照 SVTI 方式获取 SP 失败，缺少相关配置，显示为：Getting SP: Failed to get SP by SVTI because of no tunnel protection configuration with interface %s. • 尝试按照 SVTI 方式获取 SP 失败，未找到 profile，显示为：Getting SP: Failed to get SP by SVTI because profile %s was not found. • 获取 SP 时，尝试按照 SVTI 方式获取 SP 失败，profile 类型错误，显示为：Getting SP: Failed to get SP by SVTI because of wrong type of profile %s. • 按照 SVTI 方式获取 SP 时，通过 profile 查找 SP 失败，显示为：Getting SP by SVTI: Failed to find profile SP by profile %s. • 尝试按照 SVTI 方式获取 SP 失败，SP 不是 IKE 方式的，显示为：Getting SP: Failed to get SP by SVTI because SP type was not ISAKMP with profile %s. • 尝试按照 SVTI 方式获取 SP 失败，重协商 SP 的 index 或 sequence num 有变化，显示为：Getting SP: Failed to match flow because renegotiation SP's index or Seqnum changed. • 获取 SP 时，匹配 SVTI 流失败，IKE profile 不匹配，显示为：Getting SP: Failed to match SVTI flow because IKE profile was not match. • 匹配 SVTI 流失败，匹配 ACL 失败，显示为：Getting SP: Failed to match SVTI flow because flow was not match with ACL. • 尝试按照 SVTI 方式获取 SP 时，创建 larval SA 失败，显示为：Getting SP by SVTI: Failed to create larval SA. • 尝试按照 mGRE 方式获取 SP 失败，显示为：Getting SP: Failed to get SP by SVTI

	with interface %s. • 通过三层口获取 SP 时，获取接口数据失败，显示为：Getting SP by L3 interface: Failed to get interface data. • 尝试通过三层口获取 SP 失败，根据 SP ENTRY KEY 找不到 SP ENTRY，显示为：Getting SP: Failed to get SP by L3 interface because no SP entry was found by key. • 获取 SP 时，尝试通过共享源接口获取 SP 失败，根据共享源接口的 SP ENTRY KEY 找不到 SP ENTRY，显示为：Getting SP: Failed to get SP by L3 interface because no source interface SP entry was found by key. • 获取SP时通过三层口获取SP时，匹配SP失败，SP不是Isakmp方式的，显示为：Getting SP by L3 interface: Failed to match SP because SP's mode not ISAKMP. • 获取 SP 时通过三层口获取 SP 时，匹配 SP 失败，SP 协商是不完整的，显示为：Getting SP by L3 interface: Failed to match SP because SP negotiation not complete. • 获取 SP 时，IKE 模板方式且未配置 acl，任意流不触发协商，显示为：Getting SP: Rejected peer's request of any flow when SP's mode was isakmp template and no ACL was specified. • 获取 SP 时通过三层口获取 SP 时，匹配 SP 失败，通过 SP 找不到 policy，显示为：Getting SP by L3 interface: Failed to match SP because policy cannot be found by SP. • 通过三层口获取 SP 时，匹配 SP 失败，掩码校验失败，显示为：Getting SP by L3 interface: Failed to match SP because flow netmask check failed. • 通过三层口获取SP时，匹配SP失败，流重叠检测失败，显示为：Getting SP by L3 interface: Failed to match SP because flow overlap check failed. • 获取SP时通过三层口获取SP时，匹配SP失败，ike profile与ipsec profile不匹配，显示为：Getting SP by L3 interface: Failed to match SP because IKE profile was %s while IPsec used profile %s. • 获取 SP 时，匹配流失败，因为 ACL 不匹配，显示为：Getting SP: Failed to match flow because ACL not match. • 获取 SP 时，匹配流失败，重协商 SP 的 index 或 sequence num 有变化，显示为：Getting SP: Failed to match flow because renegotiation SP's index or Seqnum changed. $2：建立IPsec SA的角色，发起者或者响应者 $3：本端IP地址 $4：远端IP地址 $5-$10: 数据流 $11: 内部VPN实例 $12: 外部VPN实例 $13: 入方向AH SPI $14: 出方向AH SPI $15: 入方向ESP SPI $16: 出方向ESP SPI $17: ACL编号，默认值为4294967295 $18: ACL名称，ACL编号与ACL名称只会显示其中一种

日志等级	6
举例	IPSEC/6/IPSEC_SA_ESTABLISH_FAIL: Failed to establish IPsec SA Reason: Failed to add IPsec tunnel. SA information: Role: Responder Local address: 2.2.2.2 Remote address: 1.1.1.1 Sour addr: 192.168.2.0/255.255.255.0 Port: 0 Protocol: IP Dest addr: 192.168.1.0/255.255.255.0 Port: 0 Protocol: IP Inside VPN instance: aaa Outside VPN instance: bbb Inbound AH SPI: 192365458 Outbound AH SPI: 13654581 Inbound ESP SPI: 292334583 Outbound ESP SPI: 5923654586 ACL number: 3101
日志说明	IPsec SA创建失败
处理建议	检查本端和对端设备上的IPsec配置

67.6 IPSEC_SA_INITIATION

日志内容	Began to establish IPsec SA. Local address: [STRING] Remote address: [STRING] Sour addr: [STRING] Port: [UINT32] Protocol: [STRING] Dest addr: [STRING] Port: [UINT32] Protocol: [STRING] Inside VPN instance: [STRING] Outside VPN instance: [STRING] ACL number: [UINT32] ACL name: [STRING]
参数解释	$1：本端IP地址 $2：远端IP地址 $3-$8：数据流 $9：内部VPN实例 $10: 外部VPN实例 $11: ACL编号，默认值为4294967295 $12: ACL名称，ACL编号与ACL名称只会显示其中一种
日志等级	6
举例	IPSEC/6/IPSEC_SA_INITIATION: Began to establish IPsec SA. Local address: 2.2.2.2 Remote address: 1.1.1.1 Sour addr: 192.168.2.0/255.255.255.0 Port: 0 Protocol: IP Dest addr: 192.168.1.0/255.255.255.0 Port: 0 Protocol: IP Inside VPN instance: aaa Outside VPN instance: bbb ACL number: 3101
日志说明	开始创建IPsec SA
处理建议	无

67.7 IPSEC_SA_TERMINATE

日志内容	The IPsec SA was deleted. Reason: [STRING] SA information: Role: [STRING] Local address: [STRING] Remote address: [STRING] Sour addr: [STRING] Port: [UINT32] Protocol: [STRING] Dest addr: [STRING] Port: [UINT32] Protocol: [STRING] Inside VPN instance: [STRING] Outside VPN instance: [STRING] Inbound AH SPI: [STRING] Outbound AH SPI: [STRING] Inbound ESP SPI: [STRING] Outbound ESP SPI: [STRING] ACL number: [UINT32] ACL name: [STRING]
参数解释	$1：IPsec SA被删除的原因，如： • SA 空闲超时，显示为：SA idle timeout • 执行了 reset 命令，显示为：The reset command was executed • 内部事件导致 SA 删除，显示为：Internal event • 配置变化导致 SA 删除，显示为：Configuration change • 收到 IKE 的删除消息，显示为：An IKE SA deletion message was received $2：建立IPsec SA的角色，发起者或者响应者 $3：本端IP地址 $4：远端IP地址 $5-$10: 数据流 $11: 内部VPN实例 $12: 外部VPN实例 $13: 入方向AH SPI $14: 出方向AH SPI $15: 入方向ESP SPI $16: 出方向ESP SPI $17: ACL编号，默认值为4294967295 $18: ACL名称，ACL编号与ACL名称只会显示其中一种
日志等级	6
举例	IPSEC/6/IPSEC_SA_TERMINATE: The IPsec SA was deleted. Reason: SA idle timeout. SA information: Role: initiator Local address: 2.2.2.2 Remote address: 1.1.1.1 Sour addr: 192.168.2.0/255.255.255.0 Port: 0 Protocol: IP

	Dest addr: 192.168.1.0/255.255.255.0 Port: 0 Protocol: IP Inside VPN instance: aaa Outside VPN instance: bbb Inbound AH SPI: 192365458 Outbound AH SPI: 13654581 Inbound ESP SPI: 292334583 Outbound ESP SPI: 5923654586 ACL number: 3101
日志说明	IPsec SA被删除
处理建议	无

68 IPSG

本节介绍 IPSG（IP Source Guard）模块输出的日志信息。

68.1 IPSG_ADDENTRY_ERROR

日志内容	Failed to add an IP source guard binding (IPv4 [STRING], MAC [STRING], and VLAN [UINT16]) on interface [STRING]. [STRING]. Failed to delete an IP source guard binding (IPv6 [STRING], MAC [STRING], and VLAN [UINT16]) on interface [STRING]. [STRING].
参数解释	$1：IP地址或IPv6地址（如果没有指定，则显示为空） $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，则显示为无意义值65535） $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 • Resources not sufficient：资源不足 • Resource conflict：资源冲突 • 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 (IPv4 1.1.1.1, MAC DC2D-CB01-0001, and VLAN 1) on interface Vlan-interface1. Resources not sufficient.
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、资源冲突或未知错误
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 • 当提示资源冲突时，请检查接口下的 ACL 或 QoS 策略配置是否与 IP Source Guard 配置有冲突 • 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

68.2 IPSG_DELENTRY_ERROR

日志内容	Failed to delete an IP source guard binding (IPv4 [STRING], MAC [STRING], and VLAN [UINT16]) on interface [STRING]. [STRING]. Failed to delete an IP source guard binding (IPv6 [STRING], MAC [STRING], and VLAN [UINT16]) on interface [STRING]. [STRING].
参数解释	$1：IP地址或IPv6地址（如果没有指定，则显示为空） $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，则显示为无意义值65535） $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 (IPv4 1.1.1.1, MAC DC2D-CB01-0001, 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

69 IRDP

本节介绍 IRDP 模块输出的日志信息。

69.1 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 Ethernet1/1/0/2 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

70 IRF

本节介绍 IRF（Intelligent Resilient Framework，智能弹性架构）模块输出的日志信息。

70.1 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

70.2 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

70.3 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

70.4 IRF_MEMBER_LEFT

日志内容	Member [STRING] left the IRF fabric.
参数解释	$1：表示成员设备的编号
日志等级	4
举例	IRF/4/IRF_MEMBER_LEFT: Member 2 left the IRF fabric.
日志说明	成员设备从IRF中离开时，打印该日志
处理建议	无

70.5 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: dc2d-cbd7-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

70.6 IRF_MEMBERID_CONFLICT_REBOOT

日志内容	IRF member ID conflict. For the device to join the IRF fabric,please change the device member ID to a unique one among all the IRF member devices and reboot the device.
参数解释	无
日志等级	4
举例	IRF/4/IRF_MEMBERID_CONFLICT_REBOOT: IRF member ID conflict.For the device to join the IRF fabric,please change the device member ID to a unique one among all the IRF member devices and reboot the device.
日志说明	建立IRF或者新设备加入现有IRF时，如果有设备的成员编号冲突，则按照IRF角色选举原则，选举获胜的设备会继续正常运行，选举失败的设备的端口会被设置为Block状态，并打印该日志。请修改选举失败的设备的成员编号，该设备重新加入IRF后，会自动解除接口的Block状态
处理建议	**3.** 登录打印该日志信息的设备 **4.** 修改设备的成员编号 **5.** 重启该设备

70.7 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

70.8 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

70.9 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

70.10 IRF_NEWMEMBER_JOIN

日志内容	Member [STRING] joined the IRF fabric.
参数解释	$1：表示设备加入IRF后的成员编号
日志等级	4
举例	IRF/4/IRF_NEWMEMBER_JOIN: Member 2 joined the IRF fabric.
日志说明	IRF有新成员设备加入时，主设备打印该日志
处理建议	无

71 ISIS

本节介绍 IS-IS 模块输出的日志信息。

71.1 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

71.2 ISIS_NBR_CHG

日志内容	IS-IS [UINT32], [STRING] adjacency [STRING] [STRING], state changed to [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：当前邻接状态，包括DOWN、UP和INIT
日志等级	5
举例	ISIS/5/ISIS_NBR_CHG: IS-IS 1, Level-1 adjacency 0000.0000.8888 (Eth1/4/1/3), state changed to DOWN.
日志说明	接口IS-IS邻接状态改变
处理建议	当某接口与邻居邻接状态变为down时，检查IS-IS配置正确性和网络连通性

72 ISSU

本节介绍 ISSU 模块输出的日志信息。

72.1 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

72.2 ISSU_SWITCHOVER

日志内容	Switchover completed on [STRING].
参数解释	形式一： $1：the device、MDC名称或Context名称 形式二： $1：slot编号+CPU编号+MDC名称或Context名称 形式二： $1：chassis编号+slot编号+CPU编号+MDC名称或Context名称 本日志提示的CPU编号为扩展模块的CPU编号，不包括设备缺省的CPU编号 CPU、MDC、Context的支持情况与设备的型号有关，请以设备的实际情况为准
日志等级	5
举例	形式一： ISSU/5/ISSU_SWITCHOVER: Switchover completed on the device. 形式二： ISSU/5/ISSU_SWITCHOVER: Switchover completed on slot 1 CPU 1 in context a. 形式三： ISSU/5/ISSU_SWITCHOVER: Switchover completed on chassis 2 slot 3 in MDC a.
日志说明	在执行Switchover操作过程中，slot执行Switchover完成。如果slot上运行了MDC或者Context，会依次将slot上的MDC或者Context进行倒换，等该slot上的MDC或者Context倒换完成后，该slot才倒换完成
处理建议	无

72.3 ISSU_UPGRADE

日志内容	Upgrade completed on [STRING].
参数解释	形式一： $1：the device、MDC名称或Context名称 形式二： $1：slot编号+CPU编号+MDC名称或Context名称 形式二： $1：chassis编号+slot编号+CPU编号+MDC名称或Context名称 本日志提示的CPU编号为扩展模块的CPU编号，不包括设备缺省的CPU编号 CPU、MDC、Context的支持情况与设备的型号有关，请以设备的实际情况为准
日志等级	5
举例	形式一： ISSU/5/ISSU_UPGRADE: Upgrade completed on the device. 形式二： ISSU/5/ISSU_UPGRADE: Upgrade completed on slot 1 CPU 1 in context a. 形式三： ISSU/5/ISSU_UPGRADE: Upgrade completed on chassis 2 slot 3 in MDC a.
日志说明	在ISSU升级过程中，slot升级完成。如果slot上运行了MDC或者Context，会依次升级这些MDC或者Context，等该slot上的MDC或者Context升级完成后，该slot才升级完成
处理建议	无

73 KDNS

本节介绍 KDNS 模块输出的日志信息。

73.1 KDNS_BIND_PORT_ALLOCETED

日志内容	Failed to bind UDP [STRING] connection port [NUMBER] to VPN instance [STRING] for the DNS listener because the port has already been allocated.
参数解释	$1：UDP端口类型，包括： • IPv4 • IPv6 $2：端口号 $3：VPN实例名称
日志等级	3
举例	KDNS/3/KDNS_BIND_PORT_ALLOCETED: -MDC=1; Failed to bind UDP IPv4 connection port 53 to VPN instance vpn1 for the DNS listener because the port has already been allocated.
日志说明	由于端口已被分配，导致DNS监听器绑定UDP端口失败
处理建议	重新绑定一个UDP端口号

74 KHTTP

本节介绍 KHTTP 模块输出的日志信息。

74.1 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

74.2 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

75 L2PT

本节介绍 L2PT 模块输出的日志信息。

75.1 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 dc2d-cb00-0003.
日志说明	配置BPDU Tunnel报文的目的MAC地址失败
处理建议	无

75.2 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

75.3 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

75.4 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

76 L2TPV2

本节介绍 L2TPV2 模块输出的日志信息。

76.1 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

76.2 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

77 L2VPN

本节介绍 L2VPN 模块输出的日志信息。

77.1 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	5
举例	L2VPN/5/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

77.2 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	5
举例	L2VPN/5/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

77.3 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

77.4 L2VPN_HARD_RESOURCE_RESTORE

日志内容	Hardware resources for L2VPN are restored.
参数解释	无
日志等级	6
举例	L2VPN/6/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

77.5 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

78 L3VPN

本节介绍 L3VPN 模块输出的日志信息。

78.1 L3VPN_VRF_LICENSE_LIMIT

日志内容	The number of VPN instances is [UINT32] and has exceeded the license limit of [UINT32]. The exceeding VPN instances will be deleted.
参数解释	$1：已创建的VPN实例数量 $2：License支持创建的VPN实例最大数量
日志等级	6
举例	L3VPN/6/L3VPN_VRF_LICENSE_LIMIT: The number of VPN instances is 16 and has exceeded the license limit of 5. The exceeding VPN instances will be deleted.
日志说明	License变化导致可创建的VPN实例最大数量小于已创建的VPN实例数量，多余的VPN实例被删除
处理建议	• 根据当前 Licencse 支持的 VPN 实例数量，合理规划 VPN 实例数量 • 购买新的 License，增大支持的 VPN 实例的数量

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 restriction.
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 restriction.
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_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

79.8 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

79.9 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

79.10 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	6
举例	LAGG/6/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

79.11 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

79.12 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	6
举例	LAGG/6/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_CHANGE_DEFAULTLG_STATE_VS

日志内容	The state of link group associated with virtual server [STRING] was changed, primary link group is [STRING], backup link group is [STRING], current link group is [STRING].
参数解释	$1：虚服务器的名称 $2：主用链路组的名称 $3：备用链路组的名称 $4：当前链路组的名称
日志等级	5
举例	LB/5/LB_CHANGE_DEFAULTLG_STATE_VS: -Context=1; The state of link group associated with virtual server VS was changed, primary link group is MF, backup link group is BF, current link group is CF.
日志说明	虚服务器引用的链路组状态变化
处理建议	查看虚服务器引用的链路组的可用条件是否发生配置变化，如果配置没有变化，检测网络环境和链路状态。

80.2 LB_CHANGE_DEFAULTSF_STATE_VS

日志内容	The state of server farm associated with virtual server [STRING] was changed, primary server farm is [STRING], backup server farm is [STRING], current server farm is [STRING].
参数解释	$1：虚服务器的名称 $2：主用实服务组的名称 $3：备用实服务组的名称 $4：当前实服务组的名称
日志等级	5
举例	LB/5/LB_CHANGE_DEFAULTSF_STATE_VS: The state of server farm associated with virtual server VS was changed, primary server farm is MF, backup server farm is BF, current server farm is CF.
日志说明	虚服务器引用的实服务组状态变化
处理建议	查看虚服务器引用的实服务组的可用条件是否发生配置变化，如果配置没有变化，检测网络环境和实服务器状态

80.3 LB_CHANGE_DS_HCSTATUS

日志内容	The health state of DNS server [STRING] was changed to [STRING]. Last state was kept for [ULONG] seconds.
参数解释	$1：DNS服务器的名称 $2：DNS服务器的健康状态，包括： • Active：可用 • Inactive：不可用 $3：链路上一个状态的持续时间，单位为秒
日志等级	5
举例	LB/5/ LB_CHANGE_DS_HCSTATUS: The health state of DNS server DS was changed to Active. Last state was kept for 100 seconds.
日志说明	DNS服务器健康检测状态变化，并输出上一个状态的持续时间
处理建议	当DNS服务器的健康状态为不可用时，检测网络环境和DNS服务器状态

80.4 LB_CHANGE_DS_PROBERESULT

日志内容	The probe result of DNS server [STRING] template [STRING] was changed to [STRING].
参数解释	$1：DNS服务器的名称 $2：健康检测模板名称 $3：该模板对应的健康检测结果，包括： • Successful：成功 • Failed：失败
日志等级	5
举例	LB/5/LB_CHANGE_DS_PROBERESULT: The probe state of real server RS template ICMP was changed to Successful.
日志说明	DNS服务器的健康检测结果发生变化
处理建议	当DNS服务器的健康检测结果为失败时，检测网络环境和DNS服务器状态

80.5 LB_CHANGE_DSQUOTE_HCSTATUS

日志内容	The health state of (DNS server pool [STRING], DNS server pool member [STRING], port: [USHORT]) was changed to [STRING]. Last state was kept for [ULONG] seconds.
参数解释	$1：DNS服务器池名称 $2：DNS服务器名称 $3：端口号 $4：DNS服务器池成员的健康状态，包括： • Active：可用 • Inactive：不可用 $5：链路上一个状态的持续时间，单位为秒
日志等级	5
举例	LB/5/LB_CHANGE_DSQUOTE_HCSTATUS: The health state of (DNS server pool dp, DNS server dDNSs, port:33) was changed to Active. Last state was kept for 100 seconds.
日志说明	DNS服务器池成员的健康检测结果发生变化
处理建议	当DNS服务器池成员健康检测结果为不可用时，检测网络环境和DNS服务器状态

80.6 LB_CHANGE_DSQUOTE_PROBERESULT

日志内容	The probe state of (DNS server pool [STRING], DNS server pool member [STRING], port: [USHORT]) template [STRING] was changed to [STRING].
参数解释	$1：DNS服务器池名称 $2：DNS服务器名称 $3：端口号 $4：健康检测模板名称 $5：该模板对应的健康检测结果，包括： • Successful：成功 • Failed：失败
日志等级	5
举例	LB/5/LB_CHANGE_DSQUOTE_PROBERESULT: The probe state of (DNS server pool SF, DNS server pool member ds, port: 20) template TEMPLATE was changed to Successful.
日志说明	DNS服务器池成员的健康检测结果发生变化
处理建议	当DNS服务器池成员的健康检测结果为失败时，检测网络环境和DNS服务器池成员状态

80.7 LB_CHANGE_LG_STATE_ACTION

日志内容	The state of link group associated with action [STRING] was changed, primary link group is [STRING], backup link group is [STRING], current link group is [STRING].
参数解释	$1：负载均衡动作的名称 $2：主用链路组的名称 $3：备用链路组的名称 $4：当前链路组的名称
日志等级	5
举例	LB/5/LB_CHANGE_LG_STATE_ACTION: The state of link group associated with action ACT was changed, primary link group is MF, backup link group is BF, current link group is CF.
日志说明	负载均衡动作引用的链路组状态变化
处理建议	查看负载均衡动作引用的链路组的可用条件是否发生配置变化，如果配置没有变化，检测网络环境和链路状态

80.8 LB_CHANGE_LG_STATUS

日志内容	The number of available links in link group [STRING] reached the [STRING] percentage ([STRING]).
参数解释	$1：链路组的名称 $2：链路组的可用百分比类型，包括： • upper：最大可用百分比 • lower：最小可用百分比 $3：链路的可用百分比，0%表示未配置链路组的可用条件
日志等级	5
举例	LB/5/LB_CHANGE_LG_STATUS: The number of available links in link group lg1 reached the upper percentage (90%).
日志说明	链路组中可用链路的数量达到最大或最小可用百分比
处理建议	当链路组的可用链路数量低于最小可用百分比时，检测网络环境和链路状态

80.9 LB_CHANGE_LINK_BUSY_STATUS

日志内容	The busy state of link [STRING] was changed to [STRING].
参数解释	$1：链路的名称 $2：链路的繁忙状态，包括： • Busy：繁忙 • Normal：正常
日志等级	5
举例	LB/5/LB_CHANGE_LINK_BUSYSTATUS: The busy state of link LINK was changed to Normal.
日志说明	链路繁忙状态变化
处理建议	无需处理

80.10 LB_CHANGE_LINK_CONNNUM_OVER

日志内容	Chassis:[ChassisID],Slot:[SlotID],CPU:[CPUID].The number of connections of link [STRING] was [UINT], which had reached the upper limit.
参数解释	$1：IRF中的成员编号 $2：单板所在的槽位号 $3：CPU编号 $4：链路的名称 $5：链路的连接数
日志等级	5
举例	LB/5/LB_CHANGE_LINK_CONNNUM_OVER: Chassis:0,Slot:1,CPU:1.The number of connections of link LINK was 100, which had reached the upper limit.
日志说明	链路的连接数达到上限
处理建议	如果链路频繁达到最大连接数限制，确认通过命令**connection-limit max**配置的最大连接数是否合理，确认链路是否需要扩容

80.11 LB_CHANGE_LINK_CONNRATE_OVER

日志内容	Chassis:[ChassisID],Slot:[SlotID],CPU:[CPUID].The connection rate of link [STRING] was [UINT] per second, which had reached the upper limit.
参数解释	$1：IRF中的成员编号 $2：单板所在的槽位号 $3：CPU编号 $4：链路的名称 $5：链路的连接速率
日志等级	5
举例	LB/5/LB_CHANGE_LINK_CONNRATE_OVER: Chassis:0,Slot:1,CPU:1.The connection rate of link LINK was 100 per second, which had reached the upper limit.
日志说明	链路的连接速率达到上限
处理建议	如果链路频繁达到每秒最大连接数，确认通过命令**rate-limit connection**配置的每秒最大连接数否合理，确认链路是否需要扩容

80.12 LB_CHANGE_LINK_HCSTATUS

日志内容	The health state of link [STRING] was changed to [STRING]. Last state was kept for [STRING] seconds.
参数解释	$1：链路的名称 $2：链路的健康状态，包括： • Active：可用 • Inactive：不可用 $3：链路上一个状态的持续时间，单位为秒
日志等级	5
举例	LB/5/LB_CHANGE_LINK_HCSTATUS: The health state of link LINK was changed to Active.Last state was kept for 100 seconds.
日志说明	链路的健康检测状态变化，并输出上一个状态的持续时间
处理建议	当链路的健康状态为不可用时，检测网络环境和链路状态

80.13 LB_CHANGE_LINK_MEMORY_ALERT

日志内容	LB link can't start proximity to probe because memory threshold has been exceeded.
参数解释	-
日志等级	5
举例	LB/5/LB_CHANGE_LINK_MEMORY_ALERT: LB link can't start proximity to probe because memory threshold has been exceeded.
日志说明	设备达到内存门限，无法启动链路的就近性探测
处理建议	设备门限过限时，无法启动链路的就近性探测，需要检查当前设备内存占用情况

80.14 LB_CHANGE_LINK_PROBERESULT

日志内容	The probe state of link [STRING] template [STRING] was changed to [STRING].
参数解释	$1：链路的名称 $2：健康检测模板名称 $3：该模板对应的健康检测结果，包括： • Successful：成功 • Failed：失败
日志等级	5
举例	LB/5/LB_CHANGE_LINK_PROBERESULT: The probe state of link CNC template ICMP was changed to Successful.
日志说明	链路的健康检测结果发生变化
处理建议	当链路的健康检测结果为失败时，检测网络环境和链路状态

80.15 LB_CHANGE_LINK_SHUTDOWN

日志内容	Chassis: [ChassisID],Slot: [SlotID],CPU: [CPUID]. The state of link [STRING] changed to down.
参数解释	$1：IRF中的成员编号 $2：单板所在的槽位号 $3：CPU编号 $4：链路名称
日志等级	5
举例	LB/5/LB_CHANGE_LINK_SHUTDOWN: Chassis: 1,Slot: 2,CPU: 1. The state of link LINK changed to down.
日志说明	链路变为宕机状态
处理建议	当链路变为宕机状态时，检测网络环境和链路状态

80.16 LB_CHANGE_LINKQUOTE_CONNNUM_OVER

日志内容	Chassis:[ChassisID],Slot:[SlotID],CPU:[CPUID]. The number of connections of link group member ([STRING]-[STRING]) was [USHORT], which had reached the upper limit.
参数解释	$1：IRF中的成员编号 $2：单板所在的槽位号 $3：CPU编号 $4：链路组名称 $5：链路名称 $6：链路组成员的连接数
日志等级	5
举例	LB/5/LB_CHANGE_LINKQUOTE_CONNNUM_OVER: Chassis:1,Slot:1,CPU:1]. The number of connections of link group member (LG- LINK) was 80, which had reached the upper limit.
日志说明	链路组成员连接数达到上限
处理建议	当链路组成员连接数达到上限时，检测网络环境和链路组成员状态

80.17 LB_CHANGE_LINKQUOTE_CONNRATE_OVER

日志内容	Chassis:[ChassisID],Slot:[SlotID],CPU:[CPUID]. The connection rate of link group member ([STRING]-[STRING]) was [USHORT] per second, which had reached the upper limit.
参数解释	$1：IRF中的成员编号 $2：单板所在的槽位号 $3：CPU编号 $4：链路组名称 $5：链路名称 $6：链路组成员的连接速率
日志等级	5
举例	LB/5/LB_CHANGE_LINKQUOTE_CONNRATE_OVER: Chassis:1,Slot:1,CPU:2. The connection rate of link group member (LG-LINK) was 80 per second, which had reached the upper limit.
日志说明	链路组成员连接速率达到上限
处理建议	当链路组成员连接速率达到上限时，检测网络环境和链路组成员状态

80.18 LB_CHANGE_LINKQUOTE_HCSTATUS

日志内容	The health state of (link group [STRING], link [STRING])was changed to [STRING]. Last state was kept for [ULONG] seconds.
参数解释	$1：链路组名称 $2：链路名称 $3：链路组成员的健康状态，包括： • Active：可用 • Inactive：不可用 $4：状态保持时间
日志等级	5
举例	LB/5/LB_CHANGE_LINKQUOTE_HCSTATUS: The health state of (link group LG, link LINK) was changed to Active. Last state was kept for 200 seconds.
日志说明	链路组成员的健康状态发生变化
处理建议	当链路组成员的健康状态为不可用时，检测网络环境和链路状态

80.19 LB_CHANGE_LINKQUOTE_PROBERESULT

日志内容	The probe state of (link group [STRING], link [STRING]) template [STRING] was changed to [STRING].
参数解释	$1：链路组名称 $2：链路名称 $3：健康检测模板名称 $4：该模板对应的健康检测结果，包括： • Successful：成功 • Failed：失败
日志等级	5
举例	LB/5/LB_CHANGE_LINKQUOTE_PROBERESULT: The probe state of (link group LG, link LINK) template TEMPLATE was changed to Successful.
日志说明	链路组成员的健康检测结果发生变化
处理建议	当链路组成员的健康检测结果为失败时，检测网络环境和链路组成员状态

80.20 LB_CHANGE_READ_WRITE_STATE_VS

日志内容	The state of server farm associated with virtual server [STRING] was changed, read server farm is [STRING], write server farm is [STRING], current read-write server farm is [STRING].
参数解释	$1：虚服务器的名称 $2：读实服务组名称 $3：写实服务组名称 $4：实服务组的状态，包括： • Active：可用 • Inactive：不可用
日志等级	5
举例	LB/5/ LB_CHANGE_READ_WRITE_STATE_VS: The state of server farm associated with virtual server vs was changed, read server farm is rsr, write server farm is rsw, current read-write server farm is Active.
日志说明	虚服务器引用的读写实服务组状态变化
处理建议	无

80.21 LB_CHANGE_RS_CONNNUM_OVER

日志内容	Chassis:[ChassisID],Slot:[SlotID],CPU:[CPUID].The number of connections of real server [STRING] was [UINT], which had reached the upper limit.
参数解释	$1：IRF中的成员编号 $2：单板所在的槽位号 $3：CPU编号 $4：实服务器的名称 $5：实服务器的连接数
日志等级	5
举例	LB/5/LB_CHANGE_RS_CONNNUM_OVER: Chassis:0,Slot:1,CPU:1.The number of connections of real server RS was 100, which had reached the upper limit.
日志说明	实服务器的连接数达到上限
处理建议	如果实服务器频繁达到最大连接数限制，确认通过命令**connection-limit max**配置的最大连接数是否合理，确认服务器是否需要扩容

80.22 LB_CHANGE_RS_CONNRATE_OVER

日志内容	Chassis:[ChassisID],Slot:[SlotID],CPU:[CPUID].The connection rate of real server [STRING] was [UINT] per second, which had reached the upper limit.
参数解释	$1：IRF中的成员编号 $2：单板所在的槽位号 $3：CPU编号 $4：实服务器的名称 $5：实服务器的连接速率
日志等级	5
举例	LB/5/LB_CHANGE_RS_CONNRATE_OVER: Chassis:0,Slot:1,CPU:1.The connection rate of real server RS was 100 per second, which had reached the upper limit.
日志说明	实服务器的连接速率达到上限
处理建议	如果实服务器频繁达到每秒最大连接数，确认通过命令**rate-limit connection**配置的每秒最大连接数是否合理，确认服务器是否需要扩容

80.23 LB_CHANGE_RS_HCSTATUS

日志内容	The health state of real server [STRING] was changed to [STRING]. Last state was kept for [STRING] seconds.
参数解释	$1：实服务器的名称 $2：实服务器的健康状态，包括： • Active：可用 • Inactive：不可用 $3：实服务器上一个状态的持续时间，单位为秒
日志等级	5
举例	LB/5/LB_CHANGE_RS_HCSTATUS: The health state of real server RS was changed to Active. Last state was kept for 100 seconds.
日志说明	实服务器健康检测状态变化，并输出上一个状态的持续时间
处理建议	当实服务器的健康状态为不可用时，检测网络环境和实服务器状态

80.24 LB_CHANGE_RS_MEMORY_ALERT

日志内容	LB can't start template [STRING] to probe because memory threshold has been exceeded.
参数解释	$1：健康检测模板名称
日志等级	5
举例	LB/5/LB_CHANGE_RS_MEMORY_ALERT: LB can't start template TEMPLATE1 to probe because memory threshold has been exceeded
日志说明	设备达到内存门限，无法启动健康检测
处理建议	设备门限过限时，无法启动健康检测，需要检查当前设备内存占用情况

80.25 LB_CHANGE_RS_MONITORRESULT

日志内容	The state of (server farm [STRING], server farm member [STRING], port: [UINT16]) monitored by probe template [STRING] was changed to [STRING].
参数解释	$1：实服务组的名称 $2：实服务器组成员的名称 $3：端口 $4：探测模板名称 $4：实服务器组成员的探测结果，包括 • Normal：正常 • Busy：繁忙 • Auto shutdown：自动关闭
日志等级	5
举例	LB/5/LB_CHANGE_RS_MONITORRESULT: The state of (server farm sf, server farm member rs, port:1) monitored by probe template rst was changed to Auto shutdown.
日志说明	实服务组成员的探测结果为自动关闭
处理建议	无需处理

80.26 LB_CHANGE_RS_PROBERESULT

日志内容	The probe result of real server [STRING] template type [STRING] name [STRING] was changed to [STRING].
参数解释	$1：实服务器的名称 $2：健康检测模板类型 $3：健康检测模板名称 $3：该模板对应的健康检测结果，包括： • Successful：成功 • Failed：失败
日志等级	5
举例	LB/5/LB_CHANGE_RS_PROBERESULT: The probe state of real server RS template type ICMP name t1 was changed to Successful.
日志说明	实服务器的健康检测结果发生变化
处理建议	当实服务器的健康检测结果为失败时，检测网络环境和实服务器状态

80.27 LB_CHANGE_RS_SHUTDOWN

日志内容	Chassis: [ChassisID],Slot: [SlotID],CPU: [CPUID]. The state of real server [STRING] changed to down.
参数解释	$1：IRF中的成员编号 $2：单板所在的槽位号 $3：CPU编号 $4：实服务器名称
日志等级	5
举例	LB/5/LB_CHANGE_RS_SHUTDOWN: Chassis: 1,Slot: 1,CPU: 2. The state of real server RS changed to down.
日志说明	实服务器变为宕机状态
处理建议	当实服务器变为宕机状态时，检测网络环境和实服务器状态

80.28 LB_CHANGE_RSQUOTE_CONNNUM_OVER

日志内容	Chassis:[ChassisID],Slot:[SlotID],CPU:[CPUID]. The number of connections of server farm member ([STRING]-[STRING]-[USHORT]) was [USHORT], which had reached the upper limit.
参数解释	$1：IRF中的成员编号 $2：单板所在的槽位号 $3：CPU编号 $4：实服务组名称 $5：实服务器名称 $6：端口号 $7：实服务组成员的连接数
日志等级	5
举例	LB/5/LB_CHANGE_RSQUOTE_CONNNUM_OVER: Chassis:1,Slot:1,CPU:2. The number of connections of server farm member (SF-RS-1) was 80, which had reached the upper limit.
日志说明	实服务组成员连接数达到上限
处理建议	当实服务组成员连接数达到上限时，检测网络环境和实服务组成员状态

80.29 LB_CHANGE_RSQUOTE_CONNNUM_RECOVERY

日志内容	Chassis:[ChassisID],Slot:[SlotID],CPU:[CPUID]. The number of connections of server farm member ([STRING]-[STRING]-[USHORT]) was [USHORT], which had returned to a normal level.
参数解释	$1：IRF中的成员编号 $2：单板所在的槽位号 $3：CPU编号 $4：实服务组名称 $5：实服务器名称 $6：端口号 $7：实服务组成员的连接数
日志等级	5
举例	LB/5/LB_CHANGE_RSQUOTE_CONNNUM_RECOVERY: Chassis:2,Slot:1,CPU:1. The number of connections of server farm member (SF-RS-33) was 20, which had returned to a normal level.
日志说明	实服务组成员连接数恢复正常
处理建议	当实服务组成员连接数恢复正常时，检测网络环境和实服务组成员状态

80.30 LB_CHANGE_RSQUOTE_CONNRATE_OVER

日志内容	Chassis:[ChassisID],Slot:[SlotID],CPU:[CPUID].The connection rate of server farm member ([STRING]-[STRING]-[USHORT]) was [USHORT] per second, which had reached the upper limit.
参数解释	$1：IRF中的成员编号 $2：单板所在的槽位号 $3：CPU编号 $4：实服务组名称 $5：实服务器名称 $6：端口号 $7：实服务组成员的连接速率
日志等级	5
举例	LB/5/LB_CHANGE_RSQUOTE_CONNRATE_OVER: Chassis:1,Slot:2,CPU:1.The connection rate of server farm member (SF-RS-66) was 80 per second, which had reached the upper limit.
日志说明	实服务组成员连接速率达到上限
处理建议	当实服务组成员连接速率达到上限时，检测网络环境和实服务组成员状态

80.31 LB_CHANGE_RSQUOTE_HCSTATUS

日志内容	The health state of (server farm [STRING], server farm member [STRING], port:%[USHORT]) was changed to [STRING]. Last state was kept for [ULONG] seconds.
参数解释	$1：实服务组的名称 $2：实服务器名称 $3：端口号 $4：实服务组成员的健康状态，包括： • Active：可用 • Inactive：不可用 $5：状态保持时间
日志等级	5
举例	LB/5/LB_CHANGE_RSQUOTE_HCSTATUS: The health state of (server farm SF, server farm member RS,port:33) was changed to Active. Last state was kept for 100 seconds.
日志说明	实服务组成员的健康状态发生变化
处理建议	当实服务组成员健康状态为不可用时，检测网络环境和实服务器状态

80.32 LB_CHANGE_RSQUOTE_PROBERESULT

日志内容	The probe state of (server farm [STRING], server farm member [STRING], port: [USHORT]) template [STRING] was changed to [STRING].
参数解释	$1：实服务组名称 $2：实服务器名称 $3：端口号 $4：健康检测模板名称 $5：该模板对应的健康检测结果，包括： • Successful：成功 • Failed：失败
日志等级	5
举例	LB/5/ LB_CHANGE_RSQUOTE_PROBERESULT: The probe state of (server farm SF, real server RS, port: 20) template TEMPLATE was changed to Successful.
日志说明	实服务组成员的健康检测结果发生变化
处理建议	当实服务组成员的健康检测结果为失败时，检测网络环境和实服务组成员状态

80.33 LB_CHANGE_SF_STATE_ACTION

日志内容	The state of server farm associated with action [STRING] was changed, primary server farm is [STRING], backup server farm is [STRING], current server farm is [STRING].
参数解释	$1：负载均衡动作的名称 $2：主用实服务组的名称 $3：备用实服务组的名称 $4：当前实服务组的名称
日志等级	5
举例	LB/5/LB_CHANGE_SF_STATE_ACTION: The state of server farm associated with action ACT was changed, primary server farm is MF, backup server farm is BF, current server farm is CF.
日志说明	负载均衡动作引用的实服务组状态变化
处理建议	查看虚服务器引用的实服务组的可用条件是否发生配置变化，如果配置没有变化，检测网络环境和实服务器状态

80.34 LB_CHANGE_SF_STATUS

日志内容	The number of available real servers in server farm [STRING] reached the [STRING] percentage ([STRING]).
参数解释	$1：实服务组的名称 $2：实服务组的可用百分比类型，包括： • upper：最大可用百分比 • lower：最小可用百分比 $3：实服务组的可用百分比，0%表示未配置实服务组的可用条件
日志等级	5
举例	LB/5/LB_CHANGE_SF_STATUS: The number of available real servers in server farm sf1 reached the lower percentage (10%).
日志说明	实服务组中可用实服务器的数量达到最大或最小可用百分比
处理建议	当实服务组的可用实服务器数量低于最小可用百分比时，检测网络环境和实服务器状态

80.35 LB_CHANGE_VS_CONNNUM_OVER

日志内容	Chassis:[ChassisID],Slot:[SlotID],CPU:[CPUID].The number of connections of virtual server [STRING] was [UINT], which had reached the upper limit.
参数解释	$1：IRF中的成员编号 $2：单板所在的槽位号 $3：CPU编号 $4：虚服务器的名称 $5：虚服务器的连接数
日志等级	5
举例	LB/5/LB_CHANGE_VS_CONNNUM_OVER: Chassis:0,Slot:1,CPU:1.The number of connections of virtual server RS was 100, which had reached the upper limit.
日志说明	虚服务器的连接数达到最大
处理建议	如果虚服务器频繁达到最大连接数限制，确认通过命令**connection-limit max**配置的最大连接数是否合理，确认服务器是否需要扩容

80.36 LB_CHANGE_VS_CONNRATE_OVER

日志内容	Chassis:[ChassisID],Slot:[SlotID],CPU:[CPUID].The connection rate of virtual server [STRING] was [UINT] per second, which had reached the upper limit.
参数解释	$1：IRF中的成员编号 $2：单板所在的槽位号 $3：CPU编号 $4：虚服务器的名称 $5：虚服务器的连接速率
日志等级	5
举例	LB/5/LB_CHANGE_VS_CONNRATE_OVER: Chassis:0,Slot:1,CPU:1.The connection rate of virtual server VS was 100 per second, which had reached the upper limit.
日志说明	虚服务器的连接速率达到每秒最大连接数限制
处理建议	如果虚服务器频繁达到每秒最大连接数限制，确认通过命令**rate-limit connection**配置的每秒最大连接数是否合理，确认服务器是否需要扩容

80.37 LB_LINK_FLOW

日志内容	SIP=[STRING], SPort=[STRING], DIP= [STRING], DPort= [STRING], Proto= [STRING], App= [STRING], Link= [STRING] ([STRING]). SIP=[STRING], SPort=[STRING], DIP= [STRING], DPort= [STRING], Proto= [STRING], App= [STRING], Domain= [STRING], Link= [STRING] ([STRING]).
参数解释	$1：源IP地址 $2：源端口 $3：目的IP地址 $4：目的端口 $5：协议 $6：应用名称 $7：域名 $8：链路名称 $9：链路出口方向（外网方向）的下一跳IP地址
日志等级	6
举例	LB/6/LB _LINK_FLOW: SIP=192.168.3.10, SPort=8090, DIP=3.3.3.3, DPort=80, Proto=TCP, App=general_tcp, Link= link1 (6.6.6.6). LB/6/LB _LINK_FLOW: SIP=192.168.3.11, SPort=8080, DIP=2.2.2.2, DPort=80, Proto=TCP, App=http, Domain= www.aaa.com, Link= link2 (6.6.6.2).
日志说明	经过链路转发的流量信息
处理建议	无需处理

80.38 LB_LINK_RECOVERFORM_SHUTDOWN

日志内容	Chassis: [ChassisID],Slot: [SlotID],CPU: [CPUID]. The shutdown state of link [STRING] changed to normal.
参数解释	$1：IRF中的成员编号 $2：单板所在的槽位号 $3：CPU编号 $4：链路名称
日志等级	5
举例	LB/5/ LB_LINK_RECOVERFORM_SHUTDOWN: Chassis: 1,Slot: 2,CPU: 1. The shutdown state of link lk changed to normal.
日志说明	链路由宕机状态恢复正常
处理建议	无

80.39 LB_LINK_STATE_ACTIVE

日志内容	The state of link [STRING] is active.
参数解释	$1：链路的名称
日志等级	5
举例	LB/5/LB_LINK_STATE_ACTIVE: -MDC=1; The state of link lk is active.
日志说明	由于配置IP地址、健康检测成功或通过**undo shutdown**命令开启链路功能使得链路状态可用
处理建议	无

80.40 LB_LINK_STATE_INACTIVE

日志内容	The state of link [STRING] is inactive.
参数解释	$1：链路的名称
日志等级	5
举例	LB_LINK_STATE_INACTIVE: -MDC=1; The state of link lk is inactive.
日志说明	由于删除IP地址、健康检测结果变化或通过配置**shutdown**命令关闭链路功能导致链路状态不可用
处理建议	检查链路配置和健康检测相关配置

80.41 LB_NAT44_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];RcvVPNInstance(1042)=[STRING];SndVPNInstance(1043)=[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：源VPN名称 $11：目的VPN名称
日志等级	6
举例	LB/6/LB_NAT44_FLOW: Protocol(1001)=UDP;SrcIPAddr(1003)=10.10.10.1;SrcPort(1004)=1024;NATSrcIPAddr(1005)=20.20.20.20;NATSrcPort(1006)=1024;DstIPAddr(1007)=20.20.20.1;DstPort(1008)=21;NATDstIPAddr(1009)=20.20.20.1;NATDstPort(1010)=21;RcvVPNInstance(1042)=;SndVPNInstance(1043)=;
日志说明	对源或目的IPv4地址进行NAT转换且转换为IPv4地址时，输出日志信息 仅允许通过执行**display logbuffer**命令进行查看
处理建议	无

80.42 LB_NAT46_FLOW

日志内容	Protocol(1001)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];NATSrcIPv6Addr(1005)=[IPADDR];NATSrcPort(1006)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];NATDstIPv6Addr(1009)=[IPADDR];NATDstPort(1010)=[UINT16];RcvVPNInstance(1042)=[STRING];SndVPNInstance(1043)=[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：源VPN名称 $11：目的VPN名称
日志等级	6
举例	LB/6/LB_NAT46_FLOW: Protocol(1001)=UDP;SrcIPAddr(1003)=20.20.20.1;SrcPort(1004)=1024;NATSrcIPv6Addr(1005)=2002::1;NATSrcPort(1006)=1024;DstIPAddr(1007)=30.30.30.1;DstPort(1008)=21;NATDstIPv6Addr(1009)=3002::1;NATDstPort(1010)=21;RcvVPNInstance(1042)=;SndVPNInstance(1043)=;
日志说明	对源或目的IPv4地址进行NAT转换且转换为IPv6地址时，输出日志信息 仅允许通过执行**display logbuffer**命令进行查看
处理建议	无

80.43 LB_NAT64_FLOW

日志内容	Protocol(1001)=[STRING];SrcIPv6Addr(1003)=[IPADDR];SrcPort(1004)=[UINT16];NATSrcIPAddr(1005)=[IPADDR];NATSrcPort(1006)=[UINT16];DstIPv6Addr(1007)=[IPADDR];DstPort(1008)=[UINT16];NATDstIPAddr(1009)=[IPADDR];NATDstPort(1010)=[UINT16];RcvVPNInstance(1042)=[STRING];SndVPNInstance(1043)=[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：源VPN名称 $11：目的VPN名称
日志等级	6
举例	LB/6/LB_NAT64_FLOW: Protocol(1001)=UDP;SrcIPv6Addr(1003)=1001::1;SrcPort(1004)=1024;NATSrcIPAddr(1005)=20.20.20.1;NATSrcPort(1006)=1024;DstIPv6Addr(1007)=3001::1;DstPort(1008)=21;NATDstIPAddr(1009)=30.30.30.1;NATDstPort(1010)=21;RcvVPNInstance(1042)=;SndVPNInstance(1043)=;
日志说明	对源或目的IPv6地址进行NAT转换且转换为IPv4地址时，输出日志信息 仅允许通过执行**display logbuffer**命令进行查看。
处理建议	无

80.44 LB_NAT66_FLOW

日志内容	Protocol(1001)=[STRING];SrcIPv6Addr(1003)=[IPADDR];SrcPort(1004)=[UINT16];NATSrcIPv6Addr(1005)=[IPADDR];NATSrcPort(1006)=[UINT16];DstIPv6Addr(1007)=[IPADDR];DstPort(1008)=[UINT16];NATDstIPv6Addr(1009)=[IPADDR];NATDstPort(1010)=[UINT16];RcvVPNInstance(1042)=[STRING];SndVPNInstance(1043)=[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：源VPN名称 $11：目的VPN名称
日志等级	6
举例	LB/6/LB_NAT66_FLOW: Protocol(1001)=UDP;SrcIPv6Addr(1003)=1001::1;SrcPort(1004)=1024;NATSrcIPv6Addr(1005)=2002::1;NATSrcPort(1006)=1024;DstIPv6Addr(1007)=3001::1;DstPort(1008)=21;NATDstIPv6Addr(1009)=3002::1;NATDstPort(1010)=21;RcvVPNInstance(1042)=;SndVPNInstance(1043)=;
日志说明	对源或目的IPv6地址进行NAT转换且转换为IPv6地址时，输出日志信息 仅允许通过执行**display logbuffer**命令进行查看。
处理建议	无

80.45 LB_PROTECTION_POLICY_CK(快速日志)

日志内容	The virtual server [STRING] detected the visits of user (IP = [STRING], [STRING] = [STRING], URL = [STRING]) exceeding the threshold.
参数解释	$1：虚服务器的名称 $2：源IP地址 $3：Cookie名称 $4：Cookie值 $5：防护URL
日志等级	6
举例	UNIS LB/6/LB _PROTECTION_POLICY_CK: The virtual server vs detected the visits of user (IP = 10.10.10.10, JSESSIONID = A43E0142B4, URL = www.abc.com) exceeding the threshold.
日志说明	在虚服务器下检测到用户访问URL的次数超过阈值
处理建议	无需处理

80.46 LB_PROTECTION_POLICY_IP(快速日志)

日志内容	The virtual server [STRING] detected the visits of user (IP = [STRING], URL = [STRING]) exceeding the threshold.
参数解释	$1：虚服务器的名称 $2：源IP地址 $3：防护URL
日志等级	6
举例	UNIS LB/6/LB _PROTECTION_POLICY_IP: The virtual server vs detected the visits of user (IP = 10.10.10.10, URL = www.abc.com) exceeding the threshold.
日志说明	在虚服务器下检测到用户访问URL的次数超过阈值
处理建议	无需处理

80.47 LB_RECOVERY_LINK_CONNNUM

日志内容	Chassis:[ChassisID],Slot:[SlotID],CPU:[CPUID].The number of connections of link [STRING] was [UINT], which had returned to a normal level.
参数解释	$1：IRF中的成员编号 $2：单板所在的槽位号 $3：CPU编号 $4：链路的名称 $5：链路的连接数
日志等级	5
举例	LB/5/LB_RECOVERY_LINK_CONNNUM: Chassis:0,Slot:1,CPU:1.The number of connections of link LINK was 100, which had returned to a normal level.
日志说明	链路的连接数恢复正常
处理建议	无需处理

80.48 LB_RECOVERY_LINK_CONNRATE

日志内容	Chassis:[ChassisID],Slot:[SlotID],CPU:[CPUID].The connection rate of link [STRING] was [UINT] per second, which had returned to a normal level.
参数解释	$1：IRF中的成员编号 $2：单板所在的槽位号 $3：CPU编号 $4：链路的名称 $5：链路的连接速率
日志等级	5
举例	LB/5/LB_RECOVERY_LINK_CONNRATE: Chassis:0,Slot:1,CPU:1.The connection rate of link LINK was 100 per second, which had returned to a normal level.
日志说明	链路的连接速率恢复正常
处理建议	无需处理

80.49 LB_RECOVERY_LINKQUOTE_CONNNUM

日志内容	Chassis:[ChassisID],Slot:[SlotID],CPU:[CPUID].The number of connections of link group member ([STRING]-[STRING]) was [USHORT], which had returned to a normal level.
参数解释	$1：IRF中的成员编号 $2：单板所在的槽位号 $3：CPU编号 $4：链路组名称 $5：链路名称 $6：链路组成员的连接数
日志等级	5
举例	LB/5/LB_RECOVERY_LINKQUOTE_CONNNUM: Chassis:1,Slot:1,CPU:2.The number of connections of link group member (LG-LINK) was 10, which had returned to a normal level.
日志说明	链路组成员连接数恢复正常
处理建议	当链路组成员连接数恢复正常时，检测网络环境和链路组成员状态

80.50 LB_RECOVERY_LINKQUOTE_CONNRATE

日志内容	Chassis:[ChassisID],Slot:[SlotID],CPU:[CPUID]. The connection rate of link group member ([STRING]- [STRING]) was [USHORT] per second, which had returned to a normal level.
参数解释	$1：IRF中的成员编号 $2：单板所在的槽位号 $3：CPU编号 $4：链路组名称 $5：链路名称 $6：链路组成员的连接速率
日志等级	5
举例	LB/5/LB_RECOVERY_LINKQUOTE_CONNRATE: Chassis: 0,Slot:1,CPU:1. The connection rate of link group member (LG- LINK) was 80 per second, which had returned to a normal level.
日志说明	链路组成员的连接速率发生变化，恢复成正常状态
处理建议	当链路组成员的连接速率发生变化时，检测网络环境和链路组成员状态

80.51 LB_RECOVERY_RS_CONNNUM

日志内容	Chassis:[ChassisID],Slot:[SlotID],CPU:[CPUID].The number of connections of real server [STRING] was [UINT], which had returned to a normal level.
参数解释	$1：IRF中的成员编号 $2：单板所在的槽位号 $3：CPU编号 $4：实服务器的名称 $5：实服务器的连接数
日志等级	5
举例	LB/5/LB_RECOVERY_RS_CONNNUM: Chassis:0,Slot:1,CPU:1.The number of connections of real server RS was 100, which had returned to a normal level.
日志说明	实服务器的连接数恢复正常
处理建议	无需处理

80.52 LB_RECOVERY_RS_CONNRATE

日志内容	Chassis:[ChassisID],Slot:[SlotID],CPU:[CPUID].The connection rate of real server [STRING] was [UINT] per second, which had returned to a normal level.
参数解释	$1：IRF中的成员编号 $2：单板所在的槽位号 $3：CPU编号 $4：实服务器的名称 $5：实服务器的连接速率
日志等级	5
举例	LB/5/LB_RECOVERY_RS_CONNRATE: Chassis:0,Slot:1,CPU:1.The connection rate of real server RS was 100 per second, which had returned to a normal level.
日志说明	实服务器的连接速率恢复正常
处理建议	无需处理

80.53 LB_RECOVERY_RSQUOTE_CONNRATE

日志内容	Chassis:[ChassisID],Slot:[SlotID],CPU:[CPUID].The connection rate of server farm member ([STRING]-[STRING]-[USHORT]) was [USHORT] per second, which had returned to a normal level.
参数解释	$1：IRF中的成员编号 $2：单板所在的槽位号 $3：CPU编号 $4：实服务组名称 $5：实服务器名称 $6：端口号 $7：实服务组成员的连接速率
日志等级	5
举例	LB/5/LB_RECOVERY_RSQUOTE_CONNRATE: Chassis: 1,Slot:1,CPU:1.The connection rate of server farm member (SF-RS-80) was 10 per second, which had returned to a normal level.
日志说明	实服务组成员的连接速率发生变化，恢复成正常状态
处理建议	当实服务组成员的连接速率发生变化时，检测网络环境和实服务组成员状态

80.54 LB_RECOVERY_VS_CONNNUM

日志内容	Chassis:[ChassisID],Slot:[SlotID],CPU:[CPUID].The number of connections of virtual server [STRING] was [UINT], which had returned to a normal level.
参数解释	$1：IRF中的成员编号 $2：单板所在的槽位号 $3：CPU编号 $4：虚服务器的名称 $5：虚服务器的连接数
日志等级	5
举例	LB/5/LB_RECOVERY_VS_CONNNUM: Chassis:0,Slot:1,CPU:1.The number of connections of virtual server RS was 100, which had returned to a normal level.
日志说明	虚服务器的连接数恢复正常
处理建议	无需处理

80.55 LB_RECOVERY_VS_CONNRATE

日志内容	Chassis:[ChassisID],Slot:[SlotID],CPU:[CPUID].The connection rate of virtual server [STRING] was [UINT] per second, which had returned to a normal level.
参数解释	$1：IRF中的成员编号 $2：单板所在的槽位号 $3：CPU编号 $4：虚服务器的名称 $5：虚服务器的连接速率
日志等级	5
举例	LB/5/LB_RECOVERY_VS_CONNRATE: Chassis:0,Slot:1,CPU:1.The connection rate of virtual server VS was 100 per second, which had returned to a normal level.
日志说明	虚服务器的连接速率恢复正常
处理建议	无需处理

80.56 LB_RS_RECOVERFORM_SHUTDOWN

日志内容	Chassis: [ChassisID],Slot: [SlotID],CPU: [CPUID]. The shutdown state of real server [STRING] changed to normal.
参数解释	$1：IRF中的成员编号 $2：单板所在的槽位号 $3：CPU编号 $4：实服务器名称
日志等级	5
举例	LB/5/LB_RS_RECOVERFORM_SHUTDOWN: Chassis: 1,Slot: 1,CPU: 2. The shutdown state of real server rs1 changed to normal.
日志说明	实服务器由宕机状态恢复正常
处理建议	无

80.57 LB_SLB_LICENSE_EXPIRED

日志内容	The license for SLB has expired. Server load balancing is not available.
参数解释	无
日志等级	5
举例	LB/5/LB_SLB_LICENSE_EXPIRED: The license for SLB has expired. Server load balancing is not available.
日志说明	SLB License已过期，服务器负载均衡功能不可用
处理建议	安装SLB License

80.58 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

80.59 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_MPLSLSRID_CHG

日志内容	Please reset LDP sessions if you want to make the new MPLS LSR ID take effect.
参数解释	无
日志等级	5
举例	LDP/5/LDP_MPLSLSRID_CHG: -MDC=1; Please reset LDP sessions if you want to make the new MPLS LSR ID take effect.
日志说明	公网LDP和VPN实例LDP的LSR ID选择方式为： **1.** 如果配置了 LDP LSR ID，则 LDP 的 LSR ID 为此命令配置的值 **2.** 否则，LDP 的 LSR ID 为 MPLS LSR ID 当公网LDP或VPN实例LDP的LSR ID没配置时，修改MPLS LSR ID，会触发该日志。日志提示用户手动重启公网LDP或VPN实例LDP会话使得新配置的MPLS LSR ID生效
处理建议	当公网LDP或VPN实例LDP的LSR ID没配置时，使用命令display mpls ldp parameter查看已生效的LSR ID，与配置的MPLS LSR ID 比较，如果不一致，请手动重启LDP会话

81.2 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	5
举例	LDP/5/LDP_SESSION_CHG: Session (22.22.22.2:0, public instance) is up. LDP/5/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 manually：手动重启会话 • 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

81.3 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

81.4 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 LIPC

本节包含 LIPC（Leopard Inter-process Communication，Leopard 版本进程间通信）模块的日志消息。

82.1 PORT_CHANGE

日志内容	STCP: Node where the listening port number [INTGER] (MDC: [INTGER] VRF: [INTGER]) resides changed from LIP [INTGER] to LIP [INTGER].
参数解释	$1：LIPC全局端口号 $2：LIPC全局端口号所在的MDC $3：LIPC全局端口号所在的VRF $4：LIPC全局端口号侦听位置变化之前所在的节点 $5：LIPC全局端口号侦听位置变化之后所在的节点
日志等级	5
举例	LIPC/5/PORT_CHANGE: STCP: Node where the listening port number 620 (MDC: 1 VRF: 1) resides changed from LIP 1 to LIP 3.
日志说明	STCP模块根据业务模块的请求，为作为服务端的业务模块分配全局端口号，业务模块侦听该端口号。通常情况下，业务模块只能在申请成功的节点上侦听该端口号，如果业务模块在其他节点上同时侦听该端口号时，输出该日志。STCP会将侦听端口从原节点迁移到新侦听的节点上
处理建议	无

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 Ten-GigabitEthernet10/0/15 (IfIndex 599), neighbor's chassis ID is dc2d-cb66-ba00, port ID is GigabitEthernet6/0/5.
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 Ten-GigabitEthernet10/0/15 (IfIndex 599), neighbor's chassis ID is dc2d-cb66-ba00, port ID is GigabitEthernet6/0/5.
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 Ten-GigabitEthernet10/0/15 (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	5
举例	LLDP/5/LLDP_NEIGHBOR_AGE_OUT: Nearest bridge agent neighbor aged out on port Ten-GigabitEthernet10/0/15 (IfIndex599), neighbor's chassis ID is dc2d-cb66-ba00, port ID is GigabitEthernet6/0/5.
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_NEIGHBOR_AP_RESET

日志内容	The neighboring AP of the [STRING] agent on port [STRING] (IfIndex [UINT32]) was restarted due to aging.
参数解释	$1：代理类型 $2：接口名称 $3：接口索引
日志等级	5
举例	LLDP/5/LLDP_NEIGHBOR_AP_RESET: The neighboring AP of the nearest bridge agent on port GigabitEthernet1/0/1 (IfIndex 599) was restarted due to aging.
日志说明	AP邻居老化超时，重启AP设备，打印本信息
处理建议	无

83.6 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 Ten-GigabitEthernet0/2/6 (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

83.7 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	5
举例	LLDP/5/LLDP_REACH_NEIGHBOR_LIMIT: The number of nearest bridge agent neighbors maintained by the port Ten-GigabitEthernet10/0/15 (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 LOGIN

本节介绍 LOGIN（登录管理）模块输出的日志信息。

85.1 LOGIN_ACCOUNTING_FAILED

日志内容	Accounting failed for user [STRING] on [STRING] line.
参数解释	$1：用户名 $2：用户线类型
日志等级	5
举例	LOGIN/5/LOGIN_ACCOUNTING_FAILED: Accounting failed for user **a1** on VTY line.
日志说明	用户计费失败
处理建议	检查设备上该用户使用的计费配置是否准确

85.2 LOGIN_AUTHORIZATION_FAILED

日志内容	Authorization failed for user [STRING] on [STRING] line.
参数解释	$1：用户名 $2：用户线类型
日志等级	5
举例	LOGIN/5/LOGIN_AUTHORIZATION_FAILED: Authorization failed for user **a1** on VTY line.
日志说明	用户授权失败
处理建议	检查设备上该用户使用的授权配置是否准确

85.3 LOGIN_FAILED

日志内容	[STRING] failed to login 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

85.4 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

85.5 LOGIN_PASSWORD_CHECK_FAILED

日志内容	The password of user [STRING] failed password control check on [STRING] line.
参数解释	$1：用户名 $2：用户线类型
日志等级	5
举例	LOGIN/5/LOGIN_PASSWORD_CHECK_FAILED: The password of user **a1** failed password control check on VTY line.
日志说明	用户密码未通过密码管理功能的检查
处理建议	• 确认密码管理相关的后缀名为“dat”的文件可用 • 确保用户密码符合 Password Control 密码管理功能

85.6 LOGIN_RECORD_OBTAIN_FAILED

日志内容	Failed to obtain login history records of user [STRING] on [STRING] line.
参数解释	$1：用户名 $2：用户线类型
日志等级	5
举例	LOGIN/5/LOGIN_RECORD_OBTAIN_FAILED: Failed to obtain login history records of user a1 on VTY line.
日志说明	获取用户登录历史记录失败
处理建议	请联系技术服务人员

86 LPDT

本节介绍 LPDT 模块输出的日志信息。

86.1 LPDT_LOOPED

日志内容	Loopback exists on [STRING].
参数解释	$1：接口名
日志等级	4
举例	LPDT/4/LPDT_LOOPED: Loopback exists 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

86.2 LPDT_RECOVERED

日志内容	Loopback on [STRING] recovered.
参数解释	$1：接口名
日志等级	5
举例	LPDT/5/LPDT_RECOVERED: Loopback on Ethernet6/4/1 recovered.
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

86.3 LPDT_VLAN_LOOPED

日志内容	Loopback exists 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: Loopback exists 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

86.4 LPDT_VLAN_RECOVERED

日志内容	Loopback on [STRING] in VLAN [UINT16] recovered.
参数解释	$1：接口名 $2：VLAN ID
日志等级	5
举例	LPDT/5/LPDT_RECOVERED: Loopback on Ethernet6/4/1 in VLAN 1 recovered.
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

87 LS

本节包含本地服务器日志信息。

87.1 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 ○ device management user：设备管理用户 ○ user line：用户线 ○ user line class：用户线类 $2：用户名/用户线编号/用户线类型 $3：提醒修改密码原因 ○ the current password is a weak-password：密码是弱密码 ○ the current password is the default password：密码是缺省密码 ○ 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 ○ 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

87.2 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

87.3 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

87.4 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

87.5 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

87.6 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

87.7 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 o 但是可以做其他的尝试 o 被永久阻塞 o 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

87.8 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

87.9 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
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

87.10 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

87.11 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

87.12 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

87.13 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

87.14 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：失败原因 ○ old password is incorrect：旧密码不正确 ○ password is too short：新密码太短 ○ password has not minimum different chars：新密码不符合包含不同字符差异的最小要求（要求最少有 4 个不同字符的差异） ○ invalid password composition：无效的密码组合（密码字符的类型和长度不符合要求） ○ password has repeated chars：密码中包含连续三个或以上的相同字符 ○ password contains username：密码中包含用户名 ○ new password must be different from any previous password by a minimum of four chars：新密码至少要与历史密码保持 4 个字符差异 ○ new password must be different from old password by a minimum of four chars：新密码至少要与旧密码保持 4 个字符差异 ○ password used already：密码已经使用（新/旧密码冲突或新密码与历史密码冲突） ○ password is in update-wait time：密码仍在等待更新的时间内 ○ entered passwords did not match：输入的确认密码与新密码不一致 ○ unknown error：其他未知错误
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

87.15 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

87.16 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

87.17 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

87.18 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

87.19 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

87.20 LS_USER_ROLE_CHANGE

日志内容	Admin [STRING] [STRING] user role [STRING] for [STRING].
参数解释	$1：管理员名 $2：管理员操作 ○ added：添加 ○ deleted：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 added 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 LSPV

本节介绍 LSP 验证模块输出的日志信息。

88.1 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

89 MAC

本节介绍 MAC 模块输出的日志信息。

89.1 MAC_NOTIFICATION

日志内容	形式一： MAC address [STRING] in VLAN [UNIT32] has moved from port [STRING] to port [STRING] for [UNIT32] times. 形式二： MAC address [STRING] in VSI [STRING] has moved from [STRING] service-instance [UNIT32] to [STRING] service-instance [UNIT32] for [UNIT32] times.
参数解释	形式一： $1： MAC地址 $2：VLAN ID $3：接口名称 $4：接口名称 $5：MAC地址的迁移次数 形式二： $1：MAC地址 $2：VSI名称 $3：接口名称 $4：以太网服务实例的ID $5：接口名称 $6：以太网服务实例的ID $7：MAC地址的迁移次数
日志等级	4
举例	形式一： MAC/4/MAC_NOTIFICATION: MAC address DC2D-CB12-0034 in VLAN 500 has moved from port GE1/0/1 to port GE1/0/2 for 1 times 形式二： MAC/4/MAC_NOTIFICATION: MAC address DC2D-CB00-0002 in VSI vpna has moved from Twenty-FiveGigE1/0/1 service-instance 40 to Twenty-FiveGigE1/0/3 service-instance 30 for 152499 times.
日志说明	MAC地址在接口或以太网服务实例之间发生迁移
处理建议	无

89.2 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

89.3 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

89.4 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

90 MACA

本节介绍 MAC 地址认证模块输出的日志信息。

90.1 MACA_ENABLE_NOT_EFFECTIVE

日志内容	The MAC authentication 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	MACA/3/MACA_ENABLE_NOT_EFFECTIVE: The MAC authentication feature 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

90.2 MACA_LOGIN_FAILURE

日志内容	-IfName=[STRING]-MACAddr=[STRING]-VLANId=[STRING]-UserName=[STRING]-UserNameFormat=[STRING]; The user failed the MAC address authentication. Reason: [STRING].
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 ○ Fixed：固定用户名 ○ MAC address：MAC 地址作为用户名 $6：失败原因 ○ Authorization Mac-Address process failed：授权 MAC 地址失败 ○ Authorization VLAN process failed：授权 VLAN 失败 ○ Authorization ACL process failed：授权 ACL 失败 ○ Authorization UserProfile process failed：授权 User Profile 失败 ○ Authentication process failed：认证失败
日志等级	6
举例	MACA/6/MACA_LOGIN_FAILURE: -IfName=GigabitEthernet1/0/1-MACAddr=DC2D-CB00-0001-VLANId=1-UserName=DC2D-CB00-0001-UserNameFormat=MAC address; The user failed the MAC address authentication. Reason: VLAN authorization failed.
日志说明	接口上的用户MAC地址认证失败
处理建议	根据失败原因修改相关配置

90.3 MACA_LOGIN_SUCC

日志内容	-IfName=[STRING]-MACAddr=[STRING]-AccessVLANId=[STRING]-AuthorizationVLANID=[STRING]-UserName=[STRING]-UserNameFormat=[STRING]; The user passed MAC address authentication and got online successfully.
参数解释	$1：接口名 $2：MAC地址 $3：接入VLAN ID $4：授权VLAN ID $5：用户名 ○ Fixed：固定用户名 ○ MAC address：MAC 地址作为用户名 $6：用户名格式
日志等级	6
举例	MACA/6/MACA_LOGIN_SUCC:-IfName=GigabitEthernet1/0/4-MACAddr=dc2d-cb00-22b9-AccessVLANId=444-AuthorizationVLANID=444-UserName=00-10-84-00-22-b9-UserNameFormat=MAC address; The user passed MAC address authentication and got online successfully.
日志说明	接口上的用户MAC地址认证成功
处理建议	无

90.4 MACA_LOGOFF

日志内容	-IfName=[STRING]-MACAddr=[STRING]-VLANId=[STRING]-UserName=[STRING]-UserNameFormat=[STRING]; Session of the MAC-AUTH user was terminated.
参数解释	$1：接口名 $2：MAC地址 $3：VLAN ID $4：用户名 ○ Fixed：固定用户名 ○ MAC address：MAC 地址作为用户名 $5：用户名格式
日志等级	6
举例	MACA/6/MACA_LOGOFF:-IfName=GigabitEthernet1/0/4-MACAddr=dc2d-cb00-22b9-VLANId=444-UserName=dc-2d-cb-00-22-b9-UserNameFormat=MAC address; Session of the MAC-AUTH user was terminated.
日志说明	MAC地址认证用户下线
处理建议	无

91 MACSEC

本节介绍 MAC Security 模块输出的日志信息。

91.1 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

91.2 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

91.3 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

91.4 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

91.5 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

91.6 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

91.7 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

91.8 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

92 MBFD

本节介绍 MPLS BFD 模块输出的日志信息。

92.1 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	5
举例	MBFD/5/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/5/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

93 MBUF

本节介绍 MBUF 模块输出的日志信息。

93.1 DBL_FREE

日志内容	MBUF address: [HEX] repeated release! Seq: [UINT32], CPU ID: [UINT32], [STRING]: [STRING] Seq: [UINT32], CPU ID: [UINT32], [STRING]: [STRING] Seq: [UINT32], CPU ID: [UINT32], [STRING]: [STRING] Seq: [UINT32], CPU ID: [UINT32], [STRING]: [STRING] Seq: [UINT32], CPU ID: [UINT32], [STRING]: [STRING]
参数解释	$1：MBUF的地址 $2：栈序列号 $3：栈所在CPU的编号 $4：取值为Alloc trace时，表示申请栈；取值为Free trace时，表示释放栈 $5：栈信息 $6：栈序列号 $7：栈所在CPU的编号 $8：取值为Alloc trace时，表示申请栈；取值为Free trace时，表示释放栈 $9：栈信息 $10：栈序列号 $11：栈所在CPU的编号 $12：取值为Alloc trace时，表示申请栈；取值为Free trace时，表示释放栈 $13：栈信息 $14：栈序列号 $15：栈所在CPU的编号 $16：取值为Alloc trace时，表示申请栈；取值为Free trace时，表示释放栈 $17：栈信息 $18：栈序列号 $19：栈所在CPU的编号 $20：取值为Alloc trace时，表示申请栈；取值为Free trace时，表示释放栈 $21：栈信息
日志等级	2
举例	MBUF/2/DBL_FREE: MBUF address: 0x854f9380 repeated release! Seq: 411, CPU ID: 1, Alloc trace: bdae759c bd2becbc bd2ba850 bd2bb718 bd368d04 bd3695e4 bd369bf8 bd358dc8 bd3295b0 bd29e0f4 Seq: 412, CPU ID: 1, Free trace: bdae759c bd2becbc bd2bc020 bd369298 bd3695e4 bd369bf8 bd358dc8 bd3295b0 bd29e0f4 bd2a1e8c Seq: 413, CPU ID: 1, Free trace: bdae759c bd2becbc bd2bc020 bd3692ac bd3695e4 bd369bf8 bd358dc8 bd3295b0 bd29e0f4 bd2a1e8c Seq: 409, CPU ID: 1, Alloc trace: bdae759c bd2becbc bd2ba850 bd2bc26c bd2d3320 bd105fc4 bd007b44 bd006c88 bd102264 400646b8 Seq: 410, CPU ID: 1, Free trace: bdae759c bd2becbc bd2baefc bd2d3344 bd105fc4 bd007b44 bd006c88 bd102264 400646b8 400651b8
日志说明	MBUF被重复释放时输出该日志，本日志会记录最近使用该MBUF的5个栈信息

处理建议	根据日志中的栈信息找到重复释放MBUF的业务流程

93.2 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 o 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 o 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

93.3 STEPMEM

日志内容	MBUF address [HEX] MBUF block address [HEX] STEP ON MEMORY! Stack :[STRING]
参数解释	$1：MBUF地址 $2：MBUF数据块的地址 $3：栈信息
日志等级	2
举例	MBUF/2/STEPMEM: MBUF address 780bd380 MBUF block address 780bd388 STEP ON MEMORY! Stack :bdae759c bd2be938 bd2b7ce4 bd2bbf8c bac531ec bcfe4270 bd141b94 bdaecd50 bd2a0ca4 bd2a157c bd2a1c54 bd369048 bd3695e4 bd369bf8 bd358dc8 bd3295b0
日志说明	MBUF被写越界了
处理建议	根据日志中的栈信息找到内存写越界的流程。当MBUF被某个业务流程使用后放入MBUF队列中又被其他业务流程使用，或者其他特殊情况下，该日志中记录的栈可能不是真正导致内存写越界的栈，需要根据业务流程进一步定位

94 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。

94.1 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

94.2 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

94.3 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

94.4 MDC_KERNEL_EVENT_TOOLONG

日志内容	[STRING] [UINT16] kernel event in sequence [STRING] function [STRING] failed to finish within [UINT32] minutes.
参数解释	$1：MDC的编号 $2：内核事件的阶段 $3：内核事件阶段对应的函数的地址 $4：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

94.5 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

94.6 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

94.7 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

94.8 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

94.9 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

94.10 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

95 MFIB

本节介绍组播转发模块输出的日志信息。

95.1 MFIB_MEM_ALERT

日志内容	MFIB process received system memory alert [STRING] event.
参数解释	$1：内存告警事件类型
日志等级	5
举例	MFIB/5/MFIB_MEM_ALERT: MFIB process receive system memory alert start event.
日志说明	MFIB模块收到了系统发出的内存告警事件
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

96 MGROUP

本节主要介绍与镜像组相关的日志消息。

96.1 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

96.2 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

96.3 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

96.4 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

97 MPLS

本节介绍 MPLS 模块输出的日志信息。

97.1 MPLS_HARD_RESOURCE_NOENOUGH

日志内容	No enough hardware resource for MPLS.
参数解释	无
日志等级	4
举例	MPLS/4/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

97.2 MPLS_HARD_RESOURCE_RESTORE

日志内容	Hardware resources for MPLS are restored.
参数解释	无
日志等级	6
举例	MPLS/6/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

98 MTLK

本节介绍 Monitor Link 模块输出的日志信息。

98.1 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

99 NAT

本节介绍 NAT 模块输出的日志信息。

99.1 NAT_ADDR_BIND_CONFLICT

日志内容	Invalid configuration on interface [STRING]: [STRING]. Reason: Global IP addresses already bound to another service card.
参数解释	$1：接口名称 $2：NAT地址组名称
日志等级	4
举例	NAT/4/NAT_ADDR_BIND_CONFLICT: Invalid configuration on interface Ethernet0/0/2: nat outbound address-group 1. Reason: 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

99.2 NAT_ADDRGRP_MEMBER_CONFLICT

日志内容	The address range in address group [UINT16] overlaps with the address range in address group [UINT16].
参数解释	$1：地址组号 $2：地址组号
日志等级	4
举例	NAT/4/NAT_ADDRGRP_MEMBER_CONFLICT: The address range in address group 1 overlaps with the address range in address group 2.
日志说明	不同地址组之间的地址成员重叠时，发送该日志
处理建议	检查发生地址成员重叠的地址组的配置，修改地址成员的IP地址

99.3 NAT_ADDRGRP_RESOURCE_EXHAUST

日志内容	The address resources of [STRING] address group [INTEGER] are not enough.
参数解释	$1：地址转换模式，包括： • NO-PAT • EIM $2：地址组号
日志等级	4
举例	NAT/4/NAT_ADDRGRP_RESOURCE_EXHAUST: The address resources of NO-PAT address group 1 are not enough.
日志说明	NO-PAT/EIM模式地址资源耗尽
处理建议	请增加地址资源

99.4 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

99.5 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

99.6 NAT_FLOW

日志内容	Protocol(1001)=[STRING];Application(1002)=[STRING];Category(1174)=[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];UserName(1113)=[STRING];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：应用协议名称 $3：应用所属服务类型 $4：源IP地址 $5：源端口号 $6：转换后的源IP地址 $7：转换后的源端口号 $8：目的IP地址 $9：目的端口号 $10：转换后的目的IP地址 $11：转换后的目的端口号 $12：身份识别用户的名称 $13：入方向的报文总数 $14：入方向的字节总数 $15：出方向的报文总数 $16：出方向的字节总数 $17：源VPN名称 $18：目的VPN名称 $19：源DS-Lite Tunnel $20：目的DS-Lite Tunnel $21：创建会话的时间 $22：会话删除时间 $23：日志类型 $24：日志类型描述信息，包括： • Session created：NAT 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	NAT/6/NAT_FLOW: Protocol(1001)=TCP;Application(1002)=http;Category(1174)=Protocol;SrcIPAddr(1003)=46.2.1.77;SrcPort(1004)=63419;NatSrcIPAddr(1005)=146.2.1.190;NatSrcPort(1006)=50805;DstIPAddr(1007)=64.2.1.26;DstPort(1008)=80;NatDstIPAddr(1009)=64.2.1.26;Nat

	DstPort(1010)=80;InitPktCount(1044)=1;InitByteCount(1046)=56;RplyPktCount(1045)=0;RplyByteCount(1047)=0;RcvVPNInstance(1042)=;SndVPNInstance(1043)=;RcvDSLiteTunnelPeer(1040)=;SndDSLiteTunnelPeer(1041)=;BeginTime_e(1013)=09072021103948;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

99.7 NAT_INTERFACE_RESOURCE_EXHAUST

日志内容	The address resources of Easy-IP-EIM interface [STRING] are not enough.
参数解释	$1：接口名称
日志等级	4
举例	NAT/4/NAT_INTERFACE_RESOURCE_EXHAUST: The address resources of EASY-IP-EIM interface Route-Aggregation1 are not enough.
日志说明	Easy-IP-EIM模式接口上的地址资源耗尽
处理建议	请增加地址资源

99.8 NAT_NOPAT_IP_USAGE_ALARM

日志内容	Address group [UINT16], total IP addresses [UINT16], used IP addresses [UINT16], usage rate over [UINT16]%.
参数解释	$1：地址组号 $2：地址组中IP地址总数 $3：地址组中已使用的IP地址数 $4：地址组中IP地址使用率
日志等级	6
举例	NAT/6/NAT_NOPAT_IP_USAGE_ALARM: -Context=1; Address group 1, total IP addresses 10, used IP addresses 9, usage rate over 90%.
日志说明	NAT NO-PAT方式，当地址组中的IP地址的使用率大于设置的阈值时，发送该日志
处理建议	无

99.9 NAT_PORTBLOCKGRP_ADDRESS_WARNING

日志内容	Insufficient memory due to large [STRING] address range in port block group [UINT16]. Please reconfigure the [STRING] address range.
参数解释	$1：地址类型，包括： • local：私网地址 • global：公网地址 $2：静态端口块组号 $3：地址类型，包括： • local：私网地址 • global：公网地址
日志等级	4
举例	NAT/4/NAT_PORTBLOCKGRP_ADDRESS_WARNING: Insufficient memory due to large local address range in port block group 0. Please reconfigure the local address range.
日志说明	静态端口块组中，配置的私网或者公网地址范围太大，导致申请内存失败，则触发该日志
处理建议	修改静态端口块组中私网或者公网地址范围

99.10 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

99.11 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

99.12 NAT444_PORTBLOCK_USAGE_ALARM

日志内容	Address group [UINT16], total port blocks [UINT16], active port blocks [UINT16], usage rate over [UINT16]%.
参数解释	$1：地址组号 $2：地址组中总端口块数 $3：地址组中已分配端口块数 $4：端口块利用率
日志等级	6
举例	NAT/6/NAT444_PORTBLOCK_USAGE_ALARM: -Context=1; Address group 1003, total port blocks 10, active port blocks 9, usage rate over 90%.
日志说明	NAT444动态分配端口块，端口块使用率大于设置的阈值时，发送该日志
处理建议	请增加端口块资源

100 ND

本节介绍 ND 模块输出的日志信息。

100.1 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

100.2 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

100.3 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

100.4 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 DC2D-CB02-0001 was inconsistent with link-layer address DC2D-CB02-0002.
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

100.5 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	6
举例	ND/6/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

100.6 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_SET_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

100.7 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	6
举例	ND/6/ND_MAXNUM_IF: 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

100.8 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	ND/6/ND_MAXNUM_DEV: 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

101 NETCONF 日志

本节介绍 NETCONF 模块输出的日志信息。

101.1 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

101.2 EDIT-CONFIG

日志内容	User ([STRING], [STRING], session ID [UINT16]) performed an edit-config operation: message ID=[STRING], operation result=Succeeded. 或者 User ([STRING], [STRING], session ID [UINT16]) performed an edit-config operation: message ID=[STRING], operation result=Failed. [STRING] 或者 User ([STRING], [STRING], session ID [UINT16]) performed an edit-config operation: message ID=[STRING], operation result=Failed, XPath=[STRING], error message=[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 $4：NETCONF请求中的message-id $5：错误信息或错误行的XPath表达式 • 不配置 verbose 选项且已知错误原因时显示该内容，用来说明具体的错误信息 • 配置 verbose 选项时，该内容为错误行的 XPath 表达式 $6：错误信息。仅配置verbose选项时显示该内容
日志等级	6
举例	XMLSOAP/6/EDIT-CONFIG: -MDC=1; User (test, 192.168.100.20, session ID 1) performed an edit-config operation: message ID=101, operation result=Succeeded.
日志说明	客户端通过edit-config操作下发配置 一次下发操作中可以包含多个NETCONF配置，因此设备可能同时打印多条日志信息
处理建议	无

101.3 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请求报文由于其大小超过设备支持的上限而被丢弃
处理建议	**1.** 减小发往设备的单个 NETCONF 请求报文的大小，例如删除报文中的空格、换行、制表符等占位字符 **2.** 如果报文仍然过大，可以拆分 NETCONF 请求并分别封装后再发送给设备，建议联系技术支持

101.4 ROW-OPERATION

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: User (test, 192.168.100.20, session ID 1), message ID=1, operation=create Ifmgr/Interfaces (IfIndex="GigabitEthernet1/0/1"), result=Succeeded. Attributes: Description="This is Desc1", AdminDown=1, Speed=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

101.5 REPLY

日志内容	Sent a NETCONF reply to the client: Session ID=[UINT16], Content=[STRING]. 或者 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=2, 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

101.6 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

102 NETSHARE

本节介绍共享上网管理模块输出的日志信息。

102.1 NETSHARE_IPV4_LOG

日志内容	SrcIPAddr(1003)=[IPADDR];UserName(1113)=[STRING];RcvVPNInstance(1042)=[STRING];TerminalNum(1125)=[UINT16];PolicyName(1079)=[STRING];Action(1053)=[STRING];FreezeTime(1126)=[UINT16].
参数解释	$1：源IP地址 $2：用户名 $3：源VPN实例名称 $4：终端个数 $5：共享上网管理策略名称 $6：动作名称，包括如下取值： • Freeze：冻结 $7：冻结时间，单位为分钟
日志等级	6
举例	NETSHARE/6/NETSHARE_IPV4_LOG:SrcIPAddr(1003)=65.1.1.100;UserName(1113)=test;RcvVPNInstance(1042)=vpn1;TerminalNum(1125)=5;PolicyName(1079)=test;Action(1053)=Freeze;FreezeTime(1126)=120min.
日志说明	共享IPv4地址的终端个数超过共享上网管理策略配置的最大数目（策略动作为冻结）或手工冻结IPv4地址时输出该日志
处理建议	无

102.2 NETSHARE_IPV4_LOG

日志内容	SrcIPAddr(1003)=[IPADDR];UserName(1113)=[STRING];RcvVPNInstance(1042)=[STRING];TerminalNum(1125)=[UINT16];PolicyName(1079)=[STRING];Action(1053)=[STRING].
参数解释	$1：源IP地址 $2：用户名 $3：源VPN实例名称 $4：终端个数 $5：共享上网管理策略名称 $6：动作名称，包括如下取值： • Permit：允许 • Unfreeze：解冻
日志等级	6
举例	NETSHARE/6/NETSHARE_IPV4_LOG:SrcIPAddr(1003)=65.1.1.100;UserName(1113)=test;RcvVPNInstance(1042)=vpn1;TerminalNum(1125)=5;PolicyName(1079)=test;Action(1053)=Permit.
日志说明	共享IPv4地址的终端个数超过共享上网管理策略配置的最大数目（策略动作为允许）或手工解冻IPv4地址时输出该日志
处理建议	无

102.3 NETSHARE_IPV6_LOG

日志内容	SrcIPv6Addr(1036)=[IPADDR];UserName(1113)=[STRING];RcvVPNInstance(1042)=[STRING];TerminalNum(1125)=[UINT16];PolicyName(1079)=[STRING];Action(1053)=[STRING];FreezeTime(1126)=[UINT16].
参数解释	$1：源IP地址 $2：用户名 $3：源VPN实例名称 $4：终端个数 $5：共享上网管理策略名称 $6：动作名称，包括如下取值： • Freeze：冻结 $7：冻结时间，单位为分钟
日志等级	6
举例	NETSHARE/6/NETSHARE_IPV6_LOG:SrcIPv6Addr(1036)=3001::2;UserName(1113)=test;RcvVPNInstance(1042)=vpn1;TerminalNum(1125)=5;PolicyName(1079)=test;Action(1053)=Freeze;FreezeTime(1126)=120min.
日志说明	共享IPv6地址的终端个数超过共享上网管理策略配置的最大数目（策略动作为冻结）或手工冻结IPv6地址时输出该日志
处理建议	无

102.4 NETSHARE_IPV6_LOG

日志内容	SrcIPv6Addr(1036)=[IPADDR];UserName(1113)=[STRING];RcvVPNInstance(1042)=[STRING];TerminalNum(1125)=[UINT16];PolicyName(1079)=[STRING];Action(1053)=[STRING].
参数解释	$1：源IP地址 $2：用户名 $3：源VPN实例名称 $4：终端个数 $5：共享上网管理策略名称 $6：动作名称，包括如下取值： • Permit：允许 • Unfreeze：解冻
日志等级	6
举例	NETSHARE/6/NETSHARE_IPV6_LOG:SrcIPv6Addr(1036)=3001::2;UserName(1113)=test;RcvVPNInstance(1042)=vpn1;TerminalNum(1125)=5;PolicyName(1079)=test;Action(1053)=Permit.
日志说明	共享IPv6地址的终端个数超过共享上网管理策略配置的最大数目（策略动作为冻结）或手工解冻IPv6地址时输出该日志
处理建议	无

102.5 NETSHARE_IPV4_BLS_LOG

日志内容	SrcIPAddr(1003)=[IPADDR];UserName(1113)=[STRING];RcvVPNInstance(1042)=[STRING];PolicyName(1079)=[STRING].
参数解释	$1：源IP地址 $2：用户名 $3：源VPN实例名称 $4：共享上网管理策略名称
日志等级	6
举例	NETSHARE/6/NETSHARE_IPV4_BLS_LOG:SrcIPAddr(1003)=65.1.1.100;UserName(1113)=test;RcvVPNInstance(1042)=vpn1;PolicyName(1079)=test.
日志说明	IPv4地址已被冻结，设备检测到来自该IP地址的报文时输出日志
处理建议	无

102.6 NETSHARE_IPV6_BLS_LOG

日志内容	SrcIPv6Addr(1036)=[IPADDR];UserName(1113)=[STRING];RcvVPNInstance(1042)=[STRING];PolicyName(1079)=[STRING].
参数解释	$1：源IP地址 $2：用户名 $3：源VPN实例名称 $4：共享上网管理策略名称
日志等级	6
举例	NETSHARE/6/NETSHARE_IPV6_BLS_LOG:SrcIPv6Addr(1036)=3001::2;UserName(1113)=test;RcvVPNInstance(1042)=vpn1;PolicyName(1079)=test.
日志说明	IPv6地址已被冻结，设备检测到来自该IP地址的报文时输出日志
处理建议	无

103 NQA

本节介绍 NQA 模块输出的日志信息。

103.1 NQA_ENTRY_PROBE_RESULT

日志内容	Reaction entry [STRING] of NQA entry admin-name [STRING] operation-tag [STRING]: [STRING].
参数解释	$1：阈值告警组编号，取值范围为1～10 $2：NQA测试组的管理员名称 $3：测试操作的标签 $4：测试结果，取值为： • Probe-pass：表示测试成功 • Probe-fail：表示测试失败
日志等级	6
举例	NQA/6/NQA_ENTRY_PROBE_RESULT: Reaction entry 1 of NQA entry admin-name 1 operation-tag 1: Probe-pass.
日志说明	NQA客户端的阈值告警监测对象的数值未超出阈值，与上次探测相比发生了变化
处理建议	检测结果是失败的情况下，用户需要检查网络环境

103.2 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

103.3 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	6
举例	NQA/6/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

103.4 NQA_SET_DRIVE_FAIL

日志内容	NQA entry admin-name [STRING] operation-tag [STRING]: [STRING].
参数解释	$1：NQA测试组的管理员名称 $2：测试操作的标签 $3：NQA测试下发驱动执行时失败，失败的原因包括： • Operation failed due to configuration conflicts：配置冲突导致下发驱动失败 • Operation failed because the driver was not ready to perform the operation：驱动未准备完全导致下发驱动失败 • Operation not supported：驱动不支持该操作 • Not enough resources to complete the operation：资源不足导致下发驱动失败 • Operation failed due to an unkonwn error：一般情况导致下发驱动操作失败
日志等级	6
举例	NQA/6/NQA_SET_DRIVE_FAIL: NQA entry admin-name 1 operation-tag 1: Not enough resources to complete the operation.
日志说明	NQA测试下发驱动执行时，返回失败
处理建议	根据提示信息做相应的检查

103.5 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	6
举例	NQA/6/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

103.6 NQA_START_FAILURE

日志内容	NQA entry ([STRING]-[STRING]): [STRING]
参数解释	$1：NQA测试组的管理员名称 $2：测试操作的标签 $3：NQA测试下发驱动执行时失败，失败的原因包括： • Operation failed due to configuration conflicts：配置冲突导致下发驱动失败 • Operation failed because the driver was not ready to perform the operation：驱动未准备就绪导致下发驱动失败 • Operation not supported：驱动不支持该操作 • Not enough resources to complete the operation：资源不足导致下发驱动失败 • Operation failed due to an unknown error：其他情况导致下发驱动操作失败
日志等级	6
举例	NQA/6/NQA_START_FAILURE: NQA entry 1-1: Operation failed due to configuration conflicts.
日志说明	NQA测试下发驱动执行时，失败
处理建议	• 检查配置参数进行修改并重新启动测试 • 联系技术支持

103.7 NQA_TWAMP_LIGHT_PACKET_INVALID

日志内容	NQA TWAMP Light test session [UINT32] index [UINT32]: The number of packets captured for statistics collection is invalid.
参数解释	$1：测试会话ID $2：统计数据的序列号
日志等级	6
举例	NQA/6/ NQA_TWAMP_LIGHT_PACKET_INVALID: NQA TWAMP Light test session 1 index 7: The number of packets captured for statistics collection is invalid.
日志说明	统计的探测帧数量异常，本次探测统计结果不计入统计计数
处理建议	检查NQA TWAMP-light测试配置，可能原因为：配置的统计周期小于发送报文的周期

103.8 NQA_TWAMP_LIGHT_REACTION

日志内容	NQA TWAMP Light test session [UINT32] reaction entry [UINT32]: Detected continual violation of the [STRING] [STRING] threshold for a threshold violation monitor time of [UINT32] ms.
参数解释	$1：测试会话的ID $2：阈值告警组编号 $3：阈值告警类型，取值包括： o two-way delay：双向时延阈值告警 o two-way loss：双向丢包率阈值告警 o two-way jitter：双向抖动阈值告警 $4：阈值动作，取值包括： o upper：大于等于阈值告警的上限阈值 o lower：小于等于阈值告警的下限阈值 $5：日志告警周期
日志等级	6
举例	NQA/6/NQA_TWAMP_LIGHT_REACTION: NQA TWAMP Light test session 1 reaction entry 1: Detected continual violation of the two-way loss upper threshold for a threshold violation monitor time of 2000 ms.
日志说明	监测NQA TWAMP-light测试的探测结果，从测试统计的第一个结果大于等于阈值告警的上限阈值或者从大于阈值告警的下限阈值恢复到小于等于该下限阈值开始计时，若在监控时间内测试结果持续不变，打印该日志。
处理建议	无

103.9 NQA_TWAMP_LIGHT_START_FAILURE

日志内容	NQA TWAMP Light test session [UINT32]: Failed to start the test session. Please check the parameters.
参数解释	$1：测试会话的ID
日志等级	6
举例	NQAS/6/NQA_TWAMP_LIGHT_START_FAILURE: NQA TWAMP Light test session 1: Failed to start the test session, Please check the parameters.
日志说明	启动TWAMP-light Responder端的测试会话失败，提示用户检查配置参数
处理建议	配置TWAMP-light Responder端测试会话的反射参数时，test-session命令TWAMP-light Responder端缺少参数必配项，根据当前网络环境判断参数的必配项，并检查参数配置并重新将参数配置完整

104 NTP

本节介绍 NTP 模块输出的日志信息。

104.1 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 12/28/2012 to 02:29:12 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

104.2 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

104.3 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

104.4 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	5
举例	NTP/5/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	1. 检查 NTP 服务器及网络连接 2. 若 NTP 服务器故障，请在客户端配置新的服务器作为时钟源

104.5 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

105 OBJP

本节介绍 OBJP（对象策略）模块输出的日志信息。

105.1 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

105.2 OBJP_ACCELERATE_NOT_SUPPORT

日志内容	Failed to accelerate [STRING] object-policy [STRING]. The operation 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

105.3 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

105.4 OBJP_RULE_CREATE_SUCCESS

日志内容	RuleName(1080)=[STRING];Type(1067)=[STRING];Action(1053)=[STRING];
参数解释	$1：规则名称 $2：规则类型 $3：对当前规则采取的动作
日志等级	6
举例	OBJP/6/OBJP_RULE_CREATE_SUCCESS: RuleName(1080)=zone1-zone2;Type(1067)=IPv4;Action(1053)=Permit;
日志说明	创建对象策略规则成功
处理建议	无

105.5 OBJP_RULE_CREATE_FAIL

日志内容	RuleName(1080)=[STRING];Type(1067)=[STRING];Action(1053)=[STRING];
参数解释	$1：规则名称 $2：规则类型 $3：对当前规则采取的动作
日志等级	6
举例	OBJP/6/OBJP_RULE_CREATE_FAIL: RuleName(1080)=zone1-zone2;Type(1067)=IPv4;Action(1053)=Permit;
日志说明	创建对象策略规则失败
处理建议	无

105.6 OBJP_RULE_UPDATE_SUCCESS

日志内容	RuleName(1080)=[STRING];RuleID(1078)=[UINT32];Type(1067)=[STRING];Action(1053)=[STRING];
参数解释	$1：规则名称 $2：规则编号 $3：规则类型 $4：对当前规则采取的动作
日志等级	6
举例	OBJP/6/OBJP_RULE_UPDATE_SUCCESS: RuleName(1080)=zone1-zone2;RuleID(1078)=1;Type(1067)=IPv4;Action(1053)=Permit;
日志说明	修改对象策略规则成功
处理建议	无

105.7 OBJP_RULE_UPDATE_FAIL

日志内容	RuleName(1080)=[STRING];RuleID(1078)=[UINT32];Type(1067)=[STRING];Action(1053)=[STRING];
参数解释	$1：规则名称 $2：规则编号 $3：规则类型 $4：对当前规则采取的动作
日志等级	6
举例	OBJP/6/OBJP_RULE_UPDATE_FAIL: RuleName(1080)=zone1-zone2;RuleID[1078]=1;Type(1067)=IPv4;Action(1053)=Permit;
日志说明	修改对象策略规则失败
处理建议	无

105.8 OBJP_RULE_DELETE_SUCCESS

日志内容	RuleName(1080)=[STRING];RuleID(1078)=[UINT32];Type(1067)=[STRING];
参数解释	$1：规则名称 $2：规则编号 $3：规则类型
日志等级	6
举例	OBJP/6/OBJP_RULE_DELETE_SUCCESS: RuleName(1080)=zone1-zone2;RuleID(1078)=1;Type(1067)=IPv4;
日志说明	删除对象策略规则成功
处理建议	无

105.9 OBJP_RULE_DELETE_FAIL

日志内容	RuleName(1080)=[STRING];RuleID(1078)=[UINT32];Type(1067)=[STRING];
参数解释	$1：规则名称 $2：规则编号 $3：规则类型
日志等级	6
举例	OBJP/6/OBJP_RULE_DELETE_FAIL: RuleName(1080)=zone1-zone2;RuleID(1078)=1;Type(1067)=IPv4;
日志说明	删除对象策略规则
处理建议	无

105.10 OBJP_RULE_CLRSTAT_SUCCESS

日志内容	RuleName(1080)=[STRING];RuleID(1078)=[UINT32];Type(1067)=[STRING];
参数解释	$1：规则名称 $2：规则编号 $3：规则类型
日志等级	6
举例	OBJP/6/OBJP_RULE_CLRSTAT_SUCCESS: RuleName(1080)=zone1-zone2;RuleID(1078)=1;Type(1067)=IPv4;
日志说明	清除对象策略规则统计信息成功
处理建议	无

105.11 OBJP_RULE_CLRSTAT_FAIL

日志内容	RuleName(1080)=[STRING];RuleID(1078)=[UINT32];Type(1067)=[STRING];
参数解释	$1：规则名称 $2：规则编号 $3：规则类型
日志等级	6
举例	OBJP/6/OBJP_RULE_CLRSTAT_FAIL: RuleName(1080)=zone1-zone2;RuleID(1078)=1;Type(1067)=IPv4;
日志说明	清除对象策略规则统计信息失败
处理建议	无

105.12 OBJP_APPLY_POLICY_FAIL

日志内容	Failed to apply [STRING] object policy [STRING]. The object policy does not exist.
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_APPLY_POLICY_FAIL: Failed to apply IPv4 object policy a. The object policy does not exist.
日志说明	因为引用的对象策略不存在导致引用失败
处理建议	无

105.13 OBJP_APPLAY_INFO

日志内容	Failed to apply policy [STRING]. Reason: [STRING].
参数解释	$1：对象策略名称 $2：错误内容
日志等级	4
举例	OBJP/4/OBJP_APPLAY_INFO: Failed to apply policy P1. Reason: The operation is not supported.
日志说明	应用对象策略失败
处理建议	无

106 OFP

本节介绍 OpenFlow 模块输出的日志信息。

106.1 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

106.2 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

106.3 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

106.4 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

106.5 OFP_FAIL_OPEN_FAILED

日志内容	OpenFlow instance [UINT16]: [STRING] fail-open mode configuration failed and the secure mode is restored.
参数解释	$1：实例ID $2：连接中断模式，取值为standalone
日志等级	4
举例	OFP/4/OFP_FAIL_OPEN_FAILED: OpenFlow instance 1: standalone fail-open mode configuration failed and the secure mode is restored.
日志说明	由于系统资源不足等原因，OpenFlow实例的连接中断模式配置失败（相关命令为**fail-open mode**），将回退为缺省模式Secure
处理建议	请联系技术支持

106.6 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

106.7 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

106.8 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

106.9 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

106.10 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

106.11 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

106.12 OFP_FLOW_DEL_L2VPN_DISABLE

日志内容	[UINT32] flow entries in table [UINT8] of instance [UINT16] were deleted because L2VPN was disabled.
参数解释	$1：删除的表项个数 $2：流表ID $3：实例ID
日志等级	5
举例	OFP/5/OFP_FLOW_DEL_L2VPN_DISABLE: 5 flow entries in table 1 of instance 1 were deleted because L2VPN was disabled.
日志说明	L2VPN功能关闭导致多个流表项被删除
处理建议	无

106.13 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

106.14 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

106.15 OFP_FLOW_DEL_VSIIF_DEL

日志内容	[UINT32] flow entries in table [UINT8] of instance [UINT16] were deleted because the Vsi-interface in VSI [STRING] was deleted.
参数解释	$1：删除的表项个数 $2：流表ID $3：实例ID $4：VSI的名称
日志等级	5
举例	OFP/5/OFP_FLOW_DEL_VSIIF_DEL: 5 flow entries in table 1 of instance 1 were deleted because the Vsi-interface in VSI VSI-OFP was deleted.
日志说明	由于VSI下的VSI虚接口被删除，导致相关流表项被删除
处理建议	无

106.16 OFP_FLOW_DEL_VXLAN_DEL

日志内容	[UINT32] flow entries in table [UINT8] of instance [UINT16] were deleted because a tunnel (ifindex [UINT32]) in VXLAN [UINT32] was deleted.
参数解释	$1：删除的表项个数 $2：流表ID $3：实例ID $4：Tunnel接口索引 $5：VXLAN ID
日志等级	5
举例	OFP/5/OFP_FLOW_DEL_VXLAN_DEL: 5 flow entries in table 1 of instance 1 were deleted because a tunnel (ifindex 1693) in VXLAN 1000 was deleted.
日志说明	VXLAN隧道删除导致多个流表项被删除
处理建议	无

106.17 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

106.18 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

106.19 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

106.20 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

106.21 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

106.22 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

106.23 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

106.24 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

106.25 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

106.26 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

106.27 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

106.28 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

106.29 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

106.30 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

106.31 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

106.32 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

106.33 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

106.34 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

106.35 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

106.36 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

106.37 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

106.38 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

107 OPENSRC(RSYNC)

本节介绍 OPENSRC 模块输出的开源软件 RSYNC 日志信息。

107.1 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

107.2 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

107.3 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

108 OPTMOD

本节介绍 OPTMOD 模块输出的日志信息。

108.1 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

108.2 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	5
举例	OPTMOD/5/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

108.3 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	5
举例	OPTMOD/5/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

108.4 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

108.5 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	5
举例	OPTMOD/5/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

108.6 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	5
举例	OPTMOD/5/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

108.7 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	5
举例	OPTMOD/5/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

108.8 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	5
举例	OPTMOD/5/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

108.9 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

108.10 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

108.11 PHONY_MODULE

日志内容	[STRING]: This transceiver is not sold by UNIS. UNIS 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 UNIS. UNIS does not guarantee the correct operation of the module or assume maintenance responsibility.
日志说明	光模块非UNIS生产
处理建议	更换光模块

108.12 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	5
举例	OPTMOD/5/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

108.13 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	5
举例	OPTMOD/5/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

108.14 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	5
举例	OPTMOD/5/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

108.15 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	5
举例	OPTMOD/5/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

108.16 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	5
举例	OPTMOD/5/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

108.17 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	5
举例	OPTMOD/5/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

108.18 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	5
举例	OPTMOD/5/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

108.19 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	5
举例	OPTMOD/5/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

108.20 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	5
举例	OPTMOD/5/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

108.21 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	5
举例	OPTMOD/5/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

108.22 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

108.23 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	5
举例	OPTMOD/5/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

108.24 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	5
举例	OPTMOD/5/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

108.25 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

108.26 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	5
举例	OPTMOD/5/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

108.27 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	5
举例	OPTMOD/5/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

108.28 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	5
举例	OPTMOD/5/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

109 OSPF

本节介绍 OSPF 模块输出的日志信息。

109.1 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	6
举例	OSPF/6/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

109.2 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

109.3 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

109.4 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

109.5 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	5
举例	OSPF/5/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

109.6 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

109.7 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

109.8 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

109.9 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	6
举例	OSPF/6/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

109.10 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

110 OSPFV3

本节介绍 OSPFv3 模块输出的日志信息。

110.1 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

110.2 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

110.3 OSPFV3_NBR_CHG

日志内容	OSPFv3 [UINT32] Neighbor [STRING] ([STRING]) received [STRING] and its state 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	5
举例	OSPFV3/5/OSPFV3_NBR_CHG: OSPFv3 1 Neighbor 2.2.2.2 (Vlan100) received 1-Way and its state 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

110.4 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	5
举例	OSPFV3/5/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

111 PBB

本节介绍 PBB 模块输出的日志信息。

111.1 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

112 PBR

本节介绍 PBR 模块输出的日志信息。

112.1 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：硬件资源不足 • 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持该操作
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

113 PCAPWARE

本节介绍 PCAPWARE 模块输出的日志信息。

113.1 PCAPWARE_STOP

日志内容	Packet capture stopped because [STRING].
参数解释	$1：停止抓包的原因： • the packet file size exceeded the storage limit. • the interface went down.
日志等级	5
举例	PCAPWARE/5/PCAPWARE_STOP: Packet capture stopped because the packet file size exceeded the storage limit.
日志说明	报文捕获停止的原因： • 存储捕获报文的捕获文件大小超过了允许捕获文件占用设备存储介质的最大存储空间 • 捕获报文的接口处于 Down 状态
处理建议	• 将捕获文件设备本地的存储空间调大 • 导出设备本地的捕获文件 • 将捕获文件存储到外部服务器 • 重新使接口恢复 Up 状态

114 PCE

本节介绍 PCE 模块输出的日志信息

114.1 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	5
举例	PCE/5/PCE_PCEP_SESSION_CHG: Session (22.22.22.2, public instance) is up. PCE/5/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

115 PEX

本节介绍 PEX（Port Extender）模块输出的日志信息。

115.1 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或虚拟框号 PEX不同型号的产品允许分配的虚拟槽位号或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或虚拟框号或者配置的虚拟槽位号或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的虚拟槽位号或虚拟框号修改到正确的范围内

115.2 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

115.3 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，如forwarding、down
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 • 转发故障，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中

115.4 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，如forwarding、blocked
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

115.5 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，如blocked
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

115.6 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

115.7 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，以及 display pex-port 检查 PEX 端口配置是否存在，或者 PEX 物理端口状态是否全部为 down 或者全部 blocked 3. 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

115.8 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

116 PFILTER

本节介绍报文过滤模块输出的日志信息。

116.1 PFILTER_APPLYUSER_FAIL

日志内容	[STRING]; Failed to apply [STRING] ACL [STRING] to the [STRING] direction of user profile [STRING]. Reason: [STRING].
参数解释	$1：上线用户的标识信息 $2：ACL类型 $3：ACL编号或名称 $4：报文过滤应用方向 $5：User Profile的名称 $6：失败原因
日志等级	3
举例	PFILTER/3/PFILTER_APPLYUSER_FAIL: -MAC=dc2d-cb22-3333-IP=192.168.1.2-SVLAN=100-VPN="N/A"-Port=GigabitEthernet 5/1/5; Failed to apply IPv4 ACL 2000 to the inbound direction of user profile u1. Reason: The resources are insufficient. PFILTER/3/ PFILTER_APPLYUSER_NO_RES: -MAC=dc2d-cb22-3333-IP=192.168.1.2-SVLAN=100-VPN="N/A"-Port=GigabitEthernet 5/1/5; Failed to apply IPv6 ACL 2000 to the outbound direction of user profile u1. Reason: Packet filtering is not supported for user profiles.
日志说明	• 资源不足导致 User-Profile 应用报文过滤失败 • 设备不支持基于 User-Profile 应用报文过滤
处理建议	• 资源不足时：删除一些 ACL 规则，释放部分资源 • 不支持基于 User-Profile 应用报文过滤时：可以基于用户上线的接口引用 ACL 配置报文过滤

116.2 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

116.3 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

116.4 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

116.5 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

116.6 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

116.7 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

116.8 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

116.9 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

116.10 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

116.11 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

116.12 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

116.13 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

116.14 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

116.15 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

116.16 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

116.17 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

116.18 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

116.19 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

116.20 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

116.21 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

116.22 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	PFILTER/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

116.23 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	PFILTER/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

116.24 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

116.25 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

116.26 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

116.27 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

116.28 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

116.29 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

116.30 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

116.31 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

116.32 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

116.33 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

117 PHYD

本节介绍 PHYD 模块输出的日志信息。

117.1 DRV

日志内容	-Slot=3.1; [STRING] : Detected hardware fast-forwarding status error. Info saved in [STRING]
参数解释	$1：单板所在槽位号 $2：硬件快速转发的异常文件记录名称
日志等级	2
举例	PHYD/2/DRV: -Slot=3.1; chassis %d slot %d cpu 1 : Detected hardware fast-forwarding status error. Info saved in chassis(1)_slot(1)_fpga(1)_regs_dump_count_1.
日志说明	每隔一段时间系统对硬件快速转发的状态进行监测。当硬件快速转发的状态异常时，记录异常文件，并打印异常log信息
处理建议	保存对应异常文件，继续观察单板状态

日志内容	-Slot=3.1; [STRING] : Detected hardware fast-forwarding status error 5 times. Rebooting now.
参数解释	$1：单板所在槽位号
日志等级	2
举例	PHYD/2/DRV: -Slot=3.1; chassis %d slot %d cpu 1 : Detected hardware fast-forwarding status error 5 times. Now rebooting.
日志说明	每隔一段时间系统对硬件快速转发的状态进行监测。当连续监测5次硬件快速转发均存在异常时，打印log信息，并重启单板
处理建议	单板重启完毕后，继续观察业务情况，同时将异常文件保存

日志内容	-Slot=2.1; Detected receiving interface [STRING] status abnormal on hardware fast-forwarding [STRING]. Checkpoint [STRING] failed.
参数解释	$1：接口编号 $2：硬件加速引擎芯片号 $3：检查点编号
日志等级	4
举例	PHYD/4/DRV: -Chassis=2-Slot=2.1; Detected receiving interface HGport[2] status abnormal on hardware fast-forwarding chip0. Checkpoint 2 failed.
日志说明	每隔一段时间系统对硬件快速转发的接收接口状态进行监测，当硬件快速转发的接收接口状态异常时，打印告警log
处理建议	业务不受影响的情况下，继续观察单板状态

日志内容	Detected sending interface [STRING] status abnormal on hardware fast-forwarding [STRING].
参数解释	$1：接口编号 $2：硬件加速引擎芯片号
日志等级	4
举例	PHYD/4/DRV: -Chassis=2-Slot=2.1; Detected sending interface HGport[1] status abnormal on hardware fast-forwarding chip0
日志说明	每隔一段时间系统对硬件快速转发的发送接口状态进行监测，当硬件快速转发的发送接口状态异常时，打印告警log
处理建议	业务不受影响的情况下，继续观察单板状态

日志内容	Detected [STRING] status abnormal on hardware fast-forwarding [STRING]. Receiving status: [STRING]; sending status: [STRING].
参数解释	$1：接口编号 $2：硬件加速引擎芯片号 $3：状态 $4：状态
日志等级	4
举例	PHYD/4/DRV: -Chassis=2-Slot=2.1; Detected HGport[2] status abnormal on hardware fast-forwarding chip0. Receiving status:OK; sending status: ERROR.
日志说明	每隔一段时间系统对硬件快速转发的HiGig接口状态进行监测，当硬件快速转发的HiGig接口状态异常时，打印告警log
处理建议	业务不受影响的情况下，继续观察单板状态

日志内容	-Slot=3.1; Detected uneven distribution of sessions on hardware fast-forwarding [STRING]. DDR[STRING]: [STRING] sessions (max); DDR [STRING]: [STRING] sessions (min).
参数解释	$1：硬件加速引擎芯片号 $2：DDR接口编号 $3：会话数量 $4：DDR接口编号 $5：会话数量
日志等级	4
举例	PHYD/4/DRV: -Chassis=1-Slot=4.1; Detected uneven distribution of sessions on hardware fast-forwarding chip0. DDR[22]: 112022 sessions (max); DDR [28]: 10257 sessions (min).
日志说明	每隔一段时间系统对硬件快速转发的会话状态进行监测，当硬件快速转发的会话状态异常时，打印告警log
处理建议	业务不受影响的情况下，继续观察单板状态

日志内容	Detected [STRING] channel[STRING] ddr_mod[STRING] exintf table status abnormal
参数解释	$1：芯片号 $2：通路号 $3：DDR编号
日志等级	4
举例	PHYD/4/DRV: -Slot=2.1; Detected chip0 channel[0] ddr mod[10] exintf table status abnormal
日志说明	每隔一段时间系统对硬件快速转发的表项状态进行监测。当硬件快速表项的状态异常时，记录异常文件，并打印异常log
处理建议	保存对应异常文件，继续观察单板状态

118 PIM

本节介绍 PIM 模块输出的日志信息。

118.1 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	5
举例	PIM/5/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，检查网络是否发生拥塞

118.2 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	5
举例	PIM/5/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

119 PING

本节介绍 ping 模块输出的日志信息。

119.1 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

119.2 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

120 PKI

本节包含 PKI 日志消息。

120.1 REQUEST_CERT_FAIL

日志内容	Failed to request [STRING] certificate of domain [STRING].
参数解释	$1：证书用途 $2：PKI域名
日志等级	5
举例	PKI/5/REQUEST_CERT_FAIL: Failed to request general 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

120.2 REQUEST_CERT_SUCCESS

日志内容	Request [STRING] certificate of domain [STRING] successfully.
参数解释	$1：证书用途 $2：PKI域名
日志等级	5
举例	PKI/5/REQUEST_CERT_SUCCESS: Request general certificate of domain abc successfully.
日志说明	为PKI域申请证书成功
处理建议	无

121 PKT2CPU

本节包含 PKT2CPU 日志消息。

121.1 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=dc2d-cb00-0014; The resources are insufficient.
日志说明	硬件资源不足
处理建议	取消配置

122 PKTCPT

本节介绍 PKTCPT（Packet Capture）模块输出的日志信息。

122.1 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

122.2 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

122.3 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

122.4 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

122.5 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

122.6 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

122.7 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

122.8 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

122.9 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

122.10 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

122.11 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

122.12 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

123 PORTAL

本节介绍 PORTAL 模块输出的日志信息。

123.1 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], IPv6Input Octets=[UINT32], IPv6Output Octets=[UINT32], IPv6 Input Gigawords=[UINT32], IPv6Output Gigawords=[UINT32], SessionTime=[UINT32]; User logged off.
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 $8：用户上行IPv4流量统计 $9：用户下行IPv4流量统计 $10：用户上行IPv4流量与4G的倍数 $11：用户下行IPv4流量与4G的倍数 $12：用户上行IPv6流量统计 $13：用户下线IPv6流量统计 $14：用户上行IPv6流量与4G的倍数 $15：用户下行IPv6流量与4G的倍数 $16：在线时长，单位为秒
日志等级	6
举例	PORTAL/6/PORTAL_USER_LOGOFF: -MDC=1; UserName=abc, IPAddr=1.1.1.2, IfName=Route-Aggregation1023.4000, OuterVLAN=N/A, InnerVLAN=4000, MACAddr=dc2d-cb03-5601, Reason=User request, Input Octets=100, Output Octets=200, Input Gigawords=100, Output Gigawords=200, IPv6Input Octets=100, IPv6Output Octets=200, IPv6Input Gigawords=100, IPv6Output Gigawords=200, SessionTime=200; User logged off.
日志说明	用户下线。IPv6相关参数的显示受命令**portal user-log traffic-separate**控制，详情请参见“安全命令参考”中的“Portal”
处理建议	请根据下线详细原因选择相应的处理方式，详见表123-2

表123-1 下线原因列表

下线原因	说明	处理建议
User request.	用户正常请求下线	无
DHCP relay deleted.	DHCP中继表项被删除	请确保DHCP服务器上的配置正确
Idle timeout.	用户在规定时间内的流量没有达到设	无

	定阈值	
Session timeout.	用户上线时间达到服务器下发的会话在线时长	无
User detection failure.	用户在线探测失败	无
Force logout by RADIUS server.	RADIUS服务器强制用户下线	无
Interface down.	• 接入接口状态为 Down、Deactive • VLAN 接口接入 Portal，二层端口离开 VLAN	• 请确保用户接入接口网线连接正常且接口下没有配置 **shutdown** 命令 • 请确保用户接入单板或者接口子卡正常工作 • 请确保用户接入的二层以太网接口上开启了漫游功能
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
Authorization info changed.	在线用户授权信息变更,比如授权ACL、授权User Profile被删除	无
Force logout by access device.	设备强制用户下线	请确保接口上的Portal功能正常
User info synchronization failure.	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.	恢复用户信息失败	• 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	• 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
Accounting update failure.	用户计费更新失败	• 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
Failed to start accounting.	用户计费开始失败	• 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
User traffic reached threshold.	用户的流量达到了服务器上设置的流量阈值	无
Authorization VPN instance deleted.	授权VPN实例被删除	无

123.2 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 get 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123-2
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=dc2d-cb03-5601-Reason=Authentication Failed : 4; User failed to get 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123-2

表123-2 上线失败详细原因列表

上线失败原因	说明	处理建议
Authorization failure.	授权失败或者下发授权属性失败	• 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 • 请确保 ACL 资源充足
Received logout request.	用户正在上线过程中，收到Portal服务器的请求下线报文	请确保设备与AAA服务器之间的通信正常
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
Other error.	其他情况	-

123.3 PORTAL_USER_LOGON_SUCCESS

日志内容	-UserName=[STRING]-IPAddr=[IPADDR]-IfName=[STRING]-OuterVLAN=[UINT16]-InnerVLAN=[UINT16]-MACAddr=[MAC]:User got 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=dc2d-cb03-5601; User got online successfully.
日志说明	用户上线成功
处理建议	无

124 PORTSEC

本节介绍端口安全模块输出的日志信息。

124.1 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

124.2 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

125 POSA

本节介绍 POSA 终端的日志。

125.1 POSA_TCPLISTENPORT_NOT_OPEN

日志内容	Failed to open TCP listening port for terminal [STRING].
参数解释	$1：POSA终端模板ID
日志等级	3
举例	POSA/3/POSA_TCPLISTENPORT_NOT_OPEN: Failed to open TCP listening port for terminal 1.
日志说明	POSA终端模板1的TCP监听端口开启失败
处理建议	删除该POSA终端模板并使用一个未被占用的端口创建POSA终端模板

126 PPP

本节介绍 PPP 模块输出的日志信息。

126.1 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

126.2 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 dc2d-cba8-0949 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 UNIS 技术支持

126.3 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=dc2d-cb03-5601; The user came online successfully.
日志说明	用户上线成功
处理建议	无

126.4 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65-1
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=dc2d-cb03-5601-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65-1

表126-1 上线失败原因列表

上线失败原因	说明	处理建议
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
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

126.5 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65-2
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=dc2d-cb03-5601-Reason=Use request; The user logged off.
日志说明	用户正常下线
处理建议	无

表126-2 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

126.6 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126-3
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=dc2d-cb03-5601-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126-3

表126-3 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UNIS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
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UNIS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 • 检查计费服务器状态是否正常
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**
Session idle cut	用户在规定时间内的流量没有达到设定值	无

127 PREPROVISION

本节介绍 PREPROVISION 模块输出的日志信息。

127.1 PREPROVISION_SLOT_MISMATCH

日志内容	Preprovision check on slot [UINT32] failed because of mismatching model or interface information: Preprovisioned model=[STRING], installed model=[STRING]. Preprovisioned interface type=[STRING], actual interface type=[STRING].
参数解释	$1：成员设备的编号 $2：预配置的设备型号 $3：实际的设备型号 $4：预配置的成员设备接口信息 $5：实际的成员设备接口信息
日志等级	3
举例	PREPROVISION/3/PREPROVISION_SLOT_MISMATCH: Preprovision check on slot 2 failed because of mismatching model or interface information: Preprovisioned model=MPU, installed model=MPU. Preprovisioned interface type=GE-GE, actual interface type=XGE-XGE.
日志说明	预配置检查失败，原因是插入成员设备的实际型号与预配置的型号不匹配，或者实际接口信息与预配置的接口信息不匹配
处理建议	插入指定类型的成员设备

127.2 PREPROVISION_SUBSLOT_MISMATCH

日志内容	Preprovision check on slot [UINT32] subslot [UINT32] failed because of mismatching model or interface information: Preprovisioned model=[STRING], installed model=[STRING]. Preprovisioned interface type=[STRING], actual interface type=[STRING].
参数解释	$1：成员设备的编号 $2：子卡设备的编号 $3：预配置的子卡型号 $4：实际的子卡型号 $5：预配置的子卡接口信息 $6：实际的子卡接口信息
日志等级	3
举例	PREPROVISION/3/PREPROVISION_SLOT_MISMATCH: Preprovision check on slot 2 subslot 1 failed because of mismatching model or interface information: Preprovisioned model=EXTEND-CARD, installed model= EXTEND-CARD. Preprovisioned interface type=XGE, actual interface type=GE.
日志说明	预配置检查失败，原因是插入成员设备子卡的实际型号与预配置的型号不匹配，或者实际接口信息与预配置的接口信息不匹配
处理建议	插入指定类型的子卡

128 PTS

本节介绍 PTS（Platform Trust Services，平台可信服务）模块输出的日志信息。

128.1 PTS_AK_AUTH_FAILED

日志内容	Inconsistent authorization data for attestation key [STRING].
参数解释	$1：AK密钥的名称
日志等级	4
举例	PTS/4/PTS_AK_AUTH_FAILED: Inconsistent authorization data for attestation key abc.
日志说明	AK密钥对应的授权数据错误
处理建议	配置可信报告使用的AK密钥时使用的授权数据需要和创建该密钥时配置的授权数据一致（相关命令为**`key create`**）

128.2 PTS_AK_INVALID

日志内容	The attestation key [STRING] is incorrect.
参数解释	$1：AK密钥的名称
日志等级	4
举例	PTS/4/PTS_AK_INVALID: The attestation key abc is incorrect.
日志说明	AK密钥无效
处理建议	重新配置可信报告使用的AK密钥

128.3 PTS_AK_NO_CERT

日志内容	No certificate file found for attestation key [STRING].
参数解释	$1：AK密钥的名称
日志等级	4
举例	PTS/4/PTS_AK_NO_CERT: No certificate file found for attestation key abc.
日志说明	AK密钥缺少证书
处理建议	通过管理端为设备的AK密钥签发AK证书

128.4 PTS_AK_NO_EXIST

日志内容	Attestation key [STRING] doesn't exist.
参数解释	$1：AK密钥的名称
日志等级	4
举例	PTS/4/PTS_AK_NO_EXIST: The attestation key abc doesn't exist.
日志说明	指定名称的AK密钥不存在
处理建议	配置AK密钥（相关命令为**`key create`**）

128.5 PTS_AK_NO_LOAD

日志内容	The attestation key [STRING] is not loaded.
参数解释	$1：AK密钥的名称
日志等级	4
举例	PTS/4/PTS_AK_NO_LOAD: The attestation key abc is not loaded.
日志说明	AK密钥未加载到安全芯片
处理建议	通过**key load**命令将AK密钥加载到可信计算芯片

128.6 PTS_BTW_PCR_FAILED

日志内容	Hash value computed based on BootWare IML is not consistent with that in PCR ([UINT]).
参数解释	$1：PCR的索引
日志等级	4
举例	PTS/4/PTS_BTW_PCR_FAILED: Hash value computed based on BootWare IML is not consistent with that in PCR(0).
日志说明	使用BootWare可信度量日志计算出来的HASH值与保存在PCR中的HASH值不同，此时BootWare程序不可信
处理建议	请联系技术支持

128.7 PTS_CHECK_RM_VERSION_FAILED

日志内容	Version the RM file [STRING] is not supported.
参数解释	$1：RM文件名称
日志等级	4
举例	PTS/4/PTS_CHECK_RM_VERSION_FAILED: Version the RM file BOOTWARE_BASIC_52B.rm is not supported.
日志说明	设备不支持当前RM文件版本
处理建议	请联系技术支持

128.8 PTS_CREATE_AGED_TIMER_FAILED

日志内容	Failed to create PTS session ageing timer.
参数解释	无
日志等级	4
举例	PTS/4/PTS_CREATE_AGED_TIMER_FAILED: Failed to create PTS session ageing timer.
日志说明	创建PTS会话老化定时器失败
处理建议	1. 依次执行 undo pts 和 pts 命令重启 PTS 服务 2. 如果问题仍然存在，请联系技术支持

128.9 PTS_CREATE_CHECK_TIMER_FAILED

日志内容	Failed to create server check timer.
参数解释	无
日志等级	4
举例	PTS/4/PTS_CREATE_CHECK_TIMER_FAILED: Failed to create server check timer.
日志说明	创建Server检查定时器失败
处理建议	1. 依次执行 **undo pts** 和 **pts** 命令重启 PTS 服务 2. 如果问题仍然存在，请联系技术支持

128.10 PTS_CREATE_CONTEXT_FAILED

日志内容	Failed to create TSS context.
参数解释	无
日志等级	4
举例	PTS/4/PTS_CREATE_CONTEXT_FAILED: Failed to create TSS context.
日志说明	TSS（TPM Software Stack，TPM芯片软件栈）上下文初始化失败
处理建议	请联系技术支持

128.11 PTS_CREATE_EPOLL_FAILED

日志内容	Failed to create epoll service.
参数解释	无
日志等级	3
举例	PTS/3/PTS_CREATE_EPOLL_FAILED: Failed to create epoll service.
日志说明	PTS模块创建epoll（I/O event notification facility）服务失败
处理建议	**1.** 依次执行 undo pts 和 pts 命令重启 PTS 服务 **2.** 如果问题仍然存在，请联系技术支持

128.12 PTS_CREATE_HASH_FAILED

日志内容	Failed to create hash table.
参数解释	无
日志等级	3
举例	PTS/3/PTS_CREATE_HASH_FAILED: Failed to create hash table.
日志说明	PTS模块创建HASH表失败
处理建议	**1.** 依次执行 undo pts 和 pts 命令重启 PTS 服务 **2.** 如果问题仍然存在，请联系技术支持

128.13 PTS_CREATE_SELFVERIFY_COUNTER_FAILED

日志内容	Failed to create selfverify counter.
参数解释	无
日志等级	4
举例	PTS/4/PTS_CREATE_SELFVERIFY_COUNTER_FAILED: Failed to create selfverify counter.
日志说明	可信自检的IML计数器创建失败，此时可信自检功能不可用
处理建议	**1.** 依次执行 undo pts 和 pts 命令重启 PTS 服务 **2.** 如果问题仍然存在，请联系技术支持

128.14 PTS_CREATE_SELFVERIFY_TIMER_FAILED

日志内容	Failed to create selfverify timer.
参数解释	无
日志等级	4
举例	PTS/4/PTS_CREATE_SELFVERIFY_TIMER_FAILED: Failed to create selfverify timer.
日志说明	周期可信自检的定时器创建失败，此时周期可信自检功能不可用
处理建议	• 请联系技术支持 • 可以通过 integrity selfverify 命令手动执行可信自检

128.15 PTS_CREATE_SOCKET_FAILED

日志内容	Failed to create socket service.
参数解释	无
日志等级	3
举例	PTS/3/PTS_CREATE_SOCKET_FAILED: Failed to create socket service.
日志说明	PTS模块创建socket服务失败
处理建议	**1.** 依次执行 undo pts 和 pts 命令重启 PTS 服务 **2.** 如果问题仍然存在，请联系技术支持

128.16 PTS_CREATE_TIMER_FAILED

日志内容	Failed to create timer.
参数解释	无
日志等级	4
举例	PTS/4/PTS_CREATE_TIMER_FAILED: Failed to create timer.
日志说明	创建定时器失败 当PTS模块的任一定时器创建失败时，都会产生本日志
处理建议	**1.** 依次执行 undo pts 和 pts 命令重启 PTS 服务 **2.** 如果问题仍然存在，请联系技术支持

128.17 PTS_FILE_HASH_FAILED

日志内容	Hash value of file [STRING] is not consistent with that in the RM file.
参数解释	$1：可信度量的目标文件名称
日志等级	4
举例	PTS/4/PTS_FILE_HASH_FAILED: Hash value of file /sbin/ls is not consistent with that in the RM file.
日志说明	目标文件的HASH值与RM文件中该文件的HASH值不匹配，此时该文件不可信
处理建议	请联系技术支持

128.18 PTS_LOAD_KEY_FAILED

日志内容	Failed to load attestation key [STRING].
参数解释	$1：AK密钥的名称
日志等级	4
举例	PTS/4/PTS_LOAD_KEY_FAILED: Failed to load attestation key abc.
日志说明	向TPM芯片加载AK密钥失败
处理建议	1. 检查指定名称的 AK 密钥是否存在且处于使能状态（相关显示命令为 display tcsm key name） 2. 请联系技术支持

128.19 PTS_PARSE_IML_FAILED

日志内容	Failed to parse IML.
参数解释	无
日志等级	4
举例	PTS/4/PTS_PARSE_IML_FAILED: Failed to parse IML.
日志说明	可信度量日志解析失败
处理建议	1. 依次执行 undo pts 和 pts 命令重启 PTS 服务 2. 如果问题仍然存在，请联系技术支持

128.20 PTS_PKG_PCR_FAILED

日志内容	Hash value computed based on Package IML is not consistent with that in PCR ([UINT]).
参数解释	$1：PCR的索引
日志等级	4
举例	PTS/4/PTS_PKG_PCR_FAILED: Hash value computed based on Package IML is not consistent with that in PCR (12).
日志说明	使用Uniware软件包的可信度量日志计算出来的HASH值与保存在PCR中的HASH值不同，此时Uniware软件包不可信
处理建议	请联系技术支持

128.21 PTS_READ_PCR_FAILED

日志内容	Failed to read PCR ([UINT]).
参数解释	$1：TPM芯片的PCR索引
日志等级	4
举例	PTS/4/PTS_READ_PCR_FAILED: Failed to read PCR(0).
日志说明	PCR数据读取失败
处理建议	请联系技术支持

128.22 PTS_RM_FILE_FAILED

日志内容	Wrong signature for RM file [STRING].
参数解释	$1：RM文件名称
日志等级	4
举例	PTS/4/PTS_RM_FILE_FAILED: Wrong signature for RM file BOOTWARE_BASIC_52B.rm.
日志说明	RM文件签名错误
处理建议	请联系技术支持

128.23 PTS_RUNTIME_PCR_FAILED

日志内容	Hash value computed based on runtime IML is not consistent with that in PCR ([UINT]).
参数解释	$1：PCR的索引
日志等级	4
举例	PTS/4/PTS_RUNTIME_PCR_FAILED: Hash value computed based on runtime IML is not consistent with that in PCR (10).
日志说明	使用Runtime（运行的软件进程）相关的可信度量日志计算出来的HASH值与保存在PCR中的HASH值不同，此时Runtime相关的可执行文件不可信
处理建议	请联系技术支持

128.24 PTS_SELFVERIFY_FAILED

日志内容	Failed to start integrity selfverify. Reason: TPM doesn't exist or isn't enabled.
参数解释	$1：AK密钥的名称
日志等级	4
举例	PTS/4/PTS_SELFVERIFY_FAILED: Failed to start integrity selfverify because TPM does not exist or is not enabled.
日志说明	由于TPM芯片不存在或者被禁用，可信自检启动失败
处理建议	查看设备的可信计算芯片信息（相关显示命令为display tcsm trusted-computing-chip），确保TPM芯片可用

128.25 PTS_SELFVERIFY_START_FAILED

日志内容	Failed to start selfverify.
参数解释	无
日志等级	4
举例	PTS/4/PTS_SELFVERIFY_START_FAILED: Failed to start selfverify.
日志说明	启动可信自检失败
处理建议	**1.** 尝试重新启动可信自检 **2.** 如果问题仍然存在，请联系技术支持

128.26 PTS_TEMPLATE_HASH_FAILED

日志内容	Calculated template hash value of [STRING] is not consistent with that in IML.
参数解释	$1：可信度量的目标文件名称
日志等级	4
举例	PTS/4/PTS_TEMPLATE_HASH_FAILED: Calculated template hash value of /sbin/ls is not consistent with that in IML.
日志说明	根据目标文件的HASH值和日志度量时间等参数计算的模板HASH值与可信度量日志中的模板HASH值不同，此时该可信度量日志内容可能被篡改
处理建议	请联系技术支持

129 PWDCTL

本节介绍 Password control 模块输出的日志信息。

129.1 PWDCTL_ADD_BLACKLIST

日志内容	[STRING] was added to the blacklist for wrong password input.
参数解释	$1：用户名
日志等级	6
举例	PWDCTL/6/PWDCTL_ADD_BLACKLIST: hhh was added to the blacklist for wrong password input.
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

129.2 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 is 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

129.3 PWDCTL_DELETEBLACLIST

日志内容	User [STRING] was deleted from blacklist.
参数解释	$1：用户名
日志等级	3
举例	PWDCTL/3/PWDCTL_DELETEBLACLIST: User hhh was deleted from blacklist.
日志说明	将用户账号从黑名单中删除
处理建议	无

129.4 PWDCTL_FAILED_COPYFILE

日志内容	Failed to copy the password records to all backup files.
参数解释	无
日志等级	3
举例	PWDCTL/3/PWDCTL_FAILED_COPYFILE: Failed to copy the password records to backup file.
日志说明	设备无法将密码记录拷贝到备用主控板的记录文件
处理建议	请检查设备备用主控板文件系统存储空间是否充足

129.5 PWDCTL_FAILED_PROCMSG

日志内容	Failed to process request message.
参数解释	无
日志等级	3
举例	PWDCTL/3/PWDCTL_FAILED_PROCMSG: Failed to process request message.
日志说明	密码管理守护进程处理请求消息失败
处理建议	请联系技术支持人员

129.6 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	6
举例	PWDCTL/6/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

129.7 PWDCTL_LOCKBLACKLIST

日志内容	User [STRING] was [STRING] minutes for achieve maximum login attempts.
参数解释	$1：用户名 $2：用户尝试登录达到最大次数后，对用户账号采取不同的锁定措施： locked in *time-value* minutes：锁定一段时间，一段时间后可重新登录。*time-value*为锁定时长，单位为分钟 permanently locked：永久锁定
日志等级	3
举例	1. PWDCTL/3/PWDCTL_LOCKBLACKLIST: User hhh was locked in 1 minutes for achieve maximum login attempts. 2. PWDCTL/3/PWDCTL_LOCKBLACKLIST: User hhh was permanently locked for achieve maximum login attempts.
日志说明	用户尝试登录次数达到设定的最大值后，账号被采取不同的锁定措施（通过password-control login-attempt exceed命令配置）
处理建议	无

129.8 PWDCTL_NOTIFYWRITEFILE

日志内容	Notification of writing password records to file failed.
参数解释	无
日志等级	3
举例	PWDCTL/3/PWDCTL_NOTIFYWRITEFILE: Notification of writing password records to file failed.
日志说明	将用户密码写入密码记录文件的通知下发失败
处理建议	请联系技术支持人员

129.9 PWDCTL_RECFORMATCONV

日志内容	Failed to convert the password record format.
参数解释	无
日志等级	3
举例	PWDCTL/3/PWDCTL_RECFORMATCONV: Failed to convert the password record format.
日志说明	用户记录格式转换失败
处理建议	请联系技术支持人员

129.10 PWDCTL_UNLOCKBLACKLIST

日志内容	User [STRING] was unlocked due to lock-time aged.
参数解释	$1：用户名
日志等级	3
举例	PWDCTL/3/PWDCTL_UNLOCKBLACKLIST: User hhh was unlocked due to lock-time aged.
日志说明	超出配置的锁定时间后，用户被解除锁定
处理建议	无

129.11 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

129.12 PWDCTL_USERINLOCKING

日志内容	User [STRING] is locking for maximum times failure loged in.
参数解释	$1：用户名
日志等级	3
举例	PWDCTL/3/PWDCTL_USERINLOCKING: User hhh is locking for maximum times failure loged in.
日志说明	用户在登录失败达到最大次数被锁定期间仍尝试登录
处理建议	无

130 QOS

本节介绍 QoS 模块输出的日志信息。

130.1 QOS_AUTHCAR_APPLYUSER_FAIL

日志内容	[STRING]; Failed to apply the authorized CAR to the user. Reason: [STRING].
参数解释	$1：用户标识信息 $2：失败原因 The resources are insufficient：资源不足
日志等级	4
举例	QOS/4/QOS_AUTHCAR_APPLYUSER_FAIL: -MAC=dc2d-cb22-3333-IP=192.168.1.2-SVLAN=100-VPN=”N/A”-Port=GigabitEthernet 5/1/5; Failed to apply the authorized CAR to the user. Reason: The resources are insufficient.
日志说明	1.用户上线，DAE客户端下发授权CAR信息失败 2.用户已经上线，DAE客户端修改授权CAR信息失败
处理建议	修改DAE客户端上下发的授权CAR相关参数信息

130.2 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 ○ The resources are insufficient：资源不足
日志等级	4
举例	QOS/4/QOS_CAR_APPLYUSER_FAIL: -MAC=dc2d-cb22-3333-IP=192.168.1.2-SVLAN=100-VPN="N/A"-Port=GigabitEthernet 5/1/5; Failed to apply the inbound CAR in user profile a to the user. Reason: The resources are insufficient.
日志说明	1.用户上线，下发配置的CAR信息失败 2.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

130.3 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

130.4 QOS_GTS_APPLYUSER_FAIL

日志内容	[STRING]; Failed to apply GTS in user profile [STRING] to the user. Reason: [STRING].
参数解释	$1：用户标识信息 $2：User profile名称 $3：失败原因
日志等级	4
举例	QOS/4/QOS_GTS_APPLYUSER_FAIL: -MAC=dc2d-cb22-3333-IP=192.168.1.2/16-CVLAN=100-Port=GigabitEthernet5/1/5; Failed to apply GTS in user profile a to the user. Reason: The resources are insufficient.
日志说明	1.用户上线，下发配置的GTS信息失败 2.用户已经上线，修改GTS信息或者增加GTS应用失败
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

130.5 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

130.6 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

130.7 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

130.8 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

130.9 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

130.10 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 ○ The classifier is empty.：流分类为空，未配置任何匹配规则
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

130.11 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

130.12 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=dc2d-cb22-3333-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	1.用户上线，下发配置的QoS policy信息失败 2.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

130.13 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/4/QOS_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

130.14 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

130.15 QOS_QMPROFILE_APPLYUSER_FAIL

日志内容	[STRING]; Failed to apply queue management profile [STRING] in session group 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：Session group Profile名称 $4：失败原因
日志等级	4
举例	QOS/4/QOS_QMPROFILE_APPLYUSER_FAIL: -MAC=dc2d-cb22-3333-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.
日志说明	1.用户上线，下发配置的QMProfile信息失败 2.用户已经上线，修改QMProfile信息或者增加QMProfile应用失败
处理建议	取消QMProfile在Session group profile下的应用或者修改QMProfile的相关信息

130.16 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

130.17 QOS_POLICY_REMOVE

日志内容	QoS policy [STRING] was failed to be applied to [STRING].
参数解释	$1：QoS策略名称 $2：QoS策略应用实体（目前只有基于Tunnel接口的Hub-Spoke隧道一种类型）
日志等级	4
举例	QOS/4/QOS_POLICY_REMOVE: QoS policy p1 was failed to be applied to ADVPN session Tunnel1 192.168.0.3.
日志说明	用户修改应用在Hub-Spoke隧道上的QoS策略，导致QoS策略应用失败
处理建议	QoS策略应用失败后，会有对应失败原因的说明日志。请查看对应日志内容，按照具体失败原因排查配置

130.18 QOS_POLICY_ACTIVATE

日志内容	QoS policy [STRING] was successfully applied to [STRING].
参数解释	$1：QoS策略名称 $2：QoS策略应用实体（目前只有基于Tunnel接口的Hub-Spoke隧道一种类型）
日志等级	4
举例	QOS/4/QOS_POLICY_ACTIVATE: QoS policy p1 was successfully applied to ADVPN session Tunnel1 192.168.0.3.
日志说明	用户修改应用在Hub-Spoke隧道上的QoS策略，QoS策略应用成功
处理建议	无

131 RADIUS

本节介绍 RADIUS 模块输出的日志信息。

131.1 RADIUS_ACCT_SERVER_DOWN

日志内容	RADIUS accounting server was blocked: Server IP=[STRING], port=*[UINT32]*, VPN instance=[STRING].
参数解释	$1：计费服务器IP地址 $2：计费服务器端口号 $3：VPN实例名称，如果服务器属于公网，则显示为public
日志等级	4
举例	RADIUS/4/RADIUS_ACCT_SERVER_DOWN: RADIUS accounting server was blocked: Server IP=1.1.1.1, port=1812, VPN instance=public.
日志说明	RADIUS计费服务器状态为阻塞
处理建议	**1.** 检查 RADIUS 服务器是否开启。如果 RADIUS 服务器关闭，请重新启动 RADIUS 服务器。 **2.** 执行 ping 命令检查 RADIUS 服务器是否可达。如果 RADIUS 服务器不可达，请检查链路是否通畅。 **3.** 请收集日志信息和诊断信息，并联系技术支持。

131.2 RADIUS_ACCT_SERVER_UP

日志内容	RADIUS accounting server became active: Server IP=[STRING], port=*[UINT32]*, VPN instance=[STRING].
参数解释	$1：计费服务器IP地址 $2：计费服务器端口号 $3：VPN实例名称，如果服务器属于公网，则显示为public
日志等级	6
举例	RADIUS/6/RADIUS_ACCT_SERVER_UP: RADIUS accounting server became active: Server IP=1.1.1.1, port=1812, VPN instance=public.
日志说明	RADIUS计费服务器状态为激活
处理建议	无

131.3 RADIUS_AUTH_FAILURE

日志内容	User [STRING] at [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 at 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

131.4 RADIUS_AUTH_SERVER_DOWN

日志内容	RADIUS authentication server was blocked: Server IP=[STRING], port=*[UINT32]*, VPN instance=[STRING].
参数解释	$1：认证服务器IP地址 $2：认证服务器端口号 $3：VPN实例名称，如果服务器属于公网，则显示为public
日志等级	4
举例	RADIUS/4/RADIUS_AUTH_SERVER_DOWN: RADIUS authentication server was blocked: Server IP= 1.1.1.1, port=1812, VPN instance=public.
日志说明	RADIUS认证服务器状态为阻塞
处理建议	**1.** 检查 RADIUS 服务器是否开启。如果 RADIUS 服务器关闭，请重新启动 RADIUS 服务器。 **2.** 执行 ping 命令检查 RADIUS 服务器是否可达。如果 RADIUS 服务器不可达，请检查链路是否通畅。 **3.** 请收集日志信息和诊断信息，并联系技术支持

131.5 RADIUS_AUTH_SERVER_UP

日志内容	RADIUS authentication server became active: Server IP=[STRING], port=*[UINT32]*, VPN instance=[STRING].
参数解释	$1：认证服务器IP地址 $2：认证服务器端口号 $3：VPN实例名称，如果服务器属于公网，则显示为public
日志等级	6
举例	RADIUS/6/RADIUS_AUTH_SERVER_UP: RADIUS authentication server became active: Server IP=1.1.1.1, port=1812, VPN instance=public.
日志说明	RADIUS认证服务器状态为激活
处理建议	无

131.6 RADIUS_AUTH_SUCCESS

日志内容	User [STRING] at [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 at 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

131.7 RADIUS_REMOVE_SERVER_FAIL

日志内容	Failed to remove servers in scheme [STRING].
参数解释	$1：方案名称
日志等级	4
举例	RADIUS/4/RADIUS_REMOVE_SERVER_FAIL: Failed to remove 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

132 RBM

本节介绍 RBM（Remote Backup Management，远端备份管理）输出的日志信息。RBM 即高可靠性（HA）。

132.1 CFG_BATCH_SYNC

日志内容	Configuration synchronization didn't complete due to configuration file sending exception.
参数解释	无
日志等级	6
举例	RBM/6/ CFG_BATCH_SYNC: -Context=1; Configuration synchronization didn't complete due to configuration file sending exception.
日志说明	配置信息向对端同步失败，配置文件发送异常
处理建议	请重新执行手工同步配置信息功能

132.2 CFG_BATCH_SYNC

日志内容	Started batch configuration synchronization.
参数解释	无
日志等级	6
举例	RBM/6/ CFG_BATCH_SYNC: -Context=1; Started batch configuration synchronization..
日志说明	开始向对端批量备份配置信息
处理建议	设备正在进行批量备份配置信息时，请尽量不要对设备进行任何操作

132.3 CFG_BATCH_SYNC

日志内容	Finished batch configuration synchronization.
参数解释	无
日志等级	6
举例	RBM/6/ CFG_BATCH_SYNC: -Context=1; Finished batch configuration synchronization.
日志说明	批量备份配置信息结束
处理建议	无

132.4 CFG_BATCH_SYNC

日志内容	Configuration synchronization failed! Device Role both is primary.
参数解释	无
日志等级	6
举例	RBM/6/ CFG_BATCH_SYNC: -Context=1; Configuration synchronization failed! Device Role both is primary.
日志说明	配置信息同步失败，因为两端设备都是主管理设备
处理建议	请修改其中一台为从管理设备

132.5 CFG_COMPARE

日志内容	Started configuration consistency check.
参数解释	无
日志等级	6
举例	RBM/6/CFG_COMPARE: Started configuration consistency check.
日志说明	配置信息一致性检查开始
处理建议	无

132.6 CFG_COMPARE

日志内容	Finished configuration consistency check.
参数解释	无
日志等级	6
举例	RBM/6/CFG_COMPARE: Finished configuration consistency check.
日志说明	配置信息一致性检查结束
处理建议	无

132.7 CFG_COMPARE

日志内容	The following modules have inconsistent configuration: [STRING].
参数解释	$1：模块名称
日志等级	6
举例	RBM/6/CFG_COMPARE: The following modules have inconsistent configuration: NAT.
日志说明	配置信息一致性检查结果
处理建议	无

132.8 CFG_COMPARE

日志内容	Configuration consistency check didn't complete due to configuration file sending exception.
参数解释	无
日志等级	6
举例	RBM/6/CFG_COMPARE: -Context=1; Configuration consistency check didn't complete due to configuration file sending exception.
日志说明	配置信息一致性检查失败，配置文件发送异常
处理建议	请重新执行手工配置信息一致检查功能

132.9 DEVICE_ROLE

日志内容	The two member devices have the same role. Please assign different roles to them.
参数解释	无
日志等级	6
举例	RBM/6/DEVICE_ROLE: -Context=1; The two member devices have the same role. Please assign different roles to them.
日志说明	两端设备的管理角色相同，请重新配置管理角色
处理建议	请将两端的设备配置成不同的管理角色

132.10 RBM_CFG_CONFLICT

日志内容	VLAN or interface monitoring configuration exists. For the HA group to collaborate with VRRP and routing protocols, first delete the VLAN or interface monitoring configuration.
参数解释	无
日志等级	1
举例	RBM/1/ RBM_CFG_CONFLICT: -Context=1; VLAN or interface monitoring configuration exists. For the HA group to collaborate with VRRP and routing protocols, first delete the VLAN or interface monitoring configuration.
日志说明	因为系统中存在track vlan或track interface配置，导致HA联动VRRP和联动路由功能失效
处理建议	如果需要HA联动VRRP和联动路由功能生效，请删除track vlan或track interface配置

132.11 RBM_CFG_ROLLBCK

日志内容	Please perform configuration synchronization after configuration rollback is finished.
参数解释	无
日志等级	6
举例	RBM/6/RBM_CFG_ROLLBCK: -Context=1; Please perform configuration synchronization after configuration rollback is finished.
日志说明	配置回滚完成后请手工备份配置信息，以保证主备设备的配置信息一致
处理建议	无

132.12 RBM_CHANNEL

日志内容	Local IP=[STRING], remote IP=[STRING], status=[STRING].
参数解释	$1：HA控制通道本端IPv4地址 $2：HA控制通道对端IPv4地址 $3：状态，包括如下取值： • Connected：HA 控制通道连接成功 • Disconnected：HA 控制通道断开
日志等级	1
举例	RBM/1/RBM_CHANNEL: Local IP=1.1.1.1, remote IP=1.1.1.2, status=Connected.
日志说明	HA控制通道连接信息详情
处理建议	当HA控制通道断开时，请检查通道IP地址的正确性和网络的连通性

132.13 RBM_CHANNEL

日志内容	Local IPv6=[STRING], remote IPv6=[STRING], status=[STRING].
参数解释	$1：HA控制通道本端IPv6地址 $2：HA控制通道对端IPv6地址 $3：状态，包括如下取值： • Connected：HA 控制通道连接成功 • Disconnected：HA 控制通道断开
日志等级	1
举例	RBM/1/RBM_CHANNEL: Local IPv6=2001::1, remote IPv6=2001::2,status=Connected.
日志说明	HA控制通道连接信息详情
处理建议	当HA控制通道断开时，请检查通道IP地址的正确性和网络的连通性

132.14 RBM_CHANNEL_BIND_FAILED

日志内容	Failed to bind IP address [STRING] and port [UINT16] to the RBM channel.
参数解释	$1：IP地址 $2：端口号
日志等级	6
举例	RBM/6/RBM_CHANNEL_BIND_FAILED: -Context=1; Failed to bind IP address 1.1.1.2 and port 50001 to the RBM channel.
日志说明	高可靠性控制通道服务端绑定IP地址和端口号失败，服务端口号已被其他应用占用
处理建议	绑定端口失败后，建议更改控制通道服务端的Lcoal IP地址或Remote IP地址中的端口号

133 RDDC

本节介绍 RDDC（redundancy）模块输出的日志信息。

133.1 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

134 REPUTATION

本节介绍 IP 信誉、域名信誉和 URL 信誉模块输出的快速日志信息。

134.1 REPUTATION_MATCH_IPV4_LOG

日志内容	MsgId(1197)=[STRING];UserName(1113)=[STRING];SrcMacAddr(1021)=[MacAddr];DstMacAddr(1022)=[MacAddr];SrcIPAddr(1003)=[IPAddr];SrcPort(1004)=[UINT16];DstIPAddr(1007)=[IPAddr];DstPort(1008)=[UINT16];Protocol(1001)=[UCHAR];CriticalLevel(1202)=[UINT16];IOC(1198)=[STRING];EvilType(1199)=[STRING];VirusFamilyName(1200)=[STRING];EvilId(1201)=[STRING];Action(1053)=[STRING];AtkDirection(1134)=[STRING];PolicyName(1079)=[STRING];
参数解释	$1：信誉类型，包括如下取值： • DOMAINREPUTATION：表示域名信誉 • IPREPUTATION：表示 IP 信誉 • URLREPUTATION：表示 URL 信誉 $2：用户名 $3：源MAC地址 $4：目的MAC地址 $5：源IP地址 $6：源端口 $7：目的IP地址 $8：目的端口 $9：协议类型 $10：严重级别，取值范围为0～10，数值越大严重级别越高 $11：情报IOC $12：攻击分类名称 $13：病毒家族名称 $14：攻击分类ID $15：动作名称，包括如下取值： • block-source：表示阻断报文，并将该报文的源 IP 地址加入 IP 黑名单。 • drop：表示丢弃报文。 • permit：表示允许报文通过。 • redirect：表示重定向动作，把符合特征的报文重定向到指定的 Web 页面上。 • reset：表示通过发送 TCP 的 reset 报文从而使 TCP 连接断开。 $16：匹配方向，包括如下取值（仅IP信誉支持显示取值）： • Source：源地址 • Destination：目的地址 $17：策略名称（仅URL信誉支持显示取值）
日志等级	6
举例	REPUT/6/REPUTATION_MATCH_IPV4_LOG:MsgId(1197)=IPREPUTATION;UserName(1113)=admin;SrcMacAddr(1021)=dc2d-cbf7-9454;DstMacAddr(1022)=dc2d-cbf7-9455;SrcIPAddr(1003)=10.10.10.10;SrcPort(1004)=8080;DstIPAddr(1007)=20.20.20.20;DstPort(1008)=7070;Protocol(1001)=tcp;CriticalLevel(1202)=5;IOC(1198)=10.10.10.10;EvilType(1199)=DDOS|WEB;VirusFamilyName(1200)=VIRUS;EvilId(1201)=5;Action(1053)=drop;AtkDirection(1134)=Source;PolicyName(1079)=a;
日志说明	当报文与信誉特征库（包括IP信誉、URL信誉和域名信誉）匹配成功时会生成一条日志
处理建议	无

134.2 REPUTATION_MATCH_IPV6_LOG

日志内容	MsgId(1197)=[STRING];UserName(1113)=[STRING];SrcMacAddr(1021)=[MacAddr];DstMacAddr(1022)=[MacAddr];SrcIPv6Addr(1036)=[IPAddr];SrcPort(1004)=[UINT16];DstIPv6Addr(1037)=[IPAddr];DstPort(1008)=[UINT16];Protocol(1001)=[UCHAR];CriticalLevel(1202)=[UINT16];IOC(1198)=[STRING];EvilType(1199)=[STRING];VirusFamilyName(1200)=[STRING];EvilId(1201)=[STRING];Action(1053)=[STRING];AtkDirection(1134)=[STRING];PolicyName(1079)=[STRING];
参数解释	$1：信誉类型，包括如下取值： • DOMAINREPUTATION：表示域名信誉 • IPREPUTATION：表示 IP 信誉 • URLREPUTATION：表示 URL 信誉 $2：用户名 $3：源MAC地址 $4：目的MAC地址 $5：源IPv6地址 $6：源端口 $7：目的IPv6地址 $8：目的端口 $9：协议类型 $10：严重级别，取值范围为0～10，数值越大严重级别越高 $11：情报IOC $12：攻击分类名称 $13：病毒家族名称 $14：攻击分类ID $15：动作名称，包括如下取值： • block-source：表示阻断报文，并将该报文的源 IP 地址加入 IP 黑名单。 • drop：表示丢弃报文。 • permit：表示允许报文通过。 • redirect：表示重定向动作，把符合特征的报文重定向到指定的 Web 页面上。 • reset：表示通过发送 TCP 的 reset 报文从而使 TCP 连接断开。 $16：匹配方向，包括如下取值（仅IP信誉支持显示取值）： • Source：源地址 • Destination：目的地址 $17：策略名称（仅URL信誉支持显示取值）
日志等级	6
举例	REPUT/6/REPUTATION_MATCH_IPV6_LOG:MsgId(1197)=IPREPUTATION;UserName(1113)=admin;SrcMacAddr(1021)=dc2d-cbf7-9454;DstMacAddr(1022)=dc2d-cbf7-9455;SrcIPv6Addr(1036)=10::1;SrcPort(1004)=8080;DstIPv6Addr(1037)=100::40;DstPort(1008)=7070;Protocol(1001)=tcp;CriticalLevel(1202)=5;IOC(1198)=10::1;EvilType(1199)=DDOS|WEB;VirusFamilyName(1200)=VIRUS;EvilId(1201)=5;Action(1053)=drop;AtkDirection(1134)= Source;PolicyName(1079)=a;
日志说明	当报文与信誉特征库（包括IP信誉、URL信誉和域名信誉）匹配成功时会生成一条日志
处理建议	无

135 RIP

本节介绍 RIP 模块输出的日志信息。

135.1 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

135.2 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	6
举例	RIP/6/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

136 RIPNG

本节介绍 RIPng 模块输出的日志信息。

136.1 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

136.2 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	6
举例	RIPNG/6/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

137 RIR

本节介绍 RIR 模块输出的日志信息。

137.1 RIR_BANDWIDTH_TOMAXIMUM

日志内容	-Tunnel=[UINT32]-TotalBandwidth=[UINT64] kbps-UsedBandwidth=[UINT64] kbps. The bandwidth of the link has been fully occupied.
参数解释	$1：Tunnel接口编号 $2：Tunnel接口总带宽 $3：Tunnel接口已使用带宽
日志等级	6
举例	RIR/6/RIR_BANDWIDTH_TOMAXIMUM: -Tunnel=1-TotalBandwidth=1000 kbps-UsedBandwidth=1000 kbps. The bandwidth of the link has been fully occupied.
日志说明	Tunnel接口的带宽已被全部占用
处理建议	无

137.2 RIR_CFG_CHANGED

日志内容	Configuration changed.
参数解释	无
日志等级	6
举例	RIR/6/RIR_CFG_CHANGED: Configuration changed.
日志说明	配置发生变化，包括： • 链路编号和链路类型的配置变更 • 链路优先级和主备关系的配置变更 • 会话预计使用带宽的配置变更 • 导致链路质量由满足业务要求变为不满足业务要求，或由不满足业务要求变为满足业务要求的 SLA 配置变更等
处理建议	无

137.3 RIR_LINK_SELECT

日志内容	-SrcIPAddr=[IPADDR]-SrcPort=[UINT16]-DstIPAddr=[IPADDR]-DstPort=[UINT16]-Protocol=[STRING]-FlowID=[UINT32]. Selected tunnel [UINT32] for the session.
参数解释	$1：会话的源IP地址 $2：会话的源端口号 $3：会话的目的IP地址 $4：会话的目的端口号 $5：会话的协议类型，包括： • TCP • UDP • ICMP • IPv4 • Other：其他协议类型 $6：会话所属的业务流量模板编号 $7：会话选择的Tunnel接口编号
日志等级	6
举例	RIR/6/RIR_LINK_SELECT: -SrcIPAddr=55.1.1.2-SrcPort=51457-DstIPAddr=11.1.1.1-DstPort=8-Protocol=ICMP-FlowID=1. Selected tunnel 1 for the session.
日志说明	通过智能选路机制为会话选择链路
处理建议	无

137.4 RIR_LINKFAULT

日志内容	Link fault for tunnel [UINT32].
参数解释	$1：Tunnel接口编号
日志等级	6
举例	RIR/6/RIR_LINKFAULT: Link fault for tunnel 1.
日志说明	设备通过NQA链路通断探测检测出某链路为链路断开，或者链路处于Down状态
处理建议	无

137.5 RIR_QUALITY_DELAY

日志内容	-FlowID=[UINT32]-Tunnel=[UINT32]-DetectedDelay=[UINT32] ms-DelayThreshold=[UINT32] ms. The link became unqualified because the link delay detected by NQA was higher than the link delay threshold in the SLA.
参数解释	$1：业务流量模板编号 $2：Tunnel接口编号 $3：NQA探测出的链路时延 $4：SLA的链路时延阈值
日志等级	6
举例	RIR/6/RIR_QUALITY_DELAY: -FlowID=2-Tunnel=1-DetectedDelay=100 ms-DelayThreshold=50 ms. The link became unqualified because the link delay detected by NQA was higher than the link delay threshold in the SLA.
日志说明	由于链路时延的NQA探测值大于相应SLA的阈值，链路质量不满足业务要求
处理建议	无

137.6 RIR_QUALITY_JITTER

日志内容	-FlowID=[UINT32]-Tunnel=[UINT32]-DetectedJitter=[UINT32] ms-JitterThreshold=[UINT32] ms. The link became unqualified because the link jitter was higher than the jitter threshold in the SLA.
参数解释	$1：业务流量模板编号 $2：Tunnel接口编号 $3：NQA探测出的链路抖动 $4：SLA的链路抖动阈值
日志等级	6
举例	RIR/6/RIR_QUALITY_JITTER: -FlowID=2-Tunnel=1-DetectedJitter=100 ms-JitterThreshold=50 ms. The link became unqualified because the link jitter was higher than the jitter threshold in the SLA.
日志说明	由于链路抖动的NQA探测值大于相应SLA的阈值，链路质量不满足业务要求
处理建议	无

137.7 RIR_QUALITY_OTHER

日志内容	-FlowID=[UINT32]-Tunnel=[UINT32]. The link became unqualified because of a reason other than failing to meet the thresholds in the SLA.
参数解释	$1：业务流量模板编号 $2：Tunnel接口编号
日志等级	6
举例	RIR/6/RIR_QUALITY_OTHER: -FlowID=2-Tunnel=1. The link became unqualified because of a reason other than failing to meet the thresholds in the SLA.
日志说明	非链路质量探测值不满足SLA阈值导致的链路质量不满足要求，如Hub站点与Spoke站点的SLA阈值配置不一致
处理建议	无

137.8 RIR_QUALITY_PKTLOSS

日志内容	-FlowID=[UINT32]-Tunnel=[UINT32]-DetectedPktLoss=[UINT32]‰-PktLossThreshold=[UINT32]‰. The link became unqualified because the packet loss ratio detected by NQA was higher than the packet loss threshold in the SLA.
参数解释	$1：业务流量模板编号 $2：Tunnel接口编号 $3：NQA探测出的链路丢包率 $4：SLA的链路丢包率阈值
日志等级	6
举例	RIR/6/RIR_QUALITY_PKTLOSS: -FlowID=2-Tunnel=1-DetectedPktLoss=100‰-PktLossThreshold=50‰. The link became unqualified because the packet loss ratio detected by NQA was higher than the packet loss threshold in the SLA.
日志说明	由于链路丢包率的NQA探测值大于相应SLA的阈值，链路质量不满足业务要求
处理建议	无

138 RM

本节介绍 RM 模块输出的日志信息。

138.1 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

138.2 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

138.3 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

139 RPR

本节介绍 RPR 模块输出的日志信息。

139.1 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

139.2 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

139.3 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

139.4 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

139.5 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

139.6 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

139.7 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

139.8 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

139.9 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

139.10 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

139.11 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

139.12 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

139.13 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

139.14 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

139.15 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

139.16 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

139.17 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

139.18 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

139.19 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

139.20 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

139.21 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

139.22 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

140 RRPP

本节介绍 RRPP 模块输出的日志信息。

140.1 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

140.2 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

141 RTM

本节介绍 EAA 功能的 RTM（Real-Time Management）模块输出的日志信息。

141.1 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

141.2 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

141.3 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

142 SANDBOX

本节介绍沙箱模块输出的快速日志信息。

142.1 SANDBOX_DETECTION_IPV4_LOG

日志内容	SandboxType(1143)=[STRING];FileType(1096)=[STRING];FileName(1097)=[STRING];Protocol(1001)=[STRING];Application(1002)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];UserName(1113)=[STRING];TrtType(1144)=[STRING];Severity(1087)=[STRING];MD5(1129)=[STRING];BeginTime_c(1011)=[STRING];ThreatDir(1170)=[UINT16];AttackName(1088)=[STRING];ThreatAct(1171)=[STRING];ThreatFmly(1172)=[UINT16];StatusCode(1167)=[STRING];ThreatHttpContentLen(1173)=[STRING];RealSrcIP(1100)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
参数解释	$1：沙箱类型，包括如下取值： • AV • Windows • Win64 • WEB • Office $2：文件类型 $3：文件名称 $4：协议类型 $5：应用协议名称 $6：源IP地址 $7：源端口号 $8：目的IP地址 $9：目的端口号 $10：源安全域名称 $11：目的安全域名称 $12：身份识别用户的名称 $13：威胁类型，包括如下取值： • UNKNOWN：未知威胁 • KNOWN：已知威胁 • NORMAL：正常，表示文件不存在威胁 $14：严重级别，包括如下取值： • NOTHREAT：无威胁 • LOW：低 • MEDIUM：中 • HIGH：高 $15：MD5值 $16：沙箱检测日志生成的时间 $17：文件传输方向，包括如下取值： • download：从服务端到客户端 • upload：从客户端到服务端 $18：威胁名称 $19：威胁行为，具体取值请参见“表142-1”（威胁行为取值与沙箱的软件版本有关，表格中以ESS 6701版本为例）

	$20：威胁分类，具体取值请参见“表142-2” $21：HTTP/HTTPS应答报文状态码 $22：HTTP/HTTPS报文Content-Length字段值 $23：真实源IP地址 $24：VLAN ID $25：VXLAN ID $26：源地区 $27：目的地区
日志等级	6
举例	SANDBOX/6/SANDBOX_DETECTION_IPV4_LOG:SandboxType(1143)=WEB;FileType(1096)=exe;FileName(1097)=abc.exe;Protocol(1001)=TCP;Application(1002)=http;SrcIPAddr(1003)=192.168.7.15;SrcPort(1004)=4790;DstIPAddr(1007)=192.168.15.252;DstPort(1008)=80;SrcZoneName(1025)=spf;DstZoneName(1035)=spf;UserName(1113)=abc;TrtType(1144)=UNKNOWN;Severity(1087)=HIGH;MD5(1129)=c4ab18ce0dbd4c911ae501753d0bda89;BeginTime_c(1011)=20180320091510;ThreatDir(1170)=download;AttackName(1088)=;ThreatAct(1171)=;ThreatFmly(1172)=0;StatusCode(1167)=200;ThreatHttpContentLen(1173)=22087;RealSrcIP(1100)=2.2.2.2,3.2.2.2,3.2.2.2,2.2.2.2,2.2.2.2,2.2.2.2,2.2.2.2,2.2.2.2,2.2.2.2,3.3.3.2;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
日志说明	当沙箱检测日志产生时输出该日志
处理建议	无

142.2 SANDBOX_DETECTION_IPV6_LOG

日志内容	SandboxType(1143)=[STRING];FileType(1096)=[STRING];FileName(1097)=[STRING];Protocol(1001)=[STRING];Application(1002)=[STRING];SrcIPv6Addr(1036)=[IPADDR];SrcPort(1004)=[UINT16];DstIPv6Addr(1037)=[IPADDR];DstPort(1008)=[UINT16];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];UserName(1113)=[STRING];TrtType(1144)=[STRING];Severity(1087)=[STRING];MD5(1129)=[STRING];BeginTime_c(1011)=[STRING];ThreatDir(1170)=[UINT16];AttackName(1088)=[STRING];ThreatAct(1171)=[STRING];ThreatFmly(1172)=[UINT16];StatusCode(1167)=[STRING];ThreatHttpContentLen(1173)=[STRING];RealSrcIP(1100)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
参数解释	$1：沙箱类型，包括如下取值： • AV • Windows • Win64 • WEB • Office $2：文件类型 $3：文件名称 $4：协议类型 $5：应用协议名称 $6：源IPv6地址 $7：源端口号 $8：目的IPv6地址 $9：目的端口号 $10：源安全域名称 $11：目的安全域名称 $12：身份识别用户的名称 $13：威胁类型，包括如下取值： • UNKNOWN：未知威胁 • KNOWN：已知威胁 • NORMAL：正常，表示文件不存在威胁 $14：严重级别，包括如下取值： • NOTHREAT：无威胁 • LOW：低 • MEDIUM：中 • HIGH：高 $15：MD5值 $16：沙箱检测日志产生的时间 $17：文件传输方向，包括如下取值： • download：从服务端到客户端 • upload：从客户端到服务端 $18：威胁名称 $19：威胁行为，具体取值请参见“表142-1”（威胁行为取值与沙箱的软件版本有关，表格中以ESS 6701版本为例）

	$20：威胁分类，具体取值请参见“表142-2” $21：HTTP/HTTPS应答报文状态码 $22：HTTP/HTTPS报文Content-Length字段值 $23：真实源IP地址 $24：VLAN ID $25：VXLAN ID $26：源地区 $27：目的地区
日志等级	6
举例	SANDBOX/6/SANDBOX_DETECTION_IPV6_LOG:SandboxType(1143)=WEB;FileType(1096)=exe;FileName(1097)=abc.exe;Protocol(1001)=TCP;Application(1002)=http;SrcIPv6Addr(1036)=100::40;SrcPort(1004)=4790;DstIPv6Addr(1037)=200::40;DstPort(1008)=80;SrcZoneName(1025)=spf;DstZoneName(1035)=spf;UserName(1113)=abc;TrtType(1144)=UNKNOWN;Severity(1087)=HIGH;MD5(1129)=c4ab18ce0dbd4c911ae501753d0bda89;BeginTime_c(1011)=20180320091510;ThreatDir(1170)=download;AttackName(1088)=;ThreatAct(1171)=;ThreatFmly(1172)=0;StatusCode(1167)=200;ThreatHttpContentLen(1173)=22087;RealSrcIP(1100)=3::3;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
日志说明	当沙箱检测日志产生时输出该日志
处理建议	无

表142-1 威胁行为取值对应表

ID	威胁行为
1	设置开机自启动行为
2	包含远程注入其他进程行为
3	设置降低防火墙安全级别，或者加入白名单
4	设置绕过UAC，提升自身到管理员权限行为
5	禁用修改系统保护机制
6	检测系统中是否安装或运行杀软
7	检测自身是否在沙箱中运行，或者被调试器调试
8	有自己删除本地文件的行为
9	有DLL劫持或者映像劫持行为
10	替换自身为windows自带的exe或dll文件
11	文件名和系统关键进程相近，假冒关键进程
12	感染现有PE文件
13	加载驱动程序
14	修改IE安全策略
15	添加修改windows账号
16	添加修改windows服务
17	文档类进程有可疑网络连接行为
18	文档类进程创建可疑进程释放可疑文件
19	文档类释放可执行程序
20	自动关机重启注销
21	PE文件执行释放文档脚本类文件
22	修改host文件
23	Hook程序关键函数，修改程序流程
24	提升程序本身权限
25	脚本文件调用powershell行为
26	脚本文件恶意网络行为
27	访问敏感文件如浏览器的用户名密码文件
28	Android软件话费吸取
29	Android软件恶意广告
30	Android软件窃取隐私
31	文件类型欺骗

ID	威胁行为
32	修改文件隐藏属性
33	可执行文件恶意的网络行为
34	恶意的快捷方式文件
35	可疑的宏文件
200	病毒
201	间谍木马
202	蠕虫
203	后门
204	勒索软件
205	downloader
206	广告
207	脚本病毒
208	恶意漏洞文件
209	病毒生成器
210	加壳软件
211	启发式行为
212	风险工具
213	网络钓鱼
214	宏病毒
215	其他威胁类型

表142-2 威胁分类取值对应表

ID	威胁行为
0	其它
1	病毒
2	木马
3	蠕虫
4	后门
5	勒索软件
6	下载器
7	广告
8	脚本
9	宏病毒
10	恶意漏洞文件
11	网络钓鱼
12	风险工具
13	加壳软件
14	启发式行为
15	数字货币
16	僵尸网络
17	APT情报
18	DGA恶意域名

143 SCD

本节介绍 SCD（Server Connection Detection，服务器外联防护）模块输出的日志信息。

143.1 SCD_IPV4

日志内容	Protocol(1001)=[STRING];ServerIPAddr(1003)=[STRING];DstIPAddr(1007)=[STRING];DstPort(1008)=[STRING]; Illegal server connection.
参数解释	$1：协议类型 $2：服务器IP地址 $3：外联IP地址 $4：外联端口
日志等级	6
举例	SCD/6/SCD_IPV4:-Context=1;Protocol(1001)=TCP;ServerIPAddr(1003)=192.168.105.1;DstIPAddr(1007)=192.168.105.111;DstPort(1008)=80; Illegal server connection.
日志说明	检测到服务器与非法的外联地址建立连接
处理建议	请查看连接信息，根据业务决定是否允许服务器与此外联地址建立连接。若需要拒绝，请采取有效措施（如配置安全策略阻断此连接）

144 SCMD

本节介绍 SCM（服务控制管理）模块输出的日志信息。

144.1 PROCESS_ABNORMAL

日志内容	The process [STRING] exited abnormally. ServiceName=[STRING], ExitCode=[STRING], KillSignal=[STRING], StartTime=[STRING], StopTime=[STRING].
参数解释	$1：进程名 $2：进程脚本里定义的服务名 $3：进程退出码，取值为： • 数字表示进程退出码 • NA 表示无退出码，进程被信号关闭 $4：关闭进程的信号，取值为： • 数字表示关闭进程的信号的数值 • NA 表示没有关闭信号，进程主动退出，并非被信号关闭 $5：进程的创建时间 $6：进程的关闭时间
日志等级	4
举例	SCMD/4/PROCESS_ABNORMAL: The process diagd exited abnormally. ServiceName=DIAG, ExitCode=1, KillSignal=NA, StartTime=2019-03-06 14:18:06, StopTime=2019-03-06 14:35:25.
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： 3. 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 4. 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 5. 如果进程已恢复，但仍需要定位进程异常退出的原因，请执行第二步 6. 当使用 FTP 功能将文件上传到服务器时，请使用 binary 传输模式

144.2 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	SCMD/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

144.3 PROCESS_CORERECORD

日志内容	Exceptions occurred with process [STRING]. A core dump file was generated.
参数解释	$1：进程名
日志等级	4
举例	SCMD/4/PROCESS_CORERECORD: Exceptions occurred with process diagd. A core dump file was generated.
日志说明	进程异常退出产生了core文件。core文件用于记录进程异常退出时的相关信息，以便定位
处理建议	1. 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 2. 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 3. 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，以便工程师进一步分析定位 4. 当使用 FTP 功能将文件上传到服务器时，请使用 binary 传输模式

144.4 SCM_ABNORMAL_REBOOT

日志内容	Failed to restore process [STRING]. Reboot [STRING].
参数解释	$1：进程名 $2：chassis编号+slot编号或slot编号或the system
日志等级	3
举例	SCMD/3/SCM_ABNORMAL_REBOOT: Failed to restore process ipbased. Reboot slot 1.
日志说明	进程在设备/slot启动过程中，异常退出，尝试自动重启多次后，仍不能恢复，则自动重启设备/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

144.5 SCM_ABNORMAL_REBOOTMDC

日志内容	Failed to restore process [STRING] on [STRING] [UINT16]. Rebooting [STRING] [UINT16].
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	SCMD/3/SCM_ABNORMAL_REBOOTMDC: Failed to restore process ipbased on MDC 2. Rebooting MDC 2.
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

144.6 SCM_ABORT_RESTORE

日志内容	Failed to restore process [STRING]. Restoration aborted.
参数解释	$1：进程名
日志等级	3
举例	SCMD/3/SCM_ABORT_RESTORE: Failed to restore process ipbased. Restoration aborted.
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

144.7 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	SCMD/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

144.8 SCM_KERNEL_INIT_TOOLONG

日志内容	Kernel init in sequence [STRING] function [STRING] is still starting for [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	SCMD/4/SCM_KERNEL_INIT_TOOLONG: Kernel init in sequence 0x25e7 function 0x6645ffe2 is still starting for 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

144.9 SCM_KILL_PROCESS

日志内容	形式一： The process [STRING] was killed because it failed to stop within [STRING]. 形式二： The process [STRING] on [STRING] [UINT16] was killed because it failed to stop within [STRING].
参数解释	形式一： $1：进程名 $2：进程收到停止信号到打印该日志的时间 形式二： $1：进程名 $2：取值为MDC或context $3：MDC或context的编号 $4：进程收到停止信号到打印该日志的时间
日志等级	6
举例	SCMD/6/SCM_KILL_PROCESS: The process stamgrd was killed because it failed to stop within 30 minutes.
日志说明	某进程超过一定时间没按照指令正常停止，则系统会强制杀掉该进程
处理建议	1. 系统/MDC/Context 稳定后，使用 display process 命令查看进程是否恢复 2. 联系工程师解决

144.10 SCM_PROCESS_STARTING_TOOLONG

日志内容	形式一： The process [STRING] has not finished starting in [UINT32] hours. 形式二： The process [STRING] on [STRING] [UINT16] has not finished starting in [UINT32] hours.
参数解释	形式一： $1：进程名 $2：所用时间 形式二： $1：进程名 $2：取值为MDC或Context $3：MDC或Context的编号 $4：所用时间
日志等级	4
举例	SCMD/4/ SCM_PROCESS_STARTING_TOOLONG: The process ipbased 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

144.11 SCM_PROCESS_STILL_STARTING

日志内容	形式一： The process [STRING] is still starting for [UINT32] minutes. 形式二： The process [STRING] on [STRING] [UINT16] is still starting for [UINT32] minutes.
参数解释	形式一： $1：进程的名称 $2：所用时间 形式二： $1：进程的名称 $2：取值为MDC或Context $3：MDC或Context编号 $4：所用时间
日志等级	6
举例	SCMD/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	无

144.12 SCM_SKIP_PROCESS

日志内容	形式一： The process [STRING] was skipped because it failed to start within 6 hours. 形式二： The process [STRING] on [STRING] [UINT16] was skipped because it failed to start within 6 hours.
参数解释	形式一： $1：进程名 形式二： $1：进程名 $2：取值为MDC或context $3：MDC或context的编号
日志等级	3
举例	SCMD/3/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

145 SCRLSP

本节介绍静态 CRLSP 模块输出的日志信息。

145.1 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

146 SECDIAG

本节介绍 SECDIAG（安全诊断）模块输出的日志信息。

146.1 MONITOR_CONCURRENCY_EXCEED

日志内容	Number of concurrent sessions reached the threshold [STRING] on [STRING].
参数解释	$1：会话连接数的阈值 $2：单板所在的槽位号，形如slot xx；如果该slot支持多CPU，则形如slot xx cpu xx（分布式设备－独立运行模式） $2：设备在IRF中的成员编号，形如slot xx；如果该slot支持多CPU，则形如slot xx cpu xx（集中式IRF设备） $2：单板在IRF中的槽位号，形如chassis xx slot xx；如果该slot支持多CPU，则形如chassis xx slot xx cpu xx（分布式设备－IRF模式）
日志等级	1
举例	SECDIAG/1/MONITOR_CONCURRENCY_EXCEED: Number of concurrent sessions reached the threshold 3000 on slot 1.（分布式设备－独立运行模式）（集中式IRF设备）
日志说明	设备上的会话连接数达到了告警阈值
处理建议	适当减少会话连接数，或扩容设备

146.2 MONITOR_CONCURRENCY_BELOW

日志内容	Number of concurrent sessions dropped below the threshold on [STRING].
参数解释	$1：单板所在的槽位号，形如slot xx；如果该slot支持多CPU，则形如slot xx cpu xx（分布式设备－独立运行模式） $1：设备在IRF中的成员编号，形如slot xx；如果该slot支持多CPU，则形如slot xx cpu xx（集中式IRF设备） $1：单板在IRF中的槽位号，形如chassis xx slot xx；如果该slot支持多CPU，则形如chassis xx slot xx cpu xx（分布式设备－IRF模式）
日志等级	1
举例	SECDIAG/1/MONITOR_CONCURRENCY_BELOW: Number of concurrent sessions dropped below the threshold on slot 3 CPU 1.（分布式设备－独立运行模式）（集中式IRF设备）
日志说明	会话连接数降到阈值以下
处理建议	无

146.3 MONITOR_CONNECTION_EXCEED

日志内容	Session establishment rate reached the threshold [STRING] on [STRING].
参数解释	$1：会话新建速率的阈值 $2：单板所在的槽位号，形如slot xx；如果该slot支持多CPU，则形如slot xx cpu xx（分布式设备－独立运行模式） $2：设备在IRF中的成员编号，形如slot xx；如果该slot支持多CPU，则形如slot xx cpu xx（集中式IRF设备） $2：单板在IRF中的槽位号，形如chassis xx slot xx；如果该slot支持多CPU，则形如chassis xx slot xx cpu xx（分布式设备－IRF模式）
日志等级	1
举例	SECDIAG/1/MONITOR_CONNECTION_EXCEED: Session establishment rate reached the threshold 600 on slot 3 CPU 1.（分布式设备－独立运行模式）（集中式IRF设备）
日志说明	设备上的会话新建速率达到了告警阈值
处理建议	适当减少会话新建数，或扩容设备

146.4 MONITOR_CONNECTION_BELOW

日志内容	Session establishment rate dropped below the threshold on [STRING].
参数解释	$1：单板所在的槽位号，形如slot xx；如果该slot支持多CPU，则形如slot xx cpu xx（分布式设备－独立运行模式） $1：设备在IRF中的成员编号，形如slot xx；如果该slot支持多CPU，则形如slot xx cpu xx（集中式IRF设备） $1：单板在IRF中的槽位号，形如chassis xx slot xx；如果该slot支持多CPU，则形如chassis xx slot xx cpu xx（分布式设备－IRF模式）
日志等级	1
举例	SECDIAG/1/MONITOR_CONNECTION_BELOW: Session establishment rate dropped below the threshold on slot 3 CPU 1.（分布式设备－独立运行模式）（集中式IRF设备）
日志说明	会话新建速率降到阈值以下
处理建议	无

146.5 MONITOR_SECP_IPV4_EXCEED

日志内容	Number of IPv4 security policy rules reached the threshold [STRING].
参数解释	$1：IPv4安全策略规则数量的阈值
日志等级	1
举例	SECDIAG/1/MONITOR_SECP_IPV4_EXCEED: Number of IPv4 security policy rules reached the threshold 500.
日志说明	设备上创建的IPv4安全策略规则的数量达到了告警阈值
处理建议	适当减少IPv4安全策略规则的数量，或扩容设备

146.6 MONITOR_SECP_IPV4_BELOW

日志内容	Number of IPv4 security policy rules dropped below the threshold.
参数解释	无
日志等级	1
举例	SECDIAG/1/MONITOR_SECP_IPV4_BELOW: Number of IPv4 security policy rules dropped below the threshold.
日志说明	IPv4安全策略规则的数量降到阈值以下
处理建议	无

146.7 MONITOR_SECP_IPV6_EXCEED

日志内容	Number of IPv6 security policy rules reached the threshold [STRING].
参数解释	$1：IPv6安全策略规则数量的阈值
日志等级	1
举例	SECDIAG/1/MONITOR_SECP_IPV6_EXCEED: Number of IPv6 security policy rules reached the threshold 200.
日志说明	设备上创建的IPv6安全策略规则的数量达到了告警阈值
处理建议	适当减少IPv6安全策略的数量，或扩容设备

146.8 MONITOR_SECP_IPV6_BELOW

日志内容	Number of IPv6 security policy rules dropped below the threshold.
参数解释	无
日志等级	1
举例	SECDIAG/1/MONITOR_SECP_IPV6_BELOW: Number of IPv6 security policy rules dropped below the threshold.
日志说明	IPv6安全策略规则的数量降到阈值以下
处理建议	无

146.9 MONITOR_CONTEXT_EXCEED

日志内容	Number of contexts reached the threshold [STRING].
参数解释	$1：Context数的阈值
日志等级	1
举例	SECDIAG/1/MONITOR_CONTEXT_EXCEED: Number of contexts reached the threshold 60.
日志说明	设备上新建Context的数量达到了告警阈值
处理建议	适当减少Context的数量，或扩容设备

146.10 MONITOR_CONTEXT_BELOW

日志内容	Number of created contexts dropped below the threshold.
参数解释	无
日志等级	1
举例	SECDIAG/1/MONITOR_CONTEXT_BELOW: Number of created contexts dropped below the threshold.
日志说明	Context的数量降到阈值以下
处理建议	无

146.11 MONITOR_NAT_EXCEED

日志内容	Number of NAT server mappings and static NAT mappings reached the threshold [STRING].
参数解释	$1：NAT条目数的阈值
日志等级	1
举例	SECDIAG/1/MONITOR_NAT_EXCEED: Number of NAT server mappings and static NAT mappings reached the threshold 200.
日志说明	设备上配置的NAT条目数达到了告警阈值
处理建议	适当减少NAT条目数，或扩容设备

146.12 MONITOR_NAT_BELOW

日志内容	Number of NAT server mappings and static NAT mappings dropped below the threshold.
参数解释	无
日志等级	1
举例	SECDIAG/1/MONITOR_NAT_BELOW: Number of NAT server mappings and static NAT mappings dropped below the threshold.
日志说明	NAT条目数降到阈值以下
处理建议	无

146.13 MONITOR_BAGG_EXCEED

日志内容	Number of Layer 2 aggregate interfaces reached the threshold [STRING].
参数解释	$1：二层聚合接口数的阈值
日志等级	1
举例	SECDIAG/1/MONITOR_BAGG_EXCEED: Number of Layer 2 aggregate interfaces reached the threshold 20.
日志说明	设备上创建的二层聚合接口的数量达到了告警阈值
处理建议	适当减少二层聚合接口的数量，或扩容设备

146.14 MONITOR_BAGG_BELOW

日志内容	Number of Layer 2 aggregate interfaces dropped below the threshold.
参数解释	无
日志等级	1
举例	SECDIAG/1/MONITOR_BAGG_BELOW: Number of Layer 2 aggregate interfaces dropped below the threshold.
日志说明	二层聚合接口的数量降到阈值以下
处理建议	无

146.15 MONITOR_RAGG_EXCEED

日志内容	Number of Layer 3 aggregate interfaces reached the threshold [STRING].
参数解释	$1：三层聚合接口数的阈值
日志等级	1
举例	SECDIAG/1/MONITOR_RAGG_EXCEED: Number of Layer 3 aggregate interfaces reached the threshold 10.
日志说明	设备上创建的三层聚合接口的数量达到了告警阈值
处理建议	适当减少三层聚合接口的数量，或扩容设备

146.16 MONITOR_RAGG_BELOW

日志内容	Number of Layer 3 aggregate interfaces dropped below the threshold.
参数解释	无
日志等级	1
举例	SECDIAG/1/MONITOR_RAGG_BELOW: Number of Layer 3 aggregate interfaces dropped below the threshold.
日志说明	三层聚合接口的数量降到阈值以下
处理建议	无

146.17 MONITOR_BLADE_THROUGHPUT_EXCEED

日志内容	Total throughput of blade interfaces reached the threshold [STRING] on [STRING].
参数解释	$1：内联口吞吐量的阈值 $2：单板所在的槽位号，形如slot xx；如果该slot支持多CPU，则形如slot xx cpu xx（分布式设备－独立运行模式） $2：设备在IRF中的成员编号，形如slot xx；如果该slot支持多CPU，则形如slot xx cpu xx（集中式IRF设备） $2：单板在IRF中的槽位号，形如chassis xx slot xx；如果该slot支持多CPU，则形如chassis xx slot xx cpu xx（分布式设备－IRF模式）
日志等级	1
举例	SECDIAG/1/MONITOR_BLADE_THROUGHPUT_EXCEED: Total throughput of blade interfaces reached the threshold 1500 on slot 3 CPU 1.（分布式设备－独立运行模式）（集中式IRF设备）
日志说明	内联口的吞吐量达到了告警阈值
处理建议	适当减少内联口的吞吐量，或扩容设备

146.18 MONITOR_BLADE_THROUGHPUT_BELOW

日志内容	Total throughput of blade interfaces dropped below the threshold on [STRING].
参数解释	$1：单板所在的槽位号，形如slot xx；如果该slot支持多CPU，则形如slot xx cpu xx（分布式设备－独立运行模式） $1：设备在IRF中的成员编号，形如slot xx；如果该slot支持多CPU，则形如slot xx cpu xx（集中式IRF设备） $1：单板在IRF中的槽位号，形如chassis xx slot xx；如果该slot支持多CPU，则形如chassis xx slot xx cpu xx（分布式设备－IRF模式）
日志等级	1
举例	SECDIAG/1/MONITOR_BLADE_THROUGHPUT_BELOW: Total throughput of blade interfaces dropped below the threshold on slot 3 CPU 1.（分布式设备－独立运行模式）（集中式IRF设备）
日志说明	内联口的吞吐量降到阈值以下
处理建议	无

146.19 MONITOR_QACL_EXCEED

日志内容	QACL usage reached the threshold [STRING] on [STRING]: Total slices=[STRING], Remaining single slices=[STRING], Remaining double slices=[STRING], Remaining MQC entries=[STRING], Remaining OpenFlow entries=[STRING].
参数解释	$1：QACL资源使用率阈值 $2：单板所在的槽位号，形如slot xx cpu xx core xx（分布式设备－独立运行模式） $2：设备在IRF中的成员编号，形如slot xx cpu xx core xx（集中式IRF设备） $2：单板在IRF中的槽位号，形如chassis xx slot xx cpu xx core xx（分布式设备－IRF模式）
日志等级	1
举例	SECDIAG/1/MONITOR_QACL_EXCEED: QACL usage reached the threshold 80 on slot 5 CPU 1 core 2: Total slices=10. Remaining single slices=1. Remaining double slices=0. Remaining MQC entries=512. Remaining OpenFlow entries=256.（分布式设备－独立运行模式）（集中式IRF设备）
日志说明	QACL资源使用率的百分比达到了告警阈值
处理建议	适当减少QACL资源使用率，或扩容设备

146.20 MONITOR_QACL_BELOW

日志内容	QACL usage dropped below the threshold on [STRING].
参数解释	$1：单板所在的槽位号，形如slot xx cpu xx core xx（分布式设备－独立运行模式） $1：设备在IRF中的成员编号，形如slot xx cpu xx core xx（集中式IRF设备） $1：单板在IRF中的槽位号，形如chassis xx slot xx cpu xx core xx（分布式设备－IRF模式）
日志等级	1
举例	SECDIAG/1/MONITOR_QACL_BELOW: QACL usage dropped below the threshold on slot 5 CPU 1 core 2.（分布式设备－独立运行模式）（集中式IRF设备）
日志说明	QACL资源使用率降到阈值以下
处理建议	无

146.21 MONITOR_BANDWIDTH_EXCEED

日志内容	Inbound traffic exceeded the total bandwidth usage threshold [STRING] Mbps.
参数解释	$1：整机带宽阈值门限
日志等级	1
举例	SECDIAG/1/MONITOR_BANDWIDTH_EXCEED: Inbound traffic exceeded the total bandwidth usage threshold 100 Mbps
日志说明	设备入方向流量在持续时间内一直大于或等于带宽告警阈值
处理建议	适当减少或分担整机流量

146.22 MONITOR_BANDWIDTH_BELOW

日志内容	Inbound traffic dropped below total bandwidth usage threshold.
参数解释	无
日志等级	1
举例	SECDIAG/1/MONITOR_BANDWIDTH_BELOW: Inbound traffic dropped below total bandwidth usage threshold.
日志说明	设备入方向流量在持续时间内降到带宽告警阈值以下
处理建议	无

147 SECP

本节介绍 SECP（安全策略）模块输出的日志信息。

147.1 SECP_ACCELERATE_NO_RES

日志内容	Failed to accelerate [STRING] security-policy. The resources are insufficient.
参数解释	$1：安全策略版本
日志等级	4
举例	SECP/4/SECP_ACCELERATE_NO_RES: Failed to accelerate IPv6 security-policy. The resources are insufficient.
日志说明	因硬件资源不足，系统加速安全策略失败
处理建议	删除一些规则或者关闭其他安全策略的加速功能，释放硬件资源

147.2 SECP_ACCELERATE_NOT_SUPPORT

日志内容	Failed to accelerate [STRING] security-policy. The operation is not supported.
参数解释	$1：安全策略版本
日志等级	4
举例	SECP/4/SECP_ACCELERATE_NOT_SUPPORT: Failed to accelerate IPv6 security-policy. The operation is not supported.
日志说明	因系统不支持安全策略加速而导致安全策略加速失败
处理建议	无

147.3 SECP_ACCELERATE_UNK_ERR

日志内容	Failed to accelerate [STRING] security-policy.
参数解释	$1：安全策略版本
日志等级	4
举例	SECP/4/SECP_ACCELERATE_UNK_ERR: Failed to accelerate IPv6 security-policy.
日志说明	因系统故障导致安全策略加速失败
处理建议	无

148 SESSION

本节介绍 SESSION 模块输出的日志信息。

148.1 DENY_SESSION_IPV4_FLOW

日志内容	Protocol(1001)=[STRING];Application(1002)=[STRING];Category(1174)=[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：应用协议名称 $3：应用所属服务类型 $4：源IP地址 $5：源端口号 $6：转换后的源IP地址 $7：转换后的源端口号 $8：目的IP地址 $9：目的端口号 $10：转换后的目的IP地址 $11：转换后的目的端口号 $12：入方向的报文总数 $13：入方向的字节总数 $14：出方向的报文总数 $15：出方向的字节总数 $16：源VPN名称 $17：目的VPN名称 $18：源DS-Lite Tunnel $19：目的DS-Lite Tunnel $20：创建会话的时间 $21：会话删除时间 $22：日志类型 $23：日志类型描述信息，包括： • Session created：会话创建日志 • Normal over：正常流结束，会话删除日志 • Aged for timeout：会话老化删除日志 • 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/DENY_SESSION_IPV4_FLOW:Protocol(1001)=UDP;Application(1002)=sip;Category(1174)=aaa;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丢包会话时会发送该日志
处理建议	无

148.2 DENY_SESSION_IPV6_FLOW

日志内容	Protocol(1001)=[STRING];Application(1002)=[STRING];Category(1174)=[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：应用协议名称 $3：应用所属服务类型 $4：源IPv6地址 $5：源端口号 $6：目的IPv6地址 $7：目的端口号 $8：入方向的报文总数 $9：入方向的字节总数 $10：出方向的报文总数 $11：出方向的字节总数 $12：源VPN名称 $13：目的VPN名称 $14：创建会话的时间 $15：会话删除时间 $16：日志类型 $17：日志类型描述信息，包括： • Session created：会话创建日志 • Normal over：正常流结束，会话删除日志 • Aged for timeout：会话老化删除日志 • 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/DENY_SESSION_IPV6_FLOW: Protocol(1001)=UDP;Application(1002)=sip;Category(1174)=aaa;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丢包会话时会发送该日志
处理建议	无

148.3 SESSION_IPV4_FLOW

日志内容	Protocol(1001)=[STRING];Application(1002)=[STRING];Category(1174)=[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：应用协议名称 $3：应用所属服务类型 $4：源IP地址 $5：源端口号 $6：转换后的源IP地址 $7：转换后的源端口号 $8：目的IP地址 $9：目的端口号 $10：转换后的目的IP地址 $11：转换后的目的端口号 $12：入方向的报文总数 $13：入方向的字节总数 $14：出方向的报文总数 $15：出方向的字节总数 $16：源VPN名称 $17：目的VPN名称 $18：源DS-Lite Tunnel $19：目的DS-Lite Tunnel $20：创建会话的时间 $21：会话删除时间 $22：日志类型 $23：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;Category(1174)=aaa;Application(1002)=sip;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];Application(1002)=[STRING];Category(1174)=[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：应用协议名称 $3：应用所属服务类型 $4：源IPv6地址 $5：源端口号 $6：目的IPv6地址 $7：目的端口号 $8：入方向的报文总数 $9：入方向的字节总数 $10：出方向的报文总数 $11：出方向的字节总数 $12：源VPN名称 $13：目的VPN名称 $14：创建会话的时间 $15：会话删除时间 $16：日志类型 $17：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;Application(1002)=sip;Category(1174)=aaa;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

148.5 SESSION_IPV4_TRAFFIC

日志内容	Protocol(1001)=[STRING];Application(1002)=[STRING];Category(1174)=[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：应用协议名称 $3：应用所属服务类型 $4：源IP地址 $5：源端口号 $6：转换后的源IP地址 $7：转换后的源端口号 $8：目的IP地址 $9：目的端口号 $10：转换后的目的IP地址 $11：转换后的目的端口号 $12：入方向的报文总数 $13：入方向的字节总数 $14：出方向的报文总数 $15：出方向的字节总数 $16：源VPN名称 $17：目的VPN名称 $18：源DS-Lite Tunnel $19：目的DS-Lite Tunnel $20：创建会话的时间 $21：会话删除时间 $22：日志类型 $23：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_TRAFFIC:Protocol(1001)=UDP;Category(1174)=aaa;Application(1002)=sip;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

148.6 SESSION_IPV6_TRAFFIC

日志内容	Protocol(1001)=[STRING];Application(1002)=[STRING];Category(1174)=[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：应用协议名称 $3：应用所属服务类型 $4：源IPv6地址 $5：源端口号 $6：目的IPv6地址 $7：目的端口号 $8：入方向的报文总数 $9：入方向的字节总数 $10：出方向的报文总数 $11：出方向的字节总数 $12：源VPN名称 $13：目的VPN名称 $14：创建会话的时间 $15：会话删除时间 $16：日志类型 $17：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_TRAFFIC: Protocol(1001)=UDP;Application(1002)=sip;Category(1174)=aaa;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	设备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_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

150.7 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

150.8 SHELL_CMDFAIL

日志内容	The [STRING] command 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 “vlan 1024” 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

150.9 SHELL_COMMIT

日志内容	The configuration has been committed.
参数解释	无
日志等级	5
举例	SHELL/5/SHELL_COMMIT: The configuration has been committed.
日志说明	配置提交成功
处理建议	无

150.10 SHELL_COMMIT_DELAY

日志内容	A configuration rollback will be performed in [INT32] minutes.
参数解释	$1：用户指定的配置提交超时时间
日志等级	5
举例	SHELL/5/SHELL_COMMIT_DELAY: A configuration rollback will be performed in 3 minutes.
日志说明	用户指定配置提交超时时间成功
处理建议	请在超时时间内完成配置并提交，如果不能完成可以再次执行**configuration commit delay**命令延长时间

150.11 SHELL_COMMIT_REDELAY

日志内容	The commit delay has been reset, a configuration rollback will be performed in [INT32] minutes.
参数解释	$1：用户重新设置的超时时间
日志等级	5
举例	SHELL/5/SHELL_COMMIT_REDELAY: The commit delay has been reset, a configuration rollback will be performed in 3 minutes.
日志说明	用户在指定的超时时间之内再次配置超时时间，提示已经重置超时时间并显示当前超时时间
处理建议	无

150.12 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	达到用户指定的配置提交超时时间后，进行配置回滚
处理建议	请停止任何配置操作，即将进行配置回滚

150.13 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	配置回滚完成
处理建议	配置回滚完成，请继续操作

150.14 SHELL_COMMIT_ROLLBACKFAILED

日志内容	Settings for some commands were not rolled back upon expiration of the configuration commit delay timer. Reason: Configuration rollback is not supported for those commands.
参数解释	无
日志等级	5
举例	SHELL/5/SHELL_COMMIT_ROLLBACKFAILED: Settings for some commands were not rolled back upon expiration of the configuration commit delay timer. Reason: Configuration rollback is not supported for those commands.
日志说明	达到用户指定的配置提交超时时间后，自动进行配置回滚，配置回滚失败
处理建议	可以通过查看SHELL模块的日志信息，确认回滚失败的配置

150.15 SHELL_COMMIT_WILLROLLBACK

日志内容	A configuration rollback will be performed in 1 minute. To retain the configuration you have made after executing the configuration commit delay command, execute the commit command.
参数解释	无
日志等级	5
举例	SHELL/5/SHELL_COMMIT_WILLROLLBACK: A configuration rollback will be performed in 1 minute. To retain the configuration you have made after executing the configuration commit delay command, execute the commit command.
日志说明	用户指定的配置提交超时时间超时前1分钟
处理建议	请在超时时间内完成配置并提交，如果不能完成可以再次执行**configuration commit delay**命令延长时间

150.16 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

150.17 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
处理建议	无

150.18 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
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： **1.** 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 **2.** 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	另一个成员端口接替故障端口转发流量
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 AGENTX

日志内容	Failed to initiate AgentX. Another service is using the AgentX listening port.
参数解释	无
日志等级	4
举例	SNMP/4/AGENTX: Failed to initiate AgentX. Another service is using the AgentX listening port.
日志说明	SNMP功能启动的时候会连带启动SNMP AgentX功能。SNMP AgentX的监听端口号为TCP 705，如果TCP 705端口号被其他服务占用，则SNMP AgentX功能启动失败
处理建议	**1.** 使用 display tcp verbose 命令查看占用 TCP 705 端口号的进程 **2.** 关闭进程对应的特性 **3.** 重启 SNMP 功能

153.2 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

153.3 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

153.4 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

153.5 SNMP_INFORM_LOST

日志内容	Inform failed to reach NMS through [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 through 192.168.111.222(163): Inform coldStart(1.3.6.1.6.3.1.1.5.1).
日志说明	当NMS路由不可达，或者设备给NMS发送Inform报文超时仍未收到响应时，设备会将发送失败的Inform报文以日志的方式保存下来，以便用户查询 当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	检查设备与NMS之间是否路由可达

153.6 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 如果告警未携带MIB节点，此参数部分不会出现 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 unisLogIn(1.3.6.1.4.1.10519.256.2.2.1.1.3.0.1) with unisTerminalUserName(1.3.6.1.4.1.10519.256.2.2.1.1.2.1.0)=; unisTerminalSource(1.3.6.1.4.1.10519.256.2.2.1.1.2.2.0)=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)=UNIS;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

153.7 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=Beijing 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

153.8 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 SSH

本节介绍 SSH（Secure Shell，安全外壳）模块输出的日志信息。

154.1 SSH_WEAK_CIPHER_ALGORITHM

日志内容	SSH is configured to support CBC encryption, which may allow an attacker to recover the plaintext message from the ciphertext.
参数解释	无
日志等级	5
举例	SSH/5/SSH_WEAK_CIPHER_ALGORITHM: SSH is configured to support CBC encryption, which may allow an attacker to recover the plaintext message from the ciphertext.
日志说明	SSH客户端或服务器端包含不安全的3DES-CBC、128位AES-CBC、256位AES-CBC或者DES-CBC加密算法
处理建议	建议使用**ssh2 algorithm cipher**命令配置安全的加密算法

154.2 SSH_WEAK_MAC_ALGORITHM

日志内容	SSH is configured to support MD5 or 96-bit HMAC algorithms, which are weak.
参数解释	无
日志等级	5
举例	SSH/5/SSH_WEAK_MAC_ALGORITHM: SSH is configured to support MD5 or 96-bit HMAC algorithms, which are weak.
日志说明	SSH客户端或服务器端配置了弱强度的HMAC-MD5、HMAC-MD5-96或者HMAC-SHA1-96的HMAC算法
处理建议	建议使用**ssh2 algorithm mac**命令配置强度高的HMAC算法

155 SSHC

本节介绍 SSHC（SSH client，SSH 客户端）模块输出的日志信息。

155.1 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

156 SSHS

本节介绍 SSHS（SSH server，SSH 服务器）模块输出的日志信息。

156.1 SSHS_ACL_DENY

日志内容	The SSH connection request from [IPADDR]([STRING]) was denied by ACL rule (rule ID=[INT16]).
参数解释	$1：SSH客户端IP地址 $2：SSH客户端IP地址所在VPN $3：SSH客户端匹配ACL deny规则编号，default rule表示SSH客户化端登录被缺省的规则拒绝
日志等级	5
举例	SSHS/5/SSH_ACL_DENY: The SSH connection request from 181.1.1.10 was denied by ACL rule (rule ID=20). SSHS/5/SSH_ACL_DENY: The SSH connection request from 181.1.1.11 was denied by ACL rule (default rule).
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

156.2 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

156.3 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

156.4 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

156.5 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

156.6 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

156.7 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

156.8 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

156.9 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

156.10 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

156.11 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

156.12 SSHS_REACH_SESSION_LIMIT

日志内容	SSH client [STRING] failed to log in. The number of SSH sessions is [NUMBER], and exceeded the limit ([NUMBER]).
参数解释	$1：SSH客户端IP地址 $2：SSH客户端已经登录个数 $3：设备允许SSH客户端登录个数
日志等级	6
举例	SSHS/6/SSHS_REACH_SESSION_LIMIT: SSH client 192.168.30.117 failed to log in. The number of SSH sessions is 10, and exceeded the limit (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

156.13 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

156.14 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

156.15 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

156.16 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

156.17 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

157 SSL VPN

本节介绍 SSL VPN 模块输出的日志信息。

157.1 SSLVPN_ADD_CONTENT_TYPE

日志内容	Set the content type for file policy [STRING] in context [STRING].
参数解释	$1：文件策略名称 $2：SSLVPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_CONTENT_TYPE: Set the content type for file policy fp1 in context ctx1.
日志说明	添加需要进行改写的文件类型
处理建议	无

157.2 SSLVPN_ADD_CONTENT_TYPE_FAILED

日志内容	Failed to set the content type for file policy [STRING] in context [STRING].
参数解释	$1：文件策略名称 $2：SSLVPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_CONTENT_TYPE_FAILED: Failed to set the content type for file policy fp1 in context ctx1.
日志说明	添加需要进行改写的文件类型失败
处理建议	无

157.3 SSLVPN_ADD_CONTEXT

日志内容	Created SSL VPN context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_CONTEXT: Created SSL VPN context ctx1.
日志说明	创建SSL VPN访问实例
处理建议	无

157.4 SSLVPN_ADD_CONTEXT_FAILED

日志内容	Failed to create SSL VPN context [STRING]
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_CONTEXT_FAILED: Failed to create SSL VPN context ctx1.
日志说明	创建SSL VPN访问实例失败
处理建议	无

157.5 SSLVPN_ADD_EXCROUTEITEM

日志内容	Added exclude route (IP [STRING] mask [STRING]) to route list [STRING] in context [STRING].
参数解释	$1：路由的目的地址 $2：路由的掩码 $3：路由列表名称 $4：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_EXCROUTEITEM: Added exclude route (IP 10.0.0.0 mask 255.0.0.0) to route list rtlist in context ctx1.
日志说明	在SSL VPN访问实例视图下的路由列表中添加例外路由表项
处理建议	无

157.6 SSLVPN_ADD_EXCROUTEITEM_FAILED

日志内容	Failed to add exclude route (IP [STRING] mask [STRING]) to route list [STRING] in context [STRING]
参数解释	$1：路由的目的地址 $2：路由的掩码 $3：路由列表名称 $4：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_EXCROUTEITEM_FAILED: Failed to add exclude route (IP 10.0.0.0 mask 255.0.0.0) to route list rtlist in context ctx1.
日志说明	在SSL VPN访问实例视图下的路由列表中添加例外路由失败
处理建议	无

157.7 SSLVPN_ADD_FILEPOLICY

日志内容	Created file policy [STRING] in context [STRING].
参数解释	$1：文件策略名称 $2：SSLVPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_FILEPOLICY: Created file policy fp1 in context ctx1.
日志说明	创建文件策略
处理建议	无

157.8 SSLVPN_ADD_FILEPOLICY_FAILED

日志内容	Failed to create file policy [STRING] in context [STRING].
参数解释	$1：文件策略名称 $2：SSLVPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_FILEPOLICY_FAILED: Failed to create file policy fp1 in context ctx1.
日志说明	创建文件策略失败
处理建议	无

157.9 SSLVPN_ADD_GATEWAY

日志内容	Created SSL VPN gateway [STRING].
参数解释	$1：SSL VPN网关名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_GATEWAY: Created SSL VPN gateway gw1.
日志说明	创建SSL VPN网关
处理建议	无

157.10 SSLVPN_ADD_GATEWAY_FAILED

日志内容	Failed to create SSL VPN gateway [STRING]
参数解释	$1：SSL VPN网关名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_GATEWAY_FAILED: Failed to create SSL VPN gateway gw1.
日志说明	创建SSL VPN网关失败
处理建议	无

157.11 SSLVPN_ADD_INCROUTEITEM

日志内容	Added include route (IP [STRING] mask [STRING]) to route list [STRING] in context [STRING].
参数解释	$1：路由的目的地址 $2：路由的掩码 $3：路由列表名称 $4：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_INCROUTEITEM: Added include route (IP 10.0.0.0 mask 255.0.0.0) to route list rtlist in context ctx1.
日志说明	在SSL VPN访问实例视图下的路由列表中添加路由表项
处理建议	无

157.12 SSLVPN_ADD_INCROUTEITEM_FAILED

日志内容	Failed to add include route (IP [STRING] mask [STRING]) to route list [STRING] in context [STRING]
参数解释	$1：路由的目的地址 $2：路由的掩码 $3：路由列表名称 $4：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_INCROUTEITEM_FAILED: Failed to add include route (IP 10.0.0.0 mask 255.0.0.0) to route list rtlist in context ctx1.
日志说明	在SSL VPN访问实例视图下的路由列表中添加路由失败
处理建议	无

157.13 SSLVPN_ADD_IPADDRESSPOOL

日志内容	Created IP address pool [STRING] start-IP [STRING] end-IP [STRING].
参数解释	$1：IP地址池名称 $2：地址池的起始地址 $3：地址池的结束地址
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_IPADDRESSPOOL: Created IP address pool pool1 start-IP 20.1.1.1 end-IP 20.1.1.100.
日志说明	创建SSL VPN的地址池
处理建议	无

157.14 SSLVPN_ADD_IPADDRESSPOOL_FAILED

日志内容	Failed to create IP address pool [STRING] start-IP [STRING] end-IP [STRING]
参数解释	$1：IP地址池名称 $2：地址池的起始地址 $3：地址池的结束地址
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_IPADDRESSPOOL_FAILED: Failed to create IP address pool pool1 start-IP 20.1.1.1 end-IP 20.1.1.100.
日志说明	创建SSL VPN的地址池失败
处理建议	创建的SSL VPN地址池中的地址和已有的SSL VPN地址池中的地址有重叠

157.15 SSLVPN_ADD_IPTUNNELACIF

日志内容	Specified SSL VPN AC interface [STRING] in context [STRING].
参数解释	$1：引用的SSL VPN AC接口 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_IPTUNNELACIF: Specified SSL VPN AC interface SSLVPN-AC1 in context ctx.
日志说明	配置IP接入引用的SSL VPN AC接口
处理建议	无

157.16 SSLVPN_ADD_IPTUNNELACIF_FAILED

日志内容	Failed to specify SSL VPN AC interface [STRING] in context [STRING]
参数解释	$1：引用的SSL VPN AC接口 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_IPTUNNELACIF_FAILED: Failed to specify SSL VPN AC interface SSLVPN-AC1 in context ctx.
日志说明	配置IP接入引用的SSL VPN AC接口失败
处理建议	无

157.17 SSLVPN_ADD_IPV4_RANGE

日志内容	Specified IPv4 address range (start-IP [STRING] end-IP [STRING]) for SNAT pool [STRING].
参数解释	$1：SSL VPN SNAT IPv4地址池的起始地址 $2：SSL VPN SNAT IPv4地址池的结束地址 $3：SSL VPN SNAT地址池名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_IPV4_RANGE: Specified IPv4 address range (start-IP 192.168.1.1 end-IP 192.168.1.10) for SNAT pool sp1.
日志说明	配置SSL VPN SNAT地址池的IPv4地址范围
处理建议	无

157.18 SSLVPN_ADD_IPV4_RANGE_FAILED

日志内容	Failed to specify IPv4 address range (start-IP [STRING] end-IP [STRING]) for SNAT pool [STRING].
参数解释	$1：SSL VPN SNAT IPv4地址池的起始地址 $2：SSL VPN SNAT IPv4地址池的结束地址 $3：SSL VPN SNAT地址池名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_IPV4_RANGE_FAILED: Failed to specify IPV4 address range (start-IP 192.168.1.1 end-IP 192.168.1.10) for SNAT pool sp1.
日志说明	配置SSL VPN SNAT地址池的IPv4地址范围失败
处理建议	无

157.19 SSLVPN_ADD_IPV6_RANGE

日志内容	Specified IPv6 address range (start-IP [STRING] end-IP [STRING]) for SNAT pool [STRING].
参数解释	$1：SSL VPN SNAT IPv6地址池的起始地址 $2：SSL VPN SNAT IPv6地址池的结束地址 $3：SSL VPN SNAT地址池名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_IPV6_RANGE: Specified IPv6 address range (start-IP 2000::1 end-IP 2000::10) for SNAT pool sp1.
日志说明	配置SSL VPN SNAT地址池的IPv6地址范围
处理建议	无

157.20 SSLVPN_ADD_IPV6_RANGE_FAILED

日志内容	Failed to specify IPv6 address range (start-IP [STRING] end-IP [STRING]) for SNAT pool [STRING].
参数解释	$1：SSL VPN SNAT IPv6地址池的起始地址 $2：SSL VPN SNAT IPv6地址池的结束地址 $3：SSL VPN SNAT地址池名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_IPV6_RANGE_FAILED: Failed to specify IPv6 address range (start-IP 2000::1 end-IP 2000::10) for SNAT pool sp1.
日志说明	配置SSL VPN SNAT地址池的IPv6地址范围失败
处理建议	无

157.21 SSLVPN_ADD_LOCALPORT

日志内容	Added port forwarding entry local-port [STRING] local-name [STRING] remote-server [STRING] remote-port [STRING] [STRING] in port forwarding list [STRING] in context [STRING].
参数解释	$1：本地端口号 $2：本地地址或本地主机名称 $3：服务IP地址或完整域名 $4：TCP服务的端口号 $5：端口转发实例的描述信息，未配置时不显示 $6：端口转发列表的名称 $7：SSL VPN访问实例名称
日志等级	6
举例	• SSLVPN/6/SSLVPN_ADD_LOCALPORT: Added port forwarding entry local-port 80 local-name 127.0.0.1 remote-server 192.168.20.35 remote-port 80 in port forwarding list pflist1 in context ctx. • SSLVPN/6/SSLVPN_ADD_LOCALPORT: Added port forwarding entry local-port 80 local-name 127.0.0.1 remote-server 192.168.20.35 remote-port 80 description http in port forwarding list pflist1 in context ctx.
日志说明	在端口转发列表中添加端口转发实例
处理建议	无

157.22 SSLVPN_ADD_LOCALPORT_FAILED

日志内容	Failed to add port forwarding entry local-port [STRING] local-name [STRING] remote-server [STRING] remote-port [STRING] [STRING] in port forwarding list [STRING] in context [STRING]
参数解释	$1：企业网TCP服务映射的本地端口号 $2：本地地址或本地主机名称 $3：企业网TCP服务的IP地址或完整域名 $4：TCP服务的端口号 $5：端口转发实例的描述信息，未配置时不显示 $6：端口转发列表的名称 $7：SSL VPN访问实例名称
日志等级	6
举例	• SSLVPN/6/SSLVPN_ADD_LOCALPORT_FAILED: Failed to add port forwarding entry ocal-port 80 local-name 127.0.0.1 remote-server 192.168.20.34 remote-port 80 in port forwarding list pflist1 in context ctx. • SSLVPN/6/SSLVPN_ADD_LOCALPORT_FAILED: Failed to add port forwarding entry local-port 80 local-name 127.0.0.1 remote-server 192.168.20.34 remote-port 80 description http in port forwarding list pflist1 in context ctx.
日志说明	在端口转发列表中添加端口转发实例失败
处理建议	无

157.23 SSLVPN_ADD_NEWCONTENT

日志内容	Specified new content [STRING] for rewrite rule [STRING] in file policy [STRING] in context [STRING].
参数解释	$1：指定改写后的报文内容 $2：改写规则名称 $3：文件策略名称 $4：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_NEWCONTENT: Specified new content sslvpn rewrite htmlcode(d); for rewrite rule rw in file policy fp in context ctx.
日志说明	添加改写规则指定改写后的报文内容
处理建议	无

157.24 SSLVPN_ADD_NEWCONTENT_FAILED

日志内容	Failed to specify new content [STRING] for rewrite rule [STRING] in file policy [STRING] in context [STRING].
参数解释	$1：指定改写后的报文内容 $2：改写规则名称 $3：文件策略名称 $4：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_NEWCONTENT_FAILED: Failed to specify new content sslvpn rewrite htmlcode(d); for rewrite rule rw in file policy fp in context ctx.
日志说明	添加改写规则指定改写后的报文内容失败
处理建议	无

157.25 SSLVPN_ADD_OLDCONTENT

日志内容	Specified old content [STRING] for rewrite rule [STRING] in file policy [STRING] in context [STRING].
参数解释	$1：原始报文内容 $2：改写规则名称 $3：文件策略名称 $4：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_OLDCONTENT: Specified old content a.b.c.innerHTML = d; for rewrite rule rw in file policy fp in context ctx.
日志说明	添加改写规则原始报文内容
处理建议	无

157.26 SSLVPN_ADD_OLDCONTENT_FAILED

日志内容	Failed to specify old content [STRING] for rewrite rule [STRING] in file policy [STRING] in context [STRING].
参数解释	$1：原始报文内容 $2：改写规则名称 $3：文件策略名称 $4：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_OLDCONTENT_FAILED: Failed to specify old content a.b.c.innerHTML = d; for rewrite rule rw in file policy fp in context ctx.
日志说明	添加改写规则原始报文内容失败
处理建议	无

157.27 SSLVPN_ADD_PORTFWD

日志内容	Created port forwarding list [STRING] in context [STRING].
参数解释	$1：端口转发列表名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_PORTFWD: Created port forwarding list pf in context ctx1.
日志说明	创建端口转发列表
处理建议	无

157.28 SSLVPN_ADD_PORTFWD_FAILED

日志内容	Failed to create port forwarding list [STRING] in context [STRING]
参数解释	$1：端口转发列表名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_PORTFWD_FAILED: Failed to create port forwarding list pf in context ctx1.
日志说明	创建端口转发列表失败
处理建议	无

157.29 SSLVPN_ADD_PORTFWD_ITEM

日志内容	Created port forwarding item [STRING] in context [STRING].
参数解释	$1：端口转发表项名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_PORTFWD_ITEM: Created port forwarding item pfitem in context ctx1.
日志说明	创建端口转发表项
处理建议	无

157.30 SSLVPN_ADD_PORTFWD_ITEM_FAILED

日志内容	Failed to create port forwarding item [STRING] in context [STRING]
参数解释	$1：端口转发表项名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_PORTFWD_ITEM_FAILED: Failed to create port forwarding item pfitem in context ctx1.
日志说明	创建端口转发表项失败
处理建议	无

157.31 SSLVPN_ADD_PYGROUP

日志内容	Created policy group [STRING] in context [STRING].
参数解释	$1：策略组名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_PYGROUP: Created policy group pg in context ctx1.
日志说明	创建SSL VPN策略组
处理建议	无

157.32 SSLVPN_ADD_PYGROUP_FAILED

日志内容	Failed to create policy group [STRING] in context [STRING]
参数解释	$1：策略组名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_PYGROUP_FAILED: Failed to create policy group pg in context ctx1.
日志说明	创建SSL VPN策略组失败
处理建议	无

157.33 SSLVPN_ADD_REFER_PFWDITEM

日志内容	Assigned port forwarding item [STRING] to port forwarding list [STRING] in context [STRING].
参数解释	$1：端口转发表项名称 $2：端口转发列表名称 $3：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_REFER_PFWDITEM: Assigned port forwarding item pfitem1 to port forwarding list pflist1 in context ctx1.
日志说明	配置端口转发列表引用端口转发表项
处理建议	无

157.34 SSLVPN_ADD_REFER_PFWDITEM_FAILED

日志内容	Failed to assign port forwarding item [STRING] to port forwarding list [STRING] in context [STRING].
参数解释	$1：端口转发表项名称 $2：端口转发列表名称 $3：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_REFER_PFWDITEM_FAILED: Failed to assign port forwarding item pfitem1 to port forwarding list pflist1 in context ctx1.
日志说明	配置端口转发列表引用端口转发表项失败
处理建议	无

157.35 SSLVPN_ADD_REFER_SCUTLIST

日志内容	Assigned shortcut list [STRING] to policy group [STRING] in context [STRING].
参数解释	$1：快捷方式列表名称 $2：策略组名称 $3：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_REFER_SCUTLIST: Assigned shortcut list scutlist1 to policy group pg in context ctx1.
日志说明	配置策略组引用快捷方式列表
处理建议	无

157.36 SSLVPN_ADD_REFERIPACL

日志内容	Added IP access filter [STRING] ACL [STRING] in policy group [STRING] in context [STRING].
参数解释	$1：ACL类型，取值为IPv6或空。取值为IPv6表示IPv6类型ACL；取值为空表示IPv4类型ACL $2：高级ACL编号 $3：策略组名称 $4：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_REFERIPACL: Added IP access filter ACL 3000 in policy group pgroup in context ctx1.
日志说明	策略组下添加IP接入过滤规则
处理建议	无

157.37 SSLVPN_ADD_REFERIPACL_FAILED

日志内容	Failed to add IP access filter [STRING] ACL [STRING] in policy group [STRING] in context [STRING]
参数解释	$1：ACL类型，取值为IPv6或空。取值为IPv6表示IPv6类型ACL；取值为空表示IPv4类型ACL $2：高级ACL编号 $3：策略组名称 $4：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_REFERIPACL_FAILED: Failed to add IP access filter ACL 3000 in policy group pgroup in context ctx1.
日志说明	策略组下配置IP接入过滤功能失败
处理建议	无

157.38 SSLVPN_ADD_REFERPORTFWD

日志内容	Specified port forwarding list [STRING] for policy-group [STRING] in context [STRING].
参数解释	$1：端口转发列表名称 $2：策略组名称 $3：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_REFERPORTFWD: Specified port forwarding list pf for policy-group pg in context ctx1.
日志说明	配置策略组引用端口转发列表
处理建议	无

157.39 SSLVPN_ADD_REFERPORTFWD_FAILED

日志内容	Failed to specify port forwarding list [STRING] for policy-group [STRING] in context [STRING]
参数解释	$1：端口转发列表名称 $2：策略组名称 $3：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_REFERPORTFWD_FAILED: Failed to specify port forwarding list pf for policy-group pg in context ctx1.
日志说明	配置策略组引用端口转发列表失败
处理建议	该转发列表不存在，需先创建才能引用

157.40 SSLVPN_ADD_REFERSCUTLIST_FAILED

日志内容	Failed to assign shortcut list [STRING] to policy group [STRING] in context [STRING].
参数解释	$1：快捷方式列表名称 $2：策略组名称 $3：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_REFERSCUTLIST_FAILED: Failed to assign shortcut list scutlist1 to policy group pg in context ctx1.
日志说明	配置策略组引用快捷方式列表失败
处理建议	无

157.41 SSLVPN_ADD_REFERSHORTCUT

日志内容	Assigned shortcut [STRING] to shortcut list [STRING] in context [STRING].
参数解释	$1：快捷方式名称 $2：快捷方式列表名称 $3：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_REFERSHORTCUT: Assigned shortcut shortcut1 to shortcut list scutlist1 in context ctx1.
日志说明	配置快捷方式列表引用快捷方式
处理建议	无

157.42 SSLVPN_ADD_REFERSHORTCUT_FAILED

日志内容	Failed to assign shortcut [STRING] to shortcut list [STRING] in context [STRING].
参数解释	$1：快捷方式名称 $2：快捷方式列表名称 $3：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_REFERSHORTCUT_FAILED: Failed to assign shortcut shortcut1 to shortcut list scutlist1 in context ctx1.
日志说明	配置快捷方式列表引用快捷方式失败
处理建议	无

157.43 SSLVPN_ADD_REFERSNATPOOL

日志内容	Specified SNAT pool [STRING] for context [STRING].
参数解释	$1：SSL VPN SNAT地址池名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_REFERSNATPOOL: Specified SNAT pool sp1 for context ctx1.
日志说明	配置SSLVPN访问实例引用SNAT地址池
处理建议	无

157.44 SSLVPN_ADD_REFERSNATPOOL_FAILED

日志内容	Failed to specify SNAT pool [STRING] for context [STRING].
参数解释	$1：SSL VPN SNAT地址池名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_REFERSNATPOOL_FAILED: Failed to specify SNAT pool sp1 for context ctx1.
日志说明	配置SSLVPN访问实例引用SNAT地址池失败
处理建议	无

157.45 SSLVPN_ADD_REFERTCPACL

日志内容	Added TCP access filter [STRING] ACL [STRING] in policy group [STRING] in context [STRING].
参数解释	$1：ACL类型，取值为IPv6或空。取值为IPv6表示IPv6类型ACL；取值为空表示IPv4类型ACL $2：高级ACL编号 $3：策略组名称 $4：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_REFERTCPACL: Added TCP access filter ACL 3000 in policy group pgroup in context ctx1.
日志说明	在策略组下配置TCP接入过滤功能
处理建议	无

157.46 SSLVPN_ADD_REFERTCPACL_FAILED

日志内容	Failed to add TCP access filter [STRING] ACL [STRING] in policy group [STRING] in context [STRING]
参数解释	$1：ACL类型，取值为IPv6或空。取值为IPv6表示IPv6类型ACL；取值为空表示IPv4类型ACL $2：高级ACL编号 $3：策略组名称 $4：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_REFERTCPACL_FAILED: Failed to add TCP access filter ACL 3000 in policy group pgroup in context ctx1
日志说明	在策略组下配置TCP接入过滤功能失败
处理建议	无

157.47 SSLVPN_ADD_REFERURIACL

日志内容	Added [STRING] access filter URI ACL [STRING] to policy group [STRING] in context [STRING].
参数解释	$1：SSL VPN接入方式类型，取值包括： • IP 接入方式 • Web 接入方式 • TCP 接入方式 $2：URI ACL名称 $3：策略组名称 $4：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_REFERURIACL: Added IP access filter URI ACL uacl to policy group pgroup in context ctx1.
日志说明	策略组下添加指定接入方式的URI ACL规则
处理建议	无

157.48 SSLVPN_ADD_REFERURIACL_FAILED

日志内容	Failed to add [STRING] access filter URI ACL [STRING] to policy group [STRING] in context [STRING].
参数解释	$1：SSL VPN接入方式类型，取值包括： • IP 接入方式 • Web 接入方式 • TCP 接入方式 $2：URI ACL名称 $3：策略组名称 $4：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_REFERURIACL_FAILED: Failed to add IP access filter URI ACL uacl to policy group pgroup in context ctx1.
日志说明	策略组下添加指定接入方式的URI过滤规则失败
处理建议	无

157.49 SSLVPN_ADD_REFERURLLIST

日志内容	Specified URL list [STRING] for policy-group [STRING] in context [STRING].
参数解释	$1：URL列表名称 $2：策略组名称 $3：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_REFERURLLIST: Specified URL list urllist for policy-group pg in context ctx1.
日志说明	配置策略组引用URL列表
处理建议	无

157.50 SSLVPN_ADD_REFERURLLIST_FAILED

日志内容	Failed to specify URL list [STRING] for policy-group [STRING] in context [STRING]
参数解释	$1：URL列表名称 $2：策略组名称 $3：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_REFERURLLIST_FAILED: Failed to specify URL list urllist for policy-group pg in context ctx1.
日志说明	配置策略组引用URL列表失败
处理建议	该URL列表不存在，需先创建才能使用

157.51 SSLVPN_ADD_REFERWEBACL

日志内容	Added Web access filter [STRING] ACL [STRING] in policy group [STRING] in context [STRING].
参数解释	$1：ACL类型，取值为IPv6或空。取值为IPv6表示IPv6类型ACL；取值为空表示IPv4类型ACL $2：高级ACL编号 $3：策略组名称 $4：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_REFERWEBACL: Added Web access filter ACL 3000 in policy group pgroup in context ctx1.
日志说明	在策略组下配置Web接入过滤功能
处理建议	无

157.52 SSLVPN_ADD_REFERWEBACL_FAILED

日志内容	Failed to add Web access filter [STRING] ACL [STRING] in policy group [STRING] in context [STRING]
参数解释	$1：ACL类型，取值为IPv6或空。取值为IPv6表示IPv6类型ACL；取值为空表示IPv4类型ACL $2：高级ACL编号 $3：策略组名称 $4：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_REFERWEBACL_FAILED: Failed to add Web access filter ACL 3000 in policy group pgroup in context ctx1.
日志说明	在策略组下配置Web接入过滤功能失败
处理建议	无

157.53 SSLVPN_ADD_REWRITE_RULE

日志内容	Created rewrite rule [STRING] in file policy [STRING] in context [STRING].
参数解释	$1：改写规则名称 $2：文件策略名称 $3：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_REWRITE_RULE: Created rewrite rule rw in file policy fp in context ctx.
日志说明	创建改写规则
处理建议	无

157.54 SSLVPN_ADD_REWRITE_RULE_FAILED

日志内容	Failed to create rewrite rule [STRING] in file policy [STRING] in context [STRING].
参数解释	$1：改写规则名称 $2：文件策略名称 $3：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_REWRITE_RULE_FAILED: Failed to create rewrite rule rw in file policy fp in context ctx.
日志说明	创建改写规则失败
处理建议	无

157.55 SSLVPN_ADD_ROUTELIST

日志内容	Created IP-route-list [STRING] in context [STRING].
参数解释	$1：路由列表名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_ROUTELIST: Created IP-route-list rtlist in context ctx1.
日志说明	在SSL VPN访问实例中创建路由列表
处理建议	无

157.56 SSLVPN_ADD_ROUTELIST_FAILED

日志内容	Failed to create IP-route-list [STRING] in context [STRING]
参数解释	$1：路由列表名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_ROUTELIST_FAILED: Failed to create IP-route-list rtlist in context ctx1.
日志说明	在SSL VPN访问实例中创建路由列表失败
处理建议	无

157.57 SSLVPN_ADD_ROUTEREFER

日志内容	Configured access-route [STRING] in policy-group [STRING] in context [STRING].
参数解释	$1：下发给客户端的路由表项，取值如下： • 显示为 *ip-address mask* 时，表示将指定路由下发给客户端 • 显示为 force-all，表示强制将客户端的流量转发给 SSL VPN 网关 • 显示为 ip-route-list *list-name* 时，表示将指定路由列表中的路由表项下发给客户端 $2：策略组名称 $3：SSL VPN访问实例名称
日志等级	6
举例	• SSLVPN/6/SSLVPN_ADD_ROUTEREFER: Configured access-route ip-route-list rtlist in policy-group pg in context ctx. • SSLVPN/6/SSLVPN_ADD_ROUTEREFER: Configured access-route 1.0.0.0 255.240.0.0 in policy-group pg in context ctx. • SSLVPN/6/SSLVPN_ADD_ROUTEREFER: Configured access-route force-all in policy-group pg in context ctx.
日志说明	配置下发给客户端的路由表项
处理建议	无

157.58 SSLVPN_ADD_ROUTEREFER_FAILED

日志内容	Failed to configure access-route [STRING] in policy-group [STRING] in context [STRING]
参数解释	$1：下发给客户端的路由表项，取值如下： • 显示为 *ip-address mask* 时，表示将指定路由下发给客户端 • 显示为 force-all，表示强制将客户端的流量转发给 SSL VPN 网关 • 显示为 ip-route-list *list-name* 时，表示将指定路由列表中的路由表项下发给客户端 $2：策略组名称 $3：SSL VPN访问实例名称
日志等级	6
举例	• SSLVPN/6/SSLVPN_ADD_ROUTEREFER_FAILED: Failed to configure access-route ip-route-list rtlist in policy-group pg in context ctx. • SSLVPN/6/SSLVPN_ADD_ROUTEREFER_FAILED: Failed to configure access-route 1.0.0.0 255.240.0.0 in policy-group pg in context ctx. • SSLVPN/6/SSLVPN_ADD_ROUTEREFER_FAILED: Failed to configure access-route force-all in policy-group pg in context ctx.
日志说明	配置下发给客户端的路由表项失败
处理建议	指定的路由列表不存在，要提前创建

157.59 SSLVPN_ADD_SERVERURL

日志内容	Specified URL [STRING] for URL item [STRING] in context [STRING].
参数解释	$1：URL表项配置的URL $2：URL表项的名称 $3：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_SERVERURL: Specified URL www.abc.com for URL item item1 in context ctx1.
日志说明	配置URL表项对应资源的URL成功
处理建议	无

157.60 SSLVPN_ADD_SERVERURL_FAILED

日志内容	Failed to specify URL [STRING] for URL item [STRING] in context [STRING].
参数解释	$1：URL表项配置的URL $2：URL表项的名称 $3：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_SERVERURL_FAILED: Failed to specify URL www.abc.com for URL item item1 in context ctx1.
日志说明	配置URL表项对应资源的URL失败
处理建议	无

157.61 SSLVPN_ADD_SHORTCUT

日志内容	Created shortcut [STRING] in context [STRING].
参数解释	$1：快捷方式名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_SHORTCUT: Created shortcut shortcut1 in context ctx1.
日志说明	创建快捷方式
处理建议	无

157.62 SSLVPN_ADD_SHORTCUT_FAILED

日志内容	Failed to create shortcut [STRING] in context [STRING].
参数解释	$1：快捷方式名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_SHORTCUT_FAILED: Failed to create shortcut shortcut1 in context ctx1.
日志说明	创建快捷方式失败
处理建议	无

157.63 SSLVPN_ADD_SHORTCUTLIST

日志内容	Created shortcut list [STRING] in context [STRING].
参数解释	$1：快捷方式列表名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_SHORTCUTLIST: Created shortcut list scutlist1 in context ctx1.
日志说明	创建快捷方式列表
处理建议	无

157.64 SSLVPN_ADD_SHORTCUTLIST_FAILED

日志内容	Failed to create shortcut list [STRING] in context [STRING].
参数解释	$1：快捷方式列表名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_SHORTCUTLIST_FAILED: Failed to create shortcut list scutlist1 in context ctx1.
日志说明	创建快捷方式列表失败
处理建议	无

157.65 SSLVPN_ADD_SNATPOOL

日志内容	Created SSL VPN SNAT pool [STRING].
参数解释	$1：SSL VPN SNAT地址池名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_SNATPOOL: Created SSL VPN SNAT pool sp1.
日志说明	创建SSL VPN SNAT地址池
处理建议	无

157.66 SSLVPN_ADD_SNATPOOL_FAILED

日志内容	Failed to create SSL VPN SNAT pool [STRING].
参数解释	$1：SSL VPN SNAT地址池名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_SNATPOOL_FAILED: Failed to create SSL VPN SNAT pool sp1.
日志说明	创建SSL VPN SNAT地址池失败
处理建议	无

157.67 SSLVPN_ADD_URIACL

日志内容	Created URI ACL [STRING] in context [STRING].
参数解释	$1：URI ACL名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_URIACL: Created URI ACL uacl in context ctx1.
日志说明	创建URI ACL成功
处理建议	无

157.68 SSLVPN_ADD_URIACL_FAILED

日志内容	Failed to create URI ACL [STRING] in context [STRING].
参数解释	$1：URI ACL名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_URIACL_FAILED: Failed to create URI ACL uacl in context ctx1.
日志说明	创建URI ACL失败
处理建议	无

157.69 SSLVPN_ADD_URIACL_RULE

日志内容	Added rule [UINT32] to URI ACL [STRING] in context [STRING].
参数解释	$1：规则编号 $2：URI ACL名称 $3：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_URIACL_RULE: Added rule 5 to URI ACL uacl in context ctx1.
日志说明	添加URI ACL规则
处理建议	无

157.70 SSLVPN_ADD_URIACL_RULE_FAILED

日志内容	Failed to add rule [UINT32] to URI ACL [STRING] in context [STRING].
参数解释	$1：规则编号 $2：URI ACL名称 $3：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_URIACL_RULE_FAILED: Failed to add rule 5 to URI ACL uacl in context ctx1.
日志说明	添加URI ACL规则失败
处理建议	无

157.71 SSLVPN_ADD_URL

日志内容	Set URL (URL [STRING]) for file policy [STRING] in context [STRING].
参数解释	$1：URL内容 $2：文件策略名称 $3：SSLVPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_URL: Set URL (URL http://192.168.1.1:8080/test.js) for file policy fp1 in context ctx1.
日志说明	添加文件策略最终应用的网页文件的URL
处理建议	无

157.72 SSLVPN_ADD_URL_FAILED

日志内容	Failed to set URL (URL [STRING]) for file policy [STRING] in context [STRING].
参数解释	$1：URL内容 $2：文件策略名称 $3：SSLVPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_URL_FAILED: Failed to set URL (URL http://192.168.1.1:8080/test.js) for file policy fp1 in context ctx1.
日志说明	添加文件策略最终应用的网页文件的URL失败
处理建议	无

157.73 SSLVPN_ADD_URLITEM

日志内容	Created URL item [STRING] in context [STRING].
参数解释	$1：URL表项的名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_URLITEM: Created URL item item1 in context ctx1.
日志说明	创建URL表项成功
处理建议	无

157.74 SSLVPN_ADD_URLITEM_FAILED

日志内容	Failed to create URL item [STRING] in context [STRING].
参数解释	$1：URL表项的名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_URLITEM_FAILED: Failed to create URL item item1 in context ctx1.
日志说明	创建URL表项失败
处理建议	无

157.75 SSLVPN_ADD_URLLIST

日志内容	Created URL list [STRING] in context [STRING].
参数解释	$1：URL列表名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_URLLIST: Created URL list urllist in context ctx1.
日志说明	创建URL列表
处理建议	无

157.76 SSLVPN_ADD_URLLIST_FAILED

日志内容	Failed to create URL list [STRING] in context [STRING]
参数解释	$1：URL列表名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_URLLIST_FAILED: Failed to create URL list urllist in context ctx1.
日志说明	创建URL列表失败
处理建议	无

157.77 SSLVPN_ADD_USER

日志内容	Created user [STRING] in context [STRING].
参数解释	$1：用户的名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_USER: Created user user1 in context ctx1.
日志说明	创建SSL VPN用户
处理建议	无

157.78 SSLVPN_ADD_USER_FAILED

日志内容	Failed to create user [STRING] in context [STRING].
参数解释	$1：用户的名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ADD_USER_FAILED: Failed to create user user1 in context ctx1.
日志说明	创建SSL VPN用户失败
处理建议	无

157.79 SSLVPN_CFG_AAADOMAIN

日志内容	Specified AAA domain [STRING] for context [STRING].
参数解释	$1：ISP域名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_AAADOMAIN: Specified AAA domain myserver for context ctx1.
日志说明	配置SSL VPN访问实例使用指定的ISP域进行AAA认证
处理建议	无

157.80 SSLVPN_CFG_AAADOMAIN_FAILED

日志内容	Failed to specify AAA domain [STRING] for context [STRING].
参数解释	$1：ISP域名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_AAADOMAIN_FAILED: Failed to specify AAA domain myserver for context ctx1.
日志说明	配置SSL VPN访问实例使用指定的ISP域进行AAA认证失败
处理建议	无

157.81 SSLVPN_CFG_AUTHMODE

日志内容	Configured authentication use [STRING] in context [STRING].
参数解释	$1：SSL VPN用户登录访问实例的认证方式 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_AUTHMODE: Configured authentication use all in context ctx1.
日志说明	配置SSL VPN用户登录访问实例的认证方式
处理建议	无

157.82 SSLVPN_CFG_AUTHMODE_FAILED

日志内容	Failed to configure authentication use [STRING] in context [STRING].
参数解释	$1：SSL VPN用户登录访问实例的认证方式 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_AUTHMODE_FAILED: Failed to configure authentication use all in context ctx1.
日志说明	配置SSL VPN用户登录访问实例的认证方式失败
处理建议	无

157.83 SSLVPN_CFG_BINDIP

日志内容	Bound IP addresses [STRING] to user [STRING] in context [STRING].
参数解释	$1：IP地址列表 $2：用户的名称 $3：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_BINDIP: Bound IP addresses 10.1.1.1,10.1.1.3-10.1.1.5 to user user1 in context ctx1.
日志说明	绑定用户IP地址
处理建议	无

157.84 SSLVPN_CFG_BINDIP_FAILED

日志内容	Failed to bind IP addresses [STRING] to user [STRING] in context [STRING].
参数解释	$1：IP地址列表 $2：用户的名称 $3：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_BINDIP_FAILED: Failed to bind IP addresses 10.1.1.1,10.1.1.3-10.1.1.5 to user user1 in context ctx1.
日志说明	绑定用户IP地址失败
处理建议	无

157.85 SSLVPN_CFG_BINDIPAUTO

日志内容	Set the number of IP addresses automatically bound to user [STRING] in context [STRING] to [UINT32].
参数解释	$1：用户的名称 $2：SSL VPN访问实例名称 $3：自动分配的IP地址数目
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_BINDIPAUTO: Set the number of IP addresses automatically bound to user user1 in context ctx1 to 3.
日志说明	指定用户绑定IP地址数目
处理建议	无

157.86 SSLVPN_CFG_BINDIPAUTO_FAILED

日志内容	Failed to set the number of IP addresses automatically bound to user [STRING] in context [STRING] to [UINT32].
参数解释	$1：用户的名称 $2：SSL VPN访问实例名称 $3：自动分配的IP地址数目
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_BINDIPAUTO_FAILED: Failed to set the number of IP addresses automatically bound to user user1 in context ctx1 to 3.
日志说明	指定用户绑定IP地址数目失败
处理建议	无

157.87 SSLVPN_CFG_CERTATTRIBUTE

日志内容	Specified the attribute [STRING] as the certificate user name in context [STRING].
参数解释	$1：SSL VPN证书中作为用户名的字段 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_ CERTATTRIBUTE: Specified the attribute cn as the certificate user name in context ctx1.
日志说明	配置用户证书中作为用户名的字段
处理建议	无

157.88 SSLVPN_CFG_CERTATTRIBUTE_FAILED

日志内容	Failed to specify the attribute [STRING] as the certificate user name in context [STRING].
参数解释	$1：SSL VPN证书中作为用户名的字段 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_CERTATTRIBUTE_FAILED: Failed to specify the attribute cn as the certificate user name in context ctx1.
日志说明	配置用户证书中作为用户名的字段失败
处理建议	无

157.89 SSLVPN_CFG_CTXUSERMAX

日志内容	Set the maximum number of connections to [STRING] for each session in context [STRING].
参数解释	$1：SSL VPN访问实例的单个会话的最大连接数 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_CTXUSERMAX: Set the maximum number of connections to 50 for each session in context ctx1.
日志说明	配置SSL VPN访问实例的单个会话的最大连接数
处理建议	无

157.90 SSLVPN_CFG_CTXUSERMAX_FAILED

日志内容	Failed to set the maximum number of connections to [STRING] for each session in context [STRING].
参数解释	$1：SSL VPN访问实例的单个会话的最大连接数 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_CTXUSERMAX_FAILED: Failed to set the maximum number of connections to 50 for each session in context ctx1.
日志说明	配置SSL VPN访问实例的单个会话的最大连接数失败
处理建议	无

157.91 SSLVPN_CFG_CONTEXT_USERMAXIMUM

日志内容	Configured the maximum number of SSL VPN users in context [UINT32].
参数解释	$1：Context ID
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_CONTEXT_USERMAXIMUM: Configured the maximum number of SSL VPN users in context 2.
日志说明	配置用户Context最大登录用户数
处理建议	无

157.92 SSLVPN_CFG_CONTEXT_USERMAXIMUM_FAILED

日志内容	Failed to configure the maximum number of SSL VPN users in context [UINT32].
参数解释	$1：Context ID
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_CONTEXT_USERMAXIMUM_FAILED: Failed to configure the maximum number of SSL VPN users in context 2.
日志说明	配置用户Context最大登录用户数失败
处理建议	无

157.93 SSLVPN_CFG_CONTEXTVPN

日志内容	Associated VPN instance [STRING] with context [STRING].
参数解释	$1：SSL VPN访问实例关联的VPN实例名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_CONTEXTVPN: Associated VPN instance vpn1 with context ctx1.
日志说明	配置SSL VPN访问实例关联的VPN实例
处理建议	无

157.94 SSLVPN_CFG_CONTEXTVPN_FAILED

日志内容	Failed to associate VPN instance [STRING] with context [STRING]
参数解释	$1：SSL VPN访问实例关联的VPN实例名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_CONTEXTVPN_FAILED: Failed to associate VPN instance vpn1 with context ctx1.
日志说明	配置SSL VPN访问实例关联的VPN实例失败
处理建议	无

157.95 SSLVPN_CFG_CTX_WEBPAGECUST_FAIL

日志内容	Failed to specify template [STRING] for SSL VPN webpage customization in context [STRING].
参数解释	$1：页面模板的名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_CTX_WEBPAGECUST_FAIL: Failed to specify template user1 for SSL VPN webpage customization in context a.
日志说明	配置访问实例引用页面模板失败
处理建议	无

157.96 SSLVPN_CFG_CTX_WEBPAGECUST

日志内容	Specified template [STRING] for SSL VPN webpage customization in context [STRING].
参数解释	$1：页面模板的名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_CTX_WEBPAGECUST: Specified template user1 for SSL VPN webpage customization in context a.
日志说明	配置访问实例引用页面模板成功
处理建议	无

157.97 SSLVPN_CFG_CTXGATEWAY

日志内容	Configured gateway [STRING] [domain [STRING] | virtual-host [STRING]] in context [STRING].
参数解释	$1：SSL VPN网关名称 $2：域名称 $3：虚拟主机名称 $4：SSL VPN访问实例名称 $5：$2和$3存在其中之一或者都不存在
日志等级	6
举例	• SSLVPN/6/SSLVPN_CFG_CTXGATEWAY: Configured gateway gw domain domain1 in context ctx1. • SSLVPN/6/SSLVPN_CFG_CTXGATEWAY: Configured gateway gw virtual-host myhost1 in context ctx1. • SSLVPN/6/SSLVPN_CFG_CTXGATEWAY: Configured gateway gw in context ctx1.
日志说明	配置SSL VPN访问实例引用SSL VPN网关
处理建议	无

157.98 SSLVPN_CFG_CTXGATEWAY_FAILED

日志内容	Failed to configure gateway [STRING] [domain [STRING] | virtual-host [STRING]] in context [STRING]
参数解释	$1：SSL VPN网关名称 $2：域名称 $3：虚拟主机名称 $4：SSL VPN访问实例名称 $5：$2和$3存在其中之一或者都不存在
日志等级	6
举例	• SSLVPN/6/SSLVPN_CFG_CTXGATEWAY_FAILED: Failed to configure gateway gw domain domain1 in context ctx1. • SSLVPN/6/SSLVPN_CFG_CTXGATEWAY_FAILED: Failed to configure gateway gw virtual-host myhost1 in context ctx1. • SSLVPN/6/SSLVPN_CFG_CTXGATEWAY_FAILED: Failed to configure gateway gw in context ctx1.
日志说明	配置SSL VPN访问实例引用SSL VPN网关失败
处理建议	• 若引用的 SSL VPN 网关不存在，要提前创建该 SSL VPN 网关 • SSL VPN 访问实例引用的 SSL VPN 网关超规格，若要继续引用，请删除之前的引用

157.99 SSLVPN_CFG_DEFAULTPGROUP

日志内容	Configured default-policy-group [STRING] in context [STRING].
参数解释	$1：策略组名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_DEFAULTPGROUP: Configured default-policy group pgroup in context ctx1.
日志说明	在SSL VPN访问实例中配置缺省策略组
处理建议	无

157.100 SSLVPN_CFG_DEFAULTPGROUP_FAILED

日志内容	Failed to configure default-policy-group [STRING] in context [STRING].
参数解释	$1：策略组名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_DEFAULTPGROUP_FAILED: Failed to configure default-policy-group pgroup in context ctx1.
日志说明	在SSL VPN访问实例中配置缺省策略组失败
处理建议	指定的策略组不处在，要提前创建策略组

157.101 SSLVPN_CFG_DNSSERVER

日志内容	Specified [STRING] DNS server [STRING] in context [STRING].
参数解释	$1：DNS服务器类型，取值为primary或secondary $2：DNS服务器的IPv4地址 $3：SSL VPN访问实例名称
日志等级	6
举例	• SSLVPN/6/SSLVPN_CFG_DNSSERVER: Specified primary DNS server 1.1.1.1 in context ctx. • SSLVPN/6/SSLVPN_CFG_DNSSERVER: Specified secondary DNS server 1.1.1.2 in context ctx.
日志说明	配置客户端指定的内网DNS服务器地址
处理建议	无

157.102 SSLVPN_CFG_DNSSERVER_FAILED

日志内容	Failed to specify [STRING] DNS server [STRING] in context [STRING]
参数解释	$1：DNS服务器类型，取值为primary或secondary $2：DNS服务器的IPv4地址 $3：SSL VPN访问实例名称
日志等级	6
举例	• SSLVPN/6/SSLVPN_CFG_DNSSERVER_FAILED: Failed to specify primary DNS server 1.1.1.1 in context ctx. • SSLVPN/6/SSLVPN_CFG_DNSSERVER_FAILED: Failed to specify secondary DNS server 1.1.1.2 in context ctx.
日志说明	配置客户端指定的内网DNS服务器地址失败
处理建议	无

157.103 SSLVPN_CFG_EMOSERVER

日志内容	Specified EMO server address [STRING] and port [STRING] in context [STRING].
参数解释	$1：EMO服务器的主机名或EMO服务器的IPv4地址 $2：EMO服务器端口号 $3：SSL VPN访问实例名称
日志等级	6
举例	• SSLVPN/6/SSLVPN_CFG_EMOSERVER: Specified EMO server address 10.10.1.1 and port 9058 in context ctx1. • SSLVPN/6/SSLVPN_CFG_EMOSERVER: Specified EMO server address host and port 9058 in context ctx1.
日志说明	在SSL VPN访问实例中为客户端指定EMO（Endpoint Mobile Office，终端移动办公）服务器
处理建议	无

157.104 SSLVPN_CFG_EMOSERVER_FAILED

日志内容	Failed to specify EMO server address [STRING] and port [STRING] in context [STRING].
参数解释	$1：EMO服务器的主机名或EMO服务器的IPv4地址 $2：EMO服务器端口号 $3：SSL VPN访问实例名称
日志等级	6
举例	• SSLVPN/6/SSLVPN_CFG_EMOSERVER_FAILED: Failed to specify EMO server address 10.10.1.1 and port 9058 in context ctx1. • SSLVPN/6/SSLVPN_CFG_EMOSERVER_FAILED: Failed to specify EMO server address host and port 9058 in context ctx1.
日志说明	在SSL VPN访问实例中为客户端指定EMO（Endpoint Mobile Office，终端移动办公）服务器失败
处理建议	无

157.105 SSLVPN_CFG_GATEWAYVPN

日志内容	Specify VPN instance [STRING] for gateway [STRING].
参数解释	$1：SSL VPN网关所属的VPN实例名称 $2：SSL VPN网关名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_GATEWAYVPN: Specify VPN instance vpn1 for gateway gw1.
日志说明	配置SSL VPN网关所属的VPN实例
处理建议	无

157.106 SSLVPN_CFG_GATEWAYVPN_FAILED

日志内容	Failed to specify VPN instance [STRING] for gateway [STRING]
参数解释	$1：SSL VPN网关所属的VPN实例名称 $2：SSL VPN网关名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_GATEWAYVPN_FAILED: Failed to specify VPN instance vpn1 for gateway gw1.
日志说明	配置SSL VPN网关所属的VPN实例失败
处理建议	无

157.107 SSLVPN_CFG_GLB_WEBPAGECUST_FAIL

日志内容	Failed to specify template [STRING] for global SSL VPN webpage customization.
参数解释	$1：页面模板的名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_GLB_WEBPAGECUST_FAIL: Failed to specify template user1 for global SSL VPN webpage customization.
日志说明	配置全局引用页面模板失败
处理建议	无

157.108 SSLVPN_CFG_GLB_WEBPAGECUST

日志内容	Specified template [STRING] for global SSL VPN webpage customization.
参数解释	$1：页面模板的名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_GLB_WEBPAGECUST: Specified template user1 for global SSL VPN webpage customization.
日志说明	配置全局引用页面模板成功
处理建议	无

157.109 SSLVPN_CFG_GWIPADDRESS

日志内容	Configured IP address [STRING] and port [STRING] for gateway [STRING].
参数解释	$1：SSL VPN网关的IP地址 $2：SSL VPN网关的端口号 $3：SSL VPN网关
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_GWIPADDRESS: Configured IP address 10.10.1.1 and port 8000 for gateway gw1.
日志说明	配置SSL VPN网关的IP地址和端口号
处理建议	无

157.110 SSLVPN_CFG_GWIPADDRESS_FAILED

日志内容	Failed to configure IP address [STRING] and port [STRING] for gateway [STRING]
参数解释	$1：SSL VPN网关的IP地址 $2：SSL VPN网关的端口号 $3：SSL VPN网关
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_GWIPADDRESS_FAILED: Failed to configure IP address 10.10.1.1 and port 8000 for gateway gw1.
日志说明	配置SSL VPN网关的IP地址和端口号失败
处理建议	• 配置的 IP 地址和端口号，已经被其他 SSL VPN 网关引用 • 配置的 SSL VPN 网关的端口号和 HTTP 流量的重定向端口号冲突

157.111 SSLVPN_CFG_GWIPV6ADDRESS

日志内容	Configured IPv6 address [STRING] and port [STRING] for gateway [STRING].
参数解释	$1：SSL VPN网关的IPv6地址 $2：SSL VPN网关的端口号 $3：SSL VPN网关名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_GWIPV6ADDRESS: Configured IPv6 address 1::1 and port 1027 for gateway gw1.
日志说明	配置SSL VPN网关的IPv6地址和端口号
处理建议	无

157.112 SSLVPN_CFG_GWIPV6ADDRESS_FAILED

日志内容	Failed to configure IPv6 address [STRING] and port [STRING] for gateway [STRING].
参数解释	$1：SSL VPN网关的IPv6地址 $2：SSL VPN网关的端口号 $3：SSL VPN网关名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_GWIPV6ADDRESS_FAILED: Failed to configure IPv6 address 1::1 and port 1027 for gateway gw1.
日志说明	配置SSL VPN网关的IPv6地址和端口号失败
处理建议	• 检查配置的 IP 地址和端口号，已经被其他 SSL VPN 网关引用 • 检查 SSL VPN 网关的端口号和 HTTP 流量的重定向端口号是否发生冲突

157.113 SSLVPN_CFG_HTTPREDIRECT

日志内容	Configured HTTP-redirect port [STRING] in gateway [STRING].
参数解释	$1：重定向的HTTP流量的端口号 $2：SSL VPN网关
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_HTTPREDIRECT: Configured HTTP-redirect port 8000 in gateway gw.
日志说明	开启SSL VPN网关HTTP流量的重定向功能
处理建议	无

157.114 SSLVPN_CFG_HTTPREDIRECT_FAILED

日志内容	Failed to configure HTTP-redirect port [STRING] in gateway [STRING]
参数解释	$1：重定向的HTTP流量的端口号 $2：SSL VPN网关
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_HTTPREDIRECT_FAILED: Failed to configure HTTP-redirect port 8000 in gateway gw.
日志说明	开启SSL VPN网关HTTP流量的重定向功能失败
处理建议	该重定向的端口已被引用

157.115 SSLVPN_CFG_IMCADDRESS

日志内容	Configured the IP address [STRING] port number [STRING], and VPN instance [STRING] of the iMC server in context [STRING].
参数解释	$1：短信认证使用的iMC服务器的IPv4地址 $2：短信认证使用的iMC服务器的端口号 $3：短信认证使用的iMC服务器所属的VPN实例 $4：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_IMCADDRESS: Configured the IP address 10.10.1.1 port number 8080 and VPN instance vpn1 of the iMC server in context ctx1.
日志说明	配置SSL VPN访问实例的短信认证使用的iMC服务器的IP地址、端口号和VPN实例
处理建议	无

157.116 SSLVPN_CFG_IMCADDRESS_FAILED

日志内容	Failed to configure the IP address [STRING] port number [STRING], and VPN instance [STRING] of the IMC server in context [STRING].
参数解释	$1：短信认证使用的iMC服务器的IPv4地址 $2：短信认证使用的iMC服务器的端口号 $3：短信认证使用的iMC服务器所属的VPN实例 $4：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_IMCADDRESS_FAILED: Failed to configure the IP address 10.10.1.1 port number 8080 and VPN instance vpn1 of the IMC server in context ctx1.
日志说明	配置短信认证使用的iMC服务器的IP地址、端口号和VPN实例失败
处理建议	无

157.117 SSLVPN_CFG_IPAC_WEBRESPUSH

日志内容	Enabled automatic pushing of Web resources after IP access client login in context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_IPAC_WEBRESPUSH: Enabled automatic pushing of Web resources after IP access client login in context ctx.
日志说明	开启客户端登录SSL VPN网关后自动打开资源列表功能
处理建议	无

157.118 SSLVPN_CFG_IPAC_WEBRESPUSH_FAIL

日志内容	Failed to enable automatic pushing of Web resources after IP access client login in context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_IPAC_WEBRESPUSH_FAIL: Failed to enable automatic pushing of Web resources after IP access client login in context ctx.
日志说明	开启客户端登录SSL VPN网关后自动打开资源列表功能失败
处理建议	无

157.119 SSLVPN_CFG_IPCLIENT_AUTOACT

日志内容	Enabled automatic IP access client startup after Web login in context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_IPCLIENT_AUTOACT: Enabled automatic IP access client startup after Web login in context ctx.
日志说明	开启Web登录SSL VPN网关后自动打开客户端功能
处理建议	无

157.120 SSLVPN_CFG_IPCLIENT_AUTOACT_FAIL

日志内容	Failed to enable automatic IP access client startup after Web login in context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_IPCLIENT_AUTOACT_FAIL: Failed to enable automatic IP access client startup after Web login in context ctx.
日志说明	开启Web登录SSL VPN网关后自动打开客户端功能失败
处理建议	无

157.121 SSLVPN_CFG_IPTNL_RATE-LIMIT

日志内容	Set the IP tunnel [STRING] rate limit to [UINT32] [STRING] in context [STRING].
参数解释	$1：SSL VPN IP 接入流量方向，取值包括： • Upstream，表示上行流量 • Downstream，表示下行流量 $2：流量的最大速率 $3：流量速率的单位，取值包括： • kbps 每秒千比特 • pps 每秒报文数 $4：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_IPTNL_RATE-LIMIT: Set the IP tunnel upstream rate limit to 1000 kbps in context ctx. SSLVPN/6/SSLVPN_CFG_IPTNL_RATE-LIMIT: Set the IP tunnel downstream rate limit to 1000 pps in context ctx.
日志说明	配置IP接入流量限速
处理建议	无

157.122 SSLVPN_CFG_IPTNL_RATE-LIMIT_FAIL

日志内容	Failed to set the IP tunnel [STRING] rate limit to [UINT32] [STRING] in context [STRING].
参数解释	$1：SSL VPN IP接入流量方向，取值包括： • Upstream，表示上行流量 • Downstream，表示下行流量 $2：流量的最大速率 $3：流量速率的单位，取值包括： • kbps 每秒千比特 • pps 每秒报文数 $4：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_IPTNL_RATE-LIMIT_FAIL: Failed to set the IP tunnel upstream rate limit to 1000 kbps in context ctx. SSLVPN/6/SSLVPN_CFG_IPTNL_RATE-LIMIT_FAIL: Failed to set the IP tunnel downstream rate limit to 1000 pps in context ctx.
日志说明	配置IP接入流量限速失败
处理建议	无

157.123 SSLVPN_CFG_IPTUNNELPOOL

日志内容	Specified address-pool [STRING] mask [STRING] in context [STRING].
参数解释	$1：地址池名称 $2：地址池掩码 $3：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_IPTUNNELPOOL: Specified address-pool pool1 mask 255.255.255.0 in context ctx.
日志说明	配置IP接入引用的地址池
处理建议	无

157.124 SSLVPN_CFG_IPTUNNELPOOL_FAILED

日志内容	Failed to specify address-pool [STRING] mask [STRING] in context [STRING]
参数解释	$1：地址池名称 $2：地址池掩码 $3：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_IPTUNNELPOOL_FAILED: Failed to specify address-pool pool1 mask 255.255.255.0 in context ctx.
日志说明	配置IP接入引用的地址池失败
处理建议	无

157.125 SSLVPN_CFG_KEEPALIVE

日志内容	Configured IP Tunnel keepalive interval [STRING] seconds in context [STRING].
参数解释	$1：保活报文的发送间隔时间 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_KEEPALIVE: Configured IP Tunnel keepalive interval 50 seconds in context ctx.
日志说明	配置保活报文的发送时间间隔
处理建议	无

157.126 SSLVPN_CFG_KEEPALIVE_FAILED

日志内容	Failed to configure IP Tunnel keepalive interval [STRING] seconds in context [STRING]
参数解释	$1：保活报文的发送间隔时间，单位为seconds $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_KEEPALIVE_FAILED: Failed to configure IP Tunnel keepalive interval 50 seconds in context ctx.
日志说明	配置保活报文的发送时间间隔失败
处理建议	无

157.127 SSLVPN_CFG_LOCALPORT

日志内容	Configured port forwarding instance local-port [STRING] local-name [STRING] remote-server [STRING] remote-port [STRING] [STRING] for port forwarding item [STRING] in context [STRING].
参数解释	$1：本地端口号 $2：本地地址或本地主机名称 $3：服务IP地址或完整域名 $4：TCP服务的端口号 $5：转发实例的描述信息，未配置时不显示 $6：转发实例所属的端口转发表项名称 $7：SSL VPN访问实例名称
日志等级	6
举例	• SSLVPN/6/SSLVPN_CFG_LOCALPORT: Configured port forwarding instance local-port 80 local-name 127.0.0.1 remote-server 192.168.20.35 remote-port 80 for port forwarding item pfitem1 in context ctx. • SSLVPN/6/SSLVPN_CFG_LOCALPORT: Configured port forwarding instance local-port 80 local-name 127.0.0.1 remote-server 192.168.20.35 remote-port 80 description http for port forwarding item pfitem1 in context ctx.
日志说明	在端口转发表项中配置端口转发实例
处理建议	无

157.128 SSLVPN_CFG_LOCALPORT_FAILED

日志内容	Failed to configure port forwarding instance local-port [STRING] local-name [STRING] remote-server [STRING] remote-port [STRING] [STRING] for port forwarding item [STRING] in context [STRING]
参数解释	$1：企业网TCP服务映射的本地端口号 $2：本地地址或本地主机名称 $3：企业网TCP服务的IP地址或完整域名 $4：TCP服务的端口号 $5：转发实例的描述信息，未配置时不显示 $6：转发实例所属的端口转发表项名称 $7：SSL VPN访问实例名称
日志等级	6
举例	• SSLVPN/6/SSLVPN_CFG_LOCALPORT_FAILED: Failed to configure port forwarding instance local-port 80 local-name 127.0.0.1 remote-server 192.168.20.34 remote-port 80 for port forwarding item pfitem1 in context ctx. • SSLVPN/6/SSLVPN_CFG_LOCALPORT_FAILED: Failed to configure port forwarding instance local-port 80 local-name 127.0.0.1 remote-server 192.168.20.34 remote-port 80 description http for port forwarding item pfitemt1 in context ctx.
日志说明	在端口转发表项中配置端口转发实例失败
处理建议	无

157.129 SSLVPN_CFG_LOGINMESSAGE

日志内容	Configured SSL VPN [STRING] login message [STRING] in context [STRING].
参数解释	$1：登录页面语言类型，English或Chinese $2：登录页面欢迎信息 $3：SSL VPN访问实例名称
日志等级	6
举例	• SSLVPN/6/SSLVPN_CFG_LOGINMESSAGE: Configured SSL VPN English login message Welcome in context ctx1. • SSLVPN/6/SSLVPN_CFG_LOGINMESSAGE: Configured SSL VPN Chinese login message 你好 in context ctx1.
日志说明	配置SSL VPN登录页面的欢迎信息
处理建议	无

157.130 SSLVPN_CFG_LOGINMESSAGE_FAILED

日志内容	Failed to configure SSL VPN [STRING] login message [STRING] in context [STRING]
参数解释	$1：登录页面语言类型，English或Chinese $2：登录页面欢迎信息 $3：SSL VPN访问实例名称
日志等级	6
举例	• SSLVPN/6/SSLVPN_CFG_LOGINMESSAGE_FAILED: Failed to configure SSL VPN English login message Welcome in context ctx1. • SSLVPN/6/SSLVPN_CFG_LOGINMESSAGE_FAILED: Failed to configure SSL VPN Chinese login message 你好 in context ctx1.
日志说明	配置SSL VPN登录页面的欢迎信息失败
处理建议	无

157.131 SSLVPN_CFG_LOGO

日志内容	Configured SSL VPN logo [STRING] [STRING] in context [STRING].
参数解释	$1：是否配置页面logo，file为配置，none不配置，如$1为none则$2不显示 $2：SSLVPN页面显示的logo图标文件 $3：SSL VPN访问实例名称
日志等级	6
举例	• SSLVPN/6/SSLVPN_CFG_LOGO: Configured SSL VPN logo file 1.jpg in context ctx1. • SSLVPN/6/SSLVPN_CFG_LOGO: Configured SSL VPN logo none in context ctx1.
日志说明	配置SSL VPN页面的logo图标
处理建议	无

157.132 SSLVPN_CFG_LOGO_FAILED

日志内容	Failed to configure SSL VPN logo [STRING] [STRING] in context [STRING]
参数解释	$1：是否配置页面logo，file为配置，none为配置失败，如$1为none则$2不显示 $2：SSLVPN页面显示的logo图标文件 $3：SSL VPN访问实例名称
日志等级	6
举例	• SSLVPN/6/SSLVPN_CFG_LOGO_FAILED: Failed to configure SSL VPN logo file 1.jpg in context ctx1. • SSLVPN/6/SSLVPN_CFG_LOGO_FAILED: Failed to configure SSL VPN logo none in context ctx1.
日志说明	配置SSL VPN页面的logo图标失败
处理建议	logo文件过大

157.133 SSLVPN_CFG_MAXONLINES

日志内容	Set the maximum number of concurrent connections to [STRING] for each SSL VPN user in context [STRING].
参数解释	$1：SSL VPN访问实例的同一用户同时最大在线数 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_MAXONLINES: Set the maximum number of concurrent connections to 50 for each SSL VPN user in context ctx1.
日志说明	配置SSL VPN访问实例的同一用户同时最大在线数
处理建议	无

157.134 SSLVPN_CFG_MAXONLINES_FAILED

日志内容	Failed to set maximum number of concurrent connections to [STRING] for each SSL VPN user in context [STRING].
参数解释	$1：SSL VPN访问实例的同一用户同时最大在线数 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_MAXONLINES_FAILED: Failed to set maximum number of concurrent connections to 50 for each SSL VPN user in context ctx1.
日志说明	配置SSL VPN访问实例的同一用户同时最大在线数失败
处理建议	无

157.135 SSLVPN_CFG_MAXUSERS

日志内容	Set the maximum number of sessions to [STRING] in context [STRING].
参数解释	$1：SSL VPN访问实例的最大会话数 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_MAXUSERS: Set the maximum number of sessions to 500 in context ctx1.
日志说明	配置SSL VPN访问实例的最大会话数
处理建议	无

157.136 SSLVPN_CFG_MAXUSERS_FAILED

日志内容	Failed to set maximum number of sessions to [STRING] in context [STRING]
参数解释	$1：SSL VPN访问实例的最大会话数 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_MAXUSERS_FAILED: Failed to set maximum number of sessions to 500 in context ctx1.
日志说明	配置SSL VPN访问实例的最大会话数失败
处理建议	无

157.137 SSLVPN_CFG_MSGSERVER

日志内容	Specified message server address [STRING] and port [STRING] in context [STRING].
参数解释	$1：指定Message服务器的主机名或IPv4地址 $2：指定Message服务器使用的端口号 $3：SSL VPN访问实例名称
日志等级	6
举例	• SSLVPN/6/SSLVPN_CFG_MSGSERVER: Specified message server address 10.10.1.1 and port 8000 in context ctx1. • SSLVPN/6/SSLVPN_CFG_MSGSERVER: Specified message server address host and port 8000 in context ctx1.
日志说明	配置SSL VPN访问实例的Message服务器
处理建议	无

157.138 SSLVPN_CFG_MSGSERVER_FAILED

日志内容	Failed to specify message server address [STRING] and port [STRING] in context [STRING]
参数解释	$1：指定Message服务器的主机名或IPv4地址 $2：指定Message服务器使用的端口号 $3：SSL VPN访问实例名称
日志等级	6
举例	• SSLVPN/6/SSLVPN_CFG_MSGSERVER_FAILED: Failed to specify message server address 10.10.1.1 and port 8000 in context ctx1. • SSLVPN/6/SSLVPN_CFG_MSGSERVER_FAILED: Failed to specify message server address host and port 8000 in context ctx1.
日志说明	配置SSL VPN访问实例的Message服务器失败
处理建议	无

157.139 SSLVPN_CFG_PFWDEXECUTION

日志内容	Configured script [STRING] for port forwarding item [STRING] in context [STRING].
参数解释	$1：端口转发表项对应的资源 $2：端口转发表项名称 $3：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_PFWDEXECUTION: Configured script url('http://127.0.0.1') for port forwarding item pfitem1 in context ctx.
日志说明	在端口转发表项中配置端口转发表项对应的资源
处理建议	无

157.140 SSLVPN_CFG_PFWDEXECUTION_FAILED

日志内容	Failed to configure script [STRING] for port forwarding item [STRING] in context [STRING].
参数解释	$1：脚本代码，指定端口转发表项对应的资源 $2：端口转发表项名称 $3：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_PFWDEXECUTION_FAILED: Failed to configure script url('http://127.0.0.1') for port forwarding item pfitem1 in context ctx.
日志说明	在端口转发表项中配置端口转发表项对应的资源失败
处理建议	无

157.141 SSLVPN_CFG_SCUTEXECUTION

日志内容	Configured script [STRING] for shortcut [STRING] in context [STRING].
参数解释	$1：快捷方式对应的资源 $2：快捷方式名称 $3：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_SCUTEXECUTION: Configured script url('http://10.0.0.1') for shortcut shortcut1 in context ctx.
日志说明	在快捷方式中配置对应的资源
处理建议	无

157.142 SSLVPN_CFG_SCUTEXECUTION_FAILED

日志内容	Failed to configure script [STRING] for shortcut [STRING] in context [STRING].
参数解释	$1：脚本代码，指定快捷方式对应的资源 $2：快捷方式名称 $3：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_SCUTEXECUTION_FAILED: Failed to configure script url('http://10.0.0.1') for shortcut shortcut1 in context ctx.
日志说明	在快捷方式中配置对应的资源失败
处理建议	无

157.143 SSLVPN_CFG_SHORTCUTDESC

日志内容	Configured description [STRING] for shortcut [STRING] in context [STRING].
参数解释	$1：快捷方式的描述信息 $2：快捷方式名称 $3：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_SHORTCUTDESC: Configured description shortcut shortcut1 for shortcut shortcut1 in context ctx.
日志说明	配置快捷方式的描述信息
处理建议	无

157.144 SSLVPN_CFG_SHORTCUTDESC_FAILED

日志内容	Failed to configure description [STRING] for shortcut [STRING] in context [STRING].
参数解释	$1：快捷方式的描述信息 $2：快捷方式名称 $3：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_SHORTCUTDESC_FAILED: Failed to configure description shortcut shortcut1 for shortcut shortcut1 in context ctx.
日志说明	配置快捷方式的描述信息失败
处理建议	无

157.145 SSLVPN_CFG_SSLCLIENT

日志内容	Specified SSL client policy [STRING] for context [STRING].
参数解释	$1：SSL客户端策略名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_SSLCLIENT: Specified SSL client policy ssl for context ctx1.
日志说明	配置SSL VPN访问实例引用SSL客户端策略
处理建议	无

157.146 SSLVPN_CFG_SSLCLIENT_FAILED

日志内容	Failed to specify SSL client policy [STRING] for context [STRING].
参数解释	$1：SSL客户端策略名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_SSLCLIENT_FAILED: Failed to specify SSL client policy ssl for context ctx1.
日志说明	配置SSL VPN访问实例引用SSL客户端策略失败
处理建议	无

157.147 SSLVPN_CFG_SSLSERVER

日志内容	Specified SSL server policy [STRING] for gateway [STRING].
参数解释	$1：SSL服务器端策略名称 $2：SSL VPN网关名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_SSLSERVER: Specified SSL server policy ssl for gateway gw1.
日志说明	配置SSL VPN网关引用SSL服务器端策略
处理建议	无

157.148 SSLVPN_CFG_SSLSERVER_FAILED

日志内容	Failed to specify SSL server policy [STRING] for gateway [STRING]
参数解释	$1：SSL服务器端策略名称 $2：SSL VPN网关名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_SSLSERVER_FAILED: Failed to specify SSL server policy ssl for gateway gw1.
日志说明	配置SSL VPN网关引用SSL服务器端策略失败
处理建议	无

157.149 SSLVPN_CFG_TIMEOUTIDLE

日志内容	Configured session idle timeout to [STRING] minutes in context [STRING].
参数解释	$1：会话保持空闲状态的最长时间 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_TIMEOUTIDLE: Configured session idle timeout to 50 minutes in context ctx1.
日志说明	配置SSL VPN会话保持空闲状态的最长时间
处理建议	无

157.150 SSLVPN_CFG_TIMEOUTIDLE_FAILED

日志内容	Failed to configure session idle timeout to [STRING] minutes in context [STRING]
参数解释	$1：会话保持空闲状态的最长时间 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_TIMEOUTIDLE_FAILED: Failed to configure session idle timeout to 50 minutes in context ctx1.
日志说明	配置SSL VPN会话保持空闲状态的最长时间失败
处理建议	无

157.151 SSLVPN_CFG_TITLE

日志内容	Configured SSL VPN page [STRING] title [STRING] in context [STRING].
参数解释	$1：登录页面语言类型，English或Chinese $2：登录页面标题信息 $3：SSL VPN访问实例名称
日志等级	6
举例	• SSLVPN/6/SSLVPN_CFG_TITLE: Configured SSL VPN page English title Mytitle in context ctx1. • SSLVPN/6/SSLVPN_CFG_TITLE: Configured SSL VPN page Chinese title 公司 A in context ctx1.
日志说明	配置SSL VPN页面的标题信息
处理建议	无

157.152 SSLVPN_CFG_TITLE_FAILED

日志内容	Failed to configure SSL VPN page [STRING] title [STRING] in context [STRING]
参数解释	$1：登录页面语言类型，English或Chinese $2：登录页面标题信息 $3：SSL VPN访问实例名称
日志等级	6
举例	• SSLVPN/6/SSLVPN_CFG_TITLE_FAILED: Failed to configure SSL VPN page English title Mytitle in context ctx1. • SSLVPN/6/SSLVPN_CFG_TITLE_FAILED: Failed to configure SSL VPN page Chinese title 公司 A in context ctx1.
日志说明	配置SSL VPN页面的标题信息失败
处理建议	无

157.153 SSLVPN_CFG_TRAFFICTHRESHOLD

日志内容	Set the idle-cut traffic threshold to [STRING] Kilobytes in context [STRING].
参数解释	$1：配置的流量阈值大小 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_TRAFFICTHRESHOLD: Set the idle-cut traffic threshold to 100 Kilobytes in context ctx1.
日志说明	配置SSL VPN会话保持空闲状态的流量阈值
处理建议	无

157.154 SSLVPN_CFG_TRAFFICTHRESHOLD_FAIL

日志内容	Failed to set the idle-cut traffic threshold to [STRING] Kilobytes in context [STRING].
参数解释	$1：配置的流量阈值大小 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_TRAFFICTHRESHOLD_FAIL: Failed to set the idle-cut traffic threshold to 100 Kilobytes in context ctx1.
日志说明	配置SSL VPN会话保持空闲状态的流量阈值失败
处理建议	无

157.155 SSLVPN_CFG_URLLISTHEAD

日志内容	Configured heading [STRING] for URL-list [STRING] in context [STRING].
参数解释	$1：URL列表标题名称 $2：URL列表名称 $3：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_URLLISTHEAD: Configured heading urlhead for URL-list urllist in context ctx1.
日志说明	配置URL列表标题
处理建议	无

157.156 SSLVPN_CFG_URLLISTHEAD_FAILED

日志内容	Failed to configure heading [STRING] for URL-list [STRING] in context [STRING]
参数解释	$1：URL列表标题名称 $2：URL列表名称 $3：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CFG_URLLISTHEAD_FAILED: Failed to configure heading urlhead for URL-list urllist in context ctx1.
日志说明	配置URL列表标题失败
处理建议	无

157.157 SSLVPN_CFG_WINSSERVER

日志内容	Specified [STRING] WINS server [STRING] in context [STRING].
参数解释	$1：WINS服务器类型，取值为primary或secondary $2：WINS服务器的IPv4地址 $3：SSL VPN访问实例名称
日志等级	6
举例	• SSLVPN/6/SSLVPN_CFG_WINSSERVER: Specified primary WINS server primary 1.1.1.1 in context ctx. • SSLVPN/6/SSLVPN_CFG_WINSSERVER: Specified secondary WINS server secondary 1.1.1.2 in context ctx.
日志说明	配置为客户端指定的内网WINS服务器地址
处理建议	无

157.158 SSLVPN_CFG_WINSSERVER_FAILED

日志内容	Failed to specify [STRING] WINS server [STRING] in context [STRING]
参数解释	$1：WINS服务器类型，取值为primary或secondary $2：WINS服务器的IPv4地址 $3：SSL VPN访问实例名称
日志等级	6
举例	• SSLVPN/6/SSLVPN_CFG_WINSSERVER_FAILED: Failed to specify primary WINS server 1.1.1.1 in context ctx. • SSLVPN/6/SSLVPN_CFG_WINSSERVER_FAILED: Failed to specify secondary WINS server 1.1.1.2 in context ctx.
日志说明	配置为客户端指定的内网WINS服务器地址失败
处理建议	无

157.159 SSLVPN_CLR_AAADOMAIN

日志内容	Deleted the AAA domain specified for context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CLR_AAADOMAIN: Deleted the AAA domain specified for context ctx1.
日志说明	删除SSL VPN访问实例指定的ISP域。SSL VPN访问实例使用缺省的ISP域进行认证
处理建议	无

157.160 SSLVPN_CLR_AAADOMAIN_FAILED

日志内容	Failed to delete the AAA domain specified for context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CLR_AAADOMAIN_FAILED: Failed to delete the AAA domain specified for context ctx1.
日志说明	删除SSL VPN访问实例指定的ISP域失败。SSL VPN访问实例无法使用缺省ISP域进行认证
处理建议	无

157.161 SSLVPN_CLR_AUTHMODE

日志内容	Configured authentication use all in context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CLR_AUTHMODE: Configured authentication use all in context 2.
日志说明	设置SSL VPN用户登录访问实例的认证方式为all
处理建议	无

157.162 SSLVPN_CLR_AUTHMODE_FAILED

日志内容	Failed to configure authentication use all in context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CLR_AUTHMODE_FAILED: Failed to configure authentication use all in context 2.
日志说明	设置SSL VPN用户登录访问实例的认证方式为all失败
处理建议	无

157.163 SSLVPN_CLR_BINDIP

日志内容	Deleted IP address binding configuration for user [STRING] in context [STRING].
参数解释	$1：用户的名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CLR_BINDIP: Deleted IP address binding configuration for user user1 in context ctx1.
日志说明	删除绑定用户IP地址
处理建议	无

157.164 SSLVPN_CLR_BINDIP_FAILED

日志内容	Failed to delete IP address binding configuration for user [STRING] in context [STRING].
参数解释	$1：用户的名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CLR_BINDIP_FAILED: Failed to delete IP address binding configuration for user user1 in context ctx1.
日志说明	删除绑定用户IP地址失败
处理建议	无

157.165 SSLVPN_CLR_CERTATTRIBUTE

日志内容	Specified the attribute cn as the certificate user name in context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CLR_CERTATTRIBUTE: Specified the attribute cn as the certificate user name in context ctx1.
日志说明	将用户证书中作为用户名的字段恢复为cn字段
处理建议	无

157.166 SSLVPN_CLR_CERTATTRIBUTE_FAILED

日志内容	Failed to specify the attribute cn as the certificate user name in context [STRING]..
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CLR_CERTATTRIBUTE_FAILED: Failed to specify the attribute cn as the certificate user name in context ctx1.
日志说明	将用户证书中作为用户名的字段恢复为cn字段失败
处理建议	无

157.167 SSLVPN_CLR_CONTEXT_USERMAX

日志内容	Deleted the maximum number of SSL VPN users in context [UINT32].
参数解释	$1：Context ID
日志等级	6
举例	SSLVPN/6/SSLVPN_CLR_CONTEXT_USERMAX: Deleted the maximum number of SSL VPN users in context 2.
日志说明	删除用户Context最大登录用户数
处理建议	无

157.168 SSLVPN_CLR_CONTEXT_USERMAX_FAILED

日志内容	Failed to delete the maximum number of SSL VPN users in context [UINT32].
参数解释	$1：Context ID
日志等级	6
举例	SSLVPN/6/SSLVPN_CLR_CONTEXT_USERMAX_FAILED: Failed to delete the maximum number of SSL VPN users in context 2.
日志说明	删除用户Context最大登录用户数失败
处理建议	无

157.169 SSLVPN_CLR_CONTEXTVPN

日志内容	Deleted the associated VPN instance in context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CLR_CONTEXTVPN: Deleted the associated VPN instance in context ctx1.
日志说明	删除SSL VPN访问实例关联的VPN实例
处理建议	无

157.170 SSLVPN_CLR_CONTEXTVPN_FAILED

日志内容	Failed to delete the associated VPN instance in context [STRING]
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CLR_CONTEXTVPN_FAILED: Failed to delete the associated VPN instance in context ctx1.
日志说明	删除SSL VPN访问实例关联的VPN实例失败
处理建议	无

157.171 SSLVPN_CLR_CTXGATEWAY

日志内容	Deleted gateway in context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CLR_CTXGATEWAY: Deleted gateway in context ctx1.
日志说明	取消SSL VPN访问实例引用SSL VPN网关
处理建议	无

157.172 SSLVPN_CLR_CTXGATEWAY_FAILED

日志内容	Failed to delete gateway in context [STRING]
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CLR_CTXGATEWAY_FAILED: Failed to delete gateway in context ctx1.
日志说明	取消SSL VPN访问实例引用SSL VPN网关失败
处理建议	无

157.173 SSLVPN_CLR_DEFAULT_PGROUP

日志内容	Deleted default-policy-group in context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CLR_DEFAULT_PGROUP: Deleted default-policy-group in context ctx1.
日志说明	删除SSL VPN访问实例的缺省策略组
处理建议	无

157.174 SSLVPN_CLR_DEFAULT_PGROUP_FAILED

日志内容	Failed to delete default-policy-group in context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CLR_DEFAULT_PGROUP_FAILED: Failed to delete default-policy-group in context ctx1.
日志说明	删除SSL VPN访问实例的缺省策略组失败
处理建议	无

157.175 SSLVPN_CLR_DNSSERVER

日志内容	Deleted [STRING] DNS server in context [STRING].
参数解释	$1：DNS服务器类型，取值为primary或secondary $2：SSL VPN访问实例名称
日志等级	6
举例	• SSLVPN/6/SSLVPN_CLR_DNSSERVER: Deleted primary DNS server in context ctx. • SSLVPN/6/SSLVPN_CLR_DNSSERVER: Deleted secondary DNS server in context ctx.
日志说明	删除为客户端指定的内网DNS服务器
处理建议	无

157.176 SSLVPN_CLR_DNSSERVER_FAILED

日志内容	Failed to delete [STRING] DNS server in context [STRING]
参数解释	$1：primary/secondary，二者选其一 $2：SSL VPN访问实例名称
日志等级	6
举例	• SSLVPN/6/SSLVPN_CLR_DNSSERVER_FAILED: Failed to delete primary DNS server in context ctx. • SSLVPN/6/SSLVPN_CLR_DNSSERVER_FAILED: Failed to delete secondary DNS server in context ctx.
日志说明	删除为客户端指定的内网DNS服务器失败
处理建议	无

157.177 SSLVPN_CLR_EMOSERVER

日志内容	Deleted EMO server in context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CLR_EMOSERVER: Deleted emo-server in context ctx1.
日志说明	删除SSL VPN访问实例中为客户端指定EMO（Endpoint Mobile Office，终端移动办公）服务器
处理建议	无

157.178 SSLVPN_CLR_EMOSERVER_FAILED

日志内容	Failed to delete EMO server in context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CLR_EMOSERVER_FAILED: Failed to delete EMO server in context ctx1.
日志说明	删除SSL VPN访问实例中为客户端指定EMO（Endpoint Mobile Office，终端移动办公）服务器失败
处理建议	无

157.179 SSLVPN_CLR_GATEWAYVPN

日志内容	Deleted VPN instance for gateway [STRING].
参数解释	$1：SSL VPN网关名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CLR_GATEWAYVPN: Deleted VPN instance for gateway gw1.
日志说明	删除SSL VPN网关所属的VPN实例
处理建议	无

157.180 SSLVPN_CLR_GATEWAYVPN_FAILED

日志内容	Failed to delete VPN instance for gateway [STRING].
参数解释	$1：SSL VPN网关名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CLR_GATEWAYVPN_FAILED: Failed to delete VPN instance for gateway gw1.
日志说明	删除SSL VPN网关所属的VPN实例失
处理建议	无

157.181 SSLVPN_CLR_GWIPADDRESS

日志内容	Deleted IP address of gateway [STRING].
参数解释	$1：SSL VPN网关
日志等级	6
举例	SSLVPN/6/SSLVPN_CLR_GWIPADDRESS: Deleted IP address of gateway gw1.
日志说明	删除SSL VPN网关的IP地址
处理建议	无

157.182 SSLVPN_CLR_GWIPADDRESS_FAILED

日志内容	Failed to delete IP address of gateway [STRING]
参数解释	$1：SSL VPN网关
日志等级	6
举例	SSLVPN/6/SSLVPN_CLR_GWIPADDRESS_FAILED: Failed to delete IP address of gateway gw1.
日志说明	删除SSL VPN网关的IP地址失败
处理建议	无

157.183 SSLVPN_CLR_GWIPV6ADDRESS

日志内容	Deleted IPv6 address of gateway [STRING].
参数解释	$1：SSL VPN网关名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CLR_GWIPV6ADDRESS: Deleted IPv6 address of gateway gw1.
日志说明	删除SSL VPN网关的IPv6地址
处理建议	无

157.184 SSLVPN_CLR_GWIPV6ADDRESS_FAILED

日志内容	Failed to delete IPv6 address of gateway [STRING]
参数解释	$1：SSL VPN网关
日志等级	6
举例	SSLVPN/6/SSLVPN_CLR_GWIPV6ADDRESS_FAILED: Failed to delete IPv6 address of gateway gw1.
日志说明	删除SSL VPN网关的IPv6地址失败
处理建议	无

157.185 SSLVPN_CLR_HTTPREDIRECT

日志内容	Disabled HTTP-redirect in gateway [STRING].
参数解释	$1：SSL VPN网关
日志等级	6
举例	SSLVPN/6/SSLVPN_CLR_HTTPREDIRECT: Disabled HTTP-redirect in gateway gw.
日志说明	关闭SSL VPN网关HTTP流量的重定向功能
处理建议	无

157.186 SSLVPN_CLR_HTTPREDIRECT_FAILED

日志内容	Failed to disable HTTP-redirect in gateway [STRING]
参数解释	$1：SSL VPN网关
日志等级	6
举例	SSLVPN/6/SSLVPN_CLR_HTTPREDIRECT_FAILED: Failed to disable HTTP-redirect in gateway gw.
日志说明	关闭SSL VPN网关HTTP流量的重定向功能失败
处理建议	无

157.187 SSLVPN_CLR_IMCADDRESS

日志内容	Deleted the IP address of the iMC server in context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CLR_IMCADDRESS: Deleted the IP address of the iMC server in context ctx1.
日志说明	删除短信认证使用的iMC服务器的IP地址
处理建议	无

157.188 SSLVPN_CLR_IMCADDRESS_FAILED

日志内容	Failed to delete the IP address of the iMC server in context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CLR_IMCADDRESS_FAILED: Failed to delete the IP address of the iMC server in context ctx1.
日志说明	删除短信认证使用的iMC服务器的地址失败
处理建议	无

157.189 SSLVPN_CLR_IPAC_WEBRESPUSH

日志内容	Disabled automatic pushing of Web resources after IP access client login in context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CLR_IPAC_WEBRESPUSH: Disabled automatic pushing of Web resources after IP access client login in context ctx.
日志说明	关闭客户端登录SSL VPN网关后自动打开资源列表功能
处理建议	无

157.190 SSLVPN_CLR_IPAC_WEBRESPUSH_FAIL

日志内容	Failed to disable automatic pushing of Web resources after IP access client login in context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CLR_IPAC_WEBRESPUSH_FAIL: Failed to disable automatic pushing of Web resources after IP access client login in context ctx.
日志说明	关闭客户端登录SSL VPN网关后自动打开资源列表功能失败
处理建议	无

157.191 SSLVPN_CLR_IPCLIENT_AUTOACT

日志内容	Disabled automatic IP access client startup after Web login in context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CLR_IPCLIENT_AUTOACT: Disabled automatic IP access client startup after Web login in context ctx.
日志说明	关闭Web登录SSL VPN网关后自动打开客户端功能
处理建议	无

157.192 SSLVPN_CLR_IPCLIENT_AUTOACT_FAIL

日志内容	Failed to disable automatic IP access client startup after Web login in context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CLR_IPCLIENT_AUTOACT_FAIL: Failed to disable automatic IP access client startup after Web login in context ctx.
日志说明	关闭Web登录SSL VPN网关后自动打开客户端功能失败
处理建议	无

157.193 SSLVPN_CLR_IPTNL_RATE-LIMIT

日志内容	Deleted the rate limit configuration for IP tunnel [STRING] traffic in context [STRING].
参数解释	$1：SSL VPN IP接入流量方向，取值包括： • Upstream 上行流量 • Downstream 下行流量 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CLR_IPTNL_RATE-LIMIT: Deleted the rate limit configuration for IP tunnel upstream traffic in context ctx. SSLVPN/6/SSLVPN_CLR_IPTNL_RATE-LIMIT: Deleted the rate limit configuration for IP tunnel downstream traffic in context ctx.
日志说明	删除IP接入流量限速
处理建议	无

157.194 SSLVPN_CLR_IPTNL_RATE-LIMIT_FAIL

日志内容	Failed to delete the rate limit configuration for IP tunnel [STRING] traffic in context [STRING].
参数解释	$1：SSL VPN IP接入流量方向，取值包括： • Upstream 上行流量 • Downstream 下行流量 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CLR_IPTNL_RATE-LIMIT_FAIL: Failed to delete the rate limit configuration for IP tunnel upstream traffic in context ctx. SSLVPN/6/SSLVPN_CLR_IPTNL_RATE-LIMIT_FAIL: Failed to delete the rate limit configuration for IP tunnel downstream traffic in context ctx.
日志说明	删除IP接入流量限速失败
处理建议	无

157.195 SSLVPN_CLR_IPTUNNELPOOL

日志内容	Deleted address-pool in context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CLR_IPTUNNELPOOL: Deleted address-pool in context ctx.
日志说明	删除IP接入引用的地址池
处理建议	无

157.196 SSLVPN_CLR_IPTUNNELPOOL_FAILED

日志内容	Failed to delete address-pool in context [STRING]
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CLR_IPTUNNELPOOL_FAILED: Failed to delete address-pool in context ctx.
日志说明	删除IP接入引用的地址池失败
处理建议	无

157.197 SSLVPN_CLR_LOCALPORT

日志内容	Deleted the port forwarding instance used by port forwarding item [STRING] in context [STRING].
参数解释	$1：端口转发表项名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CLR_LOCALPORT: Deleted the port forwarding instance used by port forwarding item pfitem1 in context ctx.
日志说明	在端口转发表项中删除端口转发实例
处理建议	无

157.198 SSLVPN_CLR_LOCALPORT_FAILED

日志内容	Failed to delete the port forwarding instance used by port forwarding item [STRING] in context [STRING]
参数解释	$1：端口转发表项名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CLR_LOCALPORT_FAILED: Failed to delete the port forwarding instance used by port forwarding item pfitem1 in context ctx.
日志说明	在端口转发表项中删除端口转发实例失败
处理建议	无

157.199 SSLVPN_CLR_LOGO

日志内容	Configured SSL VPN logo UNIS in context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CLR_LOGO: Configured SSL VPN logo UNIS in context ctx1.
日志说明	配置SSL VPN页面的logo图标为UNIS
处理建议	无

157.200 SSLVPN_CLR_LOGO_FAILED

日志内容	Failed to configure SSL VPN logo UNIS in context [STRING]
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CLR_LOGO_FAILED: Failed to configure SSL VPN logo UNIS in context ctx1.
日志说明	配置SSL VPN页面的logo图标为UNIS时失败
处理建议	无

157.201 SSLVPN_CLR_MSGSERVER

日志内容	Deleted message server in context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CLR_MSGSERVER: Deleted message server in context ctx1.
日志说明	删除SSL VPN访问实例的Message服务器
处理建议	无

157.202 SSLVPN_CLR_MSGSERVER_FAILED

日志内容	Failed to delete message server in context [STRING]
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CLR_MSGSERVER_FAILED: Failed to delete message server in context ctx1.
日志说明	删除SSL VPN访问实例的Message服务器失败
处理建议	无

157.203 SSLVPN_CLR_PFWDEXECUTION

日志内容	Deleted the script for port forwarding item [STRING] in context [STRING].
参数解释	$1：端口转发表项名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CLR_PFWDEXECUTION: Deleted the script for port forwarding item pfitem1 in context ctx.
日志说明	在端口转发表项中删除端口转发表项对应的资源
处理建议	无

157.204 SSLVPN_CLR_PFWDEXECUTION_FAILED

日志内容	Failed to delete the script for port forwarding item [STRING] in context [STRING].
参数解释	$1：端口转发表项名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CLR_PFWDEXECUTION_FAILED: Failed to delete the script for port forwarding item pfitem1 in context ctx.
日志说明	在端口转发表项中删除端口转发表项对应的资源失败
处理建议	无

157.205 SSLVPN_CLR_SCUTDESCRIPTION

日志内容	Deleted the description for shortcut [STRING] in context [STRING].
参数解释	$1：快捷方式名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CLR_SCUTDESCRIPTION: Deleted the description for shortcut shortcut1 in context ctx.
日志说明	删除快捷方式的描述信息
处理建议	无

157.206 SSLVPN_CLR_SCUTDESCRIPTION_FAILED

日志内容	Failed to delete the description for shortcut [STRING] in context [STRING].
参数解释	$1：快捷方式名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CLR_SCUTDESCRIPTION_FAILED: Failed to delete the description for shortcut shortcut1 in context ctx.
日志说明	删除快捷方式的描述信息失败
处理建议	无

157.207 SSLVPN_CLR_SCUTEXECUTION

日志内容	Deleted the script for shortcut [STRING] in context [STRING].
参数解释	$1：快捷方式名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CLR_SCUTEXECUTION: Deleted the script for shortcut shortcut1 in context ctx.
日志说明	在快捷方式中删除对应的资源
处理建议	无

157.208 SSLVPN_CLR_SCUTEXECUTION_FAILED

日志内容	Failed to delete the script for shortcut [STRING] in context [STRING].
参数解释	$1：快捷方式名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CLR_SCUTEXECUTION_FAILED: Failed to delete the script for shortcut shortcut1 in context ctx.
日志说明	在快捷方式中删除对应的资源失败
处理建议	无

157.209 SSLVPN_CLR_SSLCLIENT

日志内容	Deleted the SSL client policy specified for context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CLR_SSLCLIENT: Deleted the SSL client policy specified for context ctx1.
日志说明	删除SSL VPN访问实例引用SSL客户端策略
处理建议	无

157.210 SSLVPN_CLR_SSLCLIENT_FAILED

日志内容	Failed to delete SSL client policy for context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CLR_SSLCLIENT_FAILED: Failed to delete SSL client policy for context ctx1.
日志说明	删除SSL VPN访问实例引用SSL客户端策略失败
处理建议	无

157.211 SSLVPN_CLR_SSLSERVER

日志内容	Deleted the SSL server policy specified for gateway [STRING].
参数解释	$1：SSL VPN网关名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CLR_SSLSERVER: Deleted the SSL server policy specified for gateway gw1.
日志说明	删除SSL VPN网关引用SSL服务器端策略
处理建议	无

157.212 SSLVPN_CLR_SSLSERVER_FAILED

日志内容	Failed to delete SSL server policy for gateway [STRING]
参数解释	$1：SSL VPN网关名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CLR_SSLSERVER_FAILED: Failed to delete SSL server policy for gateway gw1.
日志说明	删除SSL VPN网关引用SSL服务器端策略失败
处理建议	无

157.213 SSLVPN_CLR_TRAFFICTHRESHOLD

日志内容	Deleted the idle-cut traffic threshold in context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CLR_TRAFFICTHRESHOLD: Deleted the idle-cut traffic threshold in context ctx1.
日志说明	删除配置的SSL VPN会话保持空闲状态的流量阈值
处理建议	无

157.214 SSLVPN_CLR_TRAFFICTHRESHOLD_FAIL

日志内容	Failed to delete the idle-cut traffic threshold in context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_CLR_TRAFFICTHRESHOLD_FAIL: Failed to delete the idle-cut traffic threshold in context ctx1.
日志说明	删除配置的SSL VPN会话保持空闲状态的流量阈值失败
处理建议	无

157.215 SSLVPN_CLR_WINSSERVER

日志内容	Deleted [STRING] WINS server in context [STRING].
参数解释	$1：WINS服务器类型，取值为primary或secondary $2：SSL VPN访问实例名称
日志等级	6
举例	• SSLVPN/6/SSLVPN_CLR_WINSSERVER: Deleted primary WINS server 1.1.1.1 in context ctx. • SSLVPN/6/SSLVPN_CLR_WINSSERVER: Deleted secondary WINS server 1.1.1.2 in context ctx.
日志说明	删除为客户端指定的内网WINS服务器地址
处理建议	无

157.216 SSLVPN_CLR_WINSSERVER_FAILED

日志内容	Failed to delete [STRING] WINS server in context [STRING]
参数解释	$1：WINS服务器类型，取值为primary或secondary $2：SSL VPN访问实例名称
日志等级	6
举例	• SSLVPN/6/SSLVPN_CLR_WINSSERVER_FAILED: Failed to delete primary WINS server 1.1.1.1 in context ctx. • SSLVPN/6/SSLVPN_CLR_WINSSERVER_FAILED: Failed to delete secondary WINS server 1.1.1.2 in context ctx.
日志说明	删除为客户端指定的内网WINS服务器地址失败
处理建议	无

157.217 SSLVPN_DEL_CONTENT_TYPE

日志内容	Deleted the content type configuration for file policy [STRING] in context [STRING].
参数解释	$1：文件策略名称 $2：SSLVPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_CONTENT_TYPE: Deleted the content type configuration for file policy fp1 in context ctx1.
日志说明	删除需要进行改写的文件类型
处理建议	无

157.218 SSLVPN_DEL_CONTENT_TYPE_FAILED

日志内容	Failed to delete the content type configuration for file policy [STRING] in context [STRING].
参数解释	$1：文件策略名称 $2：SSLVPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_CONTENT_TYPE_FAILED: Failed to delete the content type configuration for file policy fp1 in context ctx1.
日志说明	删除需要进行改写的文件类型失败
处理建议	无

157.219 SSLVPN_DEL_CONTEXT

日志内容	Deleted SSL VPN context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_CONTEXT: Deleted SSL VPN context ctx1.
日志说明	删除SSL VPN访问实例
处理建议	无

157.220 SSLVPN_DEL_CONTEXT_FAILED

日志内容	Failed to delete SSL VPN context [STRING]
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_CONTEXT_FAILED: Failed to delete SSL VPN context ctx1.
日志说明	删除SSL VPN访问实例失败
处理建议	无

157.221 SSLVPN_DEL_EXCROUTEITEM

日志内容	Deleted exclude route (IP [STRING] mask [STRING]) from route list [STRING] in context [STRING].
参数解释	$1：路由的目的地址 $2：路由的掩码 $3：路由列表名称 $4：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_EXCROUTEITEM: Deleted exclude route (IP 10.0.0.0 mask 255.0.0.0) from route list rtlist in context ctx1.
日志说明	在SSL VPN访问实例视图下的路由列表中删除例外路由表项
处理建议	无

157.222 SSLVPN_DEL_EXCROUTEITEM_FAILED

日志内容	Failed to delete exclude route (IP [STRING] mask [STRING]) from route list [STRING] in context [STRING]
参数解释	$1：路由的目的地址 $2：路由的掩码 $3：路由列表名称 $4：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_EXCROUTEITEM_FAILED: Failed to delete exclude route (IP 10.0.0.0 mask 255.0.0.0) from route list rtlist in context ctx1.
日志说明	在SSL VPN访问实例视图下的路由列表中删除例外路由失败
处理建议	无

157.223 SSLVPN_DEL_FILEPOLICY

日志内容	Deleted file policy [STRING] in context [STRING].
参数解释	$1：文件策略名称 $2：SSLVPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_FILEPOLICY: Deleted file policy fp1 in context ctx1.
日志说明	删除文件策略
处理建议	无

157.224 SSLVPN_DEL_FILEPOLICY_FAILED

日志内容	Failed to delete file policy [STRING] in context [STRING].
参数解释	$1：文件策略名称 $2：SSLVPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_FILEPOLICY_FAILED: Failed to delete file policy fp1 in context ctx1.
日志说明	删除文件策略失败
处理建议	无

157.225 SSLVPN_DEL_GATEWAY

日志内容	Deleted SSL VPN gateway [STRING].
参数解释	$1：SSL VPN网关名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_GATEWAY: Deleted SSL VPN gateway gw1.
日志说明	删除SSL VPN网关
处理建议	无

157.226 SSLVPN_DEL_GATEWAY_FAILED

日志内容	Failed to delete SSL VPN gateway [STRING]
参数解释	$1：SSL VPN网关名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_GATEWAY_FAILED: Failed to delete SSL VPN gateway gw1.
日志说明	删除SSL VPN网关失败
处理建议	无

157.227 SSLVPN_DEL_INCROUTEITEM

日志内容	Deleted inlcude route (IP [STRING] mask [STRING]) from route list [STRING] in context [STRING].
参数解释	$1：路由的目的地址 $2：路由的掩码 $3：路由列表名称 $4：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_INCROUTEITEM: Deleted include route (IP 10.0.0.0 mask 255.0.0.0) from route list rtlist in context ctx1.
日志说明	在SSL VPN访问实例视图下的路由列表中删除路由表项
处理建议	无

157.228 SSLVPN_DEL_INCROUTEITEM_FAILED

日志内容	Failed to delete include route (IP [STRING] mask [STRING]) from route list [STRING] in context [STRING]
参数解释	$1：路由的目的地址 $2：路由的掩码 $3：路由列表名称 $4：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_INCROUTEITEM_FAILED: Failed to delete include route (IP 10.0.0.0 mask 255.0.0.0) from route list rtlist in context ctx1.
日志说明	在SSL VPN访问实例视图下的路由列表中删除路由失败
处理建议	无

157.229 SSLVPN_DEL_IPADDRESSPOOL

日志内容	Deleted IP address pool [STRING].
参数解释	$1：IP地址池名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_IPADDRESSPOOL: Deleted IP address pool pool1.
日志说明	删除SSL VPN的地址池
处理建议	无

157.230 SSLVPN_DEL_IPADDRESSPOOL_FAILED

日志内容	Failed to delete IP address pool [STRING]
参数解释	$1：IP地址池名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_IPADDRESSPOOL_FAILED: Failed to delete IP address pool pool1.
日志说明	删除SSL VPN的地址池失败
处理建议	无

157.231 SSLVPN_DEL_IPTUNNELACIF

日志内容	Deleted SSL VPN AC interface in context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_IPTUNNELACIF: Deleted SSL VPN AC interface in context ctx.
日志说明	删除IP接入引用的SSL VPN AC接口
处理建议	无

157.232 SSLVPN_DEL_IPTUNNELACIF_FAILED

日志内容	Failed to delete SSL VPN AC interface in context [STRING]
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_IPTUNNELACIF_FAILED: Failed to delete SSL VPN AC interface in context ctx.
日志说明	删除IP接入引用的SSL VPN AC接口失败
处理建议	无

157.233 SSLVPN_DEL_IPV4_RANGE

日志内容	Deleted the IPv4 address range of SNAT pool [STRING].
参数解释	$1：SSL VPN SNAT地址池名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_IPV4_RANGE: Deleted IPv4 address range of SNAT pool sp1.
日志说明	删除SSL VPN SNAT地址池的IPv4地址范围
处理建议	无

157.234 SSLVPN_DEL_IPV4_RANGE_FAILED

日志内容	Failed to delete the IPv4 address range of SNAT pool [STRING].
参数解释	$1：SSL VPN SNAT地址池名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_IPV4_RANGE_FAILED: Failed to delete IPv4 address range of SNAT pool sp1.
日志说明	删除SSL VPN SNAT地址池的IPv4地址范围失败
处理建议	无

157.235 SSLVPN_DEL_IPV6_RANGE

日志内容	Deleted IPv6 address range of SNAT pool [STRING].
参数解释	$1：SSL VPN SNAT地址池名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_IPV6_RANGE: Deleted IPv6 address range of SNAT pool sp1.
日志说明	删除SSL VPN SNAT地址池的IPv6地址范围
处理建议	无

157.236 SSLVPN_DEL_IPV6_RANGE_FAILED

日志内容	Failed to delete IPv6 address range of SNAT pool [STRING].
参数解释	$1：SSL VPN SNAT地址池名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_IPV6_RANGE_FAILED: Failed to delete IPv6 address range of SNAT pool sp1.
日志说明	删除SSL VPN SNAT地址池的IPv6地址范围失败
处理建议	无

157.237 SSLVPN_DEL_LOCALPORT

日志内容	Deleted port forwarding entry local-port [STRING] local-name [STRING] in port forwarding list [STRING] in context [STRING].
参数解释	$1：本地端口号 $2：本地地址或本地主机名称 $3：端口转发列表名称 $4：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_LOCALPORT: Deleted port forwarding entry local-port 80 local-name 127.0.0.1 in port forwarding list pflist1 in context ctx.
日志说明	在端口转发列表中删除端口转发实例
处理建议	无

157.238 SSLVPN_DEL_LOCALPORT_FAILED

日志内容	Failed to delete port forwarding entry local-port [STRING] local-name [STRING] in port forwarding list [STRING] in context [STRING]
参数解释	$1：本地端口号 $2：本地地址或本地主机名称 $3：转发实例的描述信息 $4：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_LOCALPORT_FAILED: Failed to delete port forwarding entry local-port 80 local-name 127.0.0.1 in port forwarding list pflist1 in context ctx.
日志说明	在端口转发列表中删除端口转发实例失败
处理建议	无

157.239 SSLVPN_DEL_NEWCONTENT

日志内容	Deleted the new content configuration for rewrite rule [STRING] in file policy [STRING] in context [STRING].
参数解释	$1：改写规则名称 $2：文件策略名称 $3：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_NEWCONTENT: Deleted the new content configuration for rewrite rule rw in file policy fp in context ctx.
日志说明	删除改写规则指定改写后的报文内容
处理建议	无

157.240 SSLVPN_DEL_NEWCONTENT_FAILED

日志内容	Failed to delete the new content configuration for rewrite rule [STRING] in file policy [STRING] in context [STRING].
参数解释	$1：改写规则名称 $2：文件策略名称 $3：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_NEWCONTENT_FAILED: Failed to delete the new content configuration for rewrite rule rw in file policy fp in context ctx.
日志说明	删除改写规则指定改写后的报文内容失败
处理建议	无

157.241 SSLVPN_DEL_OLDCONTENT

日志内容	Deleted the old content configuration for rewrite rule [STRING] in file policy [STRING] in context [STRING].
参数解释	$1：改写规则名称 $2：文件策略名称 $3：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_OLDCONTENT: Deleted the old content configuration for rewrite rule rw in file policy fp in context ctx.
日志说明	删除改写规则原始报文内容
处理建议	无

157.242 SSLVPN_DEL_OLDCONTENT_FAILED

日志内容	Failed to delete the old content configuration for rewrite rule [STRING] in file policy [STRING] in context [STRING].
参数解释	$1：改写规则名称 $2：文件策略名称 $3：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_OLDCONTENT_FAILED: Failed to delete the old content configuration for rewrite rule rw in file policy fp in context ctx.
日志说明	删除改写规则原始报文内容失败
处理建议	无

157.243 SSLVPN_DEL_PORTFWD

日志内容	Deleted port forwarding list [STRING] in context [STRING].
参数解释	$1：端口转发列表名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_PORTFWD: Deleted port forwarding list pf in context ctx1.
日志说明	删除端口转发列表
处理建议	无

157.244 SSLVPN_DEL_PORTFWD_FAILED

日志内容	Failed to delete port forwarding list [STRING] in context [STRING]
参数解释	$1：端口转发列表名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_PORTFWD_FAILED: Failed to delete port forwarding list pf in context ctx1.
日志说明	删除端口转发列表失败
处理建议	无

157.245 SSLVPN_DEL_PORTFWD_ITEM

日志内容	Deleted port forwarding item [STRING] in context [STRING].
参数解释	$1：端口转发表项名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_PORTFWD_ITEM: Deleted port forwarding item pfitem in context ctx1.
日志说明	删除端口转发表项
处理建议	无

157.246 SSLVPN_DEL_PORTFWD_ITEM_FAILED

日志内容	Failed to delete port forwarding item [STRING] in context [STRING]
参数解释	$1：端口转发表项名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_PORTFWD_ITEM_FAILED: Failed to delete port forwarding item pfitem in context ctx1.
日志说明	删除端口转发表项失败
处理建议	无

157.247 SSLVPN_DEL_PYGROUP

日志内容	Deleted policy group [STRING] in context [STRING].
参数解释	$1：策略组名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_PYGROUP: Deleted policy group pg in context ctx1.
日志说明	删除SSL VPN策略组
处理建议	无

157.248 SSLVPN_DEL_PYGROUP_FAILED

日志内容	Failed to delete policy group [STRING] in context [STRING]
参数解释	$1：策略组名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_PYGROUP_FAILED: Failed to delete policy group pg in context ctx1.
日志说明	删除SSL VPN策略组失败
处理建议	该策略组正在被引用，无法被删除

157.249 SSLVPN_DEL_REFERIPACL

日志内容	Deleted IP access filter in policy group [STRING] in context [STRING].
参数解释	$1：策略组名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_REFERIPACL: Deleted IP access filter in policy group pgroup in context ctx1.
日志说明	策略组下删除IP接入过滤功能
处理建议	无

157.250 SSLVPN_DEL_REFERIPACL_FAILED

日志内容	Failed to delete IP access filter in policy group [STRING] in context [STRING]
参数解释	$1：策略组名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_REFERIPACL_FAILED: Failed to delete IP access filter in policy group pgroup in context ctx1
日志说明	策略组下删除IP接入过滤功能失败
处理建议	无

157.251 SSLVPN_DEL_REFERPFWDITEM

日志内容	Removed port forwarding item [STRING] from port forwarding list [STRING] in context [STRING].
参数解释	$1：端口转发表项名称 $2：端口转发列表名称 $3：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_REFERPFWDITEM: Removed port forwarding item pfitem1 from port forwarding list pflist1 in context ctx1.
日志说明	删除端口转发列表引用端口转发表项
处理建议	无

157.252 SSLVPN_DEL_REFERPFWDITEM_FAILED

日志内容	Failed to remove port forwarding item [STRING] from port forwarding list [STRING] in context [STRING].
参数解释	$1：端口转发表项名称 $2：端口转发列表名称 $3：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_REFERPFWDITEM_FAILED: Failed to remove port forwarding item pfitem1 from port forwarding list pflist1 in context ctx1.
日志说明	删除端口转发列表引用端口转发表项失败
处理建议	无

157.253 SSLVPN_DEL_REFERPORTFWD

日志内容	Deleted port forwarding list used by policy-group [STRING] in context [STRING].
参数解释	$1：策略组名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_REFERPORTFWD: Deleted port forwarding list used by policy-group pg in context ctx1.
日志说明	删除策略组引用端口转发列表
处理建议	无

157.254 SSLVPN_DEL_REFERPORTFWD_FAILED

日志内容	Failed to delete port forwarding list used by policy-group [STRING] in context [STRING]
参数解释	$1：策略组名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_REFERPORTFWD_FAILED: Failed to delete port forwarding list used by policy-group pg in context ctx1.
日志说明	删除策略组引用端口转发列表失败
处理建议	无

157.255 SSLVPN_DEL_REFERSCUTLIST

日志内容	Removed shortcut list from policy group [STRING] in context [STRING].
参数解释	$1：策略组名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_REFERSCUTLIST: Removed shortcut list from policy group pg in context ctx1.
日志说明	删除策略组引用快捷方式列表
处理建议	无

157.256 SSLVPN_DEL_REFERSCUTLIST_FAILED

日志内容	Failed to remove shortcut list from policy group [STRING] in context [STRING].
参数解释	$1：策略组名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_REFERSCUTLIST_FAILED: Failed to remove shortcut list from policy group pg in context ctx1.
日志说明	删除策略组引用快捷方式列表失败
处理建议	无

157.257 SSLVPN_DEL_REFERSHORTCUT

日志内容	Removed shortcut [STRING] from shortcut list [STRING] in context [STRING].
参数解释	$1：快捷方式名称 $2：快捷方式列表名称 $3：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_REFERSHORTCUT: Removed shortcut shortcut1 from shortcut list scutlist1 in context ctx1.
日志说明	删除快捷方式列表引用快捷方式
处理建议	无

157.258 SSLVPN_DEL_REFERSHORTCUT_FAILED

日志内容	Failed to remove shortcut [STRING] from shortcut list [STRING] in context [STRING].
参数解释	$1：快捷方式名称 $2：快捷方式列表名称 $3：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_REFERSHORTCUT_FAILED: Failed to remove shortcut shortcut1 from shortcut list scutlist1 in context ctx1.
日志说明	删除快捷方式列表引用快捷方式失败
处理建议	无

157.259 SSLVPN_DEL_REFERSNATPOOL

日志内容	Deleted the SNAT pool used in context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_REFERSNATPOOL: Deleted the SNAT pool used in context ctx1.
日志说明	删除SSLVPN访问实例引用的SNAT地址池
处理建议	无

157.260 SSLVPN_DEL_REFERSNATPOOL_FAILED

日志内容	Failed to delete the SNAT pool used in context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_REFERSNATPOOL_FAILED: Failed to delete the SNAT pool used in context cxt1.
日志说明	删除SSLVPN访问实例引用的SNAT地址池失败
处理建议	无

157.261 SSLVPN_DEL_REFERTCPACL

日志内容	Deleted TCP access filter in policy group [STRING] in context [STRING].
参数解释	$1：策略组名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_REFERTCPACL: Deleted TCP access filter in policy group pgroup in context ctx1.
日志说明	在策略组下删除TCP接入过滤功能
处理建议	无

157.262 SSLVPN_DEL_REFERTCPACL_FAILED

日志内容	Failed to delete TCP access filter in policy group [STRING] in context [STRING]
参数解释	$1：策略组名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_REFERTCPACL_FAILED: Failed to delete TCP access filter in policy group pgroup in context ctx1.
日志说明	在策略组下删除TCP接入过滤功能失败
处理建议	无

157.263 SSLVPN_DEL_REFERURIACL

日志内容	Deleted [STRING] access filter URI ACL from policy group [STRING] in context [STRING].
参数解释	$1：SSL VPN接入方式类型，取值包括： • IP 接入方式 • Web 接入方式 • TCP 接入方式 $2：策略组名称 $3：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_REFERURIACL: Deleted IP access filter URI ACL from policy group pgroup in context ctx1.
日志说明	策略组下删除URI过滤规则
处理建议	无

157.264 SSLVPN_DEL_REFERURIACL_FAILED

日志内容	Failed to delete [STRING] access filter URI ACL from policy group [STRING] in context [STRING].
参数解释	$1：SSL VPN接入方式类型，取值包括： • IP 接入方式 • Web 接入方式 • TCP 接入方式 $2：策略组名称 $3：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_REFERURIACL_FAILED: Failed to delete IP access filter URI ACL from policy group pgroup in context ctx1.
日志说明	策略组下删除URI过滤规则失败
处理建议	无

157.265 SSLVPN_DEL_REFERURLITEM

日志内容	Deleted URL item [STRING] from URL list [STRING] in context [STRING].
参数解释	$1：URL表项的名称 $2：URL列表的名称 $3：SSL VPN访问实例的名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_REFERURLITEM: Deleted URL item item1 from URL list list1 in context ctx1.
日志说明	删除引用的URL表项成功
处理建议	无

157.266 SSLVPN_DEL_REFERURLITEM_FAILED

日志内容	Failed to delete URL item [STRING] from URL list [STRING] in context [STRING].
参数解释	$1：URL表项的名称 $2：URL列表的名称 $3：SSL VPN访问实例的名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_REFERURLITEM_FAILED: Failed to delete URL item item1 from URL list list1 in context ctx1.
日志说明	删除引用的URL表项失败
处理建议	无

157.267 SSLVPN_DEL_REFERURLLIST

日志内容	Deleted URL list [STRING] used by policy-group [STRING] in context [STRING].
参数解释	$1：URL列表名称 $2：策略组名称 $3：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_REFERURLLIST: Deleted URL list urllist used by policy-group pg in context ctx1.
日志说明	删除策略组引用指定的URL列表
处理建议	无

157.268 SSLVPN_DEL_REFERURLLIST_FAILED

日志内容	Failed to delete URL list [STRING] used by policy-group [STRING] in context [STRING]
参数解释	$1：URL列表名称 $2：策略组名称 $3：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_REFERURLLIST_FAILED: Failed to delete URL list urllist used by policy-group pg in context ctx1.
日志说明	删除策略组引用指定的URL列表失败
处理建议	无

157.269 SSLVPN_DEL_REFERWEBACL

日志内容	Deleted Web access filter in policy group [STRING] in context [STRING].
参数解释	$1：策略组名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_REFERWEBACL: Deleted Web access filter in policy group pgroup in context ctx1.
日志说明	在策略组下删除Web接入过滤功能
处理建议	无

157.270 SSLVPN_DEL_REFERWEBACL_FAILED

日志内容	Failed to delete Web access filter in policy group [STRING] in context [STRING]
参数解释	$1：策略组名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_REFERWEBACL_FAILED: Failed to delete Web access filter in policy group pgroup in context ctx1
日志说明	在策略组下删除Web接入过滤功能失败
处理建议	无

157.271 SSLVPN_DEL_REWRITE_RULE

日志内容	Deleted rewrite rule [STRING] from file policy [STRING] in context [STRING].
参数解释	$1：改写规则名称 $2：文件策略名称 $3：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_REWRITE_RULE: Deleted rewrite rule rw from file policy fp in context ctx.
日志说明	删除改写规则
处理建议	无

157.272 SSLVPN_DEL_REWRITE_RULE_FAILED

日志内容	Failed to delete rewrite rule [STRING] from file policy [STRING] in context [STRING].
参数解释	$1：改写规则名称 $2：文件策略名称 $3：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_REWRITE_RULE_FAILED: Failed to delete rewrite rule rw from file policy fp in context ctx.
日志说明	删除改写规则失败
处理建议	无

157.273 SSLVPN_DEL_ROUTELIST

日志内容	Deleted IP-route-list [STRING] in context [STRING].
参数解释	$1：路由列表名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_ROUTELIST: Deleted IP-route-list rtlist in context ctx1.
日志说明	在SSL VPN访问实例中删除路由列表
处理建议	无

157.274 SSLVPN_DEL_ROUTELIST_FAILED

日志内容	Failed to delete IP-route-list [STRING] in context [STRING]
参数解释	$1：路由列表名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_ROUTELIST_FAILED: Failed to delete IP-route-list rtlist in context ctx1.
日志说明	在SSL VPN访问实例中删除路由列表失败
处理建议	无

157.275 SSLVPN_DEL_ROUTEREFER

日志内容	Deleted access routes [STRING] in policy-group [STRING] in context [STRING].
参数解释	$1：取值包括force-all或空，取值为force-all表示强制删除路由表项，取值为空表示非强制删除表项 $2：策略组名称 $3：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_ROUTEREFER: Deleted access routes in policy-group pg in context ctx.
日志说明	删除下发给客户端的路由表项
处理建议	无

157.276 SSLVPN_DEL_ROUTEREFER_FAILED

日志内容	Failed to delete access routes [STRING] in policy-group [STRING] in context [STRING]
参数解释	$1：取值包括force-all或空，取值为force-all表示强制删除路由表项，取值为空表示非强制删除表项 $2：策略组名称 $3：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_ROUTEREFER_FAILED: Failed to delete access routes in policy-group pg in context ctx.
日志说明	删除下发给客户端的路由表项失败
处理建议	无

157.277 SSLVPN_DEL_SERVERURL

日志内容	Deleted URL [STRING] from URL item [STRING] in context [STRING].
参数解释	$1：URL表项配置的URL $2：URL表项的名称 $3：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_SERVERURL: Deleted URL www.abc.com from URL item item1 in context ctx1.
日志说明	删除URL表项对应资源的URL成功
处理建议	无

157.278 SSLVPN_DEL_SERVERURL_FAILED

日志内容	Failed to delete URL [STRING] from URL item [STRING] in context [STRING].
参数解释	$1：URL表项配置的URL $2：URL表项的名称 $3：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_SERVERURL_FAILED: Failed to delete URL www.abc.com from URL item item1 in context ctx1.
日志说明	删除URL表项对应资源的URL失败
处理建议	无

157.279 SSLVPN_DEL_SHORTCUT

日志内容	Deleted shortcut [STRING] in context [STRING].
参数解释	$1：快捷方式名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_SHORTCUT: Deleted shortcut shortcut1 in context ctx1.
日志说明	删除快捷方式
处理建议	无

157.280 SSLVPN_DEL_SHORTCUT_FAILED

日志内容	Failed to delete shortcut [STRING] in context [STRING].
参数解释	$1：快捷方式名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_SHORTCUT_FAILED: Failed to delete shortcut shortcut1 in context ctx1.
日志说明	删除快捷方式失败
处理建议	无

157.281 SSLVPN_DEL_SHORTCUTLIST

日志内容	Deleted shortcut list [STRING] in context [STRING].
参数解释	$1：快捷方式列表名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_SHORTCUTLIST: Deleted shortcut list scutlist1 in context ctx1.
日志说明	删除快捷方式列表
处理建议	无

157.282 SSLVPN_DEL_SHORTCUTLIST_FAILED

日志内容	Failed to delete shortcut list [STRING] in context [STRING].
参数解释	$1：快捷方式列表名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_SHORTCUTLIST_FAILED: Failed to delete shortcut list scutlist1 in context ctx1.
日志说明	删除快捷方式列表失败
处理建议	无

157.283 SSLVPN_DEL_SNATPOOL

日志内容	Deleted SSL VPN SNAT pool [STRING].
参数解释	$1：SSL VPN SNAT地址池名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_SNATPOOL: Deleted SSL VPN SNAT pool sp1.
日志说明	删除SSL VPN SNAT地址池
处理建议	无

157.284 SSLVPN_DEL_SNATPOOL_FAILED

日志内容	Failed to delete SSL VPN SNAT pool [STRING].
参数解释	$1：SSL VPN SNAT地址池名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_SNATPOOL_FAILED: Failed to delete SSL VPN SNAT pool sp1.
日志说明	删除SSL VPN SNAT地址池失败
处理建议	无

157.285 SSLVPN_DEL_URIACL

日志内容	Deleted URI ACL [STRING] in context [STRING].
参数解释	$1：URI ACL名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_URIACL: Deleted URI ACL uacl in context ctx1.
日志说明	删除URI ACL
处理建议	无

157.286 SSLVPN_DEL_URIACL_FAILED

日志内容	Failed to delete URI ACL [STRING] in context [STRING].
参数解释	$1：URI ACL名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_URIACL_FAILED: Failed to delete URI ACL uacl in context ctx1.
日志说明	删除URI ACL失败
处理建议	无

157.287 SSLVPN_DEL_URIACL_RULE

日志内容	Deleted rule [UINT32] from URI ACL [STRING] in context [STRING].
参数解释	$1：规则编号 $2：URI ACL名称 $3：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_URIACL_RULE: Deleted rule 5 from URI ACL uacl in context ctx1.
日志说明	删除URI ACL规则
处理建议	无

157.288 SSLVPN_DEL_URIACL_RULE_FAILED

日志内容	Failed to delete rule [UINT32] from URI ACL [STRING] in context [STRING].
参数解释	$1：规则编号 $2：URI ACL名称 $3：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_URIACL_RULE_FAILED: Failed to delete rule 5 from URI ACL uacl in context ctx1.
日志说明	删除URI ACL规则失败
处理建议	无

157.289 SSLVPN_DEL_URL

日志内容	Deleted the URL configuration for file policy [STRING] in context [STRING].
参数解释	$1：文件策略名称 $2：SSLVPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_URL: Deleted the URL configuration for file policy fp1 in context ctx1.
日志说明	删除文件策略最终应用的网页文件的URL
处理建议	无

157.290 SSLVPN_DEL_URL_FAILED

日志内容	Failed to delete the URL configuration for file policy [STRING] in context [STRING].
参数解释	$1：文件策略名称 $2：SSLVPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_URL_FAILED: Failed to delete the URL configuration for file policy fp1 in context ctx1.
日志说明	删除文件策略最终应用的网页文件的URL失败
处理建议	无

157.291 SSLVPN_DEL_URLITEM

日志内容	Deleted URL item [STRING] in context [STRING].
参数解释	$1：URL表项的名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_URLITEM: Deleted URL item item1 in context ctx1.
日志说明	删除URL表项成功
处理建议	无

157.292 SSLVPN_DEL_URLITEM_FAILED

日志内容	Failed to delete URL item [STRING] in context [STRING].
参数解释	$1：URL表项的名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_URLITEM_FAILED: Failed to delete URL item item1 in context ctx1.
日志说明	删除URL表项失败
处理建议	无

157.293 SSLVPN_DEL_URLLIST

日志内容	Deleted URL list [STRING] in context [STRING].
参数解释	$1：URL列表名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_URLLIST: Deleted URL list urllist in context ctx1.
日志说明	删除URL列表
处理建议	无

157.294 SSLVPN_DEL_URLLIST_FAILED

日志内容	Failed to delete URL list [STRING] in context [STRING]
参数解释	$1：URL列表名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_URLLIST_FAILED: Failed to delete URL list urllist in context ctx1.
日志说明	删除URL列表失败
处理建议	无

157.295 SSLVPN_DEL_URLMAPPING

日志内容	Deleted URL mapping from URL item [STRING] in context [STRING].
参数解释	$1：URL表项的名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_URLMAPPING: Deleted URL mapping from URL item item1 in context ctx1.
日志说明	删除URL表项配置的URL资源映射成功
处理建议	无

157.296 SSLVPN_DEL_URLMAPPING_FAILED

日志内容	Failed to delete URL mapping from URL item [STRING] in context [STRING].
参数解释	$1：URL表项的名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_URLMAPPING_FAILED: Failed to delete URL mapping from URL item item1 in context ctx1.
日志说明	删除URL表项配置的URL资源映射失败
处理建议	无

157.297 SSLVPN_DEL_USER

日志内容	Deleted user [STRING] in context [STRING].
参数解释	$1：用户的名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_USER: Deleted user user1 in context ctx1.
日志说明	删除SSL VPN用户
处理建议	无

157.298 SSLVPN_DEL_USER_FAILED

日志内容	Failed to delete user [STRING] in context [STRING].
参数解释	$1：用户的名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DEL_USER_FAILED: Failed to delete user user1 in context ctx1.
日志说明	删除SSL VPN用户失败
处理建议	无

157.299 SSLVPN_DISABLE_CONTEXT

日志内容	Disabled service in context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DISABLE_CONTEXT: Disabled service in context ctx1.
日志说明	关闭SSL VPN访问实例
处理建议	无

157.300 SSLVPN_DISABLE_CONTEXT_FAILED

日志内容	Failed to disable service in context [STRING]
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DISABLE_CONTEXT_FAILED: Failed to disable service in context ctx1.
日志说明	关闭SSL VPN访问实例失败
处理建议	无

157.301 SSLVPN_DISABLE_CRTAUTH

日志内容	Disabled certificate-authentication in context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DISABLE_CRTAUTH: Disabled certificate-authentication in context ctx1.
日志说明	在SSL VPN访问实例中关闭证书认证功能
处理建议	无

157.302 SSLVPN_DISABLE_CRTAUTH_FAILED

日志内容	Failed to disable certificate-authentication in context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DISABLE_CRTAUTH_FAILED: Failed to disable certificate-authentication in context ctx1.
日志说明	在SSL VPN访问实例中关闭证书认证功能失败
处理建议	无

157.303 SSLVPN_DISABLE_DYNAMICPWD

日志内容	Disabled dynamic-password in context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DISABLE_DYNAMICPWD: Disabled dynamic-password in context ctx1.
日志说明	在SSL VPN访问实例中关闭动态口令验证功能
处理建议	无

157.304 SSLVPN_DISABLE_DYNAMICPWD_FAILED

日志内容	Failed to disable dynamic-password in context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DISABLE_DYNAMICPWD_FAILED: Failed to disable dynamic-password in context ctx1.
日志说明	在SSL VPN访问实例中关闭动态口令验证功能失败
处理建议	无

157.305 SSLVPN_DISABLE_GATEWAY

日志内容	Disabled service in gateway [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DISABLE_GATEWAY: Disabled service in gateway gw1.
日志说明	关闭SSL VPN网关
处理建议	无

157.306 SSLVPN_DISABLE_GATEWAY_FAILED

日志内容	Failed to disable service in gateway [STRING]
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DISABLE_GATEWAY_FAILED: Failed to disable service in gateway gw1.
日志说明	关闭SSL VPN网关失败
处理建议	无

157.307 SSLVPN_DISABLE_GLOBAL_LOG

日志内容	Disabled SSL VPN logging globally.
参数解释	无
日志等级	6
举例	SSLVPN/6/SSLVPN_DISABLE_GLOBAL_LOG: Disabled SSL VPN logging globally.
日志说明	关闭SSL VPN全局日志功能
处理建议	无

157.308 SSLVPN_DISABLE_GLOBAL_LOG_FAILED

日志内容	Failed to disable SSL VPN logging globally.
参数解释	无
日志等级	6
举例	SSLVPN/6/SSLVPN_DISABLE_GLOBAL_LOG_FAILED: Failed to disable SSL VPN logging globally.
日志说明	关闭SSL VPN全局日志功能失败
处理建议	无

157.309 SSLVPN_DISABLE_GLOBALURLMASKING

日志内容	Disabled global URL masking in context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DISABLE_GLOBALURLMASKING: Disabled global URL masking in context ctx1.
日志说明	在SSL VPN访问实例中关闭全局URL伪装功能
处理建议	无

157.310 SSLVPN_DISABLE_GLOBALURLMASKING_FAILED

日志内容	Failed to disable global URL masking in context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DISABLE_GLOBALURLMASKING_FAILED: Failed to disable global URL masking in context ctx1.
日志说明	在SSL VPN访问实例中关闭全局URL伪装功能失败
处理建议	无

157.311 SSLVPN_DISABLE_IPTNL_LOG

日志内容	Disabled IP tunnel access logging in context [STRING]. Log type is [STRING].
参数解释	$1：SSL VPN访问实例名称 $2：日志类型，取值包括： • CONNECTION-CLOSE，表示连接关闭日志 • PACKET-DROP，表示丢包日志
日志等级	6
举例	SSLVPN/6/SSLVPN_DISABLE_IPTNL_LOG: Disabled IP tunnel access logging in context ctx1. Log type is CONNECTION-CLOSE.
日志说明	关闭指定类型的IP接入日志功能
处理建议	无

157.312 SSLVPN_DISABLE_IPTNL_LOG_FAIL

日志内容	Failed to disable IP tunnel access logging in context [STRING]. Log type is [STRING].
参数解释	$1：SSL VPN访问实例名称 $2：日志类型，取值包括： • CONNECTION-CLOSE，表示连接关闭日志 • PACKET-DROP，表示丢包日志
日志等级	6
举例	SSLVPN/6/SSLVPN_DISABLE_IPTNL_LOG_FAIL: Failed to disable IP tunnel access logging in context ctx1. Log type is CONNECTION-CLOSE.
日志说明	关闭指定类型的IP接入日志功能失败
处理建议	无

157.313 SSLVPN_DISABLE_PWDAUTH

日志内容	Disabled password authentication in context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DISABLE_PWDAUTH: Disabled password authentication in context ctx1.
日志说明	关闭SSL VPN访问实例的密码认证功能
处理建议	无

157.314 SSLVPN_DISABLE_PWDAUTH_FAILED

日志内容	Failed to disable password authentication in context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DISABLE_PWDAUTH_FAILED: Failed to disable password authentication in context ctx1.
日志说明	关闭SSL VPN访问实例的密码认证功能失败
处理建议	无

157.315 SSLVPN_DISABLE_SMSIMC

日志内容	Disabled iMC SMS message authentication in context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DISABLE_SMSIMC: Disabled iMC SMS message authentication in context ctx1.
日志说明	关闭SSL VPN访问实例的iMC短信认证服务
处理建议	无

157.316 SSLVPN_DISABLE_SMSIMC_FAILED

日志内容	Failed to disable iMC SMS message authentication in context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DISABLE_SMSIMC_FAILED: Failed to disable iMC SMS message authentication in context ctx1.
日志说明	关闭SSL VPN访问实例的iMC短信认证服务
处理建议	无

157.317 SSLVPN_DISABLE_URLMASKING

日志内容	Disabled URL masking for URL item [STRING] in context [STRING].
参数解释	$1：URL表项的名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DISABLE_URLMASKING: Disabled URL masking for URL item item1 in context ctx1.
日志说明	关闭URL表项对应资源的URL伪装功能
处理建议	无

157.318 SSLVPN_DISABLE_URLMASKING_FAILED

日志内容	Failed to disable URL masking for URL item [STRING] in context [STRING].
参数解释	$1：URL表项的名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DISABLE_URLMASKING_FAILED: Failed to disable URL masking for URL item item1 in context ctx1.
日志说明	关闭URL表项对应资源的URL伪装功能失败
处理建议	无

157.319 SSLVPN_DISABLE_VERIFYCODE

日志内容	Disabled code verification in context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DISABLE_VERIFYCODE: Disabled code verification in context ctx1.
日志说明	关闭SSL VPN访问实例的验证码验证功能
处理建议	无

157.320 SSLVPN_DISABLE_VERIFYCODE_FAILED

日志内容	Failed to disable code verification in context [STRING]
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_DISABLE_VERIFYCODE_FAILED: Failed to disable code verification in context ctx1.
日志说明	关闭SSL VPN访问实例的验证码验证功能失败
处理建议	无

157.321 SSLVPN_DOMAIN_URLMAPPING

日志内容	Configured domain mapping for URL item [STRING] in context [STRING]: mapped domain name=[STRING], URL rewriting=[STRING].
参数解释	$1：URL表项的名称 $2：SSL VPN访问实例名称 $3：域名映射方式映射的域名 $4：URL表项的路径改写功能是否开启，取值包括： • enabled：表示改写功能已开启 • disabled：表示改写功能已关闭
日志等级	6
举例	SSLVPN/6/SSLVPN_DOMAIN_URLMAPPING: Configured domain mapping for URL item item1 in context ctx1: mapped domain name=www.abc.com, URL rewriting=enabled.
日志说明	配置URL资源的域名映射方式成功
处理建议	无

157.322 SSLVPN_DOMAIN_URLMAPPING_FAILED

日志内容	Failed to configure domain mapping for URL item [STRING] in context [STRING]: mapped domain name=[STRING], URL rewriting=[STRING].
参数解释	$1：URL表项的名称 $2：SSL VPN访问实例名称 $3：域名映射方式映射的域名 $4：URL表项的路径改写功能是否开启，取值包括： • enabled：表示改写功能已开启 • disabled：表示改写功能已关闭
日志等级	6
举例	SSLVPN/6/SSLVPN_DOMAIN_URLMAPPING_FAILED: Failed to configure domain mapping for URL item **item1** in context **ctx1**: mapped domain name=www.abc.com, URL rewriting=enabled.
日志说明	配置URL资源的域名映射方式失败
处理建议	无

157.323 SSLVPN_ENABLE_CONTEXT

日志内容	Enabled service in context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ENABLE_CONTEXT: Enabled service in context ctx1.
日志说明	开启SSL VPN访问实例
处理建议	无

157.324 SSLVPN_ENABLE_CONTEXT_FAILED

日志内容	Failed to enable service in context [STRING]
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ENABLE_CONTEXT_FAILED: Failed to enable service in context ctx1.
日志说明	开启SSL VPN访问实例失败
处理建议	无

157.325 SSLVPN_ENABLE_CRTAUTH

日志内容	Enabled certificate-authentication in context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ENABLE_CRTAUTH: Enabled certificate-authentication in context ctx1.
日志说明	在SSL VPN访问实例中开启证书认证功能
处理建议	无

157.326 SSLVPN_ENABLE_CRTAUTH_FAILED

日志内容	Failed to enable certificate-authentication in context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ENABLE_CRTAUTH_FAILED: Failed to enable certificate-authentication in context ctx1.
日志说明	在SSL VPN访问实例中开启证书认证功能失败
处理建议	无

157.327 SSLVPN_ENABLE_DYNAMICPWD

日志内容	Enabled dynamic-password in context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ENABLE_DYNAMICPWD: Enabled dynamic password verification in context ctx1.
日志说明	在SSL VPN访问实例中开启动态口令验证功能
处理建议	无

157.328 SSLVPN_ENABLE_DYNAMICPWD_FAILED

日志内容	Failed to enable dynamic-password in context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ENABLE_DYNAMICPWD_FAILED: Failed to enable dynamic-password in context ctx1.
日志说明	在SSL VPN访问实例中开启动态口令验证功能失败
处理建议	无

157.329 SSLVPN_ENABLE_FORCELOGOUT

日志内容	Enabled force logout in context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ENABLE_FORCELOGOUT: Enabled force logout in context ctx1.
日志说明	开启SSL VPN访问实例的达到最大在线数再登录时强制下线功能
处理建议	无

157.330 SSLVPN_ENABLE_FORCELOGOUT_FAILED

日志内容	Failed to enable force logout in context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ENABLE_FORCELOGOUT_FAILED: Failed to enable force logout in context ctx1.
日志说明	开启SSL VPN访问实例的达到最大在线数再登录时强制下线功能失败
处理建议	无

157.331 SSLVPN_ENABLE_GATEWAY

日志内容	Enabled service in gateway [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ENABLE_GATEWAY: Enabled service in gateway gw1.
日志说明	开启SSL VPN网关
处理建议	无

157.332 SSLVPN_ENABLE_GATEWAY_FAILED

日志内容	Failed to enable service in gateway [STRING]
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ENABLE_GATEWAY_FAILED: Failed to enable service in gateway gw1.
日志说明	开启SSL VPN网关失败
处理建议	无

157.333 SSLVPN_ENABLE_GLOBAL_LOG

日志内容	Enabled SSL VPN logging globally.
参数解释	无
日志等级	6
举例	SSLVPN/6/SSLVPN_ENABLE_GLOBAL_LOG: Enabled SSL VPN logging globally.
日志说明	开启SSL VPN全局日志功能
处理建议	无

157.334 SSLVPN_ENABLE_GLOBAL_LOG_FAILED

日志内容	Failed to enable SSL VPN logging globally.
参数解释	无
日志等级	6
举例	SSLVPN/6/SSLVPN_ENABLE_GLOBAL_LOG_FAILED: Failed to enable SSL VPN logging globally.
日志说明	开启SSL VPN全局日志功能失败
处理建议	无

157.335 SSLVPN_ENABLE_GLOBALURLMASKING

日志内容	Enabled global URL masking in context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ENABLE_GLOBALURLMASKING: Enabled global URL masking in context ctx1.
日志说明	在SSL VPN访问实例中开启全局URL伪装功能
处理建议	无

157.336 SSLVPN_ENABLE_GLOBALURLMASKING_FAILED

日志内容	Failed to enable global URL masking in context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ENABLE_GLOBALURLMASKING_FAILED: Failed to enable global URL masking in context ctx1.
日志说明	在SSL VPN访问实例中开启全局URL伪装功能失败
处理建议	无

157.337 SSLVPN_ENABLE_IPTNL_LOG

日志内容	Enabled IP tunnel access logging in context [STRING]. Log type is [STRING].
参数解释	$1：SSL VPN访问实例名称 $2：日志类型，取值包括： • CONNECTION-CLOSE，表示连接关闭日志 • PACKET-DROP，表示丢包日志
日志等级	6
举例	SSLVPN/6/SSLVPN_ENABLE_IPTNL_LOG: Enabled IP tunnel access logging in context ctx1. Log type is CONNECTION-CLOSE.
日志说明	开启指定类型的IP接入日志功能
处理建议	无

157.338 SSLVPN_ENABLE_IPTNL_LOG_FAIL

日志内容	Failed to enable IP tunnel access logging in context [STRING]. Log type is [STRING].
参数解释	$1：SSL VPN访问实例名称 $2：日志类型，取值包括： • CONNECTION-CLOSE，表示连接关闭日志 • PACKET-DROP，表示丢包日志
日志等级	6
举例	SSLVPN/6/SSLVPN_ENABLE_IPTNL_LOG_FAIL: Failed to enable IP tunnel access logging in context ctx1. Log type is CONNECTION-CLOSE.
日志说明	开启指定类型的IP接入日志功能失败
处理建议	无

157.339 SSLVPN_ENABLE_PWDAUTH

日志内容	Enabled password authentication in context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ENABLE_PWDAUTH: Enabled password authentication in context ctx1.
日志说明	开启SSL VPN访问实例的密码认证功能
处理建议	无

157.340 SSLVPN_ENABLE_PWDAUTH_FAILED

日志内容	Failed to enable password authentication in context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ENABLE_PWDAUTH_FAILED: Failed to enable password authentication in context ctx1.
日志说明	开启SSL VPN访问实例的密码认证功能失败
处理建议	无

157.341 SSLVPN_ENABLE_SMSIMC

日志内容	Enabled iMC SMS message authentication in context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ENABLE_SMSIMC: Enabled iMC SMS message authentication in context ctx1.
日志说明	开启SSL VPN访问实例的iMC短信认证服务
处理建议	无

157.342 SSLVPN_ENABLE_SMSIMC_FAILED

日志内容	Failed to enable iMC SMS message authentication in context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ENABLE_SMSIMC_FAILED: Failed to enable iMC SMS message authentication in context ctx1.
日志说明	开启SSL VPN访问实例的iMC短信认证服务失败
处理建议	无

157.343 SSLVPN_ENABLE_URLMASKING

日志内容	Enabled URL masking for URL item [STRING] in context [STRING].
参数解释	$1：URL表项的名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ENABLE_URLMASKING: Enabled URL masking for URL item item1 in context ctx1.
日志说明	开启URL表项对应资源的URL伪装功能
处理建议	无

157.344 SSLVPN_ENABLE_URLMASKING_FAILED

日志内容	Failed to enable URL masking for URL item [STRING] in context [STRING].
参数解释	$1：URL表项的名称 $2：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ENABLE_URLMASKING_FAILED: Failed to enable URL masking for URL item item1 in context ctx1.
日志说明	开启URL表项对应资源的URL伪装功能失败
处理建议	无

157.345 SSLVPN_ENABLE_VERIFYCODE

日志内容	Enabled code verification in context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ENABLE_VERIFYCODE: Enabled code verification in context ctx1.
日志说明	开启SSL VPN访问实例的验证码验证功能
处理建议	无

157.346 SSLVPN_ENABLE_VERIFYCODE_FAILED

日志内容	Failed to enable code verification in context [STRING]
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_ENABLE_VERIFYCODE_FAILED: Failed to enable code verification in context ctx1.
日志说明	开启SSL VPN访问实例的验证码验证功能失败
处理建议	无

157.347 SSLVPN_IP_RESOURCE_DENY

日志内容	User [STRING] of context [STRING] from [STRING] denied to access [STRING]:[STRING].
参数解释	$1：用户的名称 $2：Context名称 $3：用户登录的IP $4：访问资源的IP地址 $5：访问资源的端口号
日志等级	6
举例	SSLVPNK/6/SSLVPN_IP_RESOURCE_DENY: User abc of context ctx1 from 192.168.200.130 denied to access 10.1.1.255:137.
日志说明	禁止访问该IP资源。触发生成此日志信息的原因：引用了ACL规则过滤了该资源
处理建议	检查是否引用ACL规则过滤了该资源

157.348 SSLVPN_IP_RESOURCE_FAILED

日志内容	User [STRING] of context [STRING] from [STRING] failed to access [STRING]:[STRING].
参数解释	$1：用户的名称 $2：Context名称 $3：用户登录的IP $4：访问资源的IP地址 $5：访问资源的端口号
日志等级	6
举例	SSLVPNK/6/SSLVPN_IP_RESOURCE_FAILED: User abc of context ctx1 from 192.168.200.130 failed to access 10.1.1.255:137.
日志说明	访问IP资源失败。触发生成此日志信息的原因可能有：网络不可达
处理建议	检查IP资源是否路由可达

157.349 SSLVPN_IP_RESOURCE_PERMIT

日志内容	User [STRING] of context [STRING] from [STRING] permitted to access [STRING]:[STRING].
参数解释	$1：用户的名称 $2：Context名称 $3：用户登录的IP $4：访问资源的IP地址 $5：访问资源的端口号
日志等级	6
举例	SSLVPNK/6/SSLVPN_IP_RESOURCE_PERMIT: User abc of context ctx1 from 192.168.200.130 permitted to access 10.1.1.255:137.
日志说明	用户访问IP资源
处理建议	无

157.350 SSLVPN_IPAC_ALLOC_ADDR_FAIL

日志内容	Failed to allocate IP address to user [STRING] at [STRING] in context [STRING]. Reason: [STRING].
参数解释	$1：用户的名称 $2：用户登录的IP地址 $3：Context名称 $4：SSL VPN网关为客户端虚拟网卡分配IP地址失败原因，取值如下： • Failed to obtain system resource data：获取系统资源数据失败 • No address is available in the address pool：地址池中无闲置的地址 • Failed to obtain address pool：获取地址池失败 • Available addresses in the address pool have been bound to other users：地址池中闲置的地址已被其它用户绑定
日志等级	6
举例	SSLVPN/5/SSLVPN_IPAC_ALLOC_ADDR_FAIL: Failed to allocate IP address to user abc at 192.168.68.10 in context ctx. Reason: Failed to obtain system resource data.
日志说明	SSL VPN网关为IP接入客户端虚拟网卡分配IP地址失败
处理建议	• 检查设备是否存在异常 • 检查地址池是否已配置 • 检查地址池中是否有空闲的地址 • 检查地址池中空闲的地址是否被其它用户绑定

157.351 SSLVPN_IPAC_ALLOC_ADDR_SUCCESS

日志内容	IP address [STRING] successfully allocated to user [STRING] at [STRING] in context [STRING].
参数解释	$1：SSL VPN网关为客户端虚拟网卡分配的IP地址 $2：用户的名称 $3：用户登录的IP地址 $4：Context名称
日志等级	6
举例	SSLVPN/5/SSLVPN_IPAC_ALLOC_ADDR_SUCCESS: IP address 10.1.1.1 successfully allocated to user abc at 192.168.68.10 in context ctx.
日志说明	SSL VPN网关为IP接入客户端虚拟网卡分配IP地址成功
处理建议	无

157.352 SSLVPN_IPAC_CONN_CLOSE

日志内容	IP connection was [STRING]. Reason: [STRING].
参数解释	$1：连接关闭类型，取值包括： • closed：正常关闭 • aborted：异常关闭 $2：关闭原因，取值包括： • User logout：用户下线 • Failure to find peer：查找 peer 失败 • Handshake failed：握手失败 • Change of IP address pool：地址池改变 • Failure to receive data：从连接上接收数据失败 • Local retransmission timeout：本端重传超时 • Local keepalive timeout：本端保活超时 • Local probe timeout：本端 0 窗口探测超时 • Received FIN from peer：接收到对端的 FIN • Received RST from peer：接收到对端的 RST • No authorized policy group：没有授权的 policy group • Allocated address was bound to another user：分配的地址被其他用户绑定 • Failure to update client configuration：更新客户端配置失败 • Deleted old peer：删除旧的 peer 节点 • Other：其他原因
日志等级	6
举例	SSLVPNK/6/SSLVPN_IPAC_CONN_CLOSE: IP connection was closed. Reason: User logout.
日志说明	描述IP接入业务对应的连接关闭的原因
处理建议	无

157.353 SSLVPN_IPAC_PACKET_DROP

日志内容	Dropped [STRING] IP connection [STRING] packets in context [STRING]. Reason: [STRING].
参数解释	$1：丢包个数 $2：丢包类型，取值包括： • request：请求 • reply：应答 $3：SSL VPN访问实例名称 $4：产生原因，取值包括： • Context rate limit：访问实例限速 • Buffer insufficient：缓冲区满
日志等级	6
举例	SSLVPN/6/SSLVPN_IPAC_PACKET_DROP: Dropped 5 IP connection request packets in context ctx1. Reason: Context rate limit.
日志说明	描述IP接入业务产生丢包的原因
处理建议	无

157.354 SSLVPN_IPAC_RELEASE_ADDR_SUCCESS

日志内容	User [STRING] at [STRING] in context [STRING] released IP address [STRING].
参数解释	$1：用户的名称 $2：用户登录的IP地址 $3：Context名称 $4：SSL VPN网关为客户端虚拟网卡分配的IP地址
日志等级	6
举例	SSLVPN/5/SSLVPN_IPAC_RELEASE_ADDR_SUCCESS: User abc at 192.168.68.10 in context ctx released IP address 10.1.1.1.
日志说明	SSL VPN网关成功释放了为IP接入客户端虚拟网卡分配的IP地址
处理建议	无

157.355 SSLVPN_PORT_URLMAPPING

日志内容	Configured port mapping for URL item [STRING] in context [STRING]: mapped gateway name=[STRING], virtual host name=[STRING], URL rewriting=[STRING].
参数解释	$1：URL表项的名称 $2：SSL VPN访问实例名称 $3：端口映射关联的SSL VPN网关名称 $4：虚拟主机名称 $5：URL表项的路径改写功能是否开启，取值包括： • enabled：表示改写功能已开启 • disabled：表示改写功能已关闭
日志等级	6
举例	SSLVPN/6/SSLVPN_PORT_URLMAPPING: Configured port mapping for URL item **item1** in context **ctx1**: mapped gateway name=www.abc.com, virtual host name=vhost1, URL rewriting=enabled.
日志说明	配置URL资源的端口映射方式成功
处理建议	无

157.356 SSLVPN_PORT_URLMAPPING_FAILED

日志内容	Failed to configure port mapping for URL item [STRING] in context [STRING]: mapped gateway name=[STRING], virtual host name=[STRING], URL rewriting=[STRING].
参数解释	$1：URL表项的名称 $2：SSL VPN访问实例名称 $3：端口映射关联的SSL VPN网关名称 $4：虚拟主机名称 $5：URL表项的路径改写功能是否开启，取值包括： • enabled：表示改写功能已开启 • disabled：表示改写功能已关闭
日志等级	6
举例	SSLVPN/6/SSLVPN_PORT_URLMAPPING_FAILED: Failed to configure port mapping for URL item item1 in context ctx1: mapped gateway name=gw1, virtual host name=vhost1, URL rewriting=enabled.
日志说明	配置URL资源的端口映射方式失败
处理建议	无

157.357 SSLVPN_SERVICE_UNAVAILABLE

日志内容	SSL VPN service was unavailable. Reason: [STRING].
参数解释	$1：服务不可用的原因，取值包括： • SSL VPN context not enabled • No available SSL VPN contexts
日志等级	6
举例	SSLVPNK/6/SSLVPN_SERVICE_UNAVAILABLE: SSL VPN service was unavailable. Reason: SSL VPN context not enabled.
日志说明	描述SSL VPN服务不可用的原因
处理建议	• 如果原因为 SSL VPN context not enabled，则进入指定的 SSL VPN 访问实例视图，通过 service enable 使能该访问实例 • 如果原因为 No available SSL VPN contexts，请确认访问的 IP 或域名对应的 SSL VPN gateway 是否有被访问实例引用

157.358 SSLVPN_TCP_RESOURCE_DENY

日志内容	User [STRING] of context [STRING] from [STRING] denied to access [STRING]:[STRING] (server-IP=[STRING],port-number=[STRING]).
参数解释	$1：用户的名称 $2：Context名称 $3：用户登录的IP $4：访问的远端server $5：访问的远端port $6：访问的远端server IP $7：访问的远端port
日志等级	6
举例	SSLVPNK/6/SSLVPN_TCP_RESOURCE_DENY: User abc of context ctx1 from 192.168.200.130 denied to access 10.1.1.255:137 (server-IP=10.1.1.255,port-number=137).
日志说明	禁止用户访问该TCP资源。触发生成此日志信息的原因：引用了ACL规则过滤了该资源
处理建议	检查是否引用ACL规则过滤了该资源

157.359 SSLVPN_TCP_RESOURCE_FAILED

日志内容	User [STRING] of context [STRING] from [STRING] failed to access [STRING]:[STRING] (server-IP=[STRING],port-number=[STRING]).
参数解释	$1：用户的名称 $2：Context名称 $3：用户登录的IP $4：访问的远端服务器 $5：访问的远端服务端口 $6：访问的远端server IP $7：访问的远端port
日志等级	6
举例	SSLVPNK/6/SSLVPN_TCP_RESOURCE_FAILED: User abc of context ctx1 from 192.168.200.130 failed to access 10.1.1.255:137 (server-IP=10.1.1.255,port-number=137).
日志说明	用户访问TCP资源失败。触发生成此日志信息的原因可能有：网络不可达、DNS解析失败
处理建议	• 检查网络是否可达。如果授权的资源是主机名 • 检查网络中存在路由可达的 DNS 服务器

157.360 SSLVPN_TCP_RESOURCE_PERMIT

日志内容	User [STRING] of context [STRING] from [STRING] permitted to access [STRING]:[STRING] (server-IP=[STRING],port-number=[STRING]).
参数解释	$1：用户的名称 $2：Context名称 $3：用户登录的IP $4：访问的远端server $5：访问的远端port $6：访问的远端server IP $7：访问的远端port
日志等级	6
举例	SSLVPNK/6/SSLVPN_TCP_RESOURCE_PERMIT: User abc of context ctx1 from 192.168.200.130 permitted to access 10.1.1.255:137 (server-IP=10.1.1.255,port-number=137).
日志说明	用户访问TCP资源
处理建议	无

157.361 SSLVPN_UNDO_FORCELOGOUT

日志内容	Disabled force logout in context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_UNDO_FORCELOGOUT: Disabled force logout in context ctx1.
日志说明	关闭SSL VPN访问实例的达到最大在线数再登录时强制下线功能
处理建议	无

157.362 SSLVPN_UNDO_FORCELOGOUT_FAILED

日志内容	Failed to disable force logout in context [STRING].
参数解释	$1：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_UNDO_FORCELOGOUT_FAILED: Failed to disable force logout in context ctx1.
日志说明	关闭SSL VPN访问实例的达到最大在线数再登录时强制下线功能失败
处理建议	无

157.363 SSLVPN_URLITEM_ADD_URIACL

日志内容	Specified URI ACL [STRING] for URL item [STRING] in context [STRING].
参数解释	$1：URL表项引用的URI ACL名称 $2：URL表项的名称 $3：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_URLITEM_ADD_URIACL: Specified URI ACL uriacl1 for URL item item1 in context ctx1.
日志说明	URL表项引用URI ACL过滤规则成功
处理建议	无

157.364 SSLVPN_URLITEM_ADD_URIACL_FAILED

日志内容	Failed to specify URI ACL [STRING] for URL item [STRING] in context [STRING].
参数解释	$1：URL表项引用的URI ACL名称 $2：URL表项的名称 $3：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_URLITEM_ADD_URIACL_FAILED: Failed to specify URI ACL uriacl1 for URL item item1 in context ctx1.
日志说明	URL表项引用URI ACL过滤规则失败
处理建议	无

157.365 SSLVPN_URLITEM_DEL_URIACL

日志内容	Removed URI ACL [STRING] from URL item [STRING] in context [STRING].
参数解释	$1：URL表项引用的URI ACL名称 $2：URL表项的名称 $3：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_URLITEM_DEL_URIACL: Removed URI ACL uriacl1 from URL item item1 in context ctx1.
日志说明	URL表项取消引用URI ACL成功
处理建议	无

157.366 SSLVPN_URLITEM_DEL_URIACL_FAILED

日志内容	Failed to remove URI ACL [STRING] from URL item [STRING] in context [STRING].
参数解释	$1：URL表项引用的URI ACL名称 $2：URL表项的名称 $3：SSL VPN访问实例名称
日志等级	6
举例	SSLVPN/6/SSLVPN_URLITEM_DEL_URIACL_FAILED: Failed to remove URI ACL uriacl1 from URL item item1 in context ctx1.
日志说明	URL表项取消引用URI ACL失败
处理建议	无

157.367 SSLVPN_USER_LOGIN

日志内容	User [STRING] of context [STRING] logged in from [STRING].
参数解释	$1：用户的名称 $2：Context名称 $3：用户登录的IP
日志等级	5
举例	SSLVPN/5/SSLVPN_USER_LOGIN: User abc of context ctx logged in from 192.168.200.31.
日志说明	用户登录SSL VPN网关
处理建议	无

157.368 SSLVPN_USER_LOGINFAILED

日志内容	User [STRING] of context [STRING] failed to log in from [STRING]. Reason: [STRING].
参数解释	$1：用户的名称 $2：Context名称 $3：用户登录的IP $4：登录失败的原因，取值包括： • Authentication failed. Reason: incorrectusername or password, authentication server error, or number of users reachingthe maximum allowed by an account:认证失败，原因：用户名密码错误、认证服务器错误或接入用户数达到最大限制 • Authorization failed：授权失败 • Accounting failed：计费失败 • Number of online users exceeded the limit：超过最大上线用户数 • Failed to get SMS message code from iMC server：从 iMC 服务器上获取 SMS 消息失败 • Maximum number of concurrent online connections for the user already reached：同一名称的上线用户数达到最大规格 • Login timed out：登录超时 • The authentication server is not reachable：认证服务器不可达 • The authorization server is not reachable：授权服务器不可达 • The accounting server is not reachable：计费服务器不可达 • Other：其他原因
日志等级	5
举例	SSLVPN/5/SSLVPN_USER_LOGINFAILED: User abc of context ctx failed to log in from 192.168.200.31.
日志说明	用户登录SSL VPN网关失败
处理建议	无

157.369 SSLVPN_USER_LOGOUT

日志内容	User [STRING] of context [STRING] logged out from [STRING]. Reason: [STRING].
参数解释	$1：用户的名称 $2：Context名称 $3：用户登录的IP $4：用户下线原因，取值如下： • Idle timeout：已经达到超时时间 • A logout request was received from the Web browser：接收到 Web 浏览器的下线请求 • A logout request was received from the client：接收到客户端的下线请求 • Forced logout：用户被强制下线 • A new login was attempted and logins using the account reach the maximum：一个新的同名用户登录且当前用户数目达到最大限制数，被强制下线 • Accounting update failed：更新计费失败 • Accounting session timed out：会话超时 • Interface went down：接口 down • ADM request was received：收到断开 session control 连接事件 • Idle cut for traffic not reach the minimum required amount.：没有达到配置的会话保持空闲状态的流量阈值
日志等级	5
举例	SSLVPN/5/SSLVPN_USER_LOGOUT: User abc of context ctx logged out from 192.168.200.31. Reason: A logout request was received from the Web browser.
日志说明	用户退出SSL VPN网关
处理建议	无

157.370 SSLVPN_USER_NUMBER

日志内容	The number of SSL VPN users reached the upper limit.
参数解释	无
日志等级	6
举例	SSLVPN/6/SSLVPN_USER_NUMBER: The number of SSL VPN users reached the upper limit.
日志说明	SSL VPN用户数达到上限
处理建议	无

157.371 SSLVPN_WEB_RESOURCE_DENY

日志内容	User [STRING] of context [STRING] from [STRING] denied to access [STRING] (server-IP=[STRING],port-number=[STRING]).
参数解释	$1：用户的名称 $2：Context名称 $3：用户登录的IP $4：访问资源的URL地址 $5：访问的资源的IP地址 $6：访问的资源的port
日志等级	6
举例	SSLVPNK/6/SSLVPN_WEB_RESOURCE_DENY: User abc of context ctx1 from 192.168.200.130 denied to access http://192.168.0.2:80/ (server-IP=192.168.0.2,port-number=80).
日志说明	禁止用户访问该Web资源。触发生成此日志信息的原因：引用了ACL规则过滤了该资源
处理建议	请检查是否引用ACL规则过滤了该资源

157.372 SSLVPN_WEB_RESOURCE_FAILED

日志内容	User [STRING] of context [STRING] from [STRING] failed to access [STRING] (server-IP=[STRING],port-number=[STRING]).
参数解释	$1：用户的名称 $2：Context名称 $3：用户登录的IP $4：访问资源的URL地址 $5：访问的资源的IP地址 $6：访问的资源的port
日志等级	6
举例	SSLVPNK/6/SSLVPN_WEB_RESOURCE_FAILED: User abc of context ctx1 from 192.168.200.130 failed to access http://192.168.0.2:80/ (server-IP=192.168.0.2,port-number=80).
日志说明	用户访问Web资源失败。触发生成此日志信息的原因可能有：网络不可达，DNS解析失败
处理建议	• 检查 Web 资源是否路由可达。如果授权的资源是主机名 • 检查网络中存在路由可达的 DNS 服务器

157.373 SSLVPN_WEB_RESOURCE_PERMIT

日志内容	User [STRING] of context [STRING] from [STRING] permitted to access [STRING] (server-IP=[STRING],port-number=[STRING]).
参数解释	$1：用户的名称 $2：Context名称 $3：用户登录的IP $4：访问资源的URL地址 $5：访问的资源的IP地址 $6：访问的资源的port
日志等级	6
举例	SSLVPNK/6/SSLVPN_WEB_RESOURCE_PERMIT: User abc of context ctx1 from 192.168.200.130 permitted to access http://192.168.0.2:80/ (server-IP=192.168.0.2,port-number=80).
日志说明	用户访问Web资源
处理建议	无

158 STAMGR

本节介绍 STAMGR 模块输出的日志信息。

158.1 STAMGR_ADD_FAILVLAN

日志内容	-SSID=[STRING]-UserMAC=[STRING]-APName=[STRING]-RadioID=[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：用户上线的AP $4：用户上线的Radio ID $5：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=dc2d-cb16-28cd-APName=ap1-RadioID=2; 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

158.2 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 dc2d-cb16-28cd.
日志说明	Master AC与BAS AC建立连接
处理建议	无

158.3 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 dc2d-cb16-28cd.
日志说明	客户端成功连接到BAS AC
处理建议	无

158.4 STAMGR_AUTHORACL_FAILURE

日志内容	-SSID=[STRING]-UserMAC=[STRING]-APName=[STRING]-RadioID=[STRING]; Failed to assign an ACL [STRING]. 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：用户上线的AP $4：用户上线的Radio ID $5：授权ACL编号 $6：授权ACL失败的原因 • The ACL doesn't exist：指定的 ACL 不存在 • This type of ACL is not supported：不支持指定的 ACL 类型 • The memory resource is not enough：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 • The OpenFlow tunnel was not established：OpenFlow 隧道未建立 • The OpenFlow table is full：OpenFlow 授权表项已满规格 • Unknown reason. Error code code was returned：其他未知错误并返回错误码
日志等级	5
举例	STAMGR/5/STAMGR_AUTHORACL_FAILURE:-SSID=text-wifi-UserMAC=dc2d-cb16-28cd-APName=ap1-RadioID=2; Failed to assign an ACL 2000.Reason: The ACL doesn't exist.
日志说明	下发ACL失败
处理建议	无

158.5 STAMGR_AUTHORUSERPROFILE_FAILURE

日志内容	-SSID=[STRING]-UserMAC=[STRING]-APName=[STRING]-RadioID=[STRING]; Failed to assign user profile [STRING]. 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：用户上线的AP $4：用户上线的Radio ID $5：授权User Profile名称 $6：授权User Profile失败的原因 • The user profile doesn't exist：指定的 User Profile 不存在 • No user profiles are created on the device：没有创建任何 User Profile • The memory resource is not enough：内存不足 • The OpenFlow tunnel was not established：OpenFlow 隧道未建立 • Unknown reason. Error code code was returned ：其他未知错误并返回错误码
日志等级	5
举例	STAMGR/5/STAMGR_AUTHORUSERPROFILE_FAILURE:-SSID=text-wifi-UserMAC=dc2d-cb16-28cd-APName=ap1-RadioID=2; Failed to assign user profile aaa. Reason: No user profiles are created on the device.
日志说明	下发user profile失败
处理建议	无

158.6 STAMGR_BSS_FAILURE

日志内容	-APID=[STRING]-RadioID=[STRING]-WLANID=[STRING]-ST Name=[STRING]; The number of BSSs exceeded the upper limit.
参数解释	$1：AP ID $2：Radio ID $3：WLAN ID $4：无线服务模板名称
日志等级	6
举例	STAMGR/6/SERVICE_BSS_FAILURE: -APID=1-RadioID=2-WLANID=3-ST Name=1; The number of BSSs exceeded the upper limit.
日志说明	AP大量入组超出BSS最大门限值
处理建议	无

158.7 STAMGR_CLIENT_FAILURE

日志内容	Client [STRING] failed to come online from BSS [STRING] with SSID [STRING] on AP [STRING] Radio ID [STRING] Reason: [STRING].
参数解释	$1：客户端的MAC地址 $2：BSSID $3：服务模板的SSID $4：AP的名称 $5：客户端上线失败的原因，详细内容请参见表158-1
日志等级	5
举例	STAMGR/6/STAMGR_CLIENT_FAILURE: Client dc2d-cbaf-b8d2 failed to come online from BSS dc2d-cbef-78dc with SSID 1 on AP ap1.Reason: Unknown reason.
日志说明	由于未知原因，Client上线失败
处理建议	请根据调试信息定位并解决问题

表158-1 客户端上线失败原因

失败原因	描述
Unknown error.	未知错误
Failed to process open authentication packet from the client.	开放系统认证时，Auth报文处理失败
Failed to send responses when the AC successfully processed open authentication packet from the client.	开放系统认证时，Auth报文处理成功，发送回应失败
Failed to create state timer when the AC received authentication packet in Unauth state.	Unauth状态收到Auth报文创建状态定时器失败
Failed to refresh state timer when the AC received authentication packet in Unauth state.	Unauth状态收到Auth报文更新状态定时器失败
Received association packet Unauth state.	Unauth状态收到Asso报文
Received deauthentication packet with reason code *code* in Unauth state*:* • 1: Unknown reason. • 3: Client is removed from BSS and is deauthenticated. • 6: Incorrect frame. • 9: Received association or reassociation request before authentication is complete. • 13: Invalid IE.	Unauth状态收到Deauth报文，报文中携带原因码*code*，*code*取值如下： • 1：未知原因 • 3：client 离开 BSS 并且解除认证 • 6：错误的帧导致 client 解除认证 • 9：认证完成前收到关联或重关联请求 • 13：IE 无效
Received dissociation packet with reason code *code in* Unauth state*:* • 1: Unknown reason. • 2: Prior authentication is invalid. • 4: Inactivity timer expired. • 5: Insufficient resources.	Unauth状态收到Deasso报文，报文中携带原因码*code*，*code*取值如下： • 1：未知原因 • 2：之前的认证无效 • 4：Inactive 定时器失效 • 5：资源不足

失败原因	描述
• 7: Incorrect frame. • 8: Client is removed from BSS and is disassociated. • 10: Failed to negotiate the Power Capability IE. • 11: BSS management switchover.	• 7：错误的帧导致 client 去关联 • 8：client 离开 BSS 并且解除关联 • 10：能力集 IE 协商失败 • 11：BSS 切换管理
Received Auth failure packet in Unauth state.	Unauth状态收到用户认证失败报文
Received state timer timeout in Unauth state.	Unauth状态收到状态定时器超时激励
Received deauthentication packet with reason code *code* in Auth state*:* • 1: Unknown reason. • 3: Client is removed from BSS and is deauthenticated. • 6: Incorrect frame. • 9: Received association or reassociation request before authentication is complete. • 13: Invalid IE.	Auth状态收到Deauth报文，报文中携带原因码*code*，*code*取值如下： • 1：未知原因 • 3：client 离开 BSS 并且解除认证 • 6：错误的帧导致 client 解除认证 • 9：认证完成前收到关联或重关联请求 • 13：IE 无效
Received authentication packet with inconsistent authentication algorithm or shared key in Auth state.	Auth状态收到Auth报文，认证算法或共享密钥不一致
Received state timer timeout in Auth state.	Auth状态收到状态定时器超时激励
Failed to process Add Mobile message when client association succeeded in Auth state.	Auth状态收到Asso报文，关联处理成功，同步Add mobile消息，添加客户端失败
Received inconsistent authentication algorithm or share key in Userauth state.	Userauth状态收到Auth报文，认证算法或共享密钥不一致
Failed to check association request when the AC received association packet in Userauth state.	Userauth状态收到Asso报文，检查关联请求失败
Failed to process IE when the AC received association packet in Userauth state.	Userauth状态收到Asso报文，处理IE信息失败
Failed to send association responses when the AC received association packet in Userauth state.	Userauth状态收到Asso报文，发送关联回应失败
Failed to process Add Mobile message when client association succeeded in Userauth state.	Userauth状态收到Asso报文，关联处理成功，同步Add Mobile消息，添加客户端失败
Received deauthentication packet with reason code *code* in Userauth state*:* • 1: Unknown reason. • 3: Client is removed from BSS and is deauthenticated. • 6: Incorrect frame. • 9: Received association or reassociation request before authentication is complete. • 13: Invalid IE.	Userauth状态，收到Deauth报文，报文中携带原因码*code*，*code*取值如下： • 1：未知原因 • 3：client 离开 BSS 并且解除认证 • 6：错误的帧导致 client 解除认证 • 9：认证完成前收到关联或重关联请求 • 13：IE 无效
Received dissociation packet with reason code *code* in Userauth state*：* • 1：Unknown reason.	Userauth状态，收到Deasso报文，报文中携带原因码*code*，*code*取值如下： • 1：未知原因

失败原因	描述
• 2：Prior authentication is invalid. • 4：Inactivity timer expired. • 5：Insufficient resources. • 7：Incorrect frame. • 8：Client is removed from BSS and is disassociated. • 10：Failed to negotiate the Power Capability IE. • 11：BSS management switchover.	• 2：之前的认证无效 • 4：Inactive 定时器失效 • 5：资源不足 • 7：错误的帧导致 client 解除关联 • 8：client 离开 BSS 并且解除关联 • 10：能力集 IE 协商失败 • 11：BSS 切换管理
Client authentication failed in Userauth state.	Userauth状态，用户认证失败
Failed to get backup client data while using AP private data to upgrade client.	使用AP私有数据备份升级Client，获取备份Client数据失败
Failed to set kernel forwarding table while using AP private data to upgrade client.	使用AP私有数据备份升级Client，设置内核转发表项失败
Failed to add MAC while using AP private data to upgrade client.	使用AP私有数据备份升级Client，添加MAC失败
Failed to create keepalive and idle timeout timers while using AP private data to upgrade client.	使用AP私有数据备份升级Client，创建保活和闲置定时器失败
Failed to set kernel forwarding table while upgrading client without using AP private data.	不使用AP私有数据备份升级Client，设置内核转发表项失败
Failed to add MAC while upgrading client without using AP private data.	不使用AP私有数据备份升级Client，添加MAC失败
Failed to activate client while upgrading client without using AP private data.	不使用AP私有数据备份升级Client，激活Client失败
Failed to synchronize client information to configuration thread while upgrading client without using AP private data.	不使用AP私有数据备份升级Client，同步Client信息到配置线程失败
Failed to create keepalive and idle timeout timers while upgrading client without using AP private data.	不使用AP私有数据备份升级Client，创建保活和闲置定时器失败
Failed to add MAC during inter-device client smooth creation.	设备间平滑创建Client，添加MAC失败
Failed to set kernel forwarding table during inter-device client smooth creation.	设备间平滑创建Client，设置内核转发表项失败
Failed to send Add Mobile message during inter-device client smooth creation.	设备间平滑创建Client，下发Add Mobile失败
Failed to get AP type during inter-device client smooth creation.	设备间平滑创建Client，获取AP类型失败
Failed to recover service data while recovering running client data from database.	恢复Client基本数据时，恢复各业务模块Client数据发生严重错误，恢复失败
Failed to synchronize data to service thread while recovering basic client data from database.	恢复Client基本数据时，同步数据到业务线程失败
Failed to add MAC when hierarchy device received upstream Add Mobile message.	分层设备收到上行Add Mobile消息，添加MAC表项失败
Failed to set kernel forwarding table when hierarchy	分层设备收到上行Add Mobile消息，设置内核转发表项

失败原因	描述
device received upstream Add Mobile message.	失败
Failed to synchronize upstream message when hierarchy device received upstream Add Mobile message.	分层设备收到上行Add Mobile消息，继续上同步失败
Failed to create client when hierarchy device received upstream Add Mobile message.	分层设备收到上行Add Mobile消息，创建Client失败
Failed to add MAC when hierarchy device received downstream Add Mobile message.	分层设备收到下行Add Mobile消息，添加MAC表项失败
Failed to synchronize data to service thread when hierarchy device received downstream Add Mobile message.	分层设备收到下行Add Mobile消息，同步数据到业务线程失败
Failed to set kernel forwarding table when hierarchy device received downstream Add Mobile message.	分层设备收到下行Add Mobile消息，设置内核转发表项失败
Failed to send down add pbss to driver when hierarchy device received downstream Add Mobile message.	分层设备收到下行Add Mobile消息，设置PBSS驱动失败
Failed to synchronize downstream message when hierarchy device received downstream Add Mobile message.	分层设备收到下行Add Mobile消息，继续上同步失败
Failed to create client when hierarchy device received downstream Add Mobile message.	分层设备收到下行Add Mobile消息，创建Client失败
Failed to create interval statistics timer when hierarchy device received downstream Add Mobile message.	分层设备收到下行Add Mobile消息，设置interval statistics timer定时器失败
Failed to obtain AP private data when hierarchy device received downstream Add Mobile message.	分层设备收到下行Add Mobile消息，获取AP私有数据失败
Failed to advertise Add Mobile message.	通知Add Mobile消息失败
Failed to activate client when hierarchy device received downstream client state synchronization message.	分层设备收到下行同步客户端状态消息，Client激活失败
Failed to get AP type when hierarchy device received downstream client state synchronization message.	分层设备收到下行同步客户端状态消息，获取AP类型失败
Failed to synchronize downstream message when hierarchy device received downstream client state synchronization message.	分层设备收到下行同步客户端状态消息，下行同步消息失败
The radio was in down state when hierarchy device received downstream Add Mobile message.	分层设备收到下行Add Mobile消息，Radio处于down状态
Hierarchy device failed to process the upstream Add Mobile message.	分层设备处理上同步Add Mobile消息失败
Hierarchy device failed to process downstream Add Mobile message.	分层设备处理下同步Add Mobile消息失败
Failed to process service thread during inter-device client smooth creation.	设备间平滑创建Client，业务线程相关处理失败
Failed to create client when inter-device smooth.	设备间平滑创建Client失败
Failed to process upstream client state synchronization message in Userauth state.	Userauth状态处理上同步客户端状态消息失败

失败原因	描述
Failed to process downstream client state synchronization message in Userauth state.	Userauth状态处理下同步客户端状态消息失败
Hierarchy device failed to process upstream client state synchronization message.	分层设备处理上同步客户端状态消息失败
Hierarchy device failed to process downstream client state synchronization message.	分层设备处理下同步客户端状态消息失败
AC received message for deleting the client entry.	AC上收到删除Client消息
Fit AP received message for deleting the client.	Fit AP上处理删除Client消息
Different old and new region codes.	新区域码和旧区域码不同
Failed to update IGTK.	更新IGTK失败
Failed to update GTK.	更新GTK失败
Failed to generate IGTK when the first client came online.	首个Client上线时生成IGTK失败
TKIP is used to authenticate all clients.	密钥为TKIP去认证所有Client
Channel changed.	信道切换
BssDelAllSta event logged off client normally.	BssDelAllSta事件正常删除Client
AP down.	AP下线
Radio down.	Radio去使能
Service template disabled.	关闭无线服务模板
Service template unbound.	解绑无线服务模板
Created BSS during masterAC switchover process.	主备AC切换创建BSS，删掉AP上的Client
Updated BSS base information when BSS was in deactive state.	更新BSS base模块信息时BSS处于deactive状态
Intrusion protection.	入侵保护，关闭服务
Local AC or AP deleted BSS	Local AC或者AP删除BSS导致Client下线
BssDelAllSta event logged off client abnormally.	BssDelAllSta事件中非正常删除Client
Received VLAN deleted event.	收到Vlan删除事件
CM received message for logging off client from AM.	用户管理收到认证管理报的下线消息
The reset wlan client command was executed to log off the client.	收到reset wlan client删除指定Client消息
Deleted private data on AP: DBM database recovered	DBM库恢复数据，删除AP上的私有数据
Failed to synchronize authentication succeeded message downstream.	主状态机收到用户认证成功消息下行通知Client状态信息发生失败
Client RSSI was lower than the threshold and was decreasing.	信号强度低于设定值且被标记为变弱
Configured whitelist for the first time or executed the reset wlan client all command	首次配置白名单，或者命令行输入Reset wlan client all

失败原因	描述
Received client offline websocket message	收到Client下线的websocket消息
WMAC logged off all clients associated with the radio.	WMAC模块踢除射频下所有Client
Timer for sending deassociation message timed out.	发送Deasso报文定时器超时
The client is in blacklist or deleted from whitelist.	Client在黑名单中，或者从白名单中删除
Client was added to the dynamic blacklist.	添加动态黑名单
Failed to roam out.	漫出失败
Implemented inter-AC roaming for the first time.	AC间第一次漫出
Successfully roamed to another BSS.	AC内漫出成功，强制旧的Client下线
Failed to roam in.	漫进失败
Roaming process received a message for logging off the client.	漫游业务线程收到强制Client下线的消息
Roaming process processed Down event and logged off roam-in clients.	漫游业务线程处理端口Down事件，删除漫入Client
Roaming failure.	漫游失败的处理
Successfully performed roaming but failed to recover authentication data.	漫游成功恢复认证数据失败
Roaming timed out.	漫游超时
Seamless roaming failed.	零漫游失败
Logged off clients that performed inter- or intra-AC roaming.	AC间漫入或漫出的Client直接下线
Failed to process AccessCtrlChk. Configure permitted AP group or permitted SSID.	业务模块处理accessctrlchk失败，设置permit ap-group或者设置permit-ssid
Synchronized client information to process and logged off client.	同步Client数据至配置线程，Run状态的Client则会报下线
Failed to synchronize client state to uplinkdevices.	上下行同步Client状态失败
Local AC or remote AP received Add Mobile message updated BSS and logged off clients.	Local AC或Remote AP收到Add Mobile消息时，更新BSS数据，删除Remote ap下的Client，如果Client状态为run，则报下线事件
Upgraded HA and logged off all clients.	高可靠性升级删除所有Client
Synchronized BSS data during master/backup AC switchover process.	主备切换时，同步BSS数据错误
Failed to synchronize service template data during master/backup AC switchover process.	主备切换时，同步服务模板数据失败
BSS aging timer timed out.	BSS老化定时器超时
Remote AP deleted non-local forwarding BSS.	Remote ap下，删除非本地转发的BSS
Failed to find configuration data when synchronizing data.	同步数据时没有找到对应的配置数据
BSS was deleted: BSS synchronization examination	检查是否有BSS的关键数据更新时发生失败或者没有

失败原因	描述
failed or there was no BSS data to be updated.	要同步数据，删除BSS
Failed to get BSS by using WLAN ID.	根据WLAN ID获取BSS失败
Unbound inherited service template.	去绑定继承的服务模板
STAMGR process was down automatically or manually.	STAMGR进程shutdown或者用户手工终止进程
Deleted redundant clients.	删除冗余的Client
Failed to process authorized doing nodes.	处理授权doing节点失败
Authorization failed.	授权失败
NSS value in Operating Mode Notification Action packet doesn't support mandatory VHT-MCS.	Operating Mode Notification Action报文中的NSS值不支持强制VHT-MCS
Number of sent SA requests exceeded the permitted threshold.	计数器值大于SA Request允许发送值
Local AC came online again and deleted all clients associated with the BSS.	LOCAL AC重新上线，删除BSS下关联的所有Client
Failed to upgrade hot-backup.	热备升级失败
The illegally created BSS was deleted.	删除不允许创建的BSS
Failed to process requests when receiving UserAuth Success message.	主状态机收到用户认证成功消息处理发生失败
Failed to get AP type when receiving UserAuth Successful message.	收到用户认证消息成功时获取AP类型失败
Failed to notify client of the recovery of basic client data from database.	恢复Client基本数据，通知Client完成恢复失败
Failed to recover basic client data from database.	恢复Client基本数据失败
Client already existed when the AC received Auth packet from the client and checked online clients.	收到认证报文检查重复上线的Client，Client已经存在
Client already existed during FT Over-the-DS authentication.	进行FT Over-the-DS认证处理时创建Client，Client已存在
SKA authentication failed.	SKA认证失败
Deadline timer timed out during FT authentication.	处理FT认证，deadline定时器超时
Failed to send the response for the successful shared key authentication to the client.	处理shared-key认证成功，发送回应失败
Failed to get FT data during FT authentication.	处理FT认证，FT数据信息不存在
FT authentication was performed and BSS does not support FT.	处理FT认证，BSS不支持FT认证方式
Failed to process FT authentication-success result.	处理FT认证成功结果失败
Failed to process FT authentication.	处理FT认证失败
Maximum number of clients already reached when remote request message was received.	接收到Remote Request消息，Client数量达到上限
Failed to fill authorization information while processing	处理授权信息队列消息，填充授权数据结构失败

失败原因	描述
authorization message.	
Failed to process key negotiation during 802.1X authentication.	802.1X认证，密钥协商失败
Invalid session key length during 802.1X authentication.	802.1X认证，无效的秘钥长度
802.1X authentication failed.	802.1X认证失败
802.1X server was unreachable.	802.1X认证服务器不可达
User timer timed out during 802.1X authentication.	802.1X认证，设备没有收到终端认证报文
Server timer timed out during 802.1X authentication.	802.1X认证，服务器不通
802.1X authentication configuration error.	802.1X认证，配置问题
Received nonexistent authorization VLAN group during 802.1X authentication.	802.1X认证，授权vlan group不存在
MAC authentication failed.	MAC地址认证失败
MAC server was unreachable.	MAC地址认证服务器不可达
Session time is zero during MAC authentication.	MAC地址认证，会话时间为零
Server timer timed out during MAC authentication.	MAC地址认证，服务器不通
802.1X authentication failed and the return code is *code*.	802.1X认证失败
MAC authentication failed and the return code is *code*.	MAC地址认证失败
Authorization failed for 802.1X authentication and the return code is *code*.	802.1X认证授权失败
Authorization failed for MAC authentication and the return code is *code*.	MAC地址认证授权失败
Accounting start failed for 802.1X authentication and the return code is *code*.	802.1X认证计费开始失败
Accounting start failed for MAC authentication and the return code is *code*.	MAC地址认证计费开始失败
Accounting update failed for 802.1X authentication and the return code is *code*.	802.1X认证计费更新失败
Accounting update failed for MAC authentication and the return code is *code*.	MAC地址认证计费更新失败
Failed to receive client EAP request for 802.1X authentication.	802.1X认证过程中未收到用户EAP请求报文
Failed to receive server response for 802.1X authentication.	802.1X认证过程中未收到服务器响应报文
Failed to receive server response for MAC authentication.	MAC地址认证过程中未收到服务器响应报文
Received client log-off packet during 802.1X authentication.	802.1X认证过程中收到用户log-off报文
802.1X client handshake failed.	802.1X用户握手失联

失败原因	描述
Incorrect 802.1X authentication method.	802.1X认证方式错误

158.8 STAMGR_CLIENT_OFFLINE

日志内容	Client [STRING] went offline from BSS [STRING] with SSID [STRING] on AP [STRING] Radio ID [STRING]. State changed to Unauth. Reason [STRING]
参数解释	$1：客户端的MAC地址 $2：BSSID $3：服务模板的SSID $4：客户端上线的AP名称 $5：客户端上线的Radio ID $6：客户端的下线原因，详细内容请参见表158-2
日志等级	6
举例	STAMGR/6/STAMGR_CLIENT_OFFLINE: Client dc2d-cb33-2147 went offline from BSS dc2d-cbef-78dc with SSID abc on AP ap1 Radio ID 2. State changed to Unauth. Reason: Radio down.
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

表158-2 客户端下线原因

下线原因	描述
Received disassociation frame in Run state: reason code=String.	收到disassoc报文，用户主动下线, 默认STA下线方式, 报文中携带的原因码
Unknown reason.	其他未知错误
Different old and new region codes.	新区域码和旧区域码不同
Failed to update IGTK.	更新IGTK失败
Failed to update GTK.	更新GTK失败
Failed to generate IGTK when the first client came online.	首个STA上线时生成IGTK失败
TKIP is used to authenticate all clients.	密钥为TKIP去认证所有STA
Channel changed.	信道切换
BssDelAllSta event logged off client normally.	BssDelAllSta事件正常删除STA
Radio down.	AP掉线、radio disable
Service template disabled.	关闭无线服务模板
Service template unbound.	解绑无线服务模板

下线原因	描述
Created BSS during master/backup AC switchover process.	主备AC切换创建BSS那么要删掉AP上的STA
Updated BSS base information when BSS was in deactive state.	更新BSS base模块信息时BSS处于deactive状态
Intrusion protection.	入侵保护,关闭服务
Local AC or AP deleted BSS.	local AC或者AP删除bss导致的client下线
BssDelAllSta event logged off client abnormally.	BssDelAllSta事件中非正常删除STA
Received VLAN deleted event.	收到Vlan删除事件，及client所在的Vlan被删了，导致的下线事件
CM received message for logging off client from AM.	用户管理收到认证管理报的下线消息
The reset wlan client command was executed to log off the client.	收到reset wlan client 删除指定STA消息
DBM database failed to recover client operation data.	DBM库恢复STA运行数据失败
Deleted private data on AP: DBM database recovered.	DBM库恢复数据，删除AP上的私有数据
Received deauthentication frame in Run state: reason code=String.	Run状态收到deauth报文，报文中携带的原因码。
Failed to process (re)association request in Run state.	Run状态收到association或者reassociation处理 失败
Unmatched authentication algorithm in received authentication message.	Run状态收到Auth报文，检查报文中携带的认证算法不通过
Idle timer timeout.	Run状态收到idle time 超时
Keepalive timer timeout.	Run状态收到KeepAlive超时
Received authentication failure message.	Run状态下收到用户认证失败消息
Failed to synchronize authentication succeeded message downstream.	主状态机收到用户认证成功消息下行通知STA状态信息失败
Client RSSI was lower than the threshold and was marked as decreasing.	信号强度低于设定值且被标记为变弱
Configured whitelist for the first time or executed the reset wlan client all command.	首次配置白名单，或者命令行输入Reset wlan client all
Received client offline websocket message.	收到client下线的websocket消息
WMAC logged off all clients associated with the radio.	WMAC模块剔除射频下所在STA
Timer for sending disassociation message timed out.	发送DisAsso报文定时器超时
The client is in blacklist or deleted from whitelist.	STA在黑名单中，或者从白名单中删除
Client was added to the dynamic blacklist.	添加动态黑名单
Failed to roam out.	漫出失败
Implemented inter-AC roaming for the first time.	AC间第一次漫出
Successfully roamed to another BSS.	Ac内漫出成功，踢旧的STA下线
Failed to roam in.	收到漫进请求，处理失败（不管是AC间还是AC内）

下线原因	描述
Roaming process received a message for logging off the client.	漫游业务线程收到kick STA消息
Roaming process processed Down event and logged off roam-in clients.	业务线程处理Down 事件，删除漫入STA
Roaming failure.	漫游失败的处理
Successfully performed roaming but failed to recover authentication data.	漫游成功恢复认证数据失败
Roaming timed out.	漫游超时
Seamless roaming failed.	零漫游失败
Logged off clients that performed inter- or intra-AC roaming.	AC间漫入或漫出的STA直接踢掉
Failed to process AccessCtrlChk when configured permitted AP group or permitted SSID.	业务模块处理accessctrlchk失败，设置permit ap-group或者设置permit-ssid
Synchronized client information to process and logged off client in Run state.	同步station信息至配置线程， run状态的sta则会报下线
Failed to synchronize client state to uplink/downlink devices.	上下行失败
Local AC or remote AP received add mobile message, updated BSS, and logged off clients in Run state.	local AC或者remote AP收到Add mobile消息时，更新bss数据，删除remote ap下的sta,如果STA状态为run,则报下线事件
Upgraded HA and logged off all clients.	高可靠性升级删除所有STA
Synchronized BSS data during master/backup AC switchover process.	主备切换时，同步BSS数据错误
Failed to synchronize service template data during master/backup AC switchover process.	在主备切换时，同步服务模板数据时出现了错误
BSS aging timer timed out.	老化BSS定时器超时
Remote AP deleted non-local forwarding BSS.	remote ap下，删除非本地转发的BSS
Failed to find configuration data when synchronizing data.	同步数据时没有找到对应的配置数据
BSS was deleted: BSS synchronization examination failed or there was no BSS data to be updated.	删除BSS：没有要同步的数据；检查过程出错了
Failed to get BSS by using WLAN ID.	根据wlanid获取BSS失败
Unbound inherited service template.	去绑定继承的服务模板
STAMGR process was down automatically or manually.	STAMGR进程shutdown或者用户手工中止进程
Deleted redundant clients.	删除冗余的STA
Failed to process authorized doing nodes.	处理授权doing节点失败
Authorization failed.	授权失败之后，导致的用户下线
NSS value in Operating Mode Notification Action packet doesn't support mandatory VHT-MCS.	Operating Mode Notification Action报文中的NSS值不支持VHT-MCS

下线原因	描述
Number of sent SA requests exceeded the permitted threshold.	计数器值大于SA Request允许发送值
Fit AP received message for deleting the client.	Fit AP上收到处理删除sta消息
Local AC came online again and deleted all clients associated with the BSS.	Local AC重新上线删除bss下关联的所有sta
Failed to upgrade hot backup.	热备升级失败
The illegally created BSS was deleted.	非法创建的BSS被删除
Failed to process requests when receiving UserAuth Success message.	收到用户认证成功报文时，处理请求失败
Failed to get AP type when receiving UserAuth Success message.	收到用户认证成功报文时，获取AP类型失败
The client doesn't support mandatory rate.	客户端不支持强制速率
Disabled access services for 802.11b clients.	配置了禁止802.11b客户端接入功能
The client doesn't support mandatory VHT-MCS.	客户端不支持强制VHT-MCS
Enabled the client dot11ac-only feature.	配置了仅允许802.11ac客户端接入功能
Disabled MUTxBF.	关闭了MU-TxBF功能
Disabled SUTxBF.	关闭了SU-TxBF功能
The client doesn't support mandatory MCS.	客户端不支持强制MCS
Channel bandwidth changed.	信道带宽改变
Disabled the client dot11n-only feature.	配置了仅允许802.11n客户端接入功能
Disabled short GI.	关闭了Short-GI功能
Disabled the A-MPDU aggregation method.	关闭了A-MPDU功能
Disabled the A-MSDU aggregation method.	关闭了A-MSDU功能
Disabled STBC.	关闭了STBC功能
Disabled LDPC.	关闭了LDPC功能
The MIMO capacity decreased, and the MCS supported by the AP can't satisfy the client's negotiated MCS.	MIMO降低，AP支持的MCS不满足客户端已经协商的MCS
The MIMO capacity decreased, and the VHT-MCS supported by the AP can't satisfy the client's negotiated VHT-MCS.	MIMO降低，AP支持的VHT-MCS不满足客户端已经协商的VHT-MCS
Hybrid capacity increased, which kicked off clients associated with other radios with lower Hybrid capacity.	Hybrid能力提高，导致其它Hybrid能力低的Radio的客户端下线
Failed to add MAC address.	添加MAC表项失败
The roaming entry doesn't exist while the AC was processing the roaming request during client smooth reconnection.	客户端平滑重连，处理漫游请求消息时，漫游表项不存在
Home AC processed the move out response message	AC间漫游，HA处理move out resp消息更新漫游表项

下线原因	描述
to update the roaming entry and notified the foreign AC to force the client offline during an inter-AC roaming.	时，通知FA强制客户端下线
The associated AC left from the mobility group and deleted roam-in entries and roaming entries of the client.	漫游组成员离开，删除漫入表项
Executed the **reset wlan mobility roaming** command.	执行**reset wlan mobility roaming**命令，删除客户端
Kicked client because of roaming to another bssid.	客户端漫游到另一个BSSID，强制旧的客户端下线
The roaming entry doesn't exist while the AC was processing the Add Preroam message during client smooth reconnection.	客户端平滑重连，处理ADD preroam消息时，漫游表项不存在
Deleted roaming entries of clients in the fail VLAN while processing a fail VLAN delete event.	处理FailVlan删除事件，删除漫游表项
Deleted the roaming entry of the client while processing a client delete event.	处理STA删除事件，删除漫游表项
Moving to another SSID on the same radio.	客户端从该射频接口的另一个SSID上线
Kicked the client because Oasis platform microservice deleted the password entry.	绿洲微服务删除密码表项并下发设备侧或设备侧该密码表项老化，强制通过绿洲密码上线的客户端下线
Time expired for learning client IPv4 address through DHCP.	未通过DHCP方式学习到IPv4地址的客户端下线超时时间
AP triggered (idle timeout).	闲置定制器超时，由AP上触发
AP triggered (channel change).	信道切换，由AP上触发
AP triggered (bandwidth change).	信道带宽改变，由AP上触发
Received log-off packet from 802.1X authentication client.	收到802.1X认证用户的log-off报文
802.1X client handshake failed.	802.1X认证用户握手失联
Accounting update timed out for the 802.1X authentication client.	802.1X认证用户计费更新超时
Accounting update timed out for the MAC authentication client.	MAC地址认证用户计费更新超时
802.1X authentication client idle cut on AP.	AP上闲置切断定制器超时，802.1X认证用户使用流量未达到闲置切断流量
MAC authentication client idle cut on AP.	AP上闲置切断定制器超时，MAC地址认证用户使用流量未达到闲置切断流量
Session timeout timer expired for the 802.1X authentication client.	802.1X认证用户会话时长为0
Session timeout timer expired for the MAC authentication client.	MAC地址认证用户会话时长为0
Received client disassociation message from server for the 802.1X authentication client.	802.1X认证用户收到服务器下发的删除用户消息
Received client disassociation message from server for the MAC authentication client.	MAC地址认证用户收到服务器下发的删除用户消息

下线原因	描述
Received nonexistent authorization VLAN group for the 802.1X authentication client.	802.1X认证用户收到不存在的授权vlan-group
Received nonexistent authorization VLAN group for the MAC authentication client.	MAC地址认证用户收到不存在的授权vlan-group
Total client traffic failed to reach the minimum traffic threshold.	AC上收到AP上报流量时，终端使用流量未达到闲置切断流量
Failed to obtain the client IP address before the accounting delay timer expired.	开启计费延时功能后，在配置的时间内未获取到用户IP地址

158.9 STAMGR_CLIENT_ONLINE

日志内容	Client [STRING] went online from BSS [STRING] VLAN [STRING] with SSID [STRING] on AP [STRING] Radio ID [STRING]. State changed to Run.
参数解释	$1：客户端的MAC地址 $2：BSSID $3：用户上线的VLAN ID $4：无线服务模板的SSID $5：客户端上线的AP名称 $6：客户端上线的Radio ID
日志等级	6
举例	STAMGR/6/STAMGR_CLIENT_ONLINE: Client dc2d-cb33-2147 went online from BSS dc2d-cbef-78dc VLAN 1 with SSID abc on AP ap1 Radio ID 2. 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

158.10 STAMGR_CLIENT_SNOOPING

日志内容	Detected client IP change: Client MAC: [SRTING], IP: [STRING], [STRING], [STRING], Username: [STRING], AP name: [STRING], Radio ID [UCHAR], Channel number: [UINT32], SSID: [STRING], BSSID: [STRING].
参数解释	$1：客户端的MAC地址 $2：客户端当前使用的IP地址 $3：客户端已使用的IP地址 $4：客户端已使用的IP地址 $5：客户端使用的用户名 $6：客户端上线的AP名 $7：客户端上线的Radio ID $8：客户端使用的信道号 $9：客户端上线的无线服务SSID $10：客户端上线的无线服务BSSID
日志等级	6
举例	STAMGR_CLIENT_SNOOPING: Detected client IP change: Client MAC: dc2d-cbea-17ff,IP: 4.4.4.4, IP: 1.1.1.1, IP: 2.2.2.2,IP: -NA-,User name: test, AP name: ap1, Radio ID: 1, Channel number: 161,SSID: 123, BSSID: dc2d-cbd5-261a.
日志说明	在ap1的Radio 1上使用用户名为test上线的客户端MAC地址为31ac-11ea-17ff，客户端当前使用的IP地址为：4.4.4.4,已使用的IP地址为：1.1.1.1,2.2.2.2。客户端使用的信道号为161，接入的无线服务SSID为123，BSSID为dc2d-cbd5-261a
处理建议	无

158.11 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 dc2d-cb16-28cd.
日志说明	Master AC断开与BAS AC的连接
处理建议	无

158.12 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 dc2d-cb16-28cd.
日志说明	客户端断开与BAS AC的连接
处理建议	无

158.13 STAMGR_MACA_LOGIN_FAILURE

日志内容	-Username=[STRING]-UserMAC=[STRING]-SSID=[STRING]-APName=[STRING]-RadioID=[STRING]-VLANID=[STRING]-UsernameFormat=[STRING]; A user failed MAC authentication. Reason: [STRING].

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AP
	$5：用户上线的Radio ID
	$6：用户上线的VLAN ID
	$7：用户名格式
	• fixed：固定用户名格式
	• MAC address：MAC 地址格式
	$8：用户MAC地址认证失败的原因：
	• AAA processed authentication request and returned error code *code*：AAA 处理认证请求并返回错误码 *code*，*code* 取值如下：
	  ○ 4：认证域不存在/服务类型错误/用户名或密码错误
	  ○ 8：服务器上没有添加设备 IP 地址/服务器上配置的共享密钥与设备配置的共享密钥不一致/服务器与设备网络不可达
	  ○ 26：认证域下的配置错误
	• AAA processed authorization request and returned error code code：AAA 处理授权请求并且返回错误码 code，code 取值如下：
	  ○ 8：服务器与设备网络不可达
	• AAA processed accounting-start request and returned error code code：AAA 处理计费开始请求并且返回错误码 code，code 取值如下：
	  ○ 8：服务器与设备网络不可达
	• AAA processed accounting-update request and returned error code code：AAA 处理计费更新请求并且返回错误码 code，code 取值如下：
	  ○ 8：服务器与设备网络不可达
	• Client timeout timer expired：用户定时器超时
	• Received user security information and kicked off the client：收到用户安全信息，删除用户
	• Accounting-update timer expired, and no responses were received from the server：计费更新定时器超时并且没有收到服务器回应
	• Kicked off the client when the idle timeout timer expired：Idle-cut 定时器超时，强制用户下线
	• Authentication method error：认证模式错误
	• Kicked off the client because the server-assigned session timeout timer is 0：服务器下发的会话时长为 0，强制用户下线
	• Received session disconnection event：收到服务器断开会话连接事件
	• Received nonexistent authorization VLAN group：收到不存在的授权 vlan 组
	• Client kicked out on expiration of the idle-cut timer because its total traffic had not reached the required minimum amount of traffic：在更新计费流量时，客户端使用流量低于 idle-cut 流量
	• Had failed to obtain the client IP address before the accounting delay timer

	expired：计费延迟定时器超时且客户端没有获取到 IP 地址 • Unknown reason：其它未知原因
日志等级	5
举例	STAMGR/5/STAMGR_MACA_LOGIN_FAILURE:-Username=MAC-UserMAC=dc2d-cb16-28cd-SSID=text-wifi-APName=ap1-RadioID=2-VLANID=11-UsernameFormat=fixed; A user failed MAC authentication. Reason: AAA processed authentication request and returned error code 8.
日志说明	AAA处理认证请求并且返回错误码8，用户MAC地址认证失败
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 • 在认证过程中返回的错误码可能对应多种情况，请逐一排查

158.14 STAMGR_MACA_LOGIN_SUCC

日志内容	-Username=[STRING]-UserMAC=[STRING]-SSID=[STRING]-APName=[STRING]-RadioID=[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AP $5：用户上线的Radio ID $6：用户上线的VLAN ID $7：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=dc2d-cb16-28cd-SSID=text-wifi-APName=ap1-RadioID=2-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

158.15 STAMGR_MACA_LOGOFF

日志内容	-Username=[STRING]-UserMAC=[STRING]-SSID=[STRING]-APName=[STRING]-RadioID=[STRING]-VLANID=[STRING]-UsernameFormat=[STRING]; Session for a MAC authentication user was terminated. Reason: [STRING].

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AP
	$5：用户上线的Radio ID
	$6：用户上线的VLAN ID
	$7：用户名格式
	• fixed：固定用户名格式
	• MAC address：MAC 地址格式
	$6：用户的下线原因：
	• AAA processed authentication request and returned error code code. Server reason: reason：AAA处理认证请求，设备返回错误码code，服务器返回失败原因reason，当服务器未返回失败原因时，不显示此字段。code 取值如下：
	  ○ 4：认证域不存在/服务类型错误/用户名或密码错误
	  ○ 8：服务器上没有添加设备 IP 地址/服务器上配置的共享密钥与设备配置的共享密钥不一致/服务器与设备网络不可达
	  ○ 26：认证域下的配置错误
	• AAA processed authorization request and returned error code *code. Server reason: reason*：AAA处理认证请求，设备返回错误码*code*，*服务器返回失败原因reason*，当服务器未返回失败原因时，不显示此字段。*code* 取值如下：
	  ○ 8：服务器与设备网络不可达
	• AAA processed accounting-start request and returned error code *code. Server reason: reason*：AAA处理认证请求，设备返回错误码*code*，*服务器返回失败原因reason*，当服务器未返回失败原因时，不显示此字段。*code* 取值如下：
	  ○ 8：服务器与设备网络不可达
	• AAA processed accounting-update request and returned error code *code. Server reason: reason*：AAA处理认证请求，设备返回错误码*code*，*服务器返回失败原因reason*，当服务器未返回失败原因时，不显示此字段。*code* 取值如下：
	  ○ 8：服务器与设备网络不可达
	• Client timeout timer expired：用户定时器超时
	• Received user security information and kicked off the client：收到用户安全信息，删除用户
	• Lost in shaking hands：握手失联
	• Accounting-update timer expired, and no responses were received from the server：计费更新定时器超时，没有收到服务器回应
	• Kicked off the client when the idle timeout timer expired：Idle-cut 定时器超时，强制用户下线
	• Authentication method error：认证模式错误
	• Kicked off the client because the server-assigned session timeout timer is 0：服务器下发的会话时长为 0，强制用户下线
	• Received session disconnection event：收到服务器断开会话连接事件

	• Received disassociation frame in Run state: reason code=code：在线状态收到终端去关联报文 • Received deauthentication frame in Run state: reason code=code：在线状态收到终端去认证报文 • Received disassociation packet in Userauth state：用户认证状态收到去关联报文 • Received deauthentication packet in Userauth state：用户认证状态收到去认证报文 • Received client failure message with reason code=code：其他场景收到用户上线失败消息 • Received client offline message with reason code=code：其他场景收到用户下线消息 • Unknown reason：其它未知原因
日志等级	6
举例	STAMGR/6/STAMGR_MACA_LOGOFF:-Username=MAC-UserMAC=dc2d-cb16-28cd-SSID=text-wifi-APName=ap1-RadioID=2-VLANID=11-UsernameFormat=fixed; Session for a MAC authentication user was terminated. Reason: Received user security information and kicked off the client.
日志说明	收到用户安全信息，删除用户，用户下线
处理建议	• 若用户主动下线，则不用排查问题 • 若用户异常下线，则需要根据调试信息定位并解决问题

158.16 STAMGR_ROAM_FAILED

日志内容	Client [MAC] on AP [STRING] Radio ID [STRING] failed to roam with reason code [UINT32].
参数解释	$1：发生漫游的客户端的MAC地址 $2：发生漫游的客户端接入的AP $3：发生漫游的客户端接入的Radio ID $4：漫游失败原因的结果码 ‘1’代表：漫游策略选择失败，导致漫游失败 ‘2’代表：系统内存资源不足，导致漫游失败 ‘3’代表：网络通信出现故障，导致漫游失败 ‘4’代表：本地漫游表项缺失，导致漫游失败 ‘5’代表：添加VLAN失败，导致漫游失败
日志等级	4
举例	STAMGR/4/STAMGR_ROAM_FAILED: Client dc2d-cba8-1092 on AP ap1 Radio ID 2 failed to roam with reason code 1.
日志说明	导致客户端漫游失败的原因为漫游策略选择失败
处理建议	漫游失败原因的结果码对应的处理： 1：使用 display wlan client verbose 命令查看客户端的认证方式是否改变 2：使用 display process memory 命令查看哪个模块占用内存资源较多 3：使用 display wlan mobility group 命令查看漫游组的链路是否连通 4：处理步骤同3

158.17 STAMGR_ROAM_SUCCESS

日志内容	Client [MAC] roamed from BSSID [MAC] on AP [STRING] Radio ID [STRING] of AC IP [IPADDR] to BSSID [MAC] on AP [STRING] Radio ID [STRING] of AC IP [IPADDR] successfully.
参数解释	$1：发生漫游的客户端的MAC地址 $2：客户端漫游前接入的AP的BSSID $3：客户端漫游前接入的AP $4：客户端漫游前接入的Radio ID $5：客户端漫游前接入AC的IP地址 $6：客户端漫游后接入AP的BSSID $7：客户端漫游后接入的AP $8：客户端漫游后接入的Radio ID $9：客户端漫游后接入AC的IP地址
日志等级	6
举例	STAMGR/6/STAMGR_ROAM_SUCCESS: Client dc2d-cb5f-dffd roamed from BSSID dc2d-cb89-6ad0 on AP ap1 Radio ID 2 of AC IP 172.25.0.81 to BSSID dc2d-cbab-baf0 on AP ap2 Radio ID 2 of AC IP 172.25.0.82 successfully.
日志说明	客户端漫游成功
处理建议	无需处理

158.18 STAMGR_SERVICE_FAILURE

日志内容	Service failure occurred on BSS [STRING] after service template [STRING] with SSID [STRING] was bound to radio [STRING] on AP [STRING] with AP ID [STRING]. Reason: [STRING], code=0x[STRING].
参数解释	$1：BSSID $2：服务模板的名称 $3：服务模板的SSID $4：Radio ID $5：AP的名称 $6：AP ID $7：BSS服务失败的原因，详细内容请参见表158-3 $8：错误码
日志等级	6
举例	STAMGR/6/SERVICE_FAILURE: Service failure occurred on BSS dc2d-cbef-78dc after service template st1 with SSID st1ssid was bound to radio 1 on AP ap1 with AP ID 1. Reason: Failed to activate BSS when AP came online, code=0x61140001.
日志说明	AP上线，激活BSS失败，错误码为0x61140001
处理建议	请根据调试信息定位并解决问题

表158-3 BSS 服务失败原因

失败原因	描述
Failed to create a BSS interface during smooth BSS interface creation.	平滑BSS同步创建接口，创建BSS接口失败
Replied with failure to transmit interface creation node during smooth BSS interface creation.	平滑BSS同步创建接口，回复节点传输失败
Failed to set forwarding location during smooth recovery of AP data.	平滑恢复AP数据，设置转发位置失败
Failed to initiate a series of locations during smooth recovery of AP data.	平滑恢复AP数据，初始化相关位置失败
Failed to send message of creating BSS interface to worker thread during smooth recovery of AP data.	平滑恢复AP数据，向工作线程发送创建接口消息失败
Failed to create handle during smooth recovery of AP data.	平滑恢复AP数据，创建操作所需句柄失败
Failed to activate BSS during smooth recovery of AP data.	平滑恢复AP数据，激活BSS失败
Failed to set kernel forwarding table during smooth recovery of AP data.	平滑恢复AP数据，设置内核转发表项失败
Failed to create BSS node when AP came online.	AP上线，创建BSS节点失败
Failed to create BSS handle when AP came online.	AP上线，创建BSS所需的句柄失败
Insufficient memory for creating BSS node when AP came online.	AP上线，没有足够内存资源
Failed to get radio private data while creating BSS node in general process.	创建BSS节点常用流程中，获取Radio私有数据失败
Failed to initiate a series of locations while creating BSS node in general process.	创建BSS节点常用流程中，初始化相关位置失败
Failed to set kernel forwarding table while creating BSS node in general process.	创建BSS节点常用流程中，设置内核转发表项失败
Failed to create BSS node during smooth recovery of BSS data.	平滑恢复BSS数据，创建BSS节点失败
Failed to get AP location while recovering BSS running data from DBM.	从DBM库中恢复BSS运行数据，获取AP位置失败
Failed to get radio private data while recovering BSS running data from DBM.	从DBM库中恢复BSS运行数据，获取Radio私有数据失败
Failed to add BSS index to interface index while recovering BSS running data from DBM.	从DBM库中恢复BSS运行数据，添加BSS索引到接口索引失败
Failed to create BSS handle when hierarchy device received Add WLAN message.	分层设备收到Add WLAN消息，创建BSS所需的句柄失败
Failed to initiate a series of locations when hierarchy device received Add WLAN message.	分层设备收到Add WLAN消息，初始化相关位置失败
Failed to set forwarding location when hierarchy device received Add WLAN message.	分层设备收到Add WLAN消息，设置转发位置失败
Failed to send message to worker thread when hierarchy device received Add WLAN message.	分层设备收到Add WLAN消息，发送消息到工作线程失败

失败原因	描述
Failed to set kernel forwarding table when hierarchy device received Add WLAN message.	分层设备收到Add WLAN消息，设置内核转发表项失败
Failed to activate BSS when hierarchy device received Add WLAN message.	分层设备收到Add WLAN消息，激活BSS失败
Failed to issue Add WLAN message when hierarchy device received Add WLAN message.	分层设备收到Add WLAN消息，下发Add WLAN消息失败
Failed to activate BSS when service template was bound.	绑定服务模板，激活BSS失败
Failed to create BSS node when service template was bound.	绑定服务模板，创建BSS节点失败
Failed to create BSS handle when service template was bound.	绑定服务模板，创建操作所需句柄失败
Failed to add bind node to mapped radio list of the service template while recovering service template binding information for service thread from pending database.	恢复服务模板绑定信息时，添加绑定节点到服务模板mapped链表失败
Failed to create BSS node while recovering service template binding information for service thread from pending database.	恢复服务模板绑定信息时，创建BSS节点失败
Failed to add bind node to mapped radio list of the service template while creating BSS from Merger.	从Merger创建BSS时，添加绑定节点到服务模板mapped链表失败
Failed to create BSS node while creating BSS from Merger.	从Merger创建BSS时，创建BSS节点失败
Failed to apply for memory while creating BSS node.	创建BSS节点时，申请内存空间失败
Failed to calculate BSSID while creating BSS node.	创建BSS节点时，计算BSSID失败
Service thread received interface creation failure while creating BSS interface during smooth recovery of AP data.	在平滑恢复AP数据阶段创建接口时，业务线程收到创建接口失败的结果
Failed to add BSS index to interface index while creating BSS interface during smooth recovery of AP data.	在平滑恢复AP数据阶段创建接口时，添加BSS索引失败
Failed to add VLAN on the interface while creating BSS interface during smooth recovery of AP data.	在平滑恢复AP数据阶段创建接口时，添加VLAN失败
Failed to set the source MAC address of the interface while creating BSS interface during smooth recovery of AP data.	在平滑恢复AP数据阶段创建接口时，设置BSS接口源MAC失败
Failed to set kernel forwarding table while creating BSS interface during smooth recovery of AP data.	在平滑恢复AP数据阶段创建接口时，设置内核转发表项失败
Failed to activate BSS while creating BSS interface during smooth recovery of AP data.	在平滑恢复AP数据阶段创建接口时，BSS激活失败
Replied with failure to transmit interface creation node when hierarchy device created an interface accordingly.	分层设备同步创建接口，回复节点传输失败
Failed to create BSS interface when BSS created an interface accordingly.	BSS同步创建接口，创建BSS接口失败

失败原因	描述
Failed to add BSS index to interface index when BSS created an interface accordingly.	BSS同步创建接口，添加BSS索引失败
Failed to add VLAN on the interface when BSS created an interface accordingly.	BSS同步创建接口，添加VLAN失败
Failed to set source MAC address of the interface when BSS created an interface accordingly.	BSS同步创建接口，设置src mac失败
Failed to set kernel forwarding table when BSS created an interface accordingly.	BSS同步创建接口，设置内核转发表项信息失败
Failed to issue ADD BSS message when BSS created an interface accordingly.	BSS同步创建接口，下发消息失败
Replied with failure to transmit interface creation node when hierarchy device created an interface accordingly for an invalid interface.	BSS为无效接口同步创建接口，回复节点传输失败
Created BSS rollback for failed resources while issuing ADD BSS message callback.	下发添加BSS消息回调函数中，创建BSS失败资源回滚
Failed to enable packet socket while recovering BSS running data from DBM.	从DBM恢复BSS运行数据，使能packet套接字失败
Failed to create BSS node while recovering BSS running data from DBM.	从DBM恢复BSS运行数据，创建BSS节点失败
Failed to initiate BSS while creating BSS node.	创建BSS节点，初始化BSS失败
Failed to activate BSS when service template was enabled.	服务模板处于使能状态时，激活BSS 失败
Invalid BSS interface index while upgrading BSS with AP private data.	使用AP私有数据升级BSS，接口索引无效
Failed to upgrade backup BSS to real BSS while upgrading BSS with AP private data.	使用AP私有数据升级BSS，升级到真实BSS失败
Failed to set kernel forwarding table while upgrading BSS with AP private data.	使用AP私有数据升级BSS，设置内核转发表项失败
Failed to activate BSS while upgrading BSS with AP private data.	使用AP私有数据升级BSS，激活BSS失败
Invalid BSS interface index while upgrading BSS without AP private data.	不使用AP私有数据升级BSS，接口索引无效
Failed to set kernel forwarding table while upgrading BSS without AP private data.	不使用AP私有数据升级BSS，设置内核转发表项失败
Failed to activate BSS while upgrading BSS without AP private data.	不使用AP私有数据升级BSS，激活BSS失败
Failed to create BSS interface while creating general BSS process.	创建BSS通用流程，创建接口失败
Failed to activate BSS during smooth recovery of BSS data.	BSS平滑恢复数据，激活BSS失败
Failed to activate BSS while recovering service template binding information for service thread from pending database.	从pending为业务线程恢复服务模板绑定信息，激活BSS失败
Failed to activate BSS while creating BSS from Merger.	从Merger创建BSS，激活BSS失败

失败原因	描述
Failed to activate BSS when AP came online.	AP上线，激活BSS失败
Failed to activate BSS when other module sent activation request.	其他模块通知激活，激活BSS失败
Failed to activate BSS when other module received activation request.	其他模块接收到激活通知，激活BSS失败
Failed to send response node of creating interface while creating interface during smooth recovery of AP data.	AP平滑恢复数据创建接口，回复节点传输失败
Failed to add BSS index to interface index when hierarchy device created an interface accordingly.	分层设备同步创建接口，添加BSS索引失败
Failed to add VLAN on the interface when hierarchy device created an interface accordingly.	分层设备同步创建接口，添加VLAN失败
Failed to set source MAC address of the interface when hierarchy device created an interface accordingly.	分层设备同步创建接口，设置src mac失败
Failed to set kernel forwarding table when hierarchy device created an interface accordingly.	分层设备同步创建接口，设置内核转发表项失败
Failed to activate BSS when hierarchy device created an interface accordingly.	分层设备同步创建接口，激活BSS失败
Failed to issue Add BSS message when hierarchy device created an interface accordingly.	分层设备同步创建接口，下发添加BSS消息失败
Insufficient memory when hierarchy device received BSS creation message.	分层设备收到创建BSS消息，没有足够内存
Failed to fill BSS basic data when hierarchy device received BSS creation message.	分层设备收到创建BSS消息，填充BSS基础数据失败
Failed to initiate BSS service phase when hierarchy device received BSS creation message.	分层设备收到创建BSS消息，初始化BSS服务phase失败
Failed to receive Add WLAN message when hierarchy device received BSS creation message.	分层设备收到创建BSS消息，接收Add WLAN消息失败
Failed to get radio private data because of invalid AP ID when hierarchy device received BSS creation message.	分层设备收到创建BSS消息，无效APID造成获取radio私有数据失败
Failed to get radio private data because of invalid radio ID when hierarchy device received BSS creation message.	分层设备收到创建BSS消息，无效radioid造成获取radio私有数据失败
Failed to get radio private data when hierarchy device received Add WLAN message.	分层设备收到添加wlan消息，获取radio私有数据失败
Failed to issue message when hierarchy device received Add WLAN message.	分层设备收到Add WLAN消息，下发消息失败
Failed to get BSS data through WLAN ID during smooth recovery of BSS data.	BSS平滑恢复数据，通过wlanid获取BSS数据失败
Failed to issue Add WLAN message while creating BSS node in general process.	在常用流程中创建BSS节点时，下发Add WLAN消息失败
Failed to create BSS interface when hierarchy device created an interface accordingly.	分层设备同步创建接口，创建BSS接口失败

失败原因	描述
Failed to create BSS interface when hierarchy device created an interface accordingly for an invalid interface.	分层设备为无效接口同步创建接口，创建BSS接口失败
Failed to set forwarding location while creating BSS node in general process.	在常用流程中创建BSS节点时，设置转发位置失败
Replied with failure to transmit interface creation node when BSS created an interface accordingly.	BSS同步创建接口，回复节点传输失败
Failed to update BSS key data when hierarchy device received Add WLAN message.	分层设备收到Add WLAN消息，更新BSS关键数据失败
Replied with failure to transmit interface creation node when BSS created an interface accordingly for an existing BSS.	为已存在的BSS同步创建接口，回复节点传输失败

158.19 STAMGR_SERVICE_OFF

日志内容	BSS [STRING] was deleted after service template [STRING] with SSID [STRING] was unbound from radio [STRING] on AP [STRING]. Reason: [STRING].
参数解释	$1：BSSID $2：服务模板的名称 $3：服务模板的SSID $4：Radio ID $5：AP的名称 $6：BSS删除的原因： Unknown reason：未知错误 AP down：AP下线 Deleted BSS with the Delete mark when inter-AC BSS smooth ended：AC间BSS平滑结束，删除带有“删除”标记的BSS Hierarchy device received BSS delete message：分层设备收到删除BSS的消息 Deleted AP private data from APMGR when AP smooth ended：AP平滑结束，删除APMGR中的AP私有数据 WLAS was triggered, and service was shut down temporarily：触发WLAS，临时关闭服务 Intrusion protection was triggered, and service was shut down permanently：触发入侵检测，永久关闭服务 Service module received Update WLAN message when BSS was inactive：BSS处于非活跃状态时，业务模块收到Update WLAN信息 Disabled service template：关闭服务模板 Unbound service template：解除绑定服务模板 Deleted BSS with the Delete mark when inter-AC AP smooth ended：AC间AP平滑结束，删除带有“删除”标记的BSS BSS aging timer timed out：BSS老化定时器超时 Deleted non-local forwarding BSS when AP enabled with remote AP went offline：开启了Remote AP功能的AP下线，删除其下非本地转发的BSS Failed to find configuration data while synchronizing data：同步数据时没有找到对应的配置数据 AP did not come online or service template was disabled：BSS所属的AP没有上线或者服务模板处于未使能状态 Failed to find the WLAN ID from APMGR while BSS was smoothing WLAN ID：BSS平滑WLAN ID时，在APMGR中没有找到对应的WLAN ID Unbound inherited service template：解除绑定继承的服务模板 The stamgr process became down automatically or was shut down manually：STAMGR进程down或者用户手工终止进程 Failed to use AP private data to upgrade backup BSS：使用AP私有数据进行备份升级失败 Failed to upgrade backup BSS：备份升级失败 Failed to synchronize service template data to the Merger bind list while upgrading backup data：备份数据升级时，同步服务模板数据到Merger链失败
日志等级	6
举例	STAMGR/6/SERVICE_OFF: BSS dc2d-cbef-78dc was deleted after service template st1 with SSID st1ssid was unbound from radio 1 on AP ap1. Reason: Failed to find

	configuration data while synchronizing data.
日志说明	由于同步数据时没有找到对应的配置数据，删除BSS
处理建议	若BSS正常删除，则不用排查问题 若BSS异常删除，根据异常删除原因定位并解决问题

158.20 STAMGR_STA_ADDMOB_LKUP_ENDOFIOCTL

日志内容	APID=[UINT32]-MAC=[STRING]-BSSID=[STRING]; AC doesn't need to send client information to uplink device: Client information already arrived at the end of the IOCTL tunnel.
参数解释	$1：客户端上线的 AP 的 APID $2：客户端的 MAC 地址 $3：客户端连接的无线服务的 BSSID
日志等级	7
举例	STAMGR/7/STAMGR_STA_ADDMOB_LKUP_ENDOFIOCTL: APID=667-MAC=dc2d-cb69-d7a1-BSSID=dc2d-cb01-d5a0; The AC doesn't need to send client information to uplink device: Client information already arrived at the end of the IOCTL tunnel.
日志说明	由于客户端信息到达 IOCTL 隧道末端，AC 不需要发送客户端信息给上层设备
处理建议	在传统 AC 架构下，若打印此日志信息，则不用排查问题；否则需要根据调试信息定位并解决问题 在分层 AC 架构下，若打印此日志的 AC 为 Central AC，则不用排查问题；若打印日志的 AC 为 Local AC，则需要根据调试信息定位并解决问题

158.21 STAMGR_SERVICE_ON

日志内容	BSS [STRING] was created after service template [STRING] with SSID [STRING] was bound to radio [STRING] on AP [STRING].
参数解释	$1：BSSID $2：服务模板的名称 $3：服务模板的SSID $4：Radio ID $5：AP的名称
日志等级	6
举例	STAMGR/6/SERVICE_ON: BSS dc2d-cbef-78dc was created after service template st1 with SSID 1 was bound to radio 1 on AP ap1.
日志说明	BSS创建，服务启动
处理建议	无

158.22 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 dc2d-cb16-28cd changed to 4.4.4.4.
日志说明	客户端更新IP地址
处理建议	无

158.23 STAMGR_TRIGGER_IP

日志内容	-SSID=[STRING]-UserMAC=[STRING]-APName=[STRING]-RadioID=[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AP $4：用户上线的Radio ID $5：用户上线的VLAN ID $6：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=dc2d-cb16-28cd-APName=ap1-RadioID=2-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

159 STM

本节介绍 STM（IRF）模块输出的日志信息。

159.1 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

159.2 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

159.3 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

159.4 STM_HELLOPKT_NOTSEND

日志内容	Hello thread hasn't sent packets for [UINT32] seconds.
参数解释	$1：时间值
日志等级	5
举例	STM/5/STM_HELLOPKT_NOTSEND: Hello thread hasn't sent packets for 10 seconds.
日志说明	Hello线程在xx秒的时长内一直未发送Hello报文，请尽快定位。如果邻居设备在Hello报文定时器超时时一直未收到Hello报文，会引起IRF分裂
处理建议	CPU利用率持续过高，可能导致Hello线程获取不到CPU资源无法发送Hello报文。请连续多次执行**display cpu-usage**查看系统的CPU利用率，如果CPU利用率持续过高，请进一步排查设备是否受到攻击或者是否有进程运行异常，处理异常使CPU利用率恢复到正常范围。如果CPU利用率恢复到正常范围仍不能发送Hello报文，请联系技术支持

159.5 STM_HELLOPKT_NOTRCV

日志内容	Hello thread hasn't received packets for [UINT32] seconds.
参数解释	$1：时间值
日志等级	5
举例	STM/5/STM_HELLOPKT_NOTRCV: Hello thread hasn't received packets for 10 seconds.
日志说明	Hello线程已经有xx秒钟未收到Hello报文，请尽快定位。如果设备在Hello报文定时器超时时一直未收到Hello报文，会引起IRF分裂
处理建议	**1.** 使用 display irf link 命令查看 IRF 链路是否正常 **2.** 使用 display irf topology 命令查看本设备的邻居设备 **3.** 排查邻居设备上是否未发送 Hello 报文，查看是否有邻居设备生成的 STM_HELLOPKT_NOTSEND 日志。如果是邻居设备未发送 Hello 报文，请根据 STM_HELLOPKT_NOTSEND 日志的处理建议处理

159.6 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

159.7 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

159.8 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

159.9 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

159.10 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

159.11 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

159.12 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

159.13 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

160 STP

本节介绍生成树模块输出的日志信息。

160.1 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 Ethernet1/0/4 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

160.2 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 GigabitEthernet0/4/1 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

160.3 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 GigabitEthernet0/1/1.
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

160.4 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 GigabitEthernet0/1/1 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

160.5 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

160.6 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 Ethernet1/0/2 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

160.7 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

160.8 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 Ethernet1/0/2 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

160.9 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 Ethernet1/0/2 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

160.10 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

160.11 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 GigabitEthernet0/1/1 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

160.12 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 GigabitEthernet0/1/1 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

160.13 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 GigabitEthernet0/1/1 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

160.14 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 GigabitEthernet0/1/1, 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

160.15 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

160.16 STP_STG_NUM_DETECTION

日志内容	STG count [UINT32] is smaller than the MPU's STG count [UINT32].
参数解释	$1：指定单板STG个数 $2：主控板STG个数
日志等级	4
举例	STP/4/STP_STG_NUM_DETECTION: STG count 64 is smaller than the MPU's STG count 65.
日志说明	检测到指定单板上的STG个数小于主控板上的STG个数
处理建议	配置的STP实例个数不能大于所有单板的STG个数的最小值。例如：配置STP实例数是m，所有单板中，STG个数最小的一块单板的STG数是n，m不能大于n

161 SYSEVENT

本节介绍系统事件模块输出的日志信息。

161.1 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 缺省MDC/Context上打印的日志信息不包含MDC *MDC-ID*或Context *Context-ID* 非缺省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

162 SYSLOG

本节包含 syslog 日志消息。

162.1 ENCODING

日志内容	Set the character set encoding to [STRING] for syslog messages.
参数解释	$1：字符集编码方式，取值为UTF-8或GB18030
日志等级	6
举例	SYSLOG/6/ENCODING: Set the character set encoding to UTF-8 for syslog messages..
日志说明	当用户配置信息中心输出日志字符集编码使用UTF-8时，输出该日志
处理建议	登录终端和设备的字符集编码必须一致，以免登录终端不能正常显示设备发送的中文字符

162.2 SYSLOG_LOGBUFFER_FAILURE

日志内容	Log cannot be sent to the logbuffer because of communication timeout between syslog and DBM processes.
参数解释	无
日志等级	4
举例	SYSLOG/4/SYSLOG_LOGBUFFER_FAILURE: Log cannot be sent to the logbuffer because of communication timeout between syslog and DBM processes.
日志说明	日志无法输出到日志缓冲区，因为Syslog进程和DBM进程通信超时
处理建议	请联系技术支持人员

162.3 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

162.4 SYSLOG_RESTART

日志内容	System restarted -- [STRING] [STRING] Software.
参数解释	$1：公司名 $2：软件名
日志等级	6
举例	SYSLOG/6/SYSLOG_RESTART: System restarted -- UNIS Uniware Software
日志说明	系统重启日志
处理建议	无

163 TAC

本节介绍 TAC（Trusted Access Control，可信访问控制）模块输出的日志信息。

163.1 LB_TAC_AUTH (快速日志)

日志内容	User = STRING, MessageType = STRING, IP = STRING, URL = STRING, Result = STRING, Time = STRING
参数解释	$1：用户名 $2：消息类型，包括： • AppAuth：应用鉴权 • ApiAuth：API 鉴权 $3：用户IP地址 $4：APP或API的URL地址 $5：鉴权结果，包括： • AUTH_DENY：拒绝访问 • AUTH_PERMIT：允许访问 • AUTH_REAUTH：二次认证 $6：鉴权时间
日志等级	6
举例	UNIS LB/6/ TAC_AUTH: User = admin, MessageType = AppAuth, IP = , URL = http://6.6.6.6:8080/, Result = AUTH_PERMIT, Time = 20200402154737
日志说明	输出用户鉴权日志消息
处理建议	无需处理

163.2 LB_TAC_NOTIFY_OFFLINE (快速日志)

日志内容	MessageType = STRING, User = STRING, IP = STRING, Time = STRING
参数解释	$1：消息类型，包括： • AppUserOffline：APP 用户下线 • ApiUserOffline：API 用户下线 $2：用户名 $3：用户IP地址 $4：用户下线时间
日志等级	6
举例	UNIS LB/6/ TAC_NOTIFY_OFFLINE: MessageType = ApiUserOffline, User = mAMz8WqXHtBa4R7slIbLNrEiYvuwecnf, IP = 10.1.1.1, Time = 20200401095819
日志说明	鉴权用户已下线
处理建议	无需处理

163.3 LB_TAC_NOTIFY_PERMISSIONUPDOWN (快速日志)

日志内容	MessageType = STRING, User = STRING, IP = STRING, Time = STRING, UrlCnt = [UINT16], UrlList = { STRING, STRING,…}
参数解释	$1：消息类型，包括： • AppUserAccessPermitted：APP 用户权限变更为允许访问 • ApiUserAccessPermitted：API 用户权限变更为允许访问 • AppUserAccessDenied：APP 用户权限变更为禁止访问 • ApiUserAccessDenied：API 用户权限变更为禁止访问 $2：用户名 $3：用户IP地址 $4：用户权限变更时间 $5：用户权限变更的APP或API URL数量 $6：URL列表
日志等级	6
举例	UNIS LB/6/ TAC_NOTIFY_PERMISSIONUPDOWN: MessageType = ApiUserAccessDenied, User = user1, IP = 10.1.1.1, Time = 20200401095819, UrlCnt = 2, UrlList = {http://2.0.0.2:8080/spg_api/app1_api1,http://2.0.0.2:8080/spg_api/app2_api2,}
日志说明	用户权限变更
处理建议	无需处理

164 TACACS

本节介绍 TACACS 模块输出的日志信息。

164.1 TACACS_ACCT_SERVER_DOWN

日志内容	TACACS accounting server was blocked: Server IP=[STRING], port=*[UINT32]*, VPN instance=[STRING].
参数解释	$1：计费服务器IP地址 $2：计费服务器端口号 $3：VPN实例名称，如果服务器属于公网，则显示为public
日志等级	4
举例	TACACS/4/TACACS_ACCT_SERVER_DOWN: TACACS accounting server was blocked: Server IP=1.1.1.1, port=1812, VPN instance=public.
日志说明	TACACS计费服务器状态为阻塞
处理建议	**1.** 检查 TACACS 服务器是否开启。如果 TACACS 服务器关闭，请重新启动 TACACS 服务器。 **2.** 执行 ping 命令检查 TACACS 服务器是否可达。如果 TACACS 服务器不可达，请检查链路是否通畅。 **3.** 请收集日志信息和诊断信息，并联系技术支持

164.2 TACACS_ACCT_SERVER_UP

日志内容	TACACS accounting server became active: Server IP=[STRING], port=*[UINT32]*, VPN instance=[STRING].
参数解释	$1：计费服务器IP地址 $2：计费服务器端口号 $3：VPN实例名称，如果服务器属于公网，则显示为public
日志等级	6
举例	TACACS/6/TACACS_ACCT_SERVER_UP: TACACS accounting server became active: Server IP=1.1.1.1, port=1812, VPN instance=public.
日志说明	TACACS计费服务器状态为激活
处理建议	无

164.3 TACACS_AUTH_FAILURE

日志内容	User [STRING] at [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 at 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

164.4 TACACS_AUTH_SERVER_DOWN

日志内容	TACACS authentication server was blocked: Server IP=[STRING], port=*[UINT32]*, VPN instance=[STRING].
参数解释	$1：认证服务器IP地址 $2：认证服务器端口号 $3：VPN实例名称，如果服务器属于公网，则显示为public
日志等级	4
举例	TACACS/4/TACACS_AUTH_SERVER_DOWN: TACACS authentication server was blocked: Server IP=1.1.1.1, port=1812, VPN instance=public.
日志说明	TACACS认证服务器状态为阻塞
处理建议	**1.** 检查 TACACS 服务器是否开启。如果 TACACS 服务器关闭，请重新启动 TACACS 服务器。 **2.** 执行 ping 命令检查 TACACS 服务器是否可达。如果 TACACS 服务器不可达，请检查链路是否通畅。 **3.** 请收集日志信息和诊断信息，并联系技术支持

164.5 TACACS_AUTH_SERVER_UP

日志内容	TACACS authentication server became active: Server IP=[STRING], port=*[UINT32]*, VPN instance=[STRING].
参数解释	$1：认证服务器IP地址 $2：认证服务器端口号 $3：VPN实例名称，如果服务器属于公网，则显示为public
日志等级	6
举例	TACACS/6/TACACS_AUTH_SERVER_UP: TACACS authentication server became active: Server IP=1.1.1.1, port=1812, VPN instance=public.
日志说明	TACACS认证服务器状态为激活
处理建议	无

164.6 TACACS_AUTH_SUCCESS

日志内容	User [STRING] at [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 at 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

164.7 TACACS_AUTHOR_SERVER_DOWN

日志内容	TACACS authorization server was blocked: Server IP=[STRING], port=*[UINT32]*, VPN instance=[STRING].
参数解释	$1：授权服务器IP地址 $2：授权服务器端口号 $3：VPN实例名称，如果服务器属于公网，则显示为public
日志等级	4
举例	TACACS/4/TACACS_AUTHOR_SERVER_DOWN: TACACS authorization server was blocked: Server IP=1.1.1.1, port=1812, VPN instance=public.
日志说明	TACACS授权服务器状态为阻塞
处理建议	**1.** 检查 TACACS 服务器是否开启。如果 TACACS 服务器关闭，请重新启动 TACACS 服务器。 **2.** 执行 ping 命令检查 TACACS 服务器是否可达。如果 TACACS 服务器不可达，请检查链路是否通畅。 **3.** 请收集日志信息和诊断信息，并联系技术支持

164.8 TACACS_AUTHOR_SERVER_UP

日志内容	TACACS authorization server became active: Server IP=[STRING], port=*[UINT32]*, VPN instance=[STRING].
参数解释	$1：授权服务器IP地址 $2：授权服务器端口号 $3：VPN实例名称，如果服务器属于公网，则显示为public
日志等级	6
举例	TACACS/6/TACACS_AUTHOR_SERVER_UP: TACACS authorization server became active: Server IP=1.1.1.1, port=1812, VPN instance=public.
日志说明	TACACS授权服务器状态为激活
处理建议	无

164.9 TACACS_REMOVE_SERVER_FAIL

日志内容	Failed to remove servers in scheme [STRING].
参数解释	$1：方案名称
日志等级	4
举例	TACACS/4/TACACS_REMOVE_SERVER_FAIL: Failed to remove 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

165 TCSM

本节介绍 TCSM（Trusted Computing Services Management，可信计算服务管理）模块输出的日志信息。

165.1 TCSM_CERT_BROKEN

日志内容	Certificate [STRING] is missing or corrupted.
参数解释	$1：证书的名称
日志等级	3
举例	TCSM/3/TCSM_CERT_BROKEN: Certificate ak1-cert is missing or corrupted.
日志说明	保存在存储介质中的证书文件已丢失或损坏
处理建议	1. 建议更换存储介质 2. 通过管理端为设备的 TCSM 密钥重新签发证书 3. 如果丢失/损坏的是系统预置证书（以 default 为前缀的证书），请联系技术支持

165.2 TCSM_KEY_BROKEN

日志内容	Key [STRING] is corrupted or missing.
参数解释	$1：密钥的名称
日志等级	3
举例	TCSM/3/TCSM_KEY_BROKEN: Key abc is corrupted or missing.
日志说明	保存在存储介质中的密钥文件已丢失或损坏
处理建议	1. 如果该密钥还存在，删除该密钥（相关命令为 key destroy） 2. 建议更换存储介质 3. 如果丢失/损坏的是系统预置密钥，请联系技术支持

165.3 TCSM_KEY_HIERARCHY_BROKEN

日志内容	Key hierarchy of [STRING] is corrupted.
参数解释	$1：密钥的名称
日志等级	3
举例	TCSM/3/TCSM_KEY_HIERARCHY_BROKEN: Key hierarchy of abc is corrupted.
日志说明	指定密钥的上层密钥已损坏
处理建议	**1.** 删除该密钥及其上层密钥（相关命令为 key destroy） **2.** 建议更换存储介质

165.4 TCSM_TSS_SVC_DOWN

日志内容	TSS service is down.
参数解释	无
日志等级	3
举例	TCSM/3/TCSM_TSS_SVC_DOWN: TSS service is down.
日志说明	TSS进程down
处理建议	请联系技术支持

165.5 TCSM_TSS_SVC_UP

日志内容	TSS service is up.
参数解释	无
日志等级	5
举例	TCSM/5/TCSM_TSS_SVC_DOWN: TSS service is up.
日志说明	TSS进程up
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 request from [IPADDR]([STRING]) was denied by ACL rule (rule ID=[INT32]).
参数解释	$1：Telnet客户端IP地址 $2：Telnet客户端IP地址所在VPN $3：Telnet客户端匹配ACL deny规则编号，如果未匹配已创建的ACL规则，则匹配缺省的ACL规则（deny）
日志等级	5
举例	TELNETD/5/TELNETD_ACL_DENY:The Telnet connection request from 181.1.1.10 was denied by ACL rule (rule ID=20). TELNETD/5/TELNETD_ACL_DENY:The Telnet connection request from 181.1.1.10 was denied by ACL rule (default rule).
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 $1 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 TERMINAL

本节介绍终端识别模块输出的快速日志信息。

167.1 TERMINAL_CHANGED_LOG_IP

日志内容	IPAddr(1145)=[IPADDR];PhyInterface(1148)=[STRING];OldMAC(1147)=[STRING];NewMAC(1168)=[STRING];OldVendor(1149)=[STRING];NewVendor(1150)=[STRING];OldType(1151)=[STRING];NewType(1152)=[STRING];OldModel(1153)=[STRING];NewModel(1154)=[STRING];OldSerialNum(1155)=[STRING];NewSerialNum(1156)=[STRING];OldTrmlID(1157)=[UINT32];NewTrmlID(1169)=[UINT32];Action(1053)=[STRING];Standard(1196)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];Location(1209)=[STRING];
参数解释	$1：终端IPv4地址 $2：终端接入的物理接口 $3：原终端MAC地址 $4：新终端MAC地址 $5：原厂商 $6：新厂商 $7：原类型 $8：新类型 $9：原型号 $10：新型号 $11：原序列号 $12：新序列号 $13：原终端ID $14：新终端ID $15：动作 $16：识别标准 $17：VLAN ID $18：VXLAN ID $19：地区
日志等级	4
举例	TERMINAL/4/TERMINAL_CHANGED_LOG_IP:IPAddr(1145)=1.1.1.1;PhyInterface(1148)=g2/0/0;OldMAC(1147)=dc2d-cb86-a375;NewMAC(1168)=dc2d-cb86-a376;OldVendor(1149)=DAHUA;NewVendor(1150)=HIKVISION;OldType(1151)=camera;NewType(1152)=camera;OldModel(1153)=DH-ITC2013;NewModel(1154)=DS-2CD3;OldSerialNum(1155)=1122;NewSerialNum(1156)=2233;OldTrmlID(1157)=123456;NewTrmlID(1169)=123457;Action(1053)=Drop;Standard(1196)=GB28181;VlanID(1175)=400;VNI(1213)=--;Location(1209)=China Macao;
日志说明	满足以下条件后，终端识别模块才会以快速日志的方式向日志主机发送日志： • 有流量触发 • 终端的某项信息发生变化
处理建议	无

167.2 TERMINAL_CHANGED_LOG_IPV6

日志内容	IPv6Addr(1146)=[IPADDR];PhyInterface(1148)=[STRING];OldMAC(1147)=[STRING];NewMAC(1168)=[STRING];OldVendor(1149)=[STRING];NewVendor(1150)=[STRING];OldType(1151)=[STRING];NewType(1152)=[STRING];OldModel(1153)=[STRING];NewModel(1154)=[STRING];OldSerialNum(1155)=[STRING];NewSerialNum(1156)=[STRING];OldTrmlID(1157)=[UINT32];NewTrmlID(1169)=[UINT32];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];Location(1209)=[STRING];
参数解释	$1：终端IPV6地址 $2：终端接入的物理接口 $3：原终端MAC地址 $4：新终端MAC地址 $5：原厂商 $6：新厂商 $7：原类型 $8：新类型 $9：原型号 $10：新型号 $11：原序列号 $12：新序列号 $13：原终端ID $14：新终端ID $15：VLAN ID $16：VXLAN ID $17：地区
日志等级	4
举例	TERMINAL/4/TERMINAL_CHANGED_LOG_IPV6:IPv6Addr(1146)=2001::1;PhyInterface(1148)=g2/0/0;OldMAC(1147)=dc2d-cb86-a375;NewMAC(1168)=dc2d-cb86-a376;OldVendor(1149)=DAHUA;NewVendor(1150)=HIKVISION;OldType(1151)=camera;NewType(1152)=camera;OldModel(1153)=DH-ITC2013;NewModel(1154)=DS-2CD3;OldSerialNum(1155)=1122;NewSerialNum(1156)=2233;OldTrmlID(1157)=123456;NewTrmlID(1169)=123457;VlanID(1175)=400;VNI(1213)=--;Location(1209)=China Macao;
日志说明	满足以下条件后，终端识别模块会以快速日志输出的方式向日志主机发送日志： • 有流量触发 • 终端的某项信息发生变化
处理建议	无

168 TRILL

本节介绍 TRILL 模块输出的日志信息。

168.1 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网络中上RBridge的System ID

168.2 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

168.3 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

168.4 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

168.5 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 ○ up：表示邻居关系已建立，可以正常工作 ○ initializing：表示初始状态 ○ 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

168.6 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

169 UDPI

本节介绍 UDPI（应用账号提取）模块输出的日志信息。

169.1 USER-NETLOG

日志内容	Protocol(1001)= [STRING];SrcIPAddr(1003)= [IPADDR];SrcPort(1004)= [UINT16];DstIPAddr(1007)= [IPADDR];DstPort(1008)= [UINT16]; User(1098)=%s; Application(1002)= [STRING]; Account(1101)= [STRING].
参数解释	$1：协议类型 $2：源IP地址 $3：源端口号 $4：目的IP地址 $5：目的端口号 $6：用户名 $7：应用名称 $8：用户账号
日志等级	6
举例	UDPI/6/USER-NETLOG:-Chassis=1-Slot=5.1;Protocol(1001)=UDP;SrcIPAddr(1003)=22.1.1.2;SrcPort(1004)=0;DstIPAddr(1007)=21.1.1.2;DstPort(1008)=65297;User(1098)=22.1.1.2; Application(1002)=ZhenAiWang; Account(1101)=72753475.
日志说明	当报文与应用账号特征匹配成功时输出该日志
处理建议	无

170 UFLT

本节介绍 URL 过滤模块输出的系统日志和快速日志信息。

170.1 UFLT_MATCH_IPV4_LOG（系统日志）

日志内容	Protocol(1001)=[STRING];Application(1002)=[STRING];URL(1093)=[STRING];URLCategory(1094)=[STRING];PolicyName(1079)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];UserName(1113)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
参数解释	$1：协议类型 $2：应用协议名称 $3：URL内容 $4：URL过滤分类名称 $5：URL过滤策略名称 $6：源IP地址 $7：源端口号 $8：目的IP地址 $9：目的端口号 $10：源安全域名称 $11：目的安全域名称 $12：身份识别用户的名称 $13：动作名称，包括如下取值： • Block-Source：源地址阻断 • Permit：允许 • Drop：丢弃 • Reset：重置 • Redirect：重定向 $14：VLAN ID $15：VXLAN ID $16：源地区 $17：目的地区
日志等级	6
举例	UFLT/6/UFLT_MATCH_IPV4_LOG:Protocol(1001)=TCP;Application(1002)=http;URL(1093)=google.com;URLCategory(1094)=Fashion&Beauty;PolicyName(1079)=policy1;SrcIPAddr(1003)=1.2.3.4;SrcPort(1004)=8080;DstIPAddr(1007)=6.1.1.1;DstPort(1008)=8080;SrcZoneName(1025)=spf;DstZoneName(1035)=spf;UserName(1113)=abc;Action(1053)=Drop;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
日志说明	报文与URL过滤规则匹配成功时输出该日志
处理建议	无

170.2 UFLT_MATCH_IPV6_LOG（系统日志）

日志内容	Protocol(1001)=[STRING];Application(1002)=[STRING];URL(1093)=[STRING];URLCategory(1094)=[STRING];PolicyName(1079)=[STRING];SrcIPv6Addr(1036)=[IPADDR];SrcPort(1004)=[UINT16];DstIPv6Addr(1037)=[IPADDR];DstPort(1008)=[UINT16];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];UserName(1113)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
参数解释	$1：协议类型 $2：应用协议名称 $3：URL内容 $4：URL过滤分类名称 $5：URL过滤策略名称 $6：源IPv6地址 $7：源端口号 $8：目的IPv6地址 $9：目的端口号 $10：源安全域名称 $11：目的安全域名称 $12：身份识别用户的名称 $13：动作名称，包括如下取值： • Block-source：源地址阻断 • Permit：允许 • Drop：丢弃 • Reset：重置 • Redirect：重定向 $14：VLAN ID $15：VXLAN ID $16：源地区 $17：目的地区
日志等级	6
举例	UFLT/6/UFLT_MATCH_IPV6_LOG:Protocol(1001)=TCP;Application(1002)=http;URL(1093)=google.com;URLCategory(1094)=Fashion&Beauty;PolicyName(1079)=policy1;SrcIPv6Addr(1036)=2001::2;SrcPort(1004)=51396;DstIPv6Addr(1037)=3001::2;DstPort(1008)=25;SrcZoneName(1025)=spf;DstZoneName(1035)=spf;UserName(1113)=aaa;Action(1053)=Drop;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
日志说明	IPv6报文与URL过滤规则匹配成功时输出该日志
处理建议	无

170.3 UFLT_NOT_MATCH_IPV4_LOG（系统日志）

日志内容	Protocol(1001)=[STRING];Application(1002)=[STRING];URL(1093)=[STRING];URLCategory(1094)=[STRING];PolicyName(1079)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];UserName(1113)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
参数解释	$1：协议类型 $2：应用协议名称 $3：URL内容 $4：URL过滤分类名称，未匹配URL分类时为Unknown $5：URL过滤策略名称 $6：源IP地址 $7：源端口号 $8：目的IP地址 $9：目的端口号 $10：源安全域名称 $11：目的安全域名称 $12：身份识别用户的名称 $13：动作名称，包括如下取值： • Block-source：源地址阻断 • Permit：允许 • Drop：丢弃 • Reset：重置 • Redirect：重定向 $14：VLAN ID $15：VXLAN ID $16：源地区 $17：目的地区
日志等级	6
举例	UFLT/6/UFLT_NOT_MATCH_IPV4_LOG:Protocol(1001)=TCP;Application(1002)=http;URL(1093)=google.com;URLCategory(1094)=Unknown;PolicyName(1079)=policy1;SrcIPAddr(1003)=1.2.3.4;SrcPort(1004)=8080;DstIPAddr(1007)=6.1.1.1;DstPort(1008)=8080;SrcZoneName(1025)=spf;DstZoneName(1035)=spf;UserName(1113)=abc;Action(1053)=Drop;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
日志说明	报文与URL过滤规则匹配失败时输出该日志
处理建议	无

170.4 UFLT_NOT_MATCH_IPV6_LOG（系统日志）

日志内容	Protocol(1001)=[STRING];Application(1002)=[STRING];URL(1093)=[STRING];URLCategory(1094)=[STRING];PolicyName(1079)=[STRING];SrcIPv6Addr(1036)=[IPADDR];SrcPort(1004)=[UINT16];DstIPv6Addr(1037)=[IPADDR];DstPort(1008)=[UINT16];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];UserName(1113)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
参数解释	$1：协议类型 $2：应用协议名称 $3：URL内容 $4：URL过滤分类名称，未匹配URL分类时为Unknown $5：URL过滤策略名称 $6：源IPv6地址 $7：源端口号 $8：目的IPv6地址 $9：目的端口号 $10：源安全域名称 $11：目的安全域名称 $12：身份识别用户的名称 $13：动作名称，包括如下取值： • Block-source：源地址阻断 • Permit：允许 • Drop：丢弃 • Reset：重置 • Redirect：重定向 $14：VLAN ID $15：VXLAN ID $16：源地区 $17：目的地区
日志等级	6
举例	UFLT/6/UFLT_NOT_MATCH_IPV6_LOG:Protocol(1001)=TCP;Application(1002)=http;URL(1093)=google.com;URLCategory(1094)=Unknown;PolicyName(1079)=policy1;SrcIPv6Addr(1036)=2001::2;SrcPort(1004)=51396;DstIPv6Addr(1037)=3001::2;DstPort(1008)=25;SrcZoneName(1025)=spf;DstZoneName(1035)=spf;UserName(1113)=aaa;Action(1053)=Drop;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
日志说明	IPv6报文与URL过滤规则匹配失败时输出该日志
处理建议	无

170.5 UFLT_WARNING（系统日志）

日志内容	Updated the URL filtering signature library successfully.
参数解释	无
日志等级	4
举例	UFLT/4/UFLT_WARNING: -Context=1; Updated the URL filtering signature library successfully.
日志说明	URL过滤特征库升级成功，包含如下情况： • 立即升级成功 • 本地升级成功
处理建议	无

170.6 UFLT_WARNING（系统日志）

日志内容	Rolled back the URL filtering signature library successfully.
参数解释	无
日志等级	4
举例	UFLT/4/UFLT_WARNING: -Context=1; Rolled back the URL filtering signature library successfully.
日志说明	URL过滤特征库回滚成功，包含如下情况： • 回滚到上一个版本成功 • 回滚到出厂版本成功
处理建议	无

170.7 UFLT_WARNING（系统日志）

日志内容	No available license to update URL signature.
参数解释	无
日志等级	4
举例	UFLT/4/UFLT_WARNING: -Context=1; No available license to update URL signature.
日志说明	license无效，URL过滤特征库升级失败
处理建议	无

170.8 UFLT_WARNING（系统日志）

日志内容	The signature library version is not compatible with the software version. Please use a compatible signature library version on the device.
参数解释	无
日志等级	4
举例	UFLT/4/UFLT_WARNING: -Context=1; The signature library version is not compatible with the software version. Please use a compatible signature library version on the device.
日志说明	当前系统不支持升级此版本特征库，URL过滤特征库升级失败
处理建议	无

170.9 UFLT_WARNING（系统日志）

日志内容	Failed to update signature package in phase [STRING].
参数解释	$1：升级阶段，包括如下取值： • DOWNLOAD：下载特征库阶段 • GETURLFILE：获取特征库文件下载路径阶段 • PREPARE：特征库准备阶段 • PARSE：特征库解析阶段 • UNKNOWN：未知
日志等级	4
举例	UFLT/4/UFLT_WARNING: -Context=1; Failed to update signature package in phase DOWNLOAD.
日志说明	特征库升级失败时，提示用户失败发生在特征库升级的某个阶段
处理建议	无

170.10 UFLT_WARNING（系统日志）

日志内容	uflt Copy SigPack file failed because flash is not enough.
参数解释	无
日志等级	4
举例	UFLT/4/UFLT_WARNING: -Context=1; uflt Copy SigPack file failed because flash is not enough.
日志说明	Flash存储空间不足，URL过滤特征库升级失败
处理建议	无

170.11 UFLT_MATCH_IPV4_LOG（快速日志）

日志内容	Protocol(1001)=[STRING];Application(1002)=[STRING];UserName(1113)=[STRING];SrcMacAddr(1021)=[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];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];PolicyName(1079)=[STRING];URLParentCategory(1128)=[STRING];URLCategory(1094)=[STRING];URL(1093)=[STRING];VistTime(1114)=[STRING];Client(1110)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
参数解释	$1：协议类型 $2：应用名称 $3：用户名 $4：源MAC地址 $5：源IP地址 $6：源端口号 $7：NAT地址转换后的源IP地址 $8：NAT地址转换后的源端口 $9：目的IP地址 $10：目的端口号 $11：NAT地址转换后的目的IP地址 $12：NAT地址转换后的目的端口 $13：源安全域名称 $14：目的安全域名称 $15：URL过滤策略名称 $16：URL过滤父分类名称 $17：URL过滤子分类名称 $18：URL内容 $19：访问时间 $20：客户端类型（暂不支持） $21：动作名称，包括如下取值： • Block-source：源阻断 • Permit：允许 • Drop：丢弃 • Reset：重置 • Redirect：重定向 $22：VLAN ID $23：VXLAN ID $24：源地区 $25：目的地区
日志等级	6
举例	UFLT/6/UFLT_MATCH_IPV4_LOG:Protocol(1001)=TCP;Application(1002)=SouhuNews;UserName(1113)=;SrcMacAddr(1021)=dc-2d-cb-11-93-78;SrcIPAddr(1003)=112.1.1.2;SrcPort(1004)=3887;NATSrcIPAddr(1005)=112.1.1.2;NATSrcPort(1006)=3887;DstIPAddr(1007)=114.1.1.2;DstPort(1008)=80;NATDstIPAddr(1009)=114.1.1.2;NATDstPort(1010)=8

	0;SrcZoneName(1025)=in;DstZoneName(1035)=out;PolicyName(1079)=1;URLParentCategory(1128)=SearchEngines&Portals;URLCategory(1094)=SearchEngines&Portals;URL(1093)=news.sohu.com/upload/itoolbar/itoolbar.index.loader.20140923.js;VistTime(1114)=1480688515;Client(1110)=;Action(1053)=Permit;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
日志说明	报文与URL过滤规则匹配成功时输出该日志
处理建议	无

170.12 UFLT_MATCH_IPV6_LOG（快速日志）

日志内容	Protocol(1001)=[STRING];Application(1002)=[STRING];UserName(1113)=[STRING];SrcMacAddr(1021)=[STRING];SrcIPv6Addr(1036)=[IPADDR];SrcPort(1004)=[UINT16];DstIPv6Addr(1037)=[IPADDR];DstPort(1008)=[UINT16];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];PolicyName(1079)=[STRING];URLParentCategory(1128)=[STRING];URLCategory(1094)=[STRING];URL(1093)=[STRING];VistTime(1114)=[STRING];Client(1110)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
参数解释	$1：协议类型 $2：应用名称 $3：用户名 $4：源MAC地址 $5：源IPv6地址 $6：源端口号 $7：目的IPv6地址 $8：目的端口号 $9：源安全域名称 $10：目的安全域名称 $11：URL过滤策略名称 $12：URL过滤父分类名称 $13：URL过滤子分类名称 $14：URL内容 $15：访问时间 $16：客户端类型（暂不支持） $17：动作名称，包括如下取值： • Block-source：源阻断 • Permit：允许 • Drop：丢弃 • Reset：重置 • Redirect：重定向 $18：VLAN ID $19：VXLAN ID $20：源地区 $21：目的地区
日志等级	6
举例	UFLT/6/UFLT_MATCH_IPV6_LOG:Protocol(1001)=TCP;Application(1002)=SouhuNews;UserName(1113)=;SrcMacAddr(1021)=dc-2d-cb-11-93-78;SrcIPv6Addr(1036)=2001::2;SrcPort(1004)=51396;DstIPv6Addr(1037)=3001::2;DstPort(1008)=25;SrcZoneName(1025)=in;DstZoneName(1035)=out;PolicyName(1079)=1;URLParentCategory(1128)=SearchEngines&Portals;URLCategory(1094)=SearchEngines&Portals;URL(1093)=news.sohu.com/upload/itoolbar/itoolbar.index.loader.20140923.js;VistTime(1114)=1480688515;Client(1110)=;Action(1053)=Permit;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
日志说明	IPv6报文与URL过滤规则匹配成功时输出该日志
处理建议	无

170.13 UFLT_NOT_MATCH_IPV4_LOG（快速日志）

日志内容	Protocol(1001)=[STRING];Application(1002)=[STRING];UserName(1113)=[STRING];SrcMacAddr(1021)=[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];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];PolicyName(1079)=[STRING];URLParentCategory(1128)=[STRING];URLCategory(1094)=[STRING];URL(1093)=[STRING];VistTime(1114)=[STRING];Client(1110)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
参数解释	$1：协议类型 $2：应用名称 $3：用户名 $4：源MAC地址 $5：源IP地址 $6：源端口号 $7：NAT地址转换后的源IP地址 $8：NAT地址转换后的源端口 $9：目的IP地址 $10：目的端口号 $11：NAT地址转换后的目的IP地址 $12：NAT地址转换后的目的端口 $13：源安全域名称 $14：目的安全域名称 $15：URL过滤策略名称 $16：URL过滤父分类名称，未匹配时显示为- $17：URL过滤子分类名称，未匹配时显示为Unknown $18：URL内容 $19：访问时间 $20：客户端类型（暂不支持） $21：动作名称，包括如下取值： • Block-source：源阻断 • Permit：允许 • Drop：丢弃 • Reset：重置 • Redirect：重定向 $22：VLAN ID $23：VXLAN ID $24：源地区 $25：目的地区
日志等级	6
举例	UFLT/6/UFLT_NOT_MATCH_IPV4_LOG:Protocol(1001)=TCP;Application(1002)=Souhu News;UserName(1113)=;SrcMacAddr(1021)=dc-2d-cb-11-93-78;SrcIPAddr(1003)=112.1.1.2;SrcPort(1004)=3887;NATSrcIPAddr(1005)=112.1.1.2;NATSrcPort(1006)=3887;DstIPAddr(1007)=114.1.1.2;DstPort(1008)=80;NATDstIPAddr(1009)=114.1.1.2;NATDstPort(10

	10)=80;SrcZoneName(1025)=in;DstZoneName(1035)=out;PolicyName(1079)=1;URLParentCategory(1128)=-;URLCategory(1094)=Unknown;URL(1093)=news.sohu.com/upload/itoolbar/index/toolbar_bg_130315.gif;VistTime(1114)=1480691551;Client(1110)=;Action(1053)=Permit;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
日志说明	报文与URL过滤规则匹配失败时输出该日志
处理建议	无

170.14 UFLT_NOT_MATCH_IPV6_LOG（快速日志）

日志内容	Protocol(1001)=[STRING];Application(1002)=[STRING];UserName(1113)=[STRING];SrcMacAddr(1021)=[STRING];SrcIPv6Addr(1036)=[IPADDR];SrcPort(1004)=[UINT16];DstIPv6Addr(1037)=[IPADDR];DstPort(1008)=[UINT16];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];PolicyName(1079)=[STRING];URLParentCategory(1128)=[STRING];URLCategory(1094)=[STRING];URL(1093)=[STRING];VistTime(1114)=[STRING];Client(1110)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
参数解释	$1：协议类型 $2：应用名称 $3：用户名 $4：源MAC地址 $5：源IPv6地址 $6：源端口号 $7：目的IPv6地址 $8：目的端口号 $9：源安全域名称 $10：目的安全域名称 $11：URL过滤策略名称 $12：URL过滤父分类名称，未匹配时显示为- $13：URL过滤子分类名称，未匹配时显示为Unknown $14：URL内容 $15：访问时间 $16：客户端类型（暂不支持） $17：动作名称，包括如下取值： • Block-source：源阻断 • Permit：允许 • Drop：丢弃 • Reset：重置 • Redirect：重定向 $18：VLAN ID $19：VXLAN ID $20：源地区 $21：目的地区
日志等级	6
举例	UFLT/6/UFLT_NOT_MATCH_IPV6_LOG:Protocol(1001)=TCP;Application(1002)=SouhuNews;UserName(1113)=;SrcMacAddr(1021)=dc-2d-cb-11-93-78;SrcIPv6Addr(1036)=2001::2;SrcPort(1004)=51396;DstIPv6Addr(1037)=3001::2;DstPort(1008)=25;SrcZoneName(1025)=in;DstZoneName(1035)=out;PolicyName(1079)=1;URLParentCategory(1128)=-;URLCategory(1094)=Unknown;URL(1093)=news.sohu.com/upload/itoolbar/itoolbar.index.loader.20140923.js;VistTime(1114)=1480688515;Client(1110)=;Action(1053)=Permit;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
日志说明	IPv6报文与URL过滤规则匹配失败时输出该日志
处理建议	无

171 VLAN

本节介绍接口 VLAN 模块输出的日志信息。

171.1 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

171.2 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 GigabitEthernet1/0/1.
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

171.3 VLAN_VLANSTRIP_REG_DIFF_CONFIG

日志内容	The value of the vlan-strip register is different from the configuration on interface [STRING].
参数解释	$1：接口名称
日志等级	3
举例	VLAN/3/VLAN_VLANSTRIP_REG_DIFF_CONFIG: The value of the vlan-strip register is different from the configuration on interface GigabitEthernet1/0/1.
日志说明	vlan-strip功能的配置与寄存器的对应值不一致
处理建议	检查虚拟机和宿主机相关工作环境，并重新配置vlan-strip功能。

171.4 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 GigabitEthernet1/0/1.
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

172 VRRP

本节介绍 VRRP 模块输出的日志信息。

172.1 VRRP_AUTH_FAILED

日志内容	Authentication failed in [STRING] virtual router [UINT32] (configured on [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：错误信息详细内容
日志等级	6
举例	VRRP/6/VRRP_AUTH_FAILED: Authentication failed in IPv4 virtual router 10 (configured on Ethernet0/0): Authentication type mismatch.
日志说明	收到了VRRP报文，但没有通过认证
处理建议	检查指定接口上的VRRP备份组配置。确保备份组中所有成员使用相同的验证模式和验证字

172.2 VRRP_CONFIG_ERROR

日志内容	The [STRING] virtual router [UINT32] (configured on [STRING]) detected a VRRP configuration error: [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：错误信息详细内容
日志等级	6
举例	VRRP/6/VRRP_CONFIG_ERROR: The IPv4 virtual router 10 (configured on Ethernet0/0) detected a VRRP configuration error: Virtual IP address count mismatch.
日志说明	VRRP备份组配置错误。例如：成员上的备份组虚拟IP地址的数量不一致
处理建议	检查指定接口上的VRRP备份组配置。确保备份组中所有成员使用相同的配置

172.3 VRRP_PACKET_ERROR

日志内容	The [STRING] virtual router [UINT32] (configured on [STRING]) received an error packet: [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：错误信息详细内容
日志等级	6
举例	VRRP/6/VRRP_PACKET_ERROR: The IPv4 virtual router 10 (configured on Ethernet0/0) received an error packet: CKSUM error.
日志说明	VRRP备份组收到无效VRRP报文。例如，校验和错误
处理建议	检查指定接口上的VRRP备份组配置

172.4 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
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优先级的报文或者发生了抢占
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

172.5 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

172.6 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

173 VSRP

本节介绍 VSRP 模块输出的日志信息。

173.1 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：VSRP peer name.
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

174 VXLAN

本节介绍 VXLAN 模块输出的日志信息。

174.1 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

175 WAF

本节介绍 WAF 模块输出的系统日志和快速日志信息。

175.1 WAF_IPV4_INTERZONE（快速日志）

日志内容	Protocol(1001)=[STRING]; Application(1002)=[STRING]; SrcIPAddr(1003)=[IPADDR]; SrcPort(1004)=[UINT16]; DstIPAddr(1007)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1042)=[STRING]; SrcZoneName(1025)=[STRING]; DstZoneName(1035)=[STRING]; UserName(1113)=[STRING]; PolicyName(1079)=[STRING]; AttackName(1088)=[STRING]; AttackID(1089)=[UINT32]; Category(1090)=[STRING]; Protection(1091)=[STRING]; SubProtection(1092)=[STRING]; Severity(1087)=[STRING]; Action(1053)=[STRING]; CVE(1075)=[STRING]; BID(1076)=[STRING]; MSB(1077)=[STRING]; HitDirection(1115)=[STRING]; RealSrcIP(1100)=[STRING]; SubCategory(1124)=[STRING]; InspectEngine(1182)=[STRING]; CapturePktName(1116)=[STRING]; SrcMacAddr(1021)=[STRING]; DstMacAddr(1022)=[STRING]; SrcLocation(1209)=[STRING]; HttpHost(1117)=[STRING]; HttpUserAgent(1210)=[STRING]; URL(1093)=[STRING]; HttpMethod(1206)=[STRING]; StatusCode(1167)=[STRING]; PayLoad(1135)=[STRING]; HttpRequestHeader(1207)=[SRTING]; HttpBody(1208)=[STRING]; VlanID(1175)=[UINT32]; VNI(1213)=[UINT32]; DstLocation(1214)=[STRING];
参数解释	$1：协议类型 $2：应用协议名称 $3：源IP地址 $4：源端口号 $5：目的IP地址 $6：目的端口号 $7：源VPN名称 $8：源安全域名称 $9：目的安全域名称 $10：身份识别用户的名称 $11：策略名称 $12：威胁名称 $13：威胁ID $14：攻击分类 $15：保护对象 $16：保护子对象 $17：严重级别，包括如下取值： • INVALID：未指定 • LOW：低 • MEDIUM：中 • HIGH：高 • CRITICAL：严重 $18：动作名称，包括如下取值： • Block-Source：源阻断 • Drop：丢弃 • Reset：重置 • Permit：允许 • Redirect：重定向

日志内容	Protocol(1001)=[STRING]; Application(1002)=[STRING]; SrcIPAddr(1003)=[IPADDR]; SrcPort(1004)=[UINT16]; DstIPAddr(1007)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1042)=[STRING]; SrcZoneName(1025)=[STRING]; DstZoneName(1035)=[STRING]; UserName(1113)=[STRING]; PolicyName(1079)=[STRING]; AttackName(1088)=[STRING]; AttackID(1089)=[UINT32]; Category(1090)=[STRING]; Protection(1091)=[STRING]; SubProtection(1092)=[STRING]; Severity(1087)=[STRING]; Action(1053)=[STRING]; CVE(1075)=[STRING]; BID(1076)=[STRING]; MSB(1077)=[STRING]; HitDirection(1115)=[STRING]; RealSrcIP(1100)=[STRING]; SubCategory(1124)=[STRING]; InspectEngine(1182)=[STRING]; CapturePktName(1116)=[STRING]; SrcMacAddr(1021)=[STRING]; DstMacAddr(1022)=[STRING]; SrcLocation(1209)=[STRING]; HttpHost(1117)=[STRING]; HttpUserAgent(1210)=[STRING]; URL(1093)=[STRING]; HttpMethod(1206)=[STRING]; StatusCode(1167)=[STRING]; PayLoad(1135)=[STRING]; HttpRequestHeader(1207)=[SRTING]; HttpBody(1208)=[STRING]; VlanID(1175)=[UINT32]; VNI(1213)=[UINT32]; DstLocation(1214)=[STRING];
	• Capture：捕获 • Logging：生成日志 $19：CVE（公共漏洞和暴露编号） $20：BID（软件漏洞跟踪编号） $21：MSB（微软安全公告编号） $22：命中报文方向，包括如下取值： • original：请求方向 • reply：应答方向 $23：真实源IP地址 $24：攻击子分类 $25：检测引擎，包括如下取值： • signature-library：表示通过特征检测引擎检测出攻击 • semantic-analysis：表示通过语义分析引擎检测出攻击 $26：抓包名称 $27：源MAC地址 $28：目的MAC地址 $29：攻击地区 $30：请求的主机名 $31：用户代理信息（一般指客户端浏览器信息） $32：请求URL $33：请求方法 $34：响应状态码 $35：载荷信息 $36：请求头 $37：请求体 $38：Vlan ID $39：Vxlan ID $40：目的地区

日志内容	Protocol(1001)=[STRING]; Application(1002)=[STRING]; SrcIPAddr(1003)=[IPADDR]; SrcPort(1004)=[UINT16]; DstIPAddr(1007)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1042)=[STRING]; SrcZoneName(1025)=[STRING]; DstZoneName(1035)=[STRING]; UserName(1113)=[STRING]; PolicyName(1079)=[STRING]; AttackName(1088)=[STRING]; AttackID(1089)=[UINT32]; Category(1090)=[STRING]; Protection(1091)=[STRING]; SubProtection(1092)=[STRING]; Severity(1087)=[STRING]; Action(1053)=[STRING]; CVE(1075)=[STRING]; BID(1076)=[STRING]; MSB(1077)=[STRING]; HitDirection(1115)=[STRING]; RealSrcIP(1100)=[STRING]; SubCategory(1124)=[STRING]; InspectEngine(1182)=[STRING]; CapturePktName(1116)=[STRING]; SrcMacAddr(1021)=[STRING]; DstMacAddr(1022)=[STRING]; SrcLocation(1209)=[STRING]; HttpHost(1117)=[STRING]; HttpUserAgent(1210)=[STRING]; URL(1093)=[STRING]; HttpMethod(1206)=[STRING]; StatusCode(1167)=[STRING]; PayLoad(1135)=[STRING]; HttpRequestHeader(1207)=[SRTING]; HttpBody(1208)=[STRING]; VlanID(1175)=[UINT32]; VNI(1213)=[UINT32]; DstLocation(1214)=[STRING];
日志等级	4
举例	WAF/4/WAF_IPV4_INTERZONE:-Context=1; Protocol(1001)=TCP; Application(1002)=http; SrcIPAddr(1003)=100.10.10.40; SrcPort(1004)=2999; DstIPAddr(1007)=200.10.10.40; DstPort(1008)=80; RcvVPNInstance(1042)=; SrcZoneName(1025)=spf; DstZoneName(1035)=spf; UserName(1113)=abc; PolicyName(1079)=waf; AttackName(1088)=WEB_CLIENT_Windows_Media_ASF_File_Download_SET; AttackID(1089)=5707; Category(1090)=Other; Protection(1091)=Other; SubProtection(1092)=Other; Severity(1087)=CRITICAL; Action(1053)=Reset & Logging; CVE(1075)=CVE-2014-6277 | CVE-2014-6278; BID(1076)=BID-22559; MSB(1077)=MS10-017; HitDirection(1115)=original; RealSrcIP(1100)=10.10.10.10,20.20.20.20; SubCategory(1124)=Other; InspectEngine(1182)=signature-library; CapturePktName(1116)=; SrcMacAddr(1021)=dc2d-cb01-0000; DstMacAddr(1022)=dc2d-cb02-0000; SrcLocation(1209)=中国-河南-郑州 ; HttpHost(1117)=3.3.4.10; HttpUserAgent(1210)=Cricket-A310/1.0 UP.Browser/6.3.0.7 (GUI) MMP/2.0; URL(1093)=3.3.4.10/1download/Repro.dvr-ms; HttpMethod(1206)=GET ; StatusCode(1167)=HTTP/1.1 200 OK; PayLoad(1135)=POST/YWWboLftTVobA.xml HTTP/1.1\0d\0aHost: 3.3.4.10\0d\0aContent-Type: text/xml\0d\0aContent-Length; HttpRequestHeader(1207)=Host: 58.2.3.122User-Agent: Cricket-A310/1.0 UP.Browser/6.3.0.7 (GUI) MMP/2.0Accept: */*Connection: keep-aliveContent-Length: 9245; HttpBody(1208)=; VlanID(1175)=400;VNI(1213)=--; DstLocation(1214)=SaintKittsandNevis;
日志说明	当设备检测到IPv4报文中存在WAF攻击时输出该日志
处理建议	无

175.2 WAF_IPV6_INTERZONE（快速日志）

日志内容	Protocol(1001)=[STRING]; Application(1002)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; SrcPort(1004)=[UINT16]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1042)=-[STRING]; SrcZoneName(1025)=[STRING]; DstZoneName(1035)=[STRING]; UserName(1113)=[STRING]; PolicyName(1079)=[STRING]; AttackName(1088)=[STRING]; AttackID(1089)=[UINT32]; Category(1090)=[STRING]; Protection(1091)=[STRING]; SubProtection(1092)=[STRING]; Severity(1087)=[STRING]; Action(1053)=[STRING]; CVE(1075)=[STRING]; BID(1076)=[STRING]; MSB(1077)=[STRING]; HitDirection(1115)=[STRING]; RealSrcIP(1100)=[STRING]; SubCategory(1124)=[STRING]; InspectEngine(1182)=[STRING]; CapturePktName(1116)=[STRING]; SrcMacAddr(1021)=[STRING]; DstMacAddr(1022)=[STRING]; SrcLocation(1209)=[STRING]; HttpHost(1117)=[STRING]; HttpUserAgent(1210)=[STRING]; URL(1093)=[STRING]; HttpMethod(1206)=[STRING]; StatusCode(1167)=[STRING]; PayLoad(1135)=[STRING]; HttpRequestHeader(1207)=[SRTING]; HttpBody(1208)=[STRING]; VlanID(1175)=[UINT32]; VNI(1213)=[UINT32]; DstLocation(1214)=[STRING];
参数解释	$1：协议类型 $2：应用协议名称 $3：源IPv6地址 $4：源端口号 $5：目的IPv6地址 $6：目的端口号 $7：源VPN名称 $8：源安全域名称 $9：目的安全域名称 $10：身份识别用户的名称 $11：策略名称 $12：威胁名称 $13：威胁ID $14：攻击分类 $15：保护对象 $16：保护子对象 $17：严重级别，包括如下取值： • INVALID：未指定 • LOW：低 • MEDIUM：中 • HIGH：高 • CRITICAL：严重 $18：动作名称，包括如下取值： • Block-Source：源阻断 • Drop：丢弃 • Reset：重置 • Permit：允许 • Redirect：重定向

日志内容	Protocol(1001)=[STRING]; Application(1002)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; SrcPort(1004)=[UINT16]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1042)=-[STRING]; SrcZoneName(1025)=[STRING]; DstZoneName(1035)=[STRING]; UserName(1113)=[STRING]; PolicyName(1079)=[STRING]; AttackName(1088)=[STRING]; AttackID(1089)=[UINT32]; Category(1090)=[STRING]; Protection(1091)=[STRING]; SubProtection(1092)=[STRING]; Severity(1087)=[STRING]; Action(1053)=[STRING]; CVE(1075)=[STRING]; BID(1076)=[STRING]; MSB(1077)=[STRING]; HitDirection(1115)=[STRING]; RealSrcIP(1100)=[STRING]; SubCategory(1124)=[STRING]; InspectEngine(1182)=[STRING]; CapturePktName(1116)=[STRING]; SrcMacAddr(1021)=[STRING]; DstMacAddr(1022)=[STRING]; SrcLocation(1209)=[STRING]; HttpHost(1117)=[STRING]; HttpUserAgent(1210)=[STRING]; URL(1093)=[STRING]; HttpMethod(1206)=[STRING]; StatusCode(1167)=[STRING]; PayLoad(1135)=[STRING]; HttpRequestHeader(1207)=[SRTING]; HttpBody(1208)=[STRING]; VlanID(1175)=[UINT32]; VNI(1213)=[UINT32]; DstLocation(1214)=[STRING];
	• Capture：捕获 • Logging：生成日志 $19：CVE（公共漏洞和暴露编号） $20：BID（软件漏洞跟踪编号） $21：MSB（微软安全公告编号） $22：命中报文方向，包括如下取值： • original：请求方向 • reply：应答方向 $23：真实源IP地址 $24：攻击子分类 $25：检测引擎，包括如下取值： • signature-library：表示通过特征检测引擎检测出攻击 • semantic-analysis：表示通过语义分析引擎检测出攻击 $26：抓包名称 $27：源MAC地址 $28：目的MAC地址 $29：攻击地区 $30：请求的主机名 $31：用户代理信息（一般指客户端浏览器信息） $32：请求URL $33：请求方法 $34：响应状态码 $35：载荷信息 $36：请求头 $37：请求体 $38：Vlan ID $39：Vxlan ID $40：目的地区

日志内容	Protocol(1001)=[STRING]; Application(1002)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; SrcPort(1004)=[UINT16]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1042)=-[STRING]; SrcZoneName(1025)=[STRING]; DstZoneName(1035)=[STRING]; UserName(1113)=[STRING]; PolicyName(1079)=[STRING]; AttackName(1088)=[STRING]; AttackID(1089)=[UINT32]; Category(1090)=[STRING]; Protection(1091)=[STRING]; SubProtection(1092)=[STRING]; Severity(1087)=[STRING]; Action(1053)=[STRING]; CVE(1075)=[STRING]; BID(1076)=[STRING]; MSB(1077)=[STRING]; HitDirection(1115)=[STRING]; RealSrcIP(1100)=[STRING]; SubCategory(1124)=[STRING]; InspectEngine(1182)=[STRING]; CapturePktName(1116)=[STRING]; SrcMacAddr(1021)=[STRING]; DstMacAddr(1022)=[STRING]; SrcLocation(1209)=[STRING]; HttpHost(1117)=[STRING]; HttpUserAgent(1210)=[STRING]; URL(1093)=[STRING]; HttpMethod(1206)=[STRING]; StatusCode(1167)=[STRING]; PayLoad(1135)=[STRING]; HttpRequestHeader(1207)=[SRTING]; HttpBody(1208)=[STRING]; VlanID(1175)=[UINT32]; VNI(1213)=[UINT32]; DstLocation(1214)=[STRING];
日志等级	4
举例	WAF/4/WAF_IPV6_INTERZONE:-Context=1; Protocol(1001)=TCP; Application(1002)=http; SrcIPv6Addr(1036)=100::40; SrcPort(1004)=2999; DstIPv6Addr(1037)=200::40; DstPort(1008)=80; RcvVPNInstance(1042)=; SrcZoneName(1025)=spf; DstZoneName(1035)=spf; UserName(1113)=aaa; PolicyName(1079)=waf; AttackName(1088)=WEB_CLIENT_Windows_Media_ASF_File_Download_SET; AttackID(1089)=5707; Category(1090)=Other; Protection(1091)=Other; SubProtection(1092)=Other; Severity(1087)=CRITICAL; Action(1053)=Reset & Logging; CVE(1075)=CVE-2014-6277 | CVE-2014-6278; BID(1076)=BID-22559; MSB(1077)=MS10-017; HitDirection(1115)=reply; RealSrcIP(1100)=10::1; SubCategory(1124)=Other; InspectEngine(1182)=semantic-analysis; CapturePktName(1116)=; SrcMacAddr(1021)=dc2d-cb01-0000; DstMacAddr(1022)=dc2d-cb02-0000; SrcLocation(1209)=中国-河南-郑州； HttpHost(1117)=3.3.4.10; HttpUserAgent(1210)=Cricket-A310/1.0 UP.Browser/6.3.0.7 (GUI) MMP/2.0; URL(1093)=3.3.4.10/1download/Repro.dvr-ms; HttpMethod(1206)=GET ; StatusCode(1167)=HTTP/1.1 200 OK; PayLoad(1135)=POST/YWWboLftTVobA.xml HTTP/1.1\0d\0aHost: 3.3.4.10\0d\0aContent-Type: text/xml\0d\0aContent-Length; HttpRequestHeader(1207)=Host: 58.2.3.122User-Agent: Cricket-A310/1.0 UP.Browser/6.3.0.7 (GUI) MMP/2.0Accept: */*Connection: keep-aliveContent-Length: 9245; HttpBody(1208)=; VlanID(1175)=400;VNI(1213)=--; DstLocation(1214)=SaintKittsandNevis;
日志说明	当设备检测到IPv6报文中存在WAF攻击时输出该日志
处理建议	无

175.3 WAF_WARNING（系统日志）

日志内容	Updated the WAF signature library successfully.
参数解释	无
日志等级	4
举例	WAF/4/WAF_WARNING: -Context=1; Updated the WAF signature library successfully.
日志说明	Web应用防护特征库升级成功，包含如下情况： • 立即升级成功 • 本地升级成功
处理建议	无

175.4 WAF_WARNING（系统日志）

日志内容	Rolled back the WAF signature library successfully.
参数解释	无
日志等级	4
举例	WAF/4/WAF_WARNING: -Context=1; Rolled back the WAF signature library successfully.
日志说明	Web应用防护特征库回滚成功，包含如下情况： • 回滚到上一个版本成功 • 回滚到出厂版本成功
处理建议	无

175.5 WAF_WARNING（系统日志）

日志内容	Failed to update the WAF signature library.
参数解释	无
日志等级	4
举例	WAF/4/WAF_WARNING: -Context=1; Failed to update the WAF signature library.
日志说明	Web应用防护特征库升级失败。包含如下情况： • 立即升级失败 • 本地升级失败（仅在使用 Web 方式进行升级时提示） • 定时升级失败
处理建议	无

175.6 WAF_WARNING（系统日志）

日志内容	Copy SigPack file failed because flash is not enough.
参数解释	无
日志等级	4
举例	WAF/4/WAF_WARNING: -Context=1; Copy SigPack file failed because flash is not enough.
日志说明	Flash存储空间不足，Web应用防护特征库升级失败
处理建议	无

175.7 WAF_WARNING（系统日志）

日志内容	Failed to update signature package in phase [STRING].
参数解释	$1：升级阶段，包括如下取值： • DOWNLOAD：下载特征库阶段 • GETURLFILE：获取特征库文件下载路径阶段 • PREPARE：特征库准备阶段 • PARSE：特征库解析阶段 • UNKNOWN：未知
日志等级	4
举例	WAF/4/WAF_WARNING: -Context=1; Failed to update signature package in phase PARSE.
日志说明	特征库升级失败时，提示用户失败发生在特征库升级的某个阶段
处理建议	无

176 WEB

本节介绍 WEB 模块输出的中文普通日志信息。

176.1 LOGIN

日志内容	[STRING] 从 [STRING] 登录成功.
参数解释	$1：用户名称 $2：用户IP地址
日志等级	5
举例	WEB/5/LOGIN: admin 从 127.0.0.1 登录成功.
日志说明	用户登录成功
处理建议	无

176.2 LOGIN_FAILED

日志内容	[STRING] 从 [STRING] 登录失败.
参数解释	$1：用户名称 $2：用户IP地址
日志等级	5
举例	WEB/5/LOGIN_FAILED: admin 从 127.0.0.1 登录失败.
日志说明	用户登录失败，可能的原因包括： • 设备上的 HTTP 或者 HTTPS 服务未开启 • 用户没有 HTTP 或者 HTTPS 服务的权限 • 用户不存在 • 密码校验失败 • 验证码错误 • 在线用户达到上限
处理建议	• 确保设备上的 HTTP 或者 HTTPS 服务处于开启状态 • 确保该用户具有 HTTP 或者 HTTPS 类型的接入权限 • 重新输入正确的用户名、密码、验证码 • 确保为该账户设置的最大在线用户数能够满足实际接入需求 • 其它问题，请联系技术支持人员

176.3 LOGOUT

日志内容	[STRING] 从 [STRING] 退出登录.
参数解释	$1：用户名称 $2：用户IP地址
日志等级	5
举例	WEB/5/LOGOUT: admin 从 127.0.0.1退出登录.
日志说明	用户退出登录
处理建议	无

177 WEB

本节介绍 WEB 模块输出的普通日志信息。

177.1 LOGIN

日志内容	[STRING] logged in from [STRING].
参数解释	$1：用户名称 $2：用户IP地址
日志等级	5
举例	WEB/5/LOGIN: admin logged in from 127.0.0.1.
日志说明	用户登录成功
处理建议	无

177.2 LOGIN_FAILED

日志内容	[STRING] failed to log in from [STRING].
参数解释	$1：用户名称 $2：用户IP地址
日志等级	5
举例	WEB/5/LOGIN_FAILED: admin failed to log in from 127.0.0.1.
日志说明	用户登录失败
处理建议	无

177.3 LOGOUT

日志内容	[STRING] logged out from [STRING].
参数解释	$1：用户名称 $2：用户IP地址
日志等级	5
举例	WEB/5/LOGOUT: admin logged out from 127.0.0.1.
日志说明	用户退出登录
处理建议	无

178 WEBCACHE

本节介绍 Web Cache 模块输出的日志信息。

178.1 WEBCACHE_CHECK

日志内容	Web caching is not available.Reason: The system is checking whether the Web cache directory is accessible. Please wait...
参数解释	无
日志等级	4
举例	WEBCACHE/4/WEBCACHE_CHECK Web caching is not available. Reason: The system is checking whether the Web cache directory is accessible. Please wait...
日志说明	正在检查Web Cache工作路径是否可访问，此时Web Cache功能不可使用
处理建议	等待检查完毕

178.2 WEBCACHE_AVAILABLE

日志内容	Web cache directory is accessible. Web caching is available now.
参数解释	无
日志等级	6
举例	WEBCACHE/6/WEBCACHE_AVAILABLE: Web cache directory is accessible. Web caching is available now.
日志说明	Web Cache工作路径可访问，Web Cache功能可用
处理建议	无

178.3 WEBCACHE_INAVAILABLE

日志内容	Web caching is not available. Reason: The Web cache directory is not accessible.
参数解释	无
日志等级	6
举例	WEBCACHE/6/WEBCACHE_INAVAILABLE: Web caching is not available. Reason: The Web cache directory is not accessible.
日志说明	Web Cache工作路径不可访问，Web Cache功能暂时不可用
处理建议	使用**file-directory**命令重新配置正确的Web Cache工作路径

179 WFF

本节介绍 WFF（WLAN Fast Forwarding）模块输出的日志信息。

179.1 WFF_HARDWARE_INIT_FAILED

日志内容	Firmware [UINT32] was set to pass-through mode because initialization failed.
参数解释	$1：固件编号
日志等级	5
举例	WFF/5/WFF_HARDWARE_INIT_FAILED: Firmware 0 was set to pass-through mode because initialization failed.
日志说明	固件初始化失败后，将固件设置为工作在透传模式
处理建议	无

179.2 WFF_HARDWARE_IPC_FAILED

日志内容	Firmware [UINT32] was set to pass-through mode because IPC check failed.
参数解释	$1：固件编号
日志等级	5
举例	WFF/5/WFF_HARDWARE_IPC_FAILED: Firmware 0 was set to pass-through mode because IPC check failed.
日志说明	IPC模块监控发现错误，将固件设置为工作在透传模式
处理建议	无

179.3 WFF_HARDWARE_LOOPBACK_FAILED

日志内容	Firmware [UINT32] was set to pass-through mode because loopback check failed.
参数解释	$1：固件编号
日志等级	5
举例	WFF/5/WFF_HARDWARE_LOOPBACK_FAILED: Firmware 0 was set to pass-through mode because loopback check failed.
日志说明	端口环回监控发现错误，将固件设置为工作在透传模式
处理建议	无

179.4 WFF_HARDWARE_PCIE_FAILED

日志内容	Firmware [UINT32] was set to pass-through mode because PCIE check failed.
参数解释	$1：固件编号
日志等级	5
举例	WFF/5/WFF_HARDWARE_LOOPBACK_FAILED: Firmware 0 was set to pass-through mode because PCIE check failed.
日志说明	PCIE监控发现错误，将固件设置为工作在透传模式
处理建议	无

180 WIPS

本节介绍 WIPS 模块输出的日志信息。

180.1 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

180.2 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=dc2d-cb44-5566; 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

180.3 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=dc2d-cb44-5566; 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

180.4 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=dc2d-cb44-5566; 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

180.5 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=dc2d-cb44-5566; 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

180.6 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=dc2d-cb44-5566; 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

180.7 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

180.8 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=dc2d-cb44-5566; 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

180.9 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=dc2d-cb44-5566; 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

180.10 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=dc2d-cb44-5566; 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

180.11 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=dc2d-cb44-5566; 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

180.12 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=dc2d-cb44-5566; 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

180.13 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=dc2d-cb44-5566; 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

180.14 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=DC2D-CB44-5566-AP2=DC2D-CB66-5544; 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

181 WLANAUD

本节介绍 WLANAUD 模块输出的日志信息。

181.1 WLANAUD_CLIENT_ONLINE

日志内容	• UserIP=[STRING], UserMAC=[STRING], APMAC=[STRING]. • UserMAC=[STRING], UserIP=[STRING], APName=[STRING], APMAC=[STRING], SSID=[STRING], BSSID=[STRING].
参数解释	$1：客户端的IP地址 $2：客户端的MAC地址 $3：客户端上线的AP的MAC地址 $4：客户端上线的AP名称 $5：客户端上线的SSID $6：客户端上线的BSSID
日志等级	5
举例	• WLANAUD/5/WLAN_CLIENT_ONLINE: UserIP=192.168.0.1, UserMAC=DC2D-CB33-2147, APMAC=DC2D-CBEA-17FF. • WLANAUD/5/WLAN_CLIENT_ONLINE: UserMAC=31ac-11ea-17ff, UserIP=192.168.0.1, APName=ap1,, APMAC=dc2d-cb00-3350, SSID=zhongyan, BSSID=dc2d-cb00-3352.
日志说明	客户端上线
处理建议	无

182 WMESH

本节介绍 WMESH 模块输出的日志信息。

182.1 MESH_ACTIVELINK_SWITCH

日志内容	Switch an active link from [MAC] ([CHAR]) to [MAC] ([CHAR]): peer quantity = [UINT64], link quantity = [UINT16], switch reason = [UINT32].
参数解释	$1：切换前的邻居MAC $2：切换前链路RSSI $3：切换后的邻居MAC $4：切换后链路RSSI $5：切换后邻居的数量 $6：切换后链路的数量 $7：切换原因，包括以下取值： • 1：表示首个 Mesh 链路建立 • 2：表示主动切换（未开启移动链路优化功能） • 3：表示主动切换（已开启移动链路优化功能） • 4：表示被动切换或强制断开后切换
日志等级	5
举例	WMESH/5/MESH_ACTIVELINK_SWITCH: Switch an active link from dc2d-cbd2-4b50 (55) to dc2d-cbd2-49e0 (74): peer quantity = 3, link quantity = 2, switch reason = 2.
日志说明	活跃链路切换
处理建议	无

182.2 MESH_LINKDOWN

日志内容	Mesh link on interface [CHAR] is down: peer MAC = [MAC], RSSI = [CHAR], reason: [STRING] ([STRING]).
参数解释	$1：链路接口编号 $2：邻居MAC $3：链路RSSI $4：断开原因，包括以下取值： • AP status change：AP 状态改变 • Radio status change：射频工作状态或工作参数变化 • Mesh configuration change：Mesh 配置变化，例如 Mesh Profile、Mesh 策略等 • Mesh BSS deleted：BSS 删除 • Excessive RSSI：RSSI 超过链路饱和值 • Weak RSSI：链路的 RSSI 过低 • Packet check failure：报文检查失败 • Link keepalive failure：链路保活失败 • Active link keepalive failure：MLSP 环境下，主链路保活失败 • Worst link replaced when MLSP link limit is reached：MLSP 功能的 MESH 链路数达上限后，差链路被替换 • Neighbor zerocfg status change：临时链路的邻居由零配置状态变为非零配置状态 • Neighbor refresh：临时链路的邻居需要重新发现 • Mesh link established during scan initialization or auto channel scan：非零配置自动信道扫描期间（或扫描初始化期间）建立了链路 • Unknown reason：其他原因 $5：链路断开起源，包括以下取值： • local：本端 • peer：对端
日志等级	5
举例	WMESH/5/MESH_LINKDOWN: Mesh link on interface 50 is down: peer MAC = dc2d-cbd2-4b50, RSSI = 45, reason: AP status change (peer).
日志说明	Mesh链路断开
处理建议	无

182.3 MESH_LINKUP

日志内容	Mesh link on interface [CHAR] is up: peer MAC = [MAC], peer radio mode = [UINT32], RSSI = [CHAR].
参数解释	$1：链路接口编号 $2：邻居MAC $3：邻居射频模式，包括以下取值： • 0：表示除了 11n、11ac 的模式 • 1：表示 11n 模式 • 2：表示 11ac 模式 $4：链路RSSI
日志等级	5
举例	WMESH/5/MESH_LINKUP: Mesh link on interface 51 is up: peer MAC =dc2d-cbd2-4b50, peer radio mode = 0, RSSI = 74.
日志说明	Mesh链路创建
处理建议	无

182.4 MESH_REVOPEN_MAC

日志内容	Received a link open request from AP [MAC] in confirm received state.
参数解释	$1：发送Link Open报文的AP的MAC地址
日志等级	5
举例	WMESH/5/MESH_REVOPEN_MAC: Received a link open request from AP dc2d-cbd2-4b50 in confirm received state.
日志说明	当前AP在Confirm received状态下收到该邻居AP的Link Open报文
处理建议	无

183 WRDC

本节介绍 WRDC 模块输出的日志信息。

183.1 WRDC_USER_DELETE

日志内容	-UserMAC=[STRING]-UserIP=[IPADDR]. A user was deleted.
参数解释	$1：用户MAC地址 $2：用户IP地址
日志等级	6
举例	WRDC/6/WRDC_USER_DELETE: -UserMAC=dc2d-cb11-0033-UserIP=192.168.1.2. A user was deleted.
日志说明	用户在所有AC下线后，WLAN漫游中心将用户信息删除
处理建议	无

183.2 WRDC_USER_OFFLINE

日志内容	-UserMAC=[STRING]-UserIP=[IPADDR]-ACIP =[IPADDR]; A user went offline. Reason: [STRING].
参数解释	$1：用户MAC地址 $2：用户IP地址 $3：用户所在接入设备的IP地址 $3：用户下线原因，包括： o User request：用户请求下线 o DHCP release：用户 IP 地址租约到期 o Other reason：其他原因
日志等级	6
举例	WRDC/6/WRDC_USER_OFFLINE: -UserMAC=dc2d-cb11-0033-UserIP=192.168.1.2-ACIP=192.168.3.1; A user went offline. Reason: User request.
日志说明	用户下线
处理建议	无

183.3 WRDC_USER_ONLINE

日志内容	-UserMAC=[STRING]-UserIP=[IPADDR]-ACIP=[IPADDR]. A user came online.
参数解释	$1：用户MAC地址 $2：用户IP地址 $3：用户所在接入设备的IP地址
日志等级	6
举例	WRDC/6/WRDC_USER_ONLINE: -UserMAC=dc2d-cb11-0033-UserIP=192.168.1.2-ACIP=192.168.3.1. A user came online.
日志说明	用户上线
处理建议	无

183.4 WRDC_USER_ROAM

日志内容	-UserMAC=[STRING]-UserIP=[IPADDR]. A user roamed from AC [IPADDR] to AC [IPADDR].
参数解释	$1：用户MAC地址 $2：用户IP地址 $3：用户漫游前所在接入设备的IP地址 $4：用户漫游后所在接入设备的IP地址
日志等级	6
举例	WRDC/6/WRDC_USER_ROAM: -UserMAC=dc2d-cb11-0033-UserIP=192.168.1.2. A user roamed from AC 192.168.3.1 to AC 192.168.3.2.
日志说明	用户发生漫游
处理建议	无

184 WSA

本节介绍 WSA 模块输出的日志信息。

184.1 WSA_DEVICE

日志内容	[APID: UINT32, RADIOID: UCHAR]; [STRING] detected.
参数解释	$1：AP ID $2：Radio ID $3：干扰设备类型 o Microwave ovens：微波炉 o Microwave oven inverters：新式微波炉 o Bluetooth devices：蓝牙 o Other fixed frequency devices：其他固定频率设备 o Cordless phones using fixed frequency：固定频率无绳电话 o Video devices using fixed frequency：固定频率视频传输设备 o Audio devices using fixed frequency：固定频率音频设备 o Other hopper frequency devices：其他跳频设备 o Frequency-hopping cordless phone bases：跳频无绳电话基站 o Frequency-hopping cordless networks (2.4GHz)：跳频无绳电话网(2.4GHz) o Microsoft Xboxes：微软 Xbox o Other devices：其他设备 o Frequency-hopping cordless networks (5GHz)：跳频无绳电话(5GHz)
日志等级	5
举例	WSA/5/WSA_DEVICE: [APID: 1, RADIODID: 2]; Bluetooth devices detected
日志说明	AP的Radio接口下检测到干扰设备
处理建议	检查设备是否受到攻击