

# UNIS S12600X-G 日志信息参考

资料版本：6W100-20210820

产品版本：R7743P04 及以上版本

---

Copyright © 2021 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

<b>1 简介</b> .....	<b>1</b>
1.1 日志格式说明.....	1
1.2 如何获取日志信息 .....	3
1.2.1 通过控制台获取日志 .....	3
1.2.2 通过监视终端获取日志 .....	3
1.2.3 通过日志缓冲区获取日志 .....	3
1.2.4 通过日志文件获取日志 .....	4
1.2.5 通过日志主机获取日志 .....	4
1.3 软件模块列表.....	4
1.4 文档使用说明.....	9
<b>2 AAA</b> .....	<b>9</b>
2.1 AAA_FAILURE .....	10
2.2 AAA_LAUNCH .....	10
2.3 AAA_SUCCESS.....	11
<b>3 ACL</b> .....	<b>11</b>
3.1 ACL_ACCELERATE_NO_RES .....	11
3.2 ACL_ACCELERATE_NONCONTIGUOUSMASK .....	12
3.3 ACL_ACCELERATE_NOT_SUPPORT .....	12
3.4 ACL_ACCELERATE_NOT_SUPPORTHOPBYHOP .....	12
3.5 ACL_ACCELERATE_NOT_SUPPORTMULTITCPFLAG .....	13
3.6 ACL_ACCELERATE_UNK_ERR.....	13
3.7 ACL_IPV6_STATIS_INFO .....	13
3.8 ACL_NO_MEM .....	14
3.9 ACL_STATIS_INFO.....	14
<b>4 ANCP</b> .....	<b>14</b>
4.1 ANCP_INVALID_PACKET.....	15
<b>5 APMGR</b> .....	<b>15</b>
5.1 APMGR_AC_MEM_ALERT.....	15
5.2 APMGR_ADD_AP_FAIL .....	16
5.3 APMGR_ADDBAC_INFO .....	16
5.4 APMGR_AP_OFFLINE .....	16
5.5 APMGR_AP_ONLINE.....	17

5.6 APMGR_CWC_IMG_DOWNLOAD_COMPLETE .....	17
5.7 APMGR_CWC_IMG_DOWNLOAD_START .....	17
5.8 APMGR_CWC_IMG_NO_ENOUGH_SPACE .....	18
5.9 APMGR_CWC_LOCAL_AC_DOWN .....	18
5.10 APMGR_CWC_LOCAL_AC_UP .....	19
5.11 APMGR_CWC_REBOOT .....	19
5.12 APMGR_CWC_RUN_DOWNLOAD_COMPLETE .....	19
5.13 APMGR_CWC_RUN_DOWNLOAD_START .....	20
5.14 APMGR_CWC_RUN_NO_ENOUGH_SPACE .....	20
5.15 APMGR_CWC_TUNNEL_DOWN .....	21
5.16 APMGR_CWC_TUNNEL_UP .....	21
5.17 APMGR_CWS_IMG_DOWNLOAD_COMPLETE .....	22
5.18 APMGR_CWS_IMG_DOWNLOAD_START .....	22
5.19 APMGR_CWS_LOCAL_AC_DOWN .....	23
5.20 APMGR_CWS_LOCAL_AC_UP .....	23
5.21 APMGR_CWS_RUN_DOWNLOAD_COMPLETE .....	24
5.22 APMGR_CWS_RUN_DOWNLOAD_START .....	24
5.23 APMGR_CWS_TUNNEL_DOWN .....	25
5.24 APMGR_CWS_TUNNEL_UP .....	25
5.25 APMGR_DELBAC_INFO .....	26
5.26 APMGR_LOCAL_AC_OFFLINE .....	26
5.27 APMGR_LOCAL_AC_ONLINE .....	26
<b>6 ARP .....</b>	<b>26</b>
6.1 ARP_ACTIVE_ACK_NO_REPLY .....	27
6.2 ARP_ACTIVE_ACK_NOREQUESTED_REPLY .....	27
6.3 ARP_BINDRULETOHW_FAILED .....	28
6.4 ARP_DETECTION_LOG .....	28
6.5 ARP_DUPLICATE_IPADDR_DETECT .....	29
6.6 ARP_DYNAMIC .....	29
6.7 ARP_DYNAMIC_IF .....	30
6.8 ARP_DYNAMIC_SLOT .....	30
6.9 ARP_ENTRY_CONFLICT .....	31
6.10 ARP_ENTRY_ENOUGHRESOURCE .....	31
6.11 ARP_ENTRY_INCONSISTENT .....	32
6.12 ARP_ENTRY_NORESOURCE .....	33
6.13 ARP_HOST_IP_CONFLICT .....	33

6.14 ARP_LOCALPROXY_ENABLE_FAILED .....	34
6.15 ARP_PKTQUE_ALERT .....	34
6.16 ARP_RATE_EXCEEDED .....	34
6.17 ARP_RATELIMIT_NOTSUPPORT .....	35
6.18 ARP_SENDER_IP_INVALID .....	35
6.19 ARP_SENDER_MAC_INVALID.....	36
6.20 ARP_SENDER_SMACCONFLICT .....	36
6.21 ARP_SENDER_SMACCONFLICT_VSI .....	37
6.22 ARP_SRC_MAC_FOUND_ATTACK.....	37
6.23 ARP_SUP_ENABLE_FAILED .....	38
6.24 ARP_TARGET_IP_INVALID.....	38
6.25 ARP_THRESHOLD_REACHED.....	38
6.26 ARP_USER_DUPLICATE_IPADDR_DETECT .....	39
6.27 ARP_USER_MOVE_DETECT.....	40
6.28 DUPIFIP .....	40
6.29 DUPIP .....	41
6.30 DUPVRRPIP .....	41
<b>7 ATK.....</b>	<b>41</b>
7.1 ATK_ICMP_ADDRMASK_REQ.....	42
7.2 ATK_ICMP_ADDRMASK_REQ_RAW .....	43
7.3 ATK_ICMP_ADDRMASK_REQ_RAW_SZ.....	43
7.4 ATK_ICMP_ADDRMASK_REQ_SZ .....	44
7.5 ATK_ICMP_ADDRMASK_RPL.....	45
7.6 ATK_ICMP_ADDRMASK_RPL_RAW .....	46
7.7 ATK_ICMP_ADDRMASK_RPL_RAW_SZ .....	46
7.8 ATK_ICMP_ADDRMASK_RPL_SZ.....	47
7.9 ATK_ICMP_ECHO_REQ.....	48
7.10 ATK_ICMP_ECHO_REQ_RAW .....	49
7.11 ATK_ICMP_ECHO_REQ_RAW_SZ.....	50
7.12 ATK_ICMP_ECHO_REQ_SZ .....	51
7.13 ATK_ICMP_ECHO_RPL.....	52
7.14 ATK_ICMP_ECHO_RPL_RAW .....	53
7.15 ATK_ICMP_ECHO_RPL_RAW_SZ.....	53
7.16 ATK_ICMP_ECHO_RPL_SZ .....	54
7.17 ATK_ICMP_FLOOD.....	54
7.18 ATK_ICMP_FLOOD_SZ .....	55

7.19 ATK_ICMP_INFO_REQ.....	55
7.20 ATK_ICMP_INFO_REQ_RAW .....	56
7.21 ATK_ICMP_INFO_REQ_RAW_SZ.....	56
7.22 ATK_ICMP_INFO_REQ_SZ.....	57
7.23 ATK_ICMP_INFO_RPL .....	58
7.24 ATK_ICMP_INFO_RPL_RAW .....	59
7.25 ATK_ICMP_INFO_RPL_RAW_SZ .....	59
7.26 ATK_ICMP_INFO_RPL_SZ.....	60
7.27 ATK_ICMP_LARGE.....	61
7.28 ATK_ICMP_LARGE_RAW .....	61
7.29 ATK_ICMP_LARGE_RAW_SZ.....	62
7.30 ATK_ICMP_LARGE_SZ .....	62
7.31 ATK_ICMP_PARAPROBLEM.....	63
7.32 ATK_ICMP_PARAPROBLEM_RAW .....	64
7.33 ATK_ICMP_PARAPROBLEM_RAW_SZ.....	64
7.34 ATK_ICMP_PARAPROBLEM_SZ.....	65
7.35 ATK_ICMP_PINGOFDEATH.....	66
7.36 ATK_ICMP_PINGOFDEATH_RAW.....	67
7.37 ATK_ICMP_PINGOFDEATH_RAW_SZ.....	67
7.38 ATK_ICMP_PINGOFDEATH_SZ .....	68
7.39 ATK_ICMP_REDIRECT.....	69
7.40 ATK_ICMP_REDIRECT_RAW .....	70
7.41 ATK_ICMP_REDIRECT_RAW_SZ.....	70
7.42 ATK_ICMP_REDIRECT_SZ.....	71
7.43 ATK_ICMP_SMURF .....	72
7.44 ATK_ICMP_SMURF_RAW.....	73
7.45 ATK_ICMP_SMURF_RAW_SZ .....	73
7.46 ATK_ICMP_SMURF_SZ.....	74
7.47 ATK_ICMP_SOURCEQUENCH.....	75
7.48 ATK_ICMP_SOURCEQUENCH_RAW.....	76
7.49 ATK_ICMP_SOURCEQUENCH_RAW_SZ.....	76
7.50 ATK_ICMP_SOURCEQUENCH_SZ .....	77
7.51 ATK_ICMP_TIMEEXCEED.....	78
7.52 ATK_ICMP_TIMEEXCEED_RAW .....	79
7.53 ATK_ICMP_TIMEEXCEED_RAW_SZ.....	79
7.54 ATK_ICMP_TIMEEXCEED_SZ.....	80

7.55 ATK_ICMP_TRACEROUTE .....	81
7.56 ATK_ICMP_TRACEROUTE_RAW.....	81
7.57 ATK_ICMP_TRACEROUTE_RAW_SZ.....	82
7.58 ATK_ICMP_TRACEROUTE_SZ.....	82
7.59 ATK_ICMP_TSTAMP_REQ.....	83
7.60 ATK_ICMP_TSTAMP_REQ_RAW .....	84
7.61 ATK_ICMP_TSTAMP_REQ_RAW_SZ.....	84
7.62 ATK_ICMP_TSTAMP_REQ_SZ.....	85
7.63 ATK_ICMP_TSTAMP_RPL .....	86
7.64 ATK_ICMP_TSTAMP_RPL_RAW.....	87
7.65 ATK_ICMP_TSTAMP_RPL_RAW_SZ .....	87
7.66 ATK_ICMP_TSTAMP_RPL_SZ.....	88
7.67 ATK_ICMP_TYPE.....	89
7.68 ATK_ICMP_TYPE_RAW .....	90
7.69 ATK_ICMP_TYPE_RAW_SZ.....	90
7.70 ATK_ICMP_TYPE_SZ .....	91
7.71 ATK_ICMP_UNREACHABLE .....	92
7.72 ATK_ICMP_UNREACHABLE_RAW.....	93
7.73 ATK_ICMP_UNREACHABLE_RAW_SZ.....	93
7.74 ATK_ICMP_UNREACHABLE_SZ .....	94
7.75 ATK_ICMPV6_DEST_UNREACH .....	95
7.76 ATK_ICMPV6_DEST_UNREACH_RAW.....	95
7.77 ATK_ICMPV6_DEST_UNREACH_RAW_SZ.....	96
7.78 ATK_ICMPV6_DEST_UNREACH_SZ.....	96
7.79 ATK_ICMPV6_ECHO_REQ .....	97
7.80 ATK_ICMPV6_ECHO_REQ_RAW.....	97
7.81 ATK_ICMPV6_ECHO_REQ_RAW_SZ .....	98
7.82 ATK_ICMPV6_ECHO_REQ_SZ.....	98
7.83 ATK_ICMPV6_ECHO_RPL .....	99
7.84 ATK_ICMPV6_ECHO_RPL_RAW.....	99
7.85 ATK_ICMPV6_ECHO_RPL_RAW_SZ.....	100
7.86 ATK_ICMPV6_ECHO_RPL_SZ.....	100
7.87 ATK_ICMPV6_FLOOD .....	101
7.88 ATK_ICMPV6_FLOOD_SZ.....	101
7.89 ATK_ICMPV6_GROUPQUERY.....	102
7.90 ATK_ICMPV6_GROUPQUERY_RAW .....	102

7.91 ATK_ICMPV6_GROUPQUERY_RAW_SZ .....	103
7.92 ATK_ICMPV6_GROUPQUERY_SZ .....	103
7.93 ATK_ICMPV6_GROUPREDUCTION .....	104
7.94 ATK_ICMPV6_GROUPREDUCTION_RAW .....	104
7.95 ATK_ICMPV6_GROUPREDUCTION_RAW_SZ .....	105
7.96 ATK_ICMPV6_GROUPREDUCTION_SZ .....	105
7.97 ATK_ICMPV6_GROUPREPORT .....	106
7.98 ATK_ICMPV6_GROUPREPORT_RAW .....	106
7.99 ATK_ICMPV6_GROUPREPORT_RAW_SZ .....	107
7.100 ATK_ICMPV6_GROUPREPORT_SZ .....	107
7.101 ATK_ICMPV6_LARGE .....	108
7.102 ATK_ICMPV6_LARGE_RAW .....	108
7.103 ATK_ICMPV6_LARGE_RAW_SZ .....	109
7.104 ATK_ICMPV6_LARGE_SZ .....	109
7.105 ATK_ICMPV6_PACKETTOOBIG .....	110
7.106 ATK_ICMPV6_PACKETTOOBIG_RAW .....	110
7.107 ATK_ICMPV6_PACKETTOOBIG_RAW_SZ .....	111
7.108 ATK_ICMPV6_PACKETTOOBIG_SZ .....	111
7.109 ATK_ICMPV6_PARAPROBLEM .....	112
7.110 ATK_ICMPV6_PARAPROBLEM_RAW .....	112
7.111 ATK_ICMPV6_PARAPROBLEM_RAW_SZ .....	113
7.112 ATK_ICMPV6_PARAPROBLEM_SZ .....	113
7.113 ATK_ICMPV6_TIMEEXCEED .....	114
7.114 ATK_ICMPV6_TIMEEXCEED_RAW .....	114
7.115 ATK_ICMPV6_TIMEEXCEED_RAW_SZ .....	115
7.116 ATK_ICMPV6_TIMEEXCEED_SZ .....	115
7.117 ATK_ICMPV6_TRACEROUTE .....	116
7.118 ATK_ICMPV6_TRACEROUTE_RAW .....	117
7.119 ATK_ICMPV6_TRACEROUTE_RAW_SZ .....	118
7.120 ATK_ICMPV6_TRACEROUTE_SZ .....	119
7.121 ATK_ICMPV6_TYPE .....	120
7.122 ATK_ICMPV6_TYPE_RAW .....	120
7.123 ATK_ICMPV6_TYPE_RAW_SZ .....	121
7.124 ATK_ICMPV6_TYPE_SZ .....	121
7.125 ATK_IP_OPTION .....	122
7.126 ATK_IP_OPTION_RAW .....	123

7.127	ATK_IP_OPTION_RAW_SZ	123
7.128	ATK_IP_OPTION_SZ	124
7.129	ATK_IP4_ACK_FLOOD	125
7.130	ATK_IP4_ACK_FLOOD_SZ	125
7.131	ATK_IP4_DIS_PORTSCAN	126
7.132	ATK_IP4_DIS_PORTSCAN_SZ	126
7.133	ATK_IP4_DNS_FLOOD	127
7.134	ATK_IP4_DNS_FLOOD_SZ	127
7.135	ATK_IP4_FIN_FLOOD	128
7.136	ATK_IP4_FIN_FLOOD_SZ	128
7.137	ATK_IP4_FRAGMENT	129
7.138	ATK_IP4_FRAGMENT_RAW	130
7.139	ATK_IP4_FRAGMENT_RAW_SZ	130
7.140	ATK_IP4_FRAGMENT_SZ	131
7.141	ATK_IP4_HTTP_FLOOD	131
7.142	ATK_IP4_HTTP_FLOOD_SZ	132
7.143	ATK_IP4_IMPOSSIBLE	133
7.144	ATK_IP4_IMPOSSIBLE_RAW	134
7.145	ATK_IP4_IMPOSSIBLE_RAW_SZ	134
7.146	ATK_IP4_IMPOSSIBLE_SZ	135
7.147	ATK_IP4_IPSWEEP	136
7.148	ATK_IP4_IPSWEEP_SZ	136
7.149	ATK_IP4_PORTSCAN	137
7.150	ATK_IP4_PORTSCAN_SZ	137
7.151	ATK_IP4_RST_FLOOD	138
7.152	ATK_IP4_RST_FLOOD_SZ	138
7.153	ATK_IP4_SYN_FLOOD	139
7.154	ATK_IP4_SYN_FLOOD_SZ	139
7.155	ATK_IP4_SYNACK_FLOOD	140
7.156	ATK_IP4_SYNACK_FLOOD_SZ	140
7.157	ATK_IP4_TCP_ALLFLAGS	141
7.158	ATK_IP4_TCP_ALLFLAGS_RAW	141
7.159	ATK_IP4_TCP_ALLFLAGS_RAW_SZ	142
7.160	ATK_IP4_TCP_ALLFLAGS_SZ	142
7.161	ATK_IP4_TCP_FINONLY	143
7.162	ATK_IP4_TCP_FINONLY_RAW	143



7.163	ATK_IP4_TCP_FINONLY_RAW_SZ	144
7.164	ATK_IP4_TCP_FINONLY_SZ	144
7.165	ATK_IP4_TCP_INVALIDFLAGS	145
7.166	ATK_IP4_TCP_INVALIDFLAGS_RAW	146
7.167	ATK_IP4_TCP_INVALIDFLAGS_RAW_SZ	146
7.168	ATK_IP4_TCP_INVALIDFLAGS_SZ	147
7.169	ATK_IP4_TCP_LAND	148
7.170	ATK_IP4_TCP_LAND_RAW	148
7.171	ATK_IP4_TCP_LAND_RAW_SZ	149
7.172	ATK_IP4_TCP_LAND_SZ	149
7.173	ATK_IP4_TCP_NULLFLAG	150
7.174	ATK_IP4_TCP_NULLFLAG_RAW	150
7.175	ATK_IP4_TCP_NULLFLAG_RAW_SZ	151
7.176	ATK_IP4_TCP_NULLFLAG_SZ	151
7.177	ATK_IP4_TCP_SYNFIN	152
7.178	ATK_IP4_TCP_SYNFIN_RAW	152
7.179	ATK_IP4_TCP_SYNFIN_RAW_SZ	153
7.180	ATK_IP4_TCP_SYNFIN_SZ	153
7.181	ATK_IP4_TCP_WINNUKE	154
7.182	ATK_IP4_TCP_WINNUKE_RAW	155
7.183	ATK_IP4_TCP_WINNUKE_RAW_SZ	155
7.184	ATK_IP4_TCP_WINNUKE_SZ	156
7.185	ATK_IP4_TEARDROP	157
7.186	ATK_IP4_TEARDROP_RAW	158
7.187	ATK_IP4_TEARDROP_RAW_SZ	158
7.188	ATK_IP4_TEARDROP_SZ	159
7.189	ATK_IP4_TINY_FRAGMENT	160
7.190	ATK_IP4_TINY_FRAGMENT_RAW	161
7.191	ATK_IP4_TINY_FRAGMENT_RAW_SZ	161
7.192	ATK_IP4_TINY_FRAGMENT_SZ	162
7.193	ATK_IP4_UDP_BOMB	163
7.194	ATK_IP4_UDP_BOMB_RAW	163
7.195	ATK_IP4_UDP_BOMB_RAW_SZ	164
7.196	ATK_IP4_UDP_BOMB_SZ	164
7.197	ATK_IP4_UDP_FLOOD	165
7.198	ATK_IP4_UDP_FLOOD_SZ	165

7.199	ATK_IP4_UDP_FRAGGLE.....	166
7.200	ATK_IP4_UDP_FRAGGLE_RAW .....	166
7.201	ATK_IP4_UDP_FRAGGLE_RAW_SZ.....	167
7.202	ATK_IP4_UDP_FRAGGLE_SZ .....	167
7.203	ATK_IP4_UDP_SNORK .....	168
7.204	ATK_IP4_UDP_SNORK_RAW.....	169
7.205	ATK_IP4_UDP_SNORK_RAW_SZ.....	169
7.206	ATK_IP4_UDP_SNORK_SZ.....	170
7.207	ATK_IP6_ACK_FLOOD.....	170
7.208	ATK_IP6_ACK_FLOOD_SZ .....	171
7.209	ATK_IP6_DIS_PORTSCAN.....	171
7.210	ATK_IP6_DIS_PORTSCAN_SZ.....	172
7.211	ATK_IP6_DNS_FLOOD.....	172
7.212	ATK_IP6_DNS_FLOOD_SZ.....	173
7.213	ATK_IP6_FIN_FLOOD .....	173
7.214	ATK_IP6_FIN_FLOOD_SZ.....	174
7.215	ATK_IP6_FRAGMENT .....	174
7.216	ATK_IP6_FRAGMENT_RAW .....	175
7.217	ATK_IP6_FRAGMENT_RAW_SZ .....	175
7.218	ATK_IP6_FRAGMENT_SZ.....	176
7.219	ATK_IP6_HTTP_FLOOD.....	176
7.220	ATK_IP6_HTTP_FLOOD_SZ .....	177
7.221	ATK_IP6_IMPOSSIBLE.....	177
7.222	ATK_IP6_IMPOSSIBLE_RAW .....	178
7.223	ATK_IP6_IMPOSSIBLE_RAW_SZ.....	178
7.224	ATK_IP6_IMPOSSIBLE_SZ .....	179
7.225	ATK_IP6_IPSWEEP .....	179
7.226	ATK_IP6_IPSWEEP_SZ.....	180
7.227	ATK_IP6_PORTSCAN.....	180
7.228	ATK_IP6_PORTSCAN_SZ.....	181
7.229	ATK_IP6_RST_FLOOD.....	181
7.230	ATK_IP6_RST_FLOOD_SZ .....	182
7.231	ATK_IP6_SYN_FLOOD.....	182
7.232	ATK_IP6_SYN_FLOOD_SZ .....	183
7.233	ATK_IP6_SYNACK_FLOOD .....	183
7.234	ATK_IP6_SYNACK_FLOOD_SZ.....	184

7.235	ATK_IP6_TCP_ALLFLAGS .....	184
7.236	ATK_IP6_TCP_ALLFLAGS_RAW.....	185
7.237	ATK_IP6_TCP_ALLFLAGS_RAW_SZ .....	185
7.238	ATK_IP6_TCP_ALLFLAGS_SZ.....	186
7.239	ATK_IP6_TCP_FINONLY.....	187
7.240	ATK_IP6_TCP_FINONLY_RAW .....	187
7.241	ATK_IP6_TCP_FINONLY_RAW_SZ.....	188
7.242	ATK_IP6_TCP_FINONLY_SZ .....	188
7.243	ATK_IP6_TCP_INVALIDFLAGS.....	189
7.244	ATK_IP6_TCP_INVALIDFLAGS_RAW .....	190
7.245	ATK_IP6_TCP_INVALIDFLAGS_RAW_SZ .....	190
7.246	ATK_IP6_TCP_INVALIDFLAGS_SZ .....	191
7.247	ATK_IP6_TCP_LAND.....	192
7.248	ATK_IP6_TCP_LAND_RAW .....	192
7.249	ATK_IP6_TCP_LAND_RAW_SZ.....	193
7.250	ATK_IP6_TCP_LAND_SZ .....	193
7.251	ATK_IP6_TCP_NULLFLAG.....	194
7.252	ATK_IP6_TCP_NULLFLAG_RAW .....	194
7.253	ATK_IP6_TCP_NULLFLAG_RAW_SZ.....	195
7.254	ATK_IP6_TCP_NULLFLAG_SZ .....	195
7.255	ATK_IP6_TCP_SYNFIN .....	196
7.256	ATK_IP6_TCP_SYNFIN_RAW.....	196
7.257	ATK_IP6_TCP_SYNFIN_RAW_SZ.....	197
7.258	ATK_IP6_TCP_SYNFIN_SZ.....	197
7.259	ATK_IP6_TCP_WINNUKE .....	198
7.260	ATK_IP6_TCP_WINNUKE_RAW.....	198
7.261	ATK_IP6_TCP_WINNUKE_RAW_SZ .....	199
7.262	ATK_IP6_TCP_WINNUKE_SZ.....	199
7.263	ATK_IP6_UDP_FLOOD.....	200
7.264	ATK_IP6_UDP_FLOOD_SZ.....	200
7.265	ATK_IP6_UDP_FRAGGLE.....	201
7.266	ATK_IP6_UDP_FRAGGLE_RAW .....	201
7.267	ATK_IP6_UDP_FRAGGLE_RAW_SZ.....	202
7.268	ATK_IP6_UDP_FRAGGLE_SZ .....	202
7.269	ATK_IP6_UDP_SNORK .....	203
7.270	ATK_IP6_UDP_SNORK_RAW.....	203

7.271	ATK_IP6_UDP_SNORK_RAW_SZ	204
7.272	ATK_IP6_UDP_SNORK_SZ	204
7.273	ATK_IPOPT_ABNORMAL	205
7.274	ATK_IPOPT_ABNORMAL_RAW	206
7.275	ATK_IPOPT_ABNORMAL_RAW_SZ	206
7.276	ATK_IPOPT_ABNORMAL_SZ	207
7.277	ATK_IPOPT_LOOSESRCROUTE	208
7.278	ATK_IPOPT_LOOSESRCROUTE_RAW	209
7.279	ATK_IPOPT_LOOSESRCROUTE_RAW_SZ	210
7.280	ATK_IPOPT_LOOSESRCROUTE_SZ	211
7.281	ATK_IPOPT_RECORDROUTE	212
7.282	ATK_IPOPT_RECORDROUTE_RAW	213
7.283	ATK_IPOPT_RECORDROUTE_RAW_SZ	214
7.284	ATK_IPOPT_RECORDROUTE_SZ	215
7.285	ATK_IPOPT_ROUTEALERT	216
7.286	ATK_IPOPT_ROUTEALERT_RAW	217
7.287	ATK_IPOPT_ROUTEALERT_RAW_SZ	218
7.288	ATK_IPOPT_ROUTEALERT_SZ	219
7.289	ATK_IPOPT_SECURITY	220
7.290	ATK_IPOPT_SECURITY_RAW	221
7.291	ATK_IPOPT_SECURITY_RAW_SZ	222
7.292	ATK_IPOPT_SECURITY_SZ	223
7.293	ATK_IPOPT_STREAMID	224
7.294	ATK_IPOPT_STREAMID_RAW	225
7.295	ATK_IPOPT_STREAMID_RAW_SZ	226
7.296	ATK_IPOPT_STREAMID_SZ	227
7.297	ATK_IPOPT_STRICTSRCROUTE	228
7.298	ATK_IPOPT_STRICTSRCROUTE_RAW	229
7.299	ATK_IPOPT_STRICTSRCROUTE_RAW_SZ	230
7.300	ATK_IPOPT_STRICTSRCROUTE_SZ	231
7.301	ATK_IPOPT_TIMESTAMP	232
7.302	ATK_IPOPT_TIMESTAMP_RAW	233
7.303	ATK_IPOPT_TIMESTAMP_RAW_SZ	234
7.304	ATK_IPOPT_TIMESTAMP_SZ	235
7.305	ATK_IPV6_EXT_HEADER	236
7.306	ATK_IPV6_EXT_HEADER_RAW	236

7.307 ATK_IPV6_EXT_HEADER_RAW_SZ .....	237
7.308 ATK_IPV6_EXT_HEADER_SZ .....	237
<b>8 ATM .....</b>	<b>238</b>
8.1 ATM_PVCDOWN .....	238
8.2 ATM_PVCUP .....	239
<b>9 BFD .....</b>	<b>239</b>
9.1 BFD_CHANGE_FSM .....	239
9.2 BFD_REACHED_UPPER_LIMIT .....	240
<b>10 BGP .....</b>	<b>240</b>
10.1 BGP_EXCEED_ROUTE_LIMIT .....	240
10.2 BGP_REACHED_THRESHOLD .....	241
10.3 BGP_LOG_ROUTE_FLAP .....	241
10.4 BGP_MEM_ALERT .....	242
10.5 BGP_PEER_LICENSE_REACHED .....	242
10.6 BGP_ROUTE_LICENSE_REACHED .....	242
10.7 BGP_STATE_CHANGED .....	243
10.8 BGP_STATE_CHANGED_REASON .....	243
<b>11 BLS .....</b>	<b>243</b>
11.1 BLS_ENTRY_ADD .....	244
11.2 BLS_ENTRY_DEL .....	244
11.3 BLS_IPV6_ENTRY_ADD .....	245
11.4 BLS_IPV6_ENTRY_DEL .....	245
<b>12 CFD .....</b>	<b>245</b>
12.1 CFD_CROSS_CCM .....	246
12.2 CFD_ERROR_CCM .....	246
12.3 CFD_LOST_CCM .....	247
12.4 CFD_RECEIVE_CCM .....	247
<b>13 CFGMAN .....</b>	<b>247</b>
13.1 CFGMAN_ARCHIVE_SCP_FAIL .....	248
13.2 CFGMAN_CFGCHANGED .....	249
13.3 CFGMAN_EXIT_FROM_CONFIGURE .....	250
13.4 CFGMAN_OPTCOMPLETION .....	251
13.5 CFG_SAVE_FAILED .....	252
13.6 CFG_SET_NEXTCFG_FAILED .....	253

<b>14 CONNLMT</b> .....	<b>253</b>
14.1 CONNLMT_IPV4_OVERLOAD .....	254
14.2 CONNLMT_IPV4_RECOVER .....	255
14.3 CONNLMT_IPV6_OVERLOAD .....	256
14.4 CONNLMT_IPV6_RECOVER .....	257
<b>15 DEV</b> .....	<b>257</b>
15.1 AUTOSWITCH_FAULT .....	258
15.2 AUTOSWITCH_FAULT_REBOOT .....	258
15.3 BOARD_INSERTED .....	258
15.4 BOARD_REBOOT .....	259
15.5 BOARD_REMOVED .....	259
15.6 BOARD_RUNNING_FAULT .....	260
15.7 BOARD_RUNNING_FAULT_REBOOT .....	260
15.8 BOARD_STATE_FAULT .....	261
15.9 BOARD_STATE_NORMAL .....	261
15.10 BOARD_STATE_STARTING .....	262
15.11 CFCARD_INSERTED .....	262
15.12 CFCARD_REMOVED .....	262
15.13 CHASSIS_REBOOT .....	263
15.14 DEV_CLOCK_CHANGE .....	263
15.15 DEV_FAULT_TOOLONG .....	263
15.16 FAN_ABSENT .....	264
15.17 FAN_DIRECTION_NOT_PREFERRED .....	264
15.18 FAN_FAILED .....	265
15.19 FAN_RECOVERED .....	265
15.20 MAD_DETECT .....	266
15.21 MAD_PROC .....	266
15.22 POWER_ABSENT .....	267
15.23 POWER_FAILED .....	267
15.24 POWER_MONITOR_ABSENT .....	268
15.25 POWER_MONITOR_FAILED .....	268
15.26 POWER_MONITOR_RECOVERED .....	269
15.27 POWER_RECOVERED .....	269
15.28 RPS_ABSENT .....	270
15.29 RPS_FAILED .....	270
15.30 RPS_NORMAL .....	271

15.31 SUBCARD_FAULT .....	271
15.32 SUBCARD_INSERTED .....	272
15.33 SUBCARD_REBOOT .....	272
15.34 SUBCARD_REMOVED .....	272
15.35 SYSTEM_REBOOT .....	273
15.36 TEMPERATURE_ALARM .....	274
15.37 TEMPERATURE_LOW.....	275
15.38 TEMPERATURE_NORMAL .....	276
15.39 TEMPERATURE_SHUTDOWN.....	277
15.40 TEMPERATURE_WARNING .....	278
15.41 TIMER_CREATE_FAILED_FIRST .....	279
15.42 TIMER_CREATE_FAILED_MORE.....	279
15.43 VCHK_VERSION_INCOMPATIBLE .....	280
<b>16 DHCP.....</b>	<b>280</b>
16.1 DHCP_NORESOURCES.....	280
16.2 DHCP_NOTSUPPORTED.....	280
<b>17 DHCPR .....</b>	<b>281</b>
17.1 DHCPR_SERVERCHANGE .....	281
17.2 DHCPR_SWITCHMASTER .....	281
<b>18 DHCPS .....</b>	<b>281</b>
18.1 DHCPS_ALLOCATE_IP .....	282
18.2 DHCPS_CONFLICT_IP .....	282
18.3 DHCPS_EXTEND_IP .....	283
18.4 DHCPS_FILE .....	283
18.5 DHCPS_RECLAIM_IP .....	284
18.6 DHCPS_VERIFY_CLASS.....	284
<b>19 DHCPS6 .....</b>	<b>284</b>
19.1 DHCPS6_ALLOCATE_ADDRESS .....	285
19.2 DHCPS6_ALLOCATE_PREFIX.....	285
19.3 DHCPS6_CONFLICT_ADDRESS.....	286
19.4 DHCPS6_EXTEND_ADDRESS .....	286
19.5 DHCPS6_EXTEND_PREFIX.....	287
19.6 DHCPS6_FILE .....	287
19.7 DHCPS6_RECLAIM_ADDRESS.....	288
19.8 DHCPS6_RECLAIM_PREFIX .....	288

<b>20 DHCPSP4</b> .....	<b>288</b>
20.1 DHCPSP4_FILE.....	289
20.2 DHCPSP4_UNTRUSTED_SERVER.....	289
<b>21 DHCPSP6</b> .....	<b>289</b>
21.1 DHCPSP6_FILE.....	290
<b>22 DIAG</b> .....	<b>290</b>
22.1 CPU_MINOR_RECOVERY.....	290
22.2 CPU_MINOR_THRESHOLD.....	291
22.3 CPU_SEVERE_RECOVERY.....	292
22.4 CPU_SEVERE_THRESHOLD.....	293
22.5 CPU_USAGE_LASTMINUTE.....	294
22.6 DIAG_FD_UPLIMIT_REACHED.....	295
22.7 DIAG_FD_UPLIMIT_TO_REACH.....	295
22.8 MEM_ALERT.....	296
22.9 MEM_BELOW_THRESHOLD.....	297
22.10 MEM_EXCEED_THRESHOLD.....	297
22.11 MEM_USAGE.....	298
<b>23 DLDP</b> .....	<b>298</b>
23.1 DLDP_AUTHENTICATION_FAILED.....	298
23.2 DLDP_LINK_BIDIRECTIONAL.....	298
23.3 DLDP_LINK_SHUTMODECHG.....	299
23.4 DLDP_LINK_UNIDIRECTIONAL.....	299
23.5 DLDP_NEIGHBOR_AGED.....	300
23.6 DLDP_NEIGHBOR_CONFIRMED.....	300
23.7 DLDP_NEIGHBOR_DELETED.....	301
<b>24 DOT1X</b> .....	<b>301</b>
24.1 DOT1X_CONFIG_NOTSUPPORT.....	301
24.2 DOT1X_LOGIN_FAILURE.....	302
24.3 DOT1X_LOGIN_SUCC.....	302
24.4 DOT1X_LOGIN_SUCC (in open mode).....	303
24.5 DOT1X_LOGOFF.....	303
24.6 DOT1X_LOGOFF (in open mode).....	304
24.7 DOT1X_LOGOFF_ABNORMAL.....	305
24.8 DOT1X_LOGOFF_ABNORMAL (in open mode).....	306
24.9 DOT1X_MACBINDING_EXIST.....	307
24.10 DOT1X_NOTENOUGH_EADFREEIP_RES.....	307



24.11 DOT1X_NOTENOUGH_EADFREEMSEG_RES .....	308
24.12 DOT1X_NOTENOUGH_EADFREERULE_RES .....	308
24.13 DOT1X_NOTENOUGH_EADMACREDIR_RES .....	308
24.14 DOT1X_NOTENOUGH_EADPORTREDIR_RES .....	309
24.15 DOT1X_NOTENOUGH_ENABLEDOT1X_RES .....	309
24.16 DOT1X_PEXAGG_NOMEMBER_RES .....	309
24.17 DOT1X_SMARTON_FAILURE .....	310
24.18 DOT1X_UNICAST_NOT_EFFECTIVE .....	310
<b>25 DRNI .....</b>	<b>310</b>
25.1 DRNI_AUTORECOVERY_TIMEOUT .....	311
25.2 DRNI_GLBHECK_CONSISTENCY .....	311
25.3 DRNI_GLBHECK_INCONSISTENCY .....	312
25.4 DRNI_IFCHECK_CONSISTENCY .....	312
25.5 DRNI_IFCHECK_INCONSISTENCY .....	313
25.6 DRNI_IFEVENT_DR_BIND .....	313
25.7 DRNI_IFEVENT_DR_GLOBALDOWN .....	313
25.8 DRNI_IFEVENT_DR_GLOBALUP .....	314
25.9 DRNI_IFEVENT_DR_MAC_CHANGE .....	314
25.10 DRNI_IFEVENT_DR_NOSELECTED .....	315
25.11 DRNI_IFEVENT_DR_PEERBIND .....	315
25.12 DRNI_IFEVENT_DR_PEERUNBIND .....	316
25.13 DRNI_IFEVENT_DR_PEER_NOSELECTED .....	316
25.14 DRNI_IFEVENT_DR_PEER_SELECTED .....	316
25.15 DRNI_IFEVENT_DR_PRIORITY_CHANGE .....	317
25.16 DRNI_IFEVENT_DR_SELECTED .....	317
25.17 DRNI_IFEVENT_DR_UNBIND .....	317
25.18 DRNI_IFEVENT_IPP_BIND .....	318
25.19 DRNI_IFEVENT_IPP_DOWN .....	318
25.20 DRNI_IFEVENT_IPP_UNBIND .....	319
25.21 DRNI_IFEVENT_IPP_UP .....	319
25.22 DRNI_IPP_BLOCK .....	319
25.23 DRNI_IPP_UNBLOCK .....	320
25.24 DRNI_KEEPAIVEINTERVAL_MISMATCH .....	320
25.25 DRNI_KEEPAIVELINK_DOWN .....	321
25.26 DRNI_KEEPAIVELINK_UP .....	321
25.27 DRNI_DEVICE_MADDOWN .....	322

25.28 DRNI_DEVICE_MADRECOVERY.....	322
25.29 DRNI_SYSEVENT_DEVICEROLE_CHANGE .....	323
25.30 DRNI_SYSEVENT_MAC_CHANGE.....	323
25.31 DRNI_SYSEVENT_MODE_CHANGE.....	324
25.32 DRNI_SYSEVENT_NUMBER_CHANGE.....	324
25.33 DRNI_SYSEVENT_PRIORITY_CHANGE .....	324
25.34 DRNI_VMAC_INEFFECTIVE .....	325
<b>26 DRVPLAT .....</b>	<b>325</b>
26.1 DRVPLAT.....	325
26.1.1 DRVPLAT/4/DrvDebug.....	325
26.1.2 DRVPLAT/4/DrvDebug.....	326
26.2 DRVDEBUGMOD_BSP .....	326
26.2.1 DRVPLAT/3/DrvDebug.....	326
26.2.2 DRVPLAT/3/DrvDebug.....	327
26.2.3 DRVPLAT/3/DrvDebug.....	327
26.2.4 DRVPLAT/3/DrvDebug.....	327
26.2.5 DRVPLAT/3/DrvDebug.....	328
26.2.6 DRVPLAT/3/DrvDebug.....	328
26.2.7 DRVPLAT/3/DrvDebug.....	328
26.2.8 DRVPLAT/3/DrvDebug.....	329
26.2.9 DRVPLAT/3/DrvDebug.....	329
26.2.10 DRVPLAT/3/DrvDebug.....	329
26.2.11 DRVPLAT/3/DrvDebug.....	330
26.2.12 DRVPLAT/3/DrvDebug.....	330
26.2.13 DRVPLAT/3/DrvDebug.....	330
26.3 DRVDEBUGMOD_DEVM.....	331
26.3.1 DRVPLAT/2/DrvDebug.....	331
26.3.2 DRVPLAT/2/DrvDebug.....	331
26.3.3 DRVPLAT/2/DrvDebug.....	331
26.3.4 DRVPLAT/2/DrvDebug.....	332
26.3.5 DRVPLAT/2/DrvDebug.....	332
26.3.6 DRVPLAT/2/DrvDebug.....	333
26.3.7 DRVPLAT/2/DrvDebug.....	333
26.3.8 DRVPLAT/4/DrvDebug.....	333
26.4 DRVDEBUGMOD_GOLD .....	334
26.4.1 DRVPLAT/2/DrvDebug.....	334

26.4.2	DRVPLAT/2/DrvDebug	334
26.4.3	DRVPLAT/2/DrvDebug	335
26.4.4	DRVPLAT/4/DrvDebug	335
26.4.5	DRVPLAT/4/DrvDebug	335
26.4.6	DRVPLAT/4/DrvDebug	336
26.4.7	DRVPLAT/4/DrvDebug	336
26.4.8	DRVPLAT/4/DrvDebug	336
26.4.9	DRVPLAT/4/DrvDebug	337
26.4.10	DRVPLAT/4/DrvDebug	337
26.4.11	DRVPLAT/4/DrvDebug	337
26.4.12	DRVPLAT/4/DrvDebug	338
26.5	DRVDEBUGMOD_L3	338
26.5.1	DRVPLAT/4/DrvDebug	338
26.5.2	DRVPLAT/4/DrvDebug	338
26.5.3	DRVPLAT/4/DrvDebug	339
26.5.4	DRVPLAT/4/DrvDebug	339
26.5.5	DRVPLAT/4/DrvDebug	339
26.6	DRVDEBUGMOD_PORT	340
26.6.1	DRVPLAT/4/DrvDebug	340
26.6.2	DRVPLAT/4/DrvDebug	340
26.7	DRVDEBUGMOD_POWERFAN	341
26.7.1	DRVPLAT/2/DrvDebug	341
26.7.2	DRVPLAT/2/DrvDebug	341
26.7.3	DRVPLAT/2/DrvDebug	342
26.7.4	DRVPLAT/2/DrvDebug	342
26.7.5	DRVPLAT/2/DrvDebug	343
26.7.6	DRVPLAT/2/DrvDebug	343
26.7.7	DRVPLAT/2/DrvDebug	344
26.7.8	DRVPLAT/2/DrvDebug	344
26.7.9	DRVPLAT/2/DrvDebug	344
26.7.10	DRVPLAT/2/DrvDebug	345
26.7.11	DRVPLAT/2/DrvDebug	345
26.7.12	DRVPLAT/2/DrvDebug	346
26.7.13	DRVPLAT/2/DrvDebug	346
26.7.14	DRVPLAT/2/DrvDebug	347
26.7.15	DRVPLAT/2/DrvDebug	347

26.7.16	DRVPLAT/2/DrvDebug	347
26.7.17	DRVPLAT/2/DrvDebug	348
26.7.18	DRVPLAT/2/DrvDebug	348
26.7.19	DRVPLAT/2/DrvDebug	348
26.7.20	DRVPLAT/2/DrvDebug	349
26.7.21	DRVPLAT/2/DrvDebug	349
26.7.22	DRVPLAT/2/DrvDebug	349
26.7.23	DRVPLAT/2/DrvDebug	350
26.7.24	DRVPLAT/2/DrvDebug	350
26.8	DRVDEBUGMOD_QACL	350
26.8.1	DRVPLAT/4/DrvDebug	350
26.8.2	DRVPLAT/4/DrvDebug	351
26.9	DRVDEBUGMOD_STACK	351
26.9.1	DRVPLAT/2/DrvDebug	351
26.9.2	DRVPLAT/2/DrvDebug	352
26.9.3	DRVPLAT/2/DrvDebug	352
26.9.4	DRVPLAT/4/DrvDebug	353
26.9.5	DRVPLAT/4/DrvDebug	353
26.9.6	DRVPLAT/4/DrvDebug	354
26.9.7	DRVPLAT/4/DrvDebug	354
26.9.8	DRVPLAT/4/DrvDebug	354
26.9.9	DRVPLAT/4/DrvDebug	355
26.9.10	DRVPLAT/4/DrvDebug	355
26.9.11	DRVPLAT/4/DrvDebug	356
26.9.12	DRVPLAT/4/DrvDebug	357
26.9.13	DRVPLAT/4/DrvDebug	357
26.9.14	DRVPLAT/4/DrvDebug	357
26.9.15	DRVPLAT/4/DrvDebug	358
26.9.16	DRVPLAT/4/DrvDebug	358
26.10	DRVDEBUGMOD_SWFA	358
26.10.1	DRVPLAT/4/DrvDebug	358
26.10.2	DRVPLAT/4/DrvDebug	359
26.10.3	DRVPLAT/4/DrvDebug	359
26.11	DRVDEBUGMOD_SYSM	360
26.11.1	DRVPLAT/4/DrvDebug	360
26.11.2	DRVPLAT/4/DrvDebug	360

26.11.3	DRVPLAT/4/DrvDebug	360
26.11.4	DRVPLAT/4/DrvDebug	361
26.11.5	DRVPLAT/4/DrvDebug	361
26.11.6	DRVPLAT/4/DrvDebug	362
26.11.7	DRVPLAT/4/DrvDebug	362
26.11.8	DRVPLAT/2/DrvDebug	363
26.11.9	DRVPLAT/4/DrvDebug	363
26.12	DRVDEBUGMOD_VLAN	364
26.12.1	DRVPLAT/4/DrvDebug	364
<b>27</b>	<b>EDEV</b>	<b>364</b>
27.1	ALARM_IN_REMOVED	364
27.2	ALARM_IN_REPORTED	364
27.3	EDEV_BOOTROM_UPDATE_FAILED	365
27.4	EDEV_BOOTROM_UPDATE_SUCCESS	365
27.5	EDEV_FAILOVER_GROUP_STATE_CHANGE	365
<b>28</b>	<b>eMDI</b>	<b>366</b>
28.1	EMDI_INDICATOR_OVER_THRES	366
28.2	EMDI_INDICATOR_OVER_THRES_RESUME	367
28.3	EMDI_INSTANCE_CONFLICT_FLOW	367
28.4	EMDI_INSTANCE_EXCEED	368
28.5	EMDI_INSTANCE_SAME_FLOW	368
<b>29</b>	<b>EPA</b>	<b>368</b>
29.1	EPA_ENDPOINT_ONLINE	369
29.2	EPA_ENDPOINT_OFFLINE	369
29.3	EPA_DEVICETYPE_CHANGE	370
<b>30</b>	<b>ERPS</b>	<b>370</b>
30.1	ERPS_IPP_CHECK	370
30.2	ERPS_STATE_CHANGED	371
<b>31</b>	<b>ETH</b>	<b>371</b>
31.1	ETH_SET_MAC_FAILED	371
<b>32</b>	<b>ETHDRNI</b>	<b>371</b>
32.1	ETHDRNI_MAC_INEFFECTIVE	372
<b>33</b>	<b>ETHOAM</b>	<b>372</b>
33.1	ETHOAM_CONNECTION_FAIL_DOWN	372
33.2	ETHOAM_CONNECTION_FAIL_TIMEOUT	372

33.3	ETHOAM_CONNECTION_FAIL_UNSATISF	373
33.4	ETHOAM_CONNECTION_SUCCEED	373
33.5	ETHOAM_DISABLE	373
33.6	ETHOAM_DISCOVERY_EXIT	374
33.7	ETHOAM_ENABLE	374
33.8	ETHOAM_ENTER_LOOPBACK_CTRLLED	374
33.9	ETHOAM_ENTER_LOOPBACK_CTRLING	375
33.10	ETHOAM_LOCAL_DYING_GASP	375
33.11	ETHOAM_LOCAL_ERROR_FRAME	375
33.12	ETHOAM_LOCAL_ERROR_FRAME_PERIOD	376
33.13	ETHOAM_LOCAL_ERROR_FRAME_SECOND	376
33.14	ETHOAM_LOCAL_ERROR_SYMBOL	376
33.15	ETHOAM_LOCAL_LINK_FAULT	377
33.16	ETHOAM_LOOPBACK_EXIT	377
33.17	ETHOAM_LOOPBACK_EXIT_ERROR_STATU	377
33.18	ETHOAM_LOOPBACK_NO_RESOURCE	378
33.19	ETHOAM_LOOPBACK_NOT_SUPPORT	378
33.20	ETHOAM_NO_ENOUGH_RESOURCE	378
33.21	ETHOAM_NOT_CONNECTION_TIMEOUT	379
33.22	ETHOAM_QUIT_LOOPBACK_CTRLLED	379
33.23	ETHOAM_QUIT_LOOPBACK_CTRLING	379
33.24	ETHOAM_REMOTE_CRITICAL	380
33.25	ETHOAM_REMOTE_DYING_GASP	380
33.26	ETHOAM_REMOTE_ERROR_FRAME	380
33.27	ETHOAM_REMOTE_ERROR_FRAME_PERIOD	381
33.28	ETHOAM_REMOTE_ERROR_FRAME_SECOND	381
33.29	ETHOAM_REMOTE_ERROR_SYMBOL	381
33.30	ETHOAM_REMOTE_EXIT	382
33.31	ETHOAM_REMOTE_FAILURE_RECOVER	382
33.32	ETHOAM_REMOTE_LINK_FAULT	382
<b>34</b>	<b>EVB</b>	<b>382</b>
34.1	EVB_AGG_FAILED	383
34.2	EVB_LICENSE_EXPIRE	383
34.3	EVB_VSI_OFFLINE	383
34.4	EVB_VSI_ONLINE	384

<b>35 EVIISIS</b> .....	<b>384</b>
35.1 EVIISIS_LICENSE_EXPIRED .....	384
35.2 EVIISIS_LICENSE_EXPIRED_TIME .....	385
35.3 EVIISIS_LICENSE_UNAVAILABLE .....	385
35.4 EVIISIS_NBR_CHG .....	386
<b>36 FCLINK</b> .....	<b>386</b>
36.1 FCLINK_FDISC_REJECT_NORESOURCE .....	386
36.2 FCLINK_FLOGI_REJECT_NORESOURCE .....	387
<b>37 FCOE</b> .....	<b>387</b>
37.1 FCOE__LAGG_BIND_ACTIVE .....	387
37.2 FCOE__LAGG_BIND_DEACTIVE .....	388
37.3 FCOE_INTERFACE_NOTSUPPORT_FCOE .....	388
<b>38 FCZONE</b> .....	<b>388</b>
38.1 FCZONE_DISTRIBUTE_FAILED .....	389
38.2 FCZONE_HARDZONE_DISABLED .....	389
38.3 FCZONE_HARDZONE_ENABLED .....	390
38.4 FCZONE_ISOLATE_ALLNEIGHBOR .....	390
38.5 FCZONE_ISOLATE_CLEAR_ALLVSAN .....	390
38.6 FCZONE_ISOLATE_CLEAR_VSAN .....	391
38.7 FCZONE_ISOLATE_NEIGHBOR .....	391
<b>39 FGROU</b> P .....	<b>391</b>
39.1 FLOWGROUP_APPLY_FAIL .....	392
39.2 FLOWGROUP_MODIFY_FAIL .....	392
<b>40 FIB</b> .....	<b>392</b>
40.1 FIB_FILE .....	393
40.2 FIB_PREFIX_ENOUGHRESOURCE .....	393
40.3 FIB_PREFIX_INCONSISTENT .....	394
40.4 FIB_PREFIX_NORESOURCE .....	395
40.5 FIB_VN_ENOUGHRESOURCE .....	395
40.6 FIB_VN_INCONSISTENT .....	396
40.7 FIB_VN_NORESOURCE .....	397
<b>41 FILTER</b> .....	<b>397</b>
41.1 FILTER_EXECUTION_ICMP .....	398
41.2 FILTER_EXECUTION_ICMPV6 .....	399
41.3 FILTER_IPV4_EXECUTION .....	400

41.4 FILTER_IPV6_EXECUTION.....	401
<b>42 FIPSNG.....</b>	<b>401</b>
42.1 FIPSNG_HARD_RESOURCE_NOENOUGH.....	401
42.2 FIPSNG_HARD_RESOURCE_RESTORE .....	402
<b>43 FS.....</b>	<b>402</b>
43.1 FS_UNFORMATTED_PARTITION.....	402
<b>44 FTP .....</b>	<b>402</b>
44.1 FTP_ACL_DENY .....	403
44.2 FTPD_AUTHOR_FAILED.....	403
44.3 FTP_REACH_SESSION_LIMIT .....	403
<b>45 gRPC .....</b>	<b>404</b>
45.1 GRPC_LOGIN.....	404
45.2 GRPC_LOGIN_FAILED.....	404
45.3 GRPC_LOGOUT.....	405
45.4 GRPC_SERVER_FAILED .....	405
45.5 GRPC_SUBSCRIBE_EVENT_FAILED .....	405
45.6 GRPC_RECEIVE_SUBSCRIPTION.....	406
<b>46 HA .....</b>	<b>406</b>
46.1 HA_BATCHBACKUP_FINISHED .....	406
46.2 HA_BATCHBACKUP_STARTED .....	406
46.3 HA_STANDBY_NOT_READY .....	407
46.4 HA_STANDBY_TO_MASTER .....	407
<b>47 HLTH.....</b>	<b>407</b>
47.1 LIPC_COMM_FAULTY .....	408
47.2 LIPC_COMM_RECOVER.....	408
<b>48 HQOS .....</b>	<b>408</b>
48.1 HQOS_DP_SET_FAIL .....	409
48.2 HQOS_FP_SET_FAIL .....	409
48.3 HQOS_POLICY_APPLY_FAIL .....	409
48.4 HQOS_POLICY_RECOVER_FAIL.....	410
<b>49 HTTPD .....</b>	<b>410</b>
49.1 HTTPD_CONNECT .....	410
49.2 HTTPD_CONNECT_TIMEOUT .....	411
49.3 HTTPD_DISCONNECT .....	411
49.4 HTTPD_FAIL_FOR_ACL.....	411



49.5 HTTPD_FAIL_FOR_ACP .....	412
49.6 HTTPD_REACH_CONNECT_LIMIT .....	412
<b>50 IFNET .....</b>	<b>412</b>
50.1 IF_JUMBOFRAME_WARN .....	413
50.2 IF_BUFFER_CONGESTION_CLEAR .....	413
50.3 IF_BUFFER_CONGESTION_OCCURRENCE .....	413
50.4 IF_LINKFLAP_DETECTED .....	414
50.5 INTERFACE_NOTSUPPRESSED .....	414
50.6 INTERFACE_SUPPRESSED .....	414
50.7 LINK_UPDOWN .....	415
50.8 PFC_WARNING .....	415
50.9 PHY_UPDOWN .....	415
50.10 PROTOCOL_UPDOWN .....	416
50.11 STORM_CONSTRAIN_BELOW .....	416
50.12 STORM_CONSTRAIN_CONTROLLED .....	417
50.13 STORM_CONSTRAIN_EXCEED .....	417
50.14 STORM_CONSTRAIN_NORMAL .....	418
50.15 TUNNEL_LINK_UPDOWN .....	418
50.16 TUNNEL_PHY_UPDOWN .....	418
50.17 VLAN_MODE_CHANGE .....	419
<b>51 IKE .....</b>	<b>419</b>
51.1 IKE_P1_SA_ESTABLISH_FAIL .....	420
51.2 IKE_P2_SA_ESTABLISH_FAIL .....	421
51.3 IKE_P2_SA_TERMINATE .....	421
51.4 IKE_VERIFY_CERT_FAIL .....	422
<b>52 IMA .....</b>	<b>424</b>
52.1 IMA_ALLOCATE_FAILED .....	424
52.2 IMA_DATA_ERROR .....	424
52.3 IMA_FILE_HASH_FAILED .....	424
52.4 IMA_RM_FILE_MISS .....	425
52.5 IMA_RM_HASH_MISS .....	425
52.6 IMA_TEMPLATE_ERROR .....	425
<b>53 iNQA .....</b>	<b>425</b>
53.1 INQA_BWD_LOSS_EXCEED .....	426
53.2 INQA_BWD_LOSS_RECOV .....	426
53.3 INQA_DEBUG_FAIL .....	426

53.4 INQA_FLAG_DIFF .....	427
53.5 INQA_FLAG_FAIL .....	427
53.6 INQA_FLOW_DIFF .....	427
53.7 INQA_FWD_LOSS_EXCEED .....	428
53.8 INQA_FWD_LOSS_RECOV .....	428
53.9 INQA_INIT_ERROR .....	428
53.10 INQA_INST_FAIL .....	429
53.11 INQA_INTVL_DIFF .....	429
53.12 INQA_MP_NOIF .....	429
53.13 INQA_NO_RESOURCE .....	430
53.14 INQA_NO_SUPPORT .....	430
53.15 INQA_SMOOTH_BEGIN_FAIL .....	430
53.16 INQA_SMOOTH_END_FAIL .....	430
<b>54 IP6ADDR .....</b>	<b>431</b>
54.1 IP6ADDR_CREATEADDRESS_ERROR .....	431
54.2 IP6ADDR_FUNCTION_FAIL .....	431
<b>55 IP6FW .....</b>	<b>432</b>
55.1 IPv6_MTU_SET_DRV_NOT_SUPPORT .....	432
<b>56 IPADDR .....</b>	<b>432</b>
56.1 IPADDR_HA_EVENT_ERROR .....	433
56.2 IPADDR_HA_STOP_EVENT .....	435
<b>57 IPFW .....</b>	<b>435</b>
57.1 IPFW_FAILURE .....	435
57.2 IPv4_MTU_SET_DRV_NOT_SUPPORT .....	436
<b>58 IPSEC .....</b>	<b>436</b>
58.1 IPSEC_FAILED_ADD_FLOW_TABLE .....	436
58.2 IPSEC_PACKET_DISCARDED .....	437
58.3 IPSEC_SA_ESTABLISH .....	437
58.4 IPSEC_SA_ESTABLISH_FAIL .....	438
58.5 IPSEC_SA_INITINATION .....	438
58.6 IPSEC_SA_TERMINATE .....	439
<b>59 IPSG .....</b>	<b>439</b>
59.1 IPSG_ADDENTRY_ERROR .....	440
59.2 IPSG_ADDEXCLUDEDVLAN_ERROR .....	441
59.3 IPSG_ARP_LOCALMAC_CONFLICT .....	441

59.4	IPSG_ARP_REMOTEMAC_CONFLICT	442
59.5	IPSG_DELENTY_ERROR	442
59.6	IPSG_DELEXCLUDEDVLAN_ERROR	443
59.7	IPSG_MAC_CONFLICT	443
59.8	IPSG_ND_LOCALMAC_CONFLICT	444
59.9	IPSG_ND_REMOTEMAC_CONFLICT	444
59.10	IPSG_IPV4_ALARMCLEAR	445
59.11	IPSG_IPV4_ALARMEMERGE	445
59.12	IPSG_IPV6_ALARMCLEAR	445
59.13	IPSG_IPV6_ALARMEMERGE	446
<b>60</b>	<b>IRDP</b>	<b>446</b>
60.1	IRDP_EXCEED_ADVADDR_LIMIT	446
<b>61</b>	<b>IRF</b>	<b>446</b>
61.1	IRF_LINK_BLOCK	447
61.2	IRF_LINK_DOWN	447
61.3	IRF_LINK_UP	447
61.4	IRF_MEMBERID_CONFLICT	448
61.5	IRF_MERGE	448
61.6	IRF_MERGE_NEED_REBOOT	448
61.7	IRF_MERGE_NOT_NEED_REBOOT	449
<b>62</b>	<b>ISIS</b>	<b>449</b>
62.1	ISIS_LSP_CONFLICT	449
62.2	ISIS_MEM_ALERT	450
62.3	ISIS_NBR_CHG	451
<b>63</b>	<b>ISSU</b>	<b>452</b>
63.1	ISSU_LOAD_FAILED	452
63.2	ISSU_LOAD_SUCCESS	452
63.3	ISSU_PROCESSWITCHOVER	452
63.4	ISSU_ROLLBACKCHECKNORMAL	453
<b>64</b>	<b>L2PT</b>	<b>453</b>
64.1	L2PT_ADD_GROUPMEMBER_FAILED	453
64.2	L2PT_CREATE_TUNNELGROUP_FAILED	453
64.3	L2PT_ENABLE_DROP_FAILED	454
64.4	L2PT_SET_MULTIMAC_FAILED	454

<b>65 L2TPV2</b> .....	<b>454</b>
65.1 L2TPV2_SESSION_EXCEED_LIMIT .....	454
65.2 L2TPV2_TUNNEL_EXCEED_LIMIT.....	455
<b>66 L2VPN</b> .....	<b>455</b>
66.1 L2VPN_ARP_MOBILITY_SUPPRESS (public instance) .....	455
66.2 L2VPN_ARP_MOBILITY_SUPPRESS (VPN instance) .....	456
66.3 L2VPN_ARP_MOBILITY_UNSUPPRESS (public instance) .....	456
66.4 L2VPN_ARP_MOBILITY_UNSUPPRESS (VPN instance) .....	457
66.5 L2VPN_MAC_MOBILITY_SUPPRESS .....	457
66.6 L2VPN_MAC_MOBILITY_UNSUPPRESS.....	457
66.7 L2VPN_BGPVC_CONFLICT_LOCAL .....	458
66.8 L2VPN_BGPVC_CONFLICT_REMOTE.....	458
66.9 L2VPN_HARD_RESOURCE_NOENOUGH.....	458
66.10 L2VPN_HARD_RESOURCE_RESTORE .....	459
66.11 L2VPN_LABEL_DUPLICATE .....	459
66.12 L2VPN_MLAG_AC_CONFLICT .....	460
66.13 PROCESS.....	460
<b>67 LAGG</b> .....	<b>460</b>
67.1 LAGG_ACTIVE .....	461
67.2 LAGG_AUTO_AGGREGATION .....	461
67.3 LAGG_INACTIVE_AICFG .....	462
67.4 LAGG_INACTIVE_BFD .....	462
67.5 LAGG_INACTIVE_CONFIGURATION .....	462
67.6 LAGG_INACTIVE_DUPLEX .....	463
67.7 LAGG_INACTIVE_HARDWAREVALUE .....	463
67.8 LAGG_INACTIVE_IFCFG_DEFAULT .....	463
67.9 LAGG_INACTIVE_IFCFG_LOOPPORT.....	464
67.10 LAGG_INACTIVE_IFCFG_NONAGG.....	464
67.11 LAGG_INACTIVE_KEY_INVALID .....	464
67.12 LAGG_INACTIVE_LOWER_LIMIT .....	465
67.13 LAGG_INACTIVE_NODEREMOVE .....	465
67.14 LAGG_INACTIVE_OPERSTATE.....	465
67.15 LAGG_INACTIVE_PARTNER .....	466
67.16 LAGG_INACTIVE_PARTNER_KEY_WRONG.....	466
67.17 LAGG_INACTIVE_PARTNER_MAC_WRONG.....	466
67.18 LAGG_INACTIVE_PARTNER_NONAGG .....	467

67.19 LAGG_INACTIVE_PARTNER_RDIRHANDLE.....	467
67.20 LAGG_INACTIVE_PHYSTATE .....	467
67.21 LAGG_INACTIVE_PORT_DEFAULT .....	468
67.22 LAGG_INACTIVE_RDIRHANDLE .....	468
67.23 LAGG_INACTIVE_REDUNDANCY .....	468
67.24 LAGG_INACTIVE_RESOURCE_INSUFICIE .....	469
67.25 LAGG_INACTIVE_SPEED .....	469
67.26 LAGG_INACTIVE_STANDBY .....	469
67.27 LAGG_INACTIVE_UPPER_LIMIT.....	470
67.28 LAGG_SELECTPORT_INCONSISTENT .....	470
<b>68 LDP .....</b>	<b>470</b>
68.1 LDP_MPLSLSRID_CHG.....	471
68.2 LDP_SESSION_CHG .....	472
68.3 LDP_SESSION_GR.....	473
68.4 LDP_SESSION_SP .....	473
<b>69 LIPC .....</b>	<b>474</b>
69.1 LIPC_CHECKDOWN .....	474
69.2 LIPC_MTCP_CHECK .....	474
69.3 LIPC_STCP_CHECK.....	475
69.4 LIPC_SUDP_CHECK .....	475
69.5 PORT_CHANGE.....	476
<b>70 LLDP .....</b>	<b>476</b>
70.1 LLDP_CREATE_NEIGHBOR .....	476
70.2 LLDP_DELETE_NEIGHBOR .....	477
70.3 LLDP_LESS_THAN_NEIGHBOR_LIMIT .....	477
70.4 LLDP_NEIGHBOR_AGE_OUT.....	478
70.5 LLDP_NEIGHBOR_PROTECTION_BLOCK.....	478
70.6 LLDP_NEIGHBOR_PROTECTION_DOWN.....	479
70.7 LLDP_NEIGHBOR_PROTECTION_UNBLOCK.....	479
70.8 LLDP_NEIGHBOR_PROTECTION_UP .....	479
70.9 LLDP_PVID_INCONSISTENT.....	480
70.10 LLDP_REACH_NEIGHBOR_LIMIT .....	480
<b>71 LOAD .....</b>	<b>480</b>
71.1 BOARD_LOADING .....	481
71.2 LOAD_FAILED.....	481
71.3 LOAD_FINISHED.....	481

<b>72 LOGIN</b> .....	<b>482</b>
72.1 LOGIN_FAILED .....	482
72.2 LOGIN_INVALID_USERNAME_PWD.....	482
<b>73 LPDT</b> .....	<b>482</b>
73.1 LPDT_LOOPED .....	483
73.2 LPDT_RECOVERED .....	483
73.3 LPDT_VLAN_LOOPED .....	483
73.4 LPDT_VLAN_RECOVERED.....	484
73.5 LPDT_VSI_LOOPED .....	484
73.6 LPDT_VSI_RECOVERED .....	484
73.7 LPDT_VSI_BLOCKFAIL .....	485
<b>74 LS</b> .....	<b>485</b>
74.1 LOCALSVR_PROMPTED_CHANGE_PWD .....	486
74.2 LS_ADD_USER_TO_GROUP.....	486
74.3 LS_AUTHEN_FAILURE.....	487
74.4 LS_AUTHEN_SUCCESS .....	487
74.5 LS_DEL_USER_FROM_GROUP.....	488
74.6 LS_DELETE_PASSWORD_FAIL .....	488
74.7 LS_PWD_ADDBLACKLIST .....	488
74.8 LS_PWD_CHGPWD_FOR_AGEDOUT .....	489
74.9 LS_PWD_CHGPWD_FOR_AGEOUT .....	489
74.10 LS_PWD_CHGPWD_FOR_COMPOSITION .....	489
74.11 LS_PWD_CHGPWD_FOR_FIRSTLOGIN .....	490
74.12 LS_PWD_CHGPWD_FOR_LENGTH.....	490
74.13 LS_PWD_FAILED2WRITEPASS2FILE.....	490
74.14 LS_PWD_MODIFY_FAIL.....	491
74.15 LS_PWD_MODIFY_SUCCESS.....	491
74.16 LS_REAUTHEN_FAILURE.....	492
74.17 LS_UPDATE_PASSWORD_FAIL .....	492
74.18 LS_USER_CANCEL .....	492
74.19 LS_USER_PASSWORD_EXPIRE .....	493
74.20 LS_USER_ROLE_CHANGE .....	493
<b>75 LSPV</b> .....	<b>493</b>
75.1 LSPV_PING_STATIS_INFO.....	494
<b>76 MAC</b> .....	<b>494</b>
76.1 MAC_DRIVER_ADD_ENTRY.....	494

76.2	MAC_PROTOCOLPKT_NORES_GLOBAL .....	495
76.3	MAC_PROTOCOLPKT_NORES_PORT .....	495
76.4	MAC_PROTOCOLPKT_NORES_VLAN .....	496
76.5	MAC_TABLE_FULL_GLOBAL .....	496
76.6	MAC_TABLE_FULL_PORT .....	496
76.7	MAC_TABLE_FULL_VLAN .....	497
76.8	MAC_VLAN_LEARNLIMIT_NORESOURCE .....	497
76.9	MAC_VLAN_LEARNLIMIT_NOTSUPPORT .....	497
<b>77</b>	<b>MACA.....</b>	<b>497</b>
77.1	MACA_ENABLE_NOT_EFFECTIVE .....	498
77.2	MACA_LOGIN_FAILURE .....	498
77.3	MACA_LOGIN_FAILURE (EAD) .....	499
77.4	MACA_LOGIN_SUCC .....	500
77.5	MACA_LOGIN_SUCC (in open mode) .....	500
77.6	MACA_LOGOFF .....	501
77.7	MACA_LOGOFF (in open mode).....	501
<b>78</b>	<b>MACSEC.....</b>	<b>501</b>
78.1	MACSEC_MKA_KEEPALIVE_TIMEOUT.....	502
78.2	MACSEC_MKA_PRINCIPAL_ACTOR .....	502
78.3	MACSEC_MKA_SAK_REFRESH .....	502
78.4	MACSEC_MKA_SESSION_REAUTH.....	503
78.5	MACSEC_MKA_SESSION_SECURED .....	503
78.6	MACSEC_MKA_SESSION_START .....	504
78.7	MACSEC_MKA_SESSION_STOP .....	504
78.8	MACSEC_MKA_SESSION_UNSECURED.....	505
<b>79</b>	<b>MBFD.....</b>	<b>505</b>
79.1	MBFD_TRACEROUTE_FAILURE .....	505
<b>80</b>	<b>MBUF.....</b>	<b>505</b>
80.1	MBUF_DATA_BLOCK_CREATE_FAIL.....	506
<b>81</b>	<b>MDC.....</b>	<b>506</b>
81.1	MDC_CREATE .....	506
81.2	MDC_CREATE_ERR.....	507
81.3	MDC_DELETE .....	507
81.4	MDC_KERNEL_EVENT_TOOLONG .....	508
81.5	MDC_LICENSE_EXPIRE .....	508

81.6 MDC_NO_FORMAL_LICENSE .....	508
81.7 MDC_NO_LICENSE_EXIT .....	509
81.8 MDC_OFFLINE .....	509
81.9 MDC_ONLINE .....	509
81.10 MDC_STATE_CHANGE .....	510
<b>82 MFIB .....</b>	<b>510</b>
82.1 MFIB_MEM_ALERT .....	510
82.2 MFIB_MTI_NO_ENOUGH_RESOURCE .....	511
<b>83 MGROUP .....</b>	<b>511</b>
83.1 MGROUP_APPLY_SAMPLER_FAIL .....	511
83.2 MGROUP_RESTORE_CPUCFG_FAIL .....	512
83.3 MGROUP_RESTORE_GROUP_FAIL .....	512
83.4 MGROUP_RESTORE_IFCFG_FAIL .....	513
83.5 MGROUP_SYNC_CFG_FAIL .....	513
<b>84 MOD .....</b>	<b>513</b>
84.1 MOD_ENABLE_FAIL .....	514
84.2 MOD_MODIFY_FAIL .....	514
<b>85 MPLS .....</b>	<b>514</b>
85.1 MPLS_HARD_RESOURCE_NOENOUGH .....	515
85.2 MPLS_HARD_RESOURCE_RESTORE .....	515
<b>86 MTLK .....</b>	<b>515</b>
86.1 MTLK_UPLINK_STATUS_CHANGE .....	516
<b>87 NAT .....</b>	<b>516</b>
87.1 NAT_ADDR_BIND_CONFLICT .....	516
87.2 NAT_FAILED_ADD_FLOW_RULE .....	517
87.3 NAT_FAILED_ADD_FLOW_TABLE .....	517
87.4 NAT_FLOW .....	518
87.5 NAT_SERVER_INVALID .....	519
87.6 NAT_SERVICE_CARD_RECOVER_FAILURE .....	520
<b>88 ND .....</b>	<b>520</b>
88.1 ND_COMMONPROXY_ENABLE_FAILED .....	521
88.2 ND_CONFLICT .....	521
88.3 ND_DUPADDR .....	522
88.4 ND_ENTRY_ENOUGHRESOURCE .....	522
88.5 ND_ENTRY_INCONSISTENT .....	523



88.6 ND_ENTRY_NORESOURCE .....	523
88.7 ND_HOST_IP_CONFLICT .....	524
88.8 ND_LOCALPROXY_ENABLE_FAILED .....	524
88.9 ND_MAC_CHECK .....	525
88.10 ND_NETWORKROUTE_DUPLICATE .....	525
88.11 ND_RAGUARD_DROP .....	526
88.12 ND_RATE_EXCEEDED .....	526
88.13 ND_RATELIMIT_NOTSUPPORT .....	527
88.14 ND_SET_PORT_TRUST_NORESOURCE .....	527
88.15 ND_SET_VLAN_REDIRECT_NORESOURCE .....	527
88.16 ND_SNOOPING_LEARN_ALARM .....	528
88.17 ND_SNOOPING_LEARN_ALARM_RECOVER .....	528
88.18 ND_USER_DUPLICATE_IPV6ADDR .....	529
88.19 ND_USER_MOVE .....	530
88.20 ND_USER_OFFLINE .....	530
88.21 ND_USER_ONLINE .....	531
<b>89 NETCONF .....</b>	<b>531</b>
89.1 CLI .....	531
89.2 EDIT-CONFIG .....	532
89.3 NETCONF_MSG_DEL .....	533
89.4 THREAD .....	533
<b>90 NQA .....</b>	<b>533</b>
90.1 NQA_ENTRY_PROBE_RESULT .....	534
90.2 NQA_LOG_UNREACHABLE .....	534
90.3 NQA_START_FAILURE .....	535
90.4 NQA_TWAMP_LIGHT_PACKET_INVALID .....	535
90.5 NQA_TWAMP_LIGHT_REACTION .....	536
90.6 NQA_TWAMP_LIGHT_START_FAILURE .....	536
<b>91 NSS .....</b>	<b>536</b>
91.1 NSS_ENABLE_FAIL .....	537
91.2 NSS_SESSION_TIMEOUT_FAIL .....	537
<b>92 NTP .....</b>	<b>537</b>
92.1 NTP_CLOCK_CHANGE .....	538
92.2 NTP_LEAP_CHANGE .....	538
92.3 NTP_SOURCE_CHANGE .....	538
92.4 NTP_SOURCE_LOST .....	539

92.5 NTP_STRATUM_CHANGE .....	539
<b>93 OAP .....</b>	<b>539</b>
93.1 OAP_CLIENT_DEREG .....	539
93.2 OAP_CLIENT_TIMEOUT .....	540
<b>94 OBJP .....</b>	<b>540</b>
94.1 OBJP_ACCELERATE_NO_RES .....	540
94.2 OBJP_ACCELERATE_NOT_SUPPORT .....	540
94.3 OBJP_ACCELERATE_UNK_ERR .....	541
<b>95 OFP .....</b>	<b>541</b>
95.1 OFP_ACTIVE .....	541
95.2 OFP_ACTIVE_FAILED .....	541
95.3 OFP_CONNECT .....	542
95.4 OFP_FAIL_OPEN .....	542
95.5 OFP_FAIL_OPEN_FAILED .....	542
95.6 OFP_FLOW_ADD .....	543
95.7 OFP_FLOW_ADD_ARP_FAILED .....	543
95.8 OFP_FLOW_ADD_BUSY .....	544
95.9 OFP_FLOW_ADD_BUSY_RECOVER .....	544
95.10 OFP_FLOW_ADD_DUP .....	544
95.11 OFP_FLOW_ADD_FAILED .....	545
95.12 OFP_FLOW_ADD_FAILED .....	545
95.13 OFP_FLOW_ADD_ND_FAILED .....	546
95.14 OFP_FLOW_ADD_TABLE_MISS .....	546
95.15 OFP_FLOW_ADD_TABLE_MISS_FAILED .....	547
95.16 OFP_FLOW_DEL .....	547
95.17 OFP_FLOW_DEL_L2VPN_DISABLE .....	548
95.18 OFP_FLOW_DEL_TABLE_MISS .....	548
95.19 OFP_FLOW_DEL_TABLE_MISS_FAILED .....	549
95.20 OFP_FLOW_DEL_VSIIF_DEL .....	549
95.21 OFP_FLOW_DEL_VXLAN_DEL .....	550
95.22 OFP_FLOW_MOD .....	550
95.23 OFP_FLOW_MOD_FAILED .....	551
95.24 OFP_FLOW_MOD_TABLE_MISS .....	551
95.25 OFP_FLOW_MOD_TABLE_MISS_FAILED .....	552
95.26 OFP_FLOW_RMV_GROUP .....	552
95.27 OFP_FLOW_RMV_HARDTIME .....	552

95.28	OFF_FLOW_RMV_IDLETIME	553
95.29	OFF_FLOW_RMV_METER	553
95.30	OFF_FLOW_UPDATE_FAILED	554
95.31	OFF_GROUP_ADD	554
95.32	OFF_GROUP_ADD_FAILED	555
95.33	OFF_GROUP_DEL	555
95.34	OFF_GROUP_MOD	555
95.35	OFF_GROUP_MOD_FAILED	556
95.36	OFF_GROUP_REFRESH_FAILED	556
95.37	OFF_GROUP_ROLLBACK_FAILED	556
95.38	OFF_METER_ADD	557
95.39	OFF_METER_ADD_FAILED	557
95.40	OFF_METER_DEL	557
95.41	OFF_METER_MOD	558
95.42	OFF_METER_MOD_FAILED	558
95.43	OFF_MISS_RMV_GROUP	558
95.44	OFF_MISS_RMV_HARDTIME	559
95.45	OFF_MISS_RMV_IDLETIME	559
95.46	OFF_MISS_RMV_METER	559
95.47	OFF_SMARTGROUP_BIND	560
95.48	OFF_SMARTGROUP_BIND_FAILED	560
95.49	OFF_SMARTGROUP_NEW_BIND	561
95.50	OFF_SMARTGROUP_NEW_BIND_FAILED	561
95.51	OFF_SMARTGROUP_REBIND	562
95.52	OFF_SMARTGROUP_REBIND_FAILED	563
95.53	OFF_SMARTGROUP_UNBIND	563
95.54	OFF_SMARTGROUP_UNBIND_FAILED	564
95.55	OFF_TTP_GROUP_DEL_DENY	564
95.56	PORT_MOD	565
95.57	OFF_RADARDETECTION	565
<b>96</b>	<b>OPENSRC (FreeRADIUS)</b>	<b>566</b>
96.1	HUP 事件	566
96.2	进程重启	567
96.3	进程启动	567
96.4	用户认证	568

<b>97 OPTMOD</b> .....	<b>570</b>
97.1 BIAS_HIGH .....	571
97.2 BIAS_LOW .....	571
97.3 BIAS_NORMAL .....	571
97.4 CFG_ERR .....	572
97.5 CHKSUM_ERR .....	572
97.6 FIBER_SFPMODULE_INVALID .....	572
97.7 FIBER_SFPMODULE_NOWINVALID .....	573
97.8 IO_ERR .....	573
97.9 MOD_ALM_OFF .....	573
97.10 MOD_ALM_ON .....	574
97.11 MODULE_IN .....	574
97.12 MODULE_OUT .....	574
97.13 PHONY_MODULE .....	575
97.14 RX_ALM_OFF .....	575
97.15 RX_ALM_ON .....	575
97.16 RX_POW_HIGH .....	576
97.17 RX_POW_LOW .....	576
97.18 RX_POW_NORMAL .....	576
97.19 TEMP_HIGH .....	577
97.20 TEMP_LOW .....	577
97.21 TEMP_NORMAL .....	577
97.22 TX_ALM_OFF .....	578
97.23 TX_ALM_ON .....	578
97.24 TX_POW_HIGH .....	578
97.25 TX_POW_LOW .....	579
97.26 TX_POW_NORMAL .....	579
97.27 TYPE_ERR .....	579
97.28 VOLT_HIGH .....	580
97.29 VOLT_LOW .....	580
97.30 VOLT_NORMAL .....	580
<b>98 OSPF</b> .....	<b>580</b>
98.1 OSPF_DUP_RTRID_NBR .....	581
98.2 OSPF_IP_CONFLICT_INTRA .....	581
98.3 OSPF_LAST_NBR_DOWN .....	582
98.4 OSPF_MEM_ALERT .....	582

98.5 OSPF_NBR_CHG .....	583
98.6 OSPF_NBR_CHG_REASON .....	584
98.7 OSPF_RT_LMT .....	585
98.8 OSPF_RTRID_CHG .....	585
98.9 OSPF_RTRID_CONFLICT_INTER .....	585
98.10 OSPF_RTRID_CONFLICT_INTRA .....	586
98.11 OSPF_VLINKID_CHG .....	586
<b>99 OSPFV3 .....</b>	<b>586</b>
99.1 OSPFV3_LAST_NBR_DOWN .....	587
99.2 OSPFV3_MEM_ALERT .....	587
99.3 OSPFV3_NBR_CHG .....	588
99.4 OSPFV3_RT_LMT .....	588
<b>100 PBB .....</b>	<b>588</b>
100.1 PBB_JOINAGG_WARNING .....	589
<b>101 PBR .....</b>	<b>589</b>
101.1 PBR_HARDWARE_ERROR .....	589
<b>102 PCE .....</b>	<b>589</b>
102.1 PCE_PCEP_SESSION_CHG .....	590
<b>103 PEX (IRF3.1) .....</b>	<b>590</b>
103.1 PEX_AUTOCONFIG_BAGG_ASSIGNMEMBER .....	591
103.2 PEX_AUTOCONFIG_BAGG_CREATE .....	591
103.3 PEX_AUTOCONFIG_BAGG_NORESOURCE .....	591
103.4 PEX_AUTOCONFIG_BAGG_REMOVEMEMBER .....	592
103.5 PEX_AUTOCONFIG_CAPABILITY_ENABLE .....	592
103.6 PEX_AUTOCONFIG_CASCADELIMIT .....	592
103.7 PEX_AUTOCONFIG_CONNECTION_ERROR .....	593
103.8 PEX_AUTOCONFIG_DIFFGROUPNUMBER .....	593
103.9 PEX_AUTOCONFIG_DYNAMICBAGG_STP .....	593
103.10 PEX_AUTOCONFIG_GROUP_CREATE .....	594
103.11 PEX_AUTOCONFIG_NONUMBERRESOURCE .....	594
103.12 PEX_AUTOCONFIG_NOT_CASCADEPORT .....	595
103.13 PEX_AUTOCONFIG_NUMBER_ASSIGN .....	595
103.14 PEX_LLDP_DISCOVER .....	596
103.15 PEX_MEMBERID_EXCEED .....	596
103.16 PEX_PECSP_OPEN_RCVD .....	596

103.17 PEX_PECSP_OPEN_SEND .....	597
103.18 PEX_PECSP_TIMEOUT .....	597
<b>104 PFILTER .....</b>	<b>597</b>
104.1 PFILTER_GLB_RES_CONFLICT.....	598
104.2 PFILTER_GLB_IPV4_DACT_NO_RES .....	598
104.3 PFILTER_GLB_IPV4_DACT_UNK_ERR .....	598
104.4 PFILTER_GLB_IPV6_DACT_NO_RES .....	599
104.5 PFILTER_GLB_IPV6_DACT_UNK_ERR .....	599
104.6 PFILTER_GLB_MAC_DACT_NO_RES .....	599
104.7 PFILTER_GLB_MAC_DACT_UNK_ERR.....	600
104.8 PFILTER_GLB_NO_RES .....	600
104.9 PFILTER_GLB_NOT_SUPPORT .....	600
104.10 PFILTER_GLB_UNK_ERR.....	601
104.11 PFILTER_IF_IPV4_DACT_NO_RES .....	601
104.12 PFILTER_IF_IPV4_DACT_UNK_ERR .....	601
104.13 PFILTER_IF_IPV6_DACT_NO_RES .....	602
104.14 PFILTER_IF_IPV6_DACT_UNK_ERR .....	602
104.15 PFILTER_IF_MAC_DACT_NO_RES .....	602
104.16 PFILTER_IF_MAC_DACT_UNK_ERR.....	603
104.17 PFILTER_IF_NO_RES .....	603
104.18 PFILTER_IF_NOT_SUPPORT .....	604
104.19 PFILTER_IF_RES_CONFLICT.....	604
104.20 PFILTER_IF_UNK_ERR.....	605
104.21 PFILTER_IPV4_FLOW_INFO .....	605
104.22 PFILTER_IPV4_FLOW_STATIS .....	606
104.23 PFILTER_IPV6_FLOW_INFO .....	606
104.24 PFILTER_IPV6_FLOW_STATIS .....	607
104.25 PFILTER_IPV6_STATIS_INFO .....	607
104.26 PFILTER_MAC_FLOW_INFO .....	608
104.27 PFILTER_STATIS_INFO .....	608
104.28 PFILTER_VLAN_IPV4_DACT_NO_RES .....	609
104.29 PFILTER_VLAN_IPV4_DACT_UNK_ERR.....	609
104.30 PFILTER_VLAN_IPV6_DACT_NO_RES .....	609
104.31 PFILTER_VLAN_IPV6_DACT_UNK_ERR.....	610
104.32 PFILTER_VLAN_MAC_DACT_NO_RES .....	610
104.33 PFILTER_VLAN_MAC_DACT_UNK_ERR.....	610

104.34	PFILTER_VLAN_NO_RES	611
104.35	PFILTER_VLAN_NOT_SUPPORT	611
104.36	PFILTER_VLAN_RES_CONFLICT	612
104.37	PFILTER_VLAN_UNK_ERR	612
<b>105</b>	<b>PIM</b>	<b>612</b>
105.1	PIM_NBR_DOWN	613
105.2	PIM_NBR_UP	613
<b>106</b>	<b>PING</b>	<b>613</b>
106.1	PING_STATISTICS	614
106.2	PING_VPN_STATISTICS	615
<b>107</b>	<b>PKG</b>	<b>615</b>
107.1	PKG_BOOTLOADER_FILE_FAILED	615
107.2	PKG_BOOTLOADER_FILE_SUCCESS	616
107.3	PKG_INSTALL_ACTIVATE_FAILED	616
107.4	PKG_INSTALL_ACTIVATE_SUCCESS	616
<b>108</b>	<b>PKI</b>	<b>616</b>
108.1	GET_CERT_FROM_CA_SERVER_FAIL	617
108.2	IMPORT_CERT_FAIL	618
108.3	REQUEST_CERT_FAIL	620
108.4	REQUEST_CERT_SUCCESS	620
108.5	RETRIEVE_CRL_FAIL	621
108.6	VALIDATE_CERT_FAIL	622
<b>109</b>	<b>PKT2CPU</b>	<b>624</b>
109.1	PKT2CPU_NO_RESOURCE	624
<b>110</b>	<b>PKTCPT</b>	<b>624</b>
110.1	PKTCPT_AP_OFFLINE	624
110.2	PKTCPT_ALREADY_EXIT	625
110.3	PKTCPT_CONN_FAIL	625
110.4	PKTCPT_INVALID_FILTER	625
110.5	PKTCPT_LOGIN_DENIED	626
110.6	PKTCPT_MEMORY_ALERT	626
110.7	PKTCPT_OPEN_FAIL	626
110.8	PKTCPT_OPERATION_TIMEOUT	627
110.9	PKTCPT_SERVICE_FAIL	627
110.10	PKTCPT_UNKNOWN_ERROR	627

110.11	PKTCPT_UPLOAD_ERROR .....	628
110.12	PKTCPT_WRITE_FAIL.....	628
<b>111</b>	<b>PoE .....</b>	<b>628</b>
111.1	POE_AI_CLEAR .....	629
111.2	POE_AI_DETECTIONMODE_NONE .....	629
111.3	POE_AI_DETECTIONMODE_SIMPLE .....	629
111.4	POE_AI_DISCONNECT_AC .....	630
111.5	POE_AI_DISCONNECT_DELAY .....	630
111.6	POE_AI_FORCE_PoE.....	630
111.7	POE_AI_HIGH_INRUSH .....	631
111.8	POE_AI_LEGACY.....	631
111.9	POE_AI_MAXPOWER.....	631
111.10	POE_AI_RESTART .....	632
<b>112</b>	<b>PORTAL.....</b>	<b>632</b>
112.1	PORTAL_RULE_FAILED .....	632
<b>113</b>	<b>PORTSEC.....</b>	<b>633</b>
113.1	PORTSEC_ACL_FAILURE .....	633
113.2	PORTSEC_CAR_FAILURE.....	634
113.3	PORTSEC_CREATEAC_FAILURE.....	634
113.4	PORTSEC_LEARNED_MACADDR .....	634
113.5	PORTSEC_NTK_NOT_EFFECTIVE .....	635
113.6	PORTSEC_PORTMODE_NOT_EFFECTIVE .....	635
113.7	PORTSEC_PROFILE_FAILURE .....	635
113.8	PORTSEC_URL_FAILURE .....	636
113.9	PORTSEC_VIOLATION .....	636
113.10	PORTSEC_VLANMACLIMIT .....	637
<b>114</b>	<b>PPP .....</b>	<b>637</b>
114.1	IPPOOL_ADDRESS_EXHAUSTED .....	637
114.2	PPP_USER_LOGOFF .....	638
114.3	PPP_USER_LOGON_FAILED .....	639
114.4	PPP_USER_LOGON_SUCCESS .....	640
<b>115</b>	<b>PTP .....</b>	<b>640</b>
115.1	PTP_MASTER_CLOCK_CHANGE .....	641
115.2	PTP_PKTLOST.....	642
115.3	PTP_PKTLOST_RECOVER.....	643



115.4	PTP_PORT_BMCINFO_CHANGE .....	643
115.5	PTP_PORT_STATE_CHANGE .....	644
115.6	PTP_SRC_CHANGE .....	645
115.7	PTP_SRC_SWITCH .....	646
115.8	PTP_TIME_LOCK.....	646
115.9	PTP_TIME_NOT_LOCK.....	647
<b>116</b>	<b>PTS .....</b>	<b>647</b>
116.1	PTS_AK_AUTH_FAILED.....	647
116.2	PTS_AK_INVALID .....	648
116.3	PTS_AK_NO_CERT .....	648
116.4	PTS_AK_NO_EXIST .....	648
116.5	PTS_AK_NO_LOAD .....	649
116.6	PTS_BTW_PCR_FAILED.....	649
116.7	PTS_CHECK_RM_VERSION_FAILED.....	649
116.8	PTS_CREATE_AGED_TIMER_FAILED .....	650
116.9	PTS_CREATE_CHECK_TIMER_FAILED.....	650
116.10	PTS_CREATE_CONTEXT_FAILED.....	650
116.11	PTS_CREATE_EPOLL_FAILED .....	651
116.12	PTS_CREATE_HASH_FAILED.....	651
116.13	PTS_CREATE_SELFVERIFY_COUNTER_FAILED.....	651
116.14	PTS_CREATE_SELFVERIFY_TIMER_FAILED .....	652
116.15	PTS_CREATE_SOCKET_FAILED .....	652
116.16	PTS_CREATE_TIMER_FAILED.....	652
116.17	PTS_FILE_HASH_FAILED.....	653
116.18	PTS_LOAD_KEY_FAILED .....	653
116.19	PTS_PARSE_IML_FAILED .....	653
116.20	PTS_PKG_PCR_FAILED .....	654
116.21	PTS_READ_PCR_FAILED.....	654
116.22	PTS_RM_FILE_FAILED .....	654
116.23	PTS_RUNTIME_PCR_FAILED .....	655
116.24	PTS_SELFVERIFY_FAILED .....	655
116.25	PTS_SELFVERIFY_START_FAILED .....	655
116.26	PTS_TEMPLATE_HASH_FAILED .....	656
<b>117</b>	<b>PWDCTL .....</b>	<b>656</b>
117.1	PWDCTL_ADD_BLACKLIST.....	656
117.2	PWDCTL_CHANGE_PASSWORD .....	657

117.3 PWDCTL_FAILED_COPYFILE .....	657
117.4 PWDCTL_FAILED_PROCMMSG.....	657
117.5 PWDCTL_FAILED_TO_WRITEPWD .....	658
117.6 PWDCTL_FAILED_TO_OPENFILE .....	658
117.7 PWDCTL_NOENOUGHSPACE .....	658
117.8 PWDCTL_NOTFOUNDUSER .....	659
117.9 PWDCTL_NOTIFYWRITEFILE .....	659
117.10 PWDCTL_RECFORMATCONV.....	659
117.11 PWDCTL_UPDATETIME.....	660
<b>118 QOS .....</b>	<b>660</b>
118.1 QOS_MIRROR_SYNC_CFG_FAIL .....	660
118.2 QOS_CAR_APPLYUSER_FAIL .....	661
118.3 QOS_CBWFQ_REMOVED .....	661
118.4 QOS_GTS_APPLYUSER_FAIL .....	662
118.5 QOS_IFA_CONFIG_FAIL.....	662
118.6 QOS_IFA_REFRESH_FAIL.....	663
118.7 QOS_LR_APPLYIF_FAIL .....	663
118.8 QOS_NOT_ENOUGH_BANDWIDTH.....	664
118.9 QOS_NOT_ENOUGH_NNIBANDWIDTH .....	664
118.10 QOS_POLICY_APPLYCOPP_CBFAIL .....	665
118.11 QOS_POLICY_APPLYCOPP_FAIL .....	665
118.12 QOS_POLICY_APPLYGLOBAL_CBFAIL .....	666
118.13 QOS_POLICY_APPLYGLOBAL_FAIL .....	666
118.14 QOS_POLICY_APPLYIF_CBFAIL .....	667
118.15 QOS_POLICY_APPLYIF_FAIL .....	667
118.16 QOS_POLICY_APPLYUSER_FAIL.....	668
118.17 QOS_POLICY_APPLYVLAN_CBFAIL .....	668
118.18 QOS_POLICY_APPLYVLAN_FAIL .....	669
118.19 QOS_QMPROFILE_APPLYIF_FAIL .....	669
118.20 QOS_QMPROFILE_APPLYUSER_FAIL .....	670
118.21 QOS_QMPROFILE_MODIFYQUEUE_FAIL .....	670
118.22 QOS_QUEUE_APPLYIF_FAIL .....	671
118.23 QOS_UNI_RESTORE_FAIL.....	671
118.24 QOS_WRED_TABLE_APPLYFABRIC_FAIL .....	672
118.25 QOS_WRED_TABLE_CFG_FAIL .....	672

<b>119 RADIUS</b> .....	<b>672</b>
119.1 RADIUS_ACCT_SERVER_DOWN .....	673
119.2 RADIUS_ACCT_SERVER_UP.....	673
119.3 RADIUS_AUTH_FAILURE .....	674
119.4 RADIUS_AUTH_SERVER_DOWN .....	674
119.5 RADIUS_AUTH_SERVER_UP.....	675
119.6 RADIUS_AUTH_SUCCESS .....	675
119.7 RADIUS_REMOVE_SERVER_FAIL .....	675
<b>120 RDDC</b> .....	<b>676</b>
120.1 RDDC_ACTIVENODE_CHANGE.....	676
<b>121 RESMON</b> .....	<b>676</b>
121.1 RESMON_MINOR .....	677
121.2 RESMON_MINOR_RECOVERY.....	677
121.3 RESMON_SEVERE.....	678
121.4 RESMON_SEVERE_RECOVERY .....	678
121.5 RESMON_USEDUP .....	679
121.6 RESMON_USEDUP_RECOVERY .....	679
<b>122 RIP</b> .....	<b>679</b>
122.1 RIP_MEM_ALERT .....	680
122.2 RIP_RT_LMT .....	680
<b>123 RIPNG</b> .....	<b>680</b>
123.1 RIPNG_MEM_ALERT.....	680
123.2 RIPNG_RT_LMT.....	681
<b>124 RM</b> .....	<b>681</b>
124.1 RM_ACRT_REACH_LIMIT.....	681
124.2 RM_ACRT_REACH_THRESVALUE .....	682
124.3 RM_THRESHLD_VALUE_REACH.....	682
124.4 RM_TOTAL_THRESHLD_VALUE_REACH.....	682
<b>125 RPR</b> .....	<b>683</b>
125.1 RPR_EXCEED_MAX_SEC_MAC .....	683
125.2 RPR_EXCEED_MAX_SEC_MAC_OVER .....	683
125.3 RPR_EXCEED_MAX_STATION .....	684
125.4 RPR_EXCEED_MAX_STATION_OVER .....	684
125.5 RPR_EXCEED_RESERVED_RATE .....	684
125.6 RPR_EXCEED_RESERVED_RATE_OVER.....	685

125.7 RPR_IP_DUPLICATE .....	685
125.8 RPR_IP_DUPLICATE_OVER.....	685
125.9 RPR_JUMBO_INCONSISTENT .....	686
125.10 RPR_JUMBO_INCONSISTENT_OVER.....	686
125.11 RPR_LAGGCONFIG_INCONSISTENT .....	686
125.12 RPR_LAGGCONFIG_INCONSISTENT_OVER .....	687
125.13 RPR_MISCABLING .....	687
125.14 RPR_MISCABLING_OVER .....	687
125.15 RPR_PROTECTION_INCONSISTENT.....	688
125.16 RPR_PROTECTION_INCONSISTENT_OVER.....	688
125.17 RPR_SEC_MAC_DUPLICATE.....	688
125.18 RPR_SEC_MAC_DUPLICATE_OVER .....	689
125.19 RPR_TOPOLOGY_INCONSISTENT .....	689
125.20 RPR_TOPOLOGY_INCONSISTENT_OVER.....	689
125.21 RPR_TOPOLOGY_INSTABILITY.....	690
125.22 RPR_TOPOLOGY_INSTABILITY_OVER .....	690
125.23 RPR_TOPOLOGY_INVALID .....	690
125.24 RPR_TOPOLOGY_INVALID_OVER.....	691
<b>126 RRPP .....</b>	<b>691</b>
126.1 RRPP_IPP_CHECK.....	691
126.2 RRPP_RING_FAIL.....	691
126.3 RRPP_RING_RESTORE.....	692
<b>127 RTM .....</b>	<b>692</b>
127.1 RTM_EMAIL_SUCCESS .....	692
127.2 RTM_EMAIL_FAILED .....	693
127.3 RTM_ENVIRONMENT.....	693
127.4 RTM_TCL_LOAD_FAILED .....	694
127.5 RTM_TCL_MODIFY.....	694
127.6 RTM_TCL_NOT_EXIST .....	694
<b>128 SAVA.....</b>	<b>694</b>
128.1 SAVA_SET_DRV_FAILED .....	695
128.2 SAVA_SPOOFING_DETECTED.....	695
<b>129 SAVI.....</b>	<b>695</b>
129.1 SAVI_FILTER_ENTRY_ADD.....	696
129.2 SAVI_FILTER_ENTRY_DEL .....	696
129.3 SAVI_SPOOFING_DETECTED .....	697

<b>130 SCMD</b> .....	<b>697</b>
130.1 PROCESS_ABNORMAL .....	698
130.2 PROCESS_ACTIVEFAILED.....	698
130.3 PROCESS_CORERECORD .....	699
130.4 SCM_ABNORMAL_REBOOT.....	699
130.5 SCM_ABNORMAL_REBOOTMDC .....	700
130.6 SCM_ABORT_RESTORE .....	700
130.7 SCM_INSMOD_ADDON_TOOLONG.....	701
130.8 SCM_KERNEL_INIT_TOOLONG.....	701
130.9 SCM_KILL_PROCESS .....	702
130.10 SCM_PROCESS_HEALTHY .....	702
130.11 SCM_PROCESS_STARTING_TOOLONG .....	703
130.12 SCM_PROCESS_STILL_STARTING.....	704
130.13 SCM_PROCESS_UNHEALTHY.....	704
130.14 SCM_SKIP_PROCESS .....	705
<b>131 SCRLSP</b> .....	<b>705</b>
131.1 SCRLSP_LABEL_DUPLICATE .....	705
<b>132 SESSION</b> .....	<b>706</b>
132.1 SESSION_IPV4_FLOW .....	707
132.2 SESSION_IPV6_FLOW .....	709
<b>133 SFLOW</b> .....	<b>710</b>
133.1 SFLOW_HARDWARE_ERROR .....	710
<b>134 SHELL</b> .....	<b>710</b>
134.1 SHELL_CMD.....	710
134.2 SHELL_CMD_CONFIRM.....	711
134.3 SHELL_CMD_EXECUTEFAIL.....	711
134.4 SHELL_CMD_INPUT.....	712
134.5 SHELL_CMD_INPUT_TIMEOUT .....	712
134.6 SHELL_CMD_INVALID_CHARACTER.....	713
134.7 SHELL_CMD_MATCHFAIL .....	713
134.8 SHELL_CMDDENY.....	713
134.9 SHELL_CMDFAIL .....	714
134.10 SHELL_COMMIT .....	714
134.11 SHELL_COMMIT_DELAY .....	714
134.12 SHELL_COMMIT_REDELAY .....	715
134.13 SHELL_COMMIT_ROLLBACK.....	715

134.14	SHELL_COMMIT_ROLLBACKDONE .....	715
134.15	SHELL_COMMIT_WILLROLLBACK .....	716
134.16	SHELL_CRITICAL_CMDFAIL .....	716
134.17	SHELL_LOGIN.....	716
134.18	SHELL_LOGOUT.....	717
<b>135</b>	<b>SLSP .....</b>	<b>717</b>
135.1	SLSP_LABEL_DUPLICATE .....	717
<b>136</b>	<b>SMARTMC .....</b>	<b>717</b>
136.1	ERROR .....	718
<b>137</b>	<b>SMLK .....</b>	<b>718</b>
137.1	SMLK_PORT_INACTIVE.....	718
137.2	SMLK_LINK_SWITCH .....	719
<b>138</b>	<b>SNMP .....</b>	<b>719</b>
138.1	SNMP_ACL_RESTRICTION .....	719
138.2	SNMP_AUTHENTICATION_FAILURE.....	719
138.3	SNMP_GET .....	720
138.4	SNMP_INFORM_LOST .....	720
138.5	SNMP_NOTIFY.....	721
138.6	SNMP_SET .....	722
138.7	SNMP_USM_NOTINTIMEWINDOW .....	722
<b>139</b>	<b>SOCKET .....</b>	<b>722</b>
139.1	SOCKET_TCP_UNREAD.....	723
<b>140</b>	<b>SSHC .....</b>	<b>723</b>
140.1	SSHC_ALGORITHM_MISMATCH .....	723
140.2	SSHC_AUTH_PASSWORD_FAIL.....	724
140.3	SSHC_AUTH_PUBLICKEY_FAIL .....	724
140.4	SSHC_CERT_VERIFY_FAIL.....	725
140.5	SSHC_CONNECT_FAIL.....	726
140.6	SSHC_DECRYPT_FAIL .....	727
140.7	SSHC_DISCONNECT .....	727
140.8	SSHC_ENCRYPT_FAIL .....	727
140.9	SSHC_HOST_NAME_ERROR.....	728
140.10	SSHC_KEY_EXCHANGE_FAIL .....	728
140.11	SSHC_MAC_ERROR .....	728
140.12	SSHC_PUBLICKEY_NOT_EXIST.....	729

140.13 SSHC_VERSION_MISMATCH.....	729
<b>141 SSSH.....</b>	<b>729</b>
141.1 SSSH_ACL_DENY .....	729
141.2 SSSH_ALGORITHM_MISMATCH.....	730
141.3 SSSH_AUTH_EXCEED_RETRY_TIMES .....	730
141.4 SSSH_AUTH_FAIL .....	731
141.5 SSSH_AUTH_KBDINT_FAIL.....	731
141.6 SSSH_AUTH_PWD_FAIL .....	732
141.7 SSSH_AUTH_SUCCESS.....	732
141.8 SSSH_AUTH_TIMEOUT .....	732
141.9 SSSH_AUTHOR_FAIL .....	733
141.10 SSSH_CERT_VERIFY_FAIL.....	734
141.11 SSSH_CONNECT.....	735
141.12 SSSH_DECRYPT_FAIL .....	736
141.13 SSSH_DISCONNECT .....	736
141.14 SSSH_ENCRYPT_FAIL .....	736
141.15 SSSH_LOG.....	737
141.16 SSSH_MAC_ERROR .....	737
141.17 SSSH_REACH_SESSION_LIMIT .....	738
141.18 SSSH_REACH_USER_LIMIT .....	738
141.19 SSSH_SCP_OPER.....	738
141.20 SSSH_SFTP_OPER.....	739
141.21 SSSH_SRV_UNAVAILABLE .....	739
141.22 SSSH_VERSION_MISMATCH.....	740
<b>142 STAMGR.....</b>	<b>740</b>
142.1 STAMGR_ADD_FAILVLAN .....	740
142.2 STAMGR_ADDBAC_INFO.....	740
142.3 STAMGR_ADDSTA_INFO .....	741
142.4 STAMGR_AUTHORACL_FAILURE .....	741
142.5 STAMGR_AUTHORUSERPROFILE_FAILURE.....	742
142.6 STAMGR_CLIENT_OFFLINE.....	742
142.7 STAMGR_CLIENT_ONLINE .....	742
142.8 STAMGR_DELBAC_INFO.....	743
142.9 STAMGR_DELSTA_INFO .....	743
142.10 STAMGR_DOT1X_LOGIN_FAILURE .....	743
142.11 STAMGR_DOT1X_LOGIN_SUCC .....	744

142.12	STAMGR_DOT1X_LOGOFF	744
142.13	STAMGR_MACA_LOGIN_FAILURE	745
142.14	STAMGR_MACA_LOGIN_SUCC	745
142.15	STAMGR_MACA_LOGOFF	746
142.16	STAMGR_STAIPCHANGE_INFO	746
142.17	STAMGR_TRIGGER_IP	747
<b>143</b>	<b>STM</b>	<b>747</b>
143.1	STM_AUTO_UPDATE_FAILED	748
143.2	STM_AUTO_UPDATE_FINISHED	749
143.3	STM_AUTO_UPDATING	749
143.4	STM_HELLOPKT_NOTSEND	750
143.5	STM_HELLOPKT_NOTRCV	750
143.6	STM_LINK_DOWN	750
143.7	STM_LINK_TIMEOUT	751
143.8	STM_LINK_UP	751
143.9	STM_MERGE	751
143.10	STM_MERGE_NEED_REBOOT	752
143.11	STM_MERGE_NOT_NEED_REBOOT	752
143.12	STM_PHY_DOWN	752
143.13	STM_PHY_UP	753
143.14	STM_SAMEMAC	753
143.15	STM_SOMER_CHECK	753
<b>144</b>	<b>STP</b>	<b>753</b>
144.1	STP_BPDU_PROTECTION	754
144.2	STP_BPDU_RECEIVE_EXPIRY	754
144.3	STP_CONSISTENCY_CHECK	754
144.4	STP_CONSISTENCY_RESTITUTION	755
144.5	STP_DETECTED_TC	755
144.6	STP_DISABLE	755
144.7	STP_DISCARDING	756
144.8	STP_DISPUTE	756
144.9	STP_DISPUTE_RESTITUTION	756
144.10	STP_EDGEPORT_INACTIVE	757
144.11	STP_ENABLE	757
144.12	STP_FORWARDING	757
144.13	STP_LOOP_PROTECTION	758



144.14 STP_LOOPBACK_PROTECTION.....	758
144.15 STP_NOT_ROOT .....	758
144.16 STP_NOTIFIED_TC .....	759
144.17 STP_PORT_TYPE_INCONSISTENCY.....	759
144.18 STP_PVID_INCONSISTENCY .....	759
144.19 STP_PVST_BPDU_PROTECTION.....	760
144.20 STP_ROOT_PROTECTION .....	760
144.21 STP_STG_NUM_DETECTION.....	760
<b>145 SYSEVENT .....</b>	<b>761</b>
145.1 EVENT_TIMEOUT .....	761
<b>146 SYSLOG .....</b>	<b>761</b>
146.1 SYSLOG_LOGBUFFER_FAILURE .....	761
146.2 SYSLOG_LOGFILE_CREATE .....	762
146.3 SYSLOG_LOGFILE_FULL .....	762
146.4 SYSLOG_LOGFILE_OVERWRITE .....	762
146.5 SYSLOG_NO_SPACE.....	763
146.6 SYSLOG_RESTART .....	763
146.7 SYSLOG_RTM_EVENT_BUFFER_FULL .....	763
146.8 SYSLOG_START.....	764
<b>147 TACACS.....</b>	<b>764</b>
147.1 TACACS_ACCT_SERVER_DOWN .....	764
147.2 TACACS_ACCT_SERVER_UP.....	765
147.3 TACACS_AUTH_FAILURE .....	765
147.4 TACACS_AUTH_SERVER_DOWN .....	766
147.5 TACACS_AUTH_SERVER_UP.....	766
147.6 TACACS_AUTH_SUCCESS .....	767
147.7 TACACS_AUTHOR_SERVER_DOWN.....	767
147.8 TACACS_AUTHOR_SERVER_UP .....	768
147.9 TACACS_REMOVE_SERVER_FAIL .....	768
<b>148 TCSM.....</b>	<b>768</b>
148.1 TCSM_CERT_BROKEN.....	769
148.2 TCSM_KEY_BROKEN .....	769
148.3 TCSM_KEY_HIERARCHY_BROKEN .....	769
148.4 TCSM_TSS_SVC_DOWN.....	770
148.5 TCSM_TSS_SVC_UP .....	770

<b>149 TELNETD</b> .....	<b>770</b>
149.1 TELNETD_ACL_DENY.....	770
149.2 TELNETD_REACH_SESSION_LIMIT.....	771
<b>150 TRACK</b> .....	<b>771</b>
150.1 TRACK_STATE_CHANGE.....	771
<b>151 TRILL</b> .....	<b>772</b>
151.1 TRILL_DUP_SYSTEMID .....	772
151.2 TRILL_INTF_CAPABILITY .....	772
151.3 TRILL_LICENSE_EXPIRED.....	773
151.4 TRILL_LICENSE_EXPIRED_TIME .....	773
151.5 TRILL_LICENSE_UNAVAILABLE .....	773
151.6 TRILL_MEM_ALERT .....	774
151.7 TRILL_NBR_CHG.....	774
<b>152 VCF</b> .....	<b>774</b>
152.1 VCF_AGGR_CREAT .....	775
152.2 VCF_AGGR_DELETE .....	775
152.3 VCF_AGGR_FAILED.....	776
152.4 VCF_AUTO_ANALYZE_USERDEF .....	776
152.5 VCF_AUTO_NO_USERDEF .....	777
152.6 VCF_AUTO_START .....	777
152.7 VCF_AUTO_STATIC_CMD.....	778
152.8 VCF_BGP .....	778
152.9 VCF_DOWN_LINK.....	779
152.10 VCF_DRIVER_INIT .....	779
152.11 VCF_FAILED_ADD_IRFPORT.....	779
152.12 VCF_GET_IMAGE .....	780
152.13 VCF_GET_TEMPLATE .....	780
152.14 VCF_INSTALL_IMAGE.....	781
152.15 VCF_IRF_FINISH .....	781
152.16 VCF_IRF_FOUND .....	782
152.17 VCF_IRF_START .....	782
152.18 VCF_LOOPBACK_START .....	783
152.19 VCF_LOOPBACK_START_FAILED.....	783
152.20 VCF_LOOPBACK_ALLOC .....	784
152.21 VCF_LOOPBACK_NO_FREE_IP.....	784
152.22 VCF_LOOPBACK_RECLAIM.....	785

152.23 VCF_REBOOT.....	785
152.24 VCF_SKIP_INSTALL .....	786
152.25 VCF_STATIC_CMD_ERROR.....	786
152.26 VCF_UP_LINK.....	786
152.27 VCF_WHITE_LIST_CHECK.....	787
<b>153 VLAN.....</b>	<b>787</b>
153.1 VLAN_CREATEFAIL .....	787
153.2 VLAN_FAILED .....	787
153.3 VLAN_QINQETHTYPE_FAILED .....	788
153.4 VLAN_VLANMAPPING_FAILED.....	788
153.5 VLAN_VLANTRANSPARENT_FAILED.....	788
<b>154 VRRP .....</b>	<b>788</b>
154.1 VRRP_STATUS_CHANGE .....	789
154.2 VRRP_VF_STATUS_CHANGE.....	790
154.3 VRRP_VMAC_INEFFECTIVE .....	790
<b>155 VSRP .....</b>	<b>790</b>
155.1 VSRP_BIND_FAILED .....	791
<b>156 VXLAN .....</b>	<b>791</b>
156.1 VXLAN_LICENSE_UNAVAILABLE .....	791
<b>157 WEB.....</b>	<b>791</b>
157.1 LOGIN.....	792
157.2 LOGIN_FAILED .....	792
157.3 LOGOUT .....	792
<b>158 WIPS .....</b>	<b>792</b>
158.1 APFLOOD.....	793
158.2 AP_CHANNEL_CHANGE.....	793
158.3 ASSOCIATEOVERFLOW .....	793
158.4 HONEYPOT .....	794
158.5 HTGREENMODE.....	794
158.6 MAN_IN_MIDDLE .....	794
158.7 WIPS_DOS .....	795
158.8 WIPS_FLOOD.....	795
158.9 WIPS_MALF .....	796
158.10 WIPS_SPOOF .....	797
158.11 WIPS_WEAKIV.....	797



# 1 简介

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

除了 UNIS S12600-G 特有的日志信息外，本文还包含 UNIS S12600-G Release R7743PXX 版本基于的 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 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： $facility \times 8 + severity$ <ul style="list-style-type: none"><li>• <b>facility</b> 表示日志主机的记录工具，由 <b>info-center loghost</b> 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。</li><li>• <b>severity</b> 表示日志信息的严重等级，具体含义请参见<a href="#">表 1-2</a></li></ul>
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 <ul style="list-style-type: none"><li>• 百分号（%）：表示该日志信息为 <b>Informational</b> 级别及以上级别的日志</li><li>• 星号（*）：表示该日志信息为 <b>Debug</b> 级别的日志</li></ul>
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 <ul style="list-style-type: none"><li>• 日志主机方向：时间戳精确到秒，用户可以通过 <b>info-center timestamp loghost</b> 命令自定义时间显示格式</li><li>• 非日志主机方向：时间戳精确到毫秒，用户可以通过 <b>info-center timestamp</b> 命令自定义时间显示格式</li></ul>
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 <a href="#">表 1-2</a>
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：

字段	描述
	<ul style="list-style-type: none"> <li>• -MDC=XX, 表示生成该日志的 MDC 的编号</li> <li>• -DevIp=XXX.XXX.XXX.XXX, 表示日志发送者的源 IP</li> <li>• -Slot=XX, 表示生成该日志的 Slot 编号</li> <li>• -Chassis=XX-Slot=XX, 表示生成该日志的 Chassis 编号和 Slot 编号</li> </ul> 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 <a href="#">表1-3</a> 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 日志重性等级说明

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

本文使用[表 1-3](#)定义的方式表示日志描述字段中的可变参数域。

表1-3 可变参数域

参数标识	参数类型
INT16	有符号的16位整数
UINT16	无符号的16位整数
INT32	有符号的32位整数
UINT32	无符号的32位整数
INT64	有符号的64位整数
UINT64	无符号的64位整数

参数标识	参数类型
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 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”。

### 1.2.1 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。

### 1.2.2 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。

### 1.2.3 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。

## 1.2.4 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。

## 1.2.5 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。

## 1.3 软件模块列表

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

表1-4 软件模块列表

模块名	模块全称
AAA	Authentication, Authorization and Accounting
ACL	Access Control List
ANCP	Access Node Control Protocol
APMGR	Access Point Management
ARP	Address Resolution Protocol
ATK	ATK Detect and Defense
ATM	Asynchronous Transfer Mode
BFD	Bidirectional Forwarding Detection
BGP	Border Gateway Protocol
BLS	Blacklist
CFD	Connectivity Fault Detection
CFGMAN	Configuration Management
CONNLMT	Connect Limit
DEV	Device Management



模块名	模块全称
DHCP	Dynamic Host Configuration Protocol
DHCPR	IPv4 DHCP Relay
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
DRNI	Distributed Resilient Network Interconnect
EDEV	Extender Device Management
ERPS	Ethernet Ring Protection Switching
ETH	Ethernet
ETHDRNI	Ethernet Distributed Resilient Network Interconnect
ETHOAM	Ethernet Operation, Administration and Maintenance
EVB	Ethernet Virtual Bridging
EVIISIS	Ethernet Virtual Interconnect Intermediate System-to-Intermediate System
FCOE	Fibre Channel Over Ethernet
FCLINK	Fibre Channel Link
FCZONE	Fibre Channel Zone
FIB	Forwarding Information Base
FILTER	Filter
FIPSNG	FIP Snooping
FS	File System
FTP	File Transfer Protocol
gRPC	Google Remote Procedure Call
HA	High Availability
HQOS	Hierarchical QoS
HTTPD	Hypertext Transfer Protocol Daemon
HLTH	Health
IFNET	Interface Net Management
IKE	Internet Key Exchange
iNQA	Intelligent Network Quality Analyzer
IMA	Integrity Measurements Architecture

模块名	模块全称
IP6ADDR	IPv6 address
IP6FW	IPv6 Forwarding
IPADDR	IP address
IPFW	IP Forwarding
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
L2PT	Layer 2 Protocol Tunneling
L2TPV2	Layer 2 Tunneling Protocol Version 2
L2VPN	Layer 2 VPN
LAGG	Link Aggregation
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
MTLK	Monitor Link
NAT	Network Address Translate
NETCONF	Network Configuration Protocol
ND	Neighbor Discovery

模块名	模块全称
NQA	Network Quality Analyzer
NSS	Session-based NetStream
NTP	Network Time Protocol
OAP	Open Application Platform
OPENSRC(FreeRADIUS)	Open Source
OBJP	Object Policy
OFPP	OpenFlow Protocol
OPTMOD	Optical Module
OSPF	Open Shortest Path First
OSPFV3	Open Shortest Path First Version 3
PFILTER	Packet Filter
PBB	Provider Backbone Bridge
PBR	Policy Based Route
PCE	Path Computation Element
PEX	Port Extender
PIM	Protocol Independent Multicast
PING	Packet Internet Groper
PKG	Package
PKI	Public Key Infrastructure
PKT2CPU	Packet to CPU
PKTCPT	Packet Capture
PoE	Power over Ethernet
PORTAL	Portal
PORTSEC	Port Security
PPP	Point to Point Protocol
PTP	Precision Time Protocol
PTS	Platform Trust Services
PWDCTL	Password Control
QOS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RESMON	RESOURCE MONITER
RDDC	Redundancy
RIP	Routing Information Protocol
RIPNG	Routing Information Protocol Next Generation
RM	Routing Management

模块名	模块全称
RPR	Resilient Packet Ring
RRPP	Rapid Ring Protect Protocol
RTM	Real-Time Management
SCMD	Service Control Manager
SCRLSP	Static CRLSP
SESSION	Session
SFLOW	Sampler Flow
SHELL	Shell
SLSP	Static LSP
SMARTMC	Smart Management Center
SMLK	Smart Link
SNMP	Simple Network Management Protocol
SSHC	Secure Shell Client
SSHS	Secure Shell Server
STAMGR	Station Management
STM	Stack Topology Management
STP	Spanning Tree Protocol
SYSEVENT	System Event
SYSLOG	System Log
TCSM	Trusted Computing Services Management
TACACS	Terminal Access Controller Access Control System
TELNETD	Telnet Daemon
TRILL	Transparent Interconnect of Lots of Links
TSTREAM	Telemetry Stream
VCF	Vertical Converged Framework
VLAN	Virtual Local Area Network
VRRP	Virtual Router Redundancy Protocol
VSRP	Virtual Service Redundancy Protocol
VXLAN	Virtual eXtensible LAN
WEB	Web
WIPS	Wireless Intrusion Prevention System

## 1.4 文档使用说明

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

本文以表格的形式对日志信息进行介绍。有关表中各项的含义请参考[表 1-5](#)。

表1-5 日志信息表内容说明

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

## 2 AAA

本节介绍 AAA 模块输出的日志信息。

## 2.1 AAA\_FAILURE

日志内容	-AAAType=[STRING]-AAADomain=[STRING]-Service=[STRING]-UserName=[STRING]; AAA failed.
参数解释	\$1: AAA类型 \$2: AAA方案 \$3: 服务 \$4: 用户名称
日志等级	5
举例	AAA/5/AAA_FAILURE: -AAAType=AUTHOR-AAADomain=domain1-Service=login-UserName=cwf@system; AAA failed.
日志说明	由于未收到服务器响应, 用户名/密码错误, 或其他原因(例如用户申请的服务类型不正确), 用户的AAA请求被拒绝
处理建议	<ul style="list-style-type: none"><li>• 检查设备与服务器的连接</li><li>• 重新输入用户名和密码</li><li>• 检查服务器上的设置(例如服务类型)是否正确</li></ul>

## 2.2 AAA\_LAUNCH

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

## 2.3 AAA\_SUCCESS

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

# 3 ACL

本节介绍 ACL 模块输出的日志信息。

## 3.1 ACL\_ACCELERATE\_NO\_RES

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

## 3.2 ACL\_ACCELERATE\_NONCONTIGUOUSMASK

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

## 3.3 ACL\_ACCELERATE\_NOT\_SUPPORT

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

## 3.4 ACL\_ACCELERATE\_NOT\_SUPPORTHOPBYHOP

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



### 3.5 ACL\_ACCELERATE\_NOT\_SUPPORTMULTITCPFLAG

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

### 3.6 ACL\_ACCELERATE\_UNK\_ERR

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

### 3.7 ACL\_IPV6\_STATIS\_INFO

日志内容	IPv6 ACL [UINT32] [STRING] [UINT64] packet(s).
参数解释	\$1: ACL编号 \$2: IPv6 ACL规则的ID及内容 \$3: 匹配上规则的报文个数
日志等级	6
举例	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

## 3.8 ACL\_NO\_MEM

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

## 3.9 ACL\_STATIS\_INFO

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

# 4 ANCP

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

## 4.1 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

# 5 APMGR

本节介绍 AP 管理模块输出的日志信息。

## 5.1 APMGR\_AC\_MEM\_ALERT

日志内容	The memory utilization has reached the threshold.
参数解释	无
日志等级	4
举例	APMGR/4/APMGR_AC_MEM_ALERT: The memory utilization 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

## 5.2 APMGR\_ADD\_AP\_FAIL

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

## 5.3 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

## 5.4 APMGR\_AP\_OFFLINE

日志内容	AP [STRING] went offline. State changed to Idle.
参数解释	\$1: AP的名称
日志等级	6
举例	APMGR/6/APMGR_AP_OFFLINE: AP ap1 went offline. State changed to Idle.
日志说明	AP下线，状态变为Idle状态
处理建议	<ul style="list-style-type: none"><li>若 AP 主动下线，则不用排查问题</li><li>若 AP 异常下线，需要根据调试信息定位并解决问题</li></ul>

## 5.5 APMGR\_AP\_ONLINE

日志内容	AP [STRING] went online. State changed to Run.
参数解释	\$1: AP的名称
日志等级	6
举例	APMGR/6/APMGR_AP_ONLINE: AP ap1 went 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

## 5.6 APMGR\_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	APMGR/6/APMGR_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

## 5.7 APMGR\_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	APMGR/6/APMGR_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

## 5.8 APMGR\_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	APMGR/6/APMGR_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

## 5.9 APMGR\_CWC\_LOCAL\_AC\_DOWN

日志内容	CAPWAP tunnel to Central AC [STRING] went down. Reason: [STRING].
参数解释	<p>\$1: Central AC的IP地址</p> <p>\$2: 隧道断开的原因</p> <ul style="list-style-type: none"><li>Added local AC IP address: 添加新的 Local AC IP 地址</li><li>Deleted local AC IP address: Local AC IP 地址被删除</li><li>Local AC interface used for CAPWAP tunnel went down: CAPWAP 隧道使用的 Local AC 接口 DOWN</li><li>Local AC config changed: Local AC 配置改变</li><li>N/A: 不涉及</li></ul>
日志等级	4
举例	APMGR/4/APMGR_CWC_LOCAL_AC_DOWN: CAPWAP tunnel to Central AC 2.2.2.1 went down. Reason: Added local AC IP address.
日志说明	Central AC与Local AC之间隧道断开及断开原因
处理建议	<ul style="list-style-type: none"><li>检查 Central AC 与 Local AC 的连接是否正常</li><li>检查 Central AC 上的配置</li><li>检查 Local AC 上的配置</li></ul>

## 5.10 APMGR\_CWC\_LOCAL\_AC\_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	APMGR/6/APMGR_CWC_LOCAL_AC_UP: CAPWAP tunnel to Central AC 2.2.2.1 went up.
日志说明	Central AC与Local AC建立CAPWAP隧道
处理建议	无

## 5.11 APMGR\_CWC\_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 <ul style="list-style-type: none"><li>• AP was reset: AP 重启</li><li>• Image was downloaded successfully: 版本文件下载成功</li><li>• Stayed in idle state for a long time: 长时间处于 idle 状态</li></ul>
日志等级	6
举例	APMGR/6/APMGR_CWC_REBOOT: AP in State Run is rebooting. Reason: AP was reset.
日志说明	AP重启及重启原因
处理建议	无

## 5.12 APMGR\_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	APMGR/6/APMGR_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

## 5.13 APMGR\_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	APMGR/6/APMGR_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

## 5.14 APMGR\_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	APMGR/6/APMGR_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



## 5.15 APMGR\_CWC\_TUNNEL\_DOWN

日志内容	CAPWAP tunnel to AC [STRING] went down. Reason: [STRING].
参数解释	<p>\$1: AC的IP地址</p> <p>\$2: 隧道断开原因</p> <ul style="list-style-type: none"> <li>• Added AP IP address: 添加新的 AP IP 地址</li> <li>• Deleted AP IP address: AP IP 地址被删除</li> <li>• AP interface used for CAPWAP tunnel went down: CAPWAP 隧道使用的 AP 接口 DOWN</li> <li>• AP config changed: AP 配置改变</li> <li>• AP was reset: AP 重启</li> <li>• Number of echo retransmission attempts exceeded the limit: 超过 echo 报文重传次数</li> <li>• Full retransmission queue: 重传队列满</li> <li>• Data channel timer expired: 数据隧道定时器超时</li> <li>• Backup AC IP address changed: 备 AC IP 地址改变</li> <li>• Backup tunnel changed to master tunnel: 备隧道切换成主隧道</li> <li>• Failed to change backup tunnel to master tunnel: 备切主失败</li> <li>• Backup method changed: 备份模式改变</li> <li>• N/A: 不涉及</li> </ul>
日志等级	6
举例	APMGR/6/APMGR_CWC_TUNNEL_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

## 5.16 APMGR\_CWC\_TUNNEL\_UP

日志内容	[STRING] CAPWAP tunnel to AC [STRING] went up.
参数解释	<p>\$1: 与AC连接的隧道的主备类型</p> <ul style="list-style-type: none"> <li>○ Master: 主隧道</li> <li>○ Backup: 备隧道</li> </ul> <p>\$2: AC的IP地址</p>
日志等级	6
举例	APMGR/6/APMGR_CWC_TUNNEL_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

## 5.17 APMGR\_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	APMGR/6/APMGR_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

## 5.18 APMGR\_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	APMGR/6/APMGR_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

## 5.19 APMGR\_CWS\_LOCAL\_AC\_DOWN

日志内容	CAPWAP tunnel to local AC [STRING] went down. Reason: [STRING].
参数解释	<p>\$1: Local AC的IP地址</p> <p>\$2: 隧道断开的原因:</p> <ul style="list-style-type: none"><li>○ Neighbor dead timer expired: 邻居截止定时器超时</li><li>○ Local AC was deleted: Local AC 被删除</li><li>○ Serial number changed: 序列号改变</li><li>○ Processed join request in Run state: 在 Run 状态下处理 join request 报文</li><li>○ Failed to retransmit message: 处理重传消息失败</li><li>○ N/A: 不涉及</li></ul>
日志等级	4
举例	APMGR/4/APMGR_CWS_LOCAL_AC_DOWN: CAPWAP tunnel to local AC 1.1.1.1 went down. Reason: Serial number changed.
日志说明	Central AC与Local AC之间隧道断开及断开原因
处理建议	<ul style="list-style-type: none"><li>• 检查 Central AC 与 Local AC 的连接是否正常</li><li>• 检查 Central AC 上的配置</li><li>• 检查 Local AC 上的配置</li></ul>

## 5.20 APMGR\_CWS\_LOCAL\_AC\_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	APMGR/6/APMGR_CWS_LOCAL_AC_UP: CAPWAP tunnel to local AC 1.1.1.1 went up.
日志说明	Central AC与 Local AC建立CAPWAP隧道
处理建议	无

## 5.21 APMGR\_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	APMGR/6/APMGR_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

## 5.22 APMGR\_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	APMGR/6/APMGR_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

## 5.23 APMGR\_CWS\_TUNNEL\_DOWN

日志内容	CAPWAP tunnel to AP [STRING] went down. Reason: [STRING].
参数解释	<p>\$1: AC端配置的AP名称</p> <p>\$2: 隧道断开原因</p> <ul style="list-style-type: none"> <li>Neighbor dead timer expired: 邻居截止定时器超时</li> <li>AP was reset: AP 重启</li> <li>AP was deleted: AP 被删除</li> <li>Serial number changed: 序列号改变</li> <li>Processed join request in Run state: 在 Run 状态下处理 join request 报文</li> <li>Failed to retransmit message: 处理重传消息失败</li> <li>Received WTP tunnel down event from AP: 接收到来自 AP 的 WTP DOWN 隧道事件</li> <li>Backup AC closed the backup tunnel: 备 AC DOWN 自身的隧道</li> <li>Tunnel switched: 由于隧道切换</li> <li>N/A: 不涉及</li> </ul>
日志等级	6
举例	APMGR/6/APMGR_CWS_TUNNEL_DOWN: CAPWAP tunnel to AP ap1 went down. Reason: AP was reset.
日志说明	AP下线及下线原因
处理建议	<ul style="list-style-type: none"> <li>检查设备 AP 与设备 AC 的连接是否正常</li> <li>检查 AP 上的配置</li> <li>检查 AC 上的配置</li> </ul>

## 5.24 APMGR\_CWS\_TUNNEL\_UP

日志内容	[STRING] CAPWAP tunnel to AP [STRING] went up.
参数解释	<p>\$1: 与AP连接的隧道的主备类型</p> <ul style="list-style-type: none"> <li>Master: 主隧道</li> <li>Backup: 备隧道</li> </ul> <p>\$2: AP名称</p>
日志等级	6
举例	APMGR/6/APMGR_CWS_TUNNEL_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

## 5.25 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

## 5.26 APMGR\_LOCAL\_AC\_OFFLINE

日志内容	Local AC [STRING] went offline. State changed to Idle.
参数解释	\$1: Local AC的名称
日志等级	6
举例	APMGR/6/APMGR_LOCAL_AC_OFFLINE: Local AC ac1 went offline. State changed to Idle.
日志说明	Local AC下线, 状态变为Idle状态
处理建议	<ul style="list-style-type: none"><li>若 Local AC 主动下线, 则不用排查问题</li><li>若 Local AC 异常下线, 需要根据调试信息定位并解决问题</li></ul>

## 5.27 APMGR\_LOCAL\_AC\_ONLINE

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

# 6 ARP

本节介绍 ARP 模块输出的日志信息。

## 6.1 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 Ethernet0/1/0.
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	<ol style="list-style-type: none"><li>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）</li><li>2. 请联系技术支持</li></ol>

## 6.2 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

## 6.3 ARP\_BINDRULETOHW\_FAILED

日志内容	Failed to download binding rule to hardware on the interface [STRING], SrcIP [IPADDR], SrcMAC [MAC], VLAN [UINT16], Gateway MAC [MAC].
参数解释	\$1: 接口名称. \$2: 源IP地址 \$3: 源MAC地址. \$4: VLAN编号. \$5: 网关MAC地址.
日志等级	5
举例	ARP/5/ARP_BINDRULETOHW_FAILED: Failed to download binding rule to hardware on the interface Ethernet1/0/1, SrcIP 1.1.1.132, SrcMAC 0015-E944-A947, VLAN 1, Gateway MAC 00A1-B812-1108.
日志说明	由于硬件资源不足、内存不足或其他硬件错误导致绑定规则下发失败
处理建议	<ol style="list-style-type: none"> <li>1. 使用 <b>display qos-acl resource</b> 查看硬件 ACL 资源是否充足</li> <li>2. 如果充足，则请执行步骤 2</li> <li>3. 如果不充足，则请取消部分 ACL 配置或接受当前结果</li> <li>4. 使用 <b>display memory</b> 查看内存资源是否充足</li> <li>5. 如果充足，则请执行步骤 3</li> <li>6. 如果不充足，则请取消部分配置或接受当前结果</li> <li>7. 硬件发生错误，请取消最后一次相关配置，并重新尝试</li> </ol>

## 6.4 ARP\_DETECTION\_LOG

日志内容	Detected an ARP attack on interface [STRING]: IP [STRING], MAC [STRING], VLAN [STRING]. [UINT32] packet(s) dropped.
参数解释	\$1: 接口名称 \$2: IP 地址 \$3: MAC 地址 \$4: VLAN ID \$5: 丢弃的报文数
日志等级	5
举例	ARP/5/ARP_INSPECTION: -MDC=1; Detected an ARP attack on interface GigabitEthernet1/0/1: IP 1.1.1.1, MAC 1-1-1, VLAN 100. 2 packet(s) dropped.
日志说明	ARP Detection发现接口下连接的用户发起的攻击，并丢弃了该用户发送的报文
处理建议	检查攻击来源



## 6.5 ARP\_DUPLICATE\_IPADDR\_DETECT

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

## 6.6 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	ARP/6/ARP_DYNAMIC: The maximum number of dynamic ARP entries for the device reached.
日志说明	设备学到的ARP表项总数到达最大值
处理建议	不需处理

## 6.7 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	ARP/6/ARP_DYNAMIC_IF: The maximum number of dynamic ARP entries for interface GigabitEthernet1/0/1 reached.
日志说明	接口学到的ARP表项总数到达最大值
处理建议	无需处理

## 6.8 ARP\_DYNAMIC\_SLOT

日志内容	形式一： The maximum number of dynamic ARP entries for slot [INT32] reached. 形式二： The maximum number of dynamic ARP entries for chassis [INT32] slot [INT32] reached.
参数解释	形式一： \$1: slot编号 形式二： \$1: chassis编号 \$2: slot编号
日志等级	6
举例	ARP/6/ARP_DYNAMIC_SLOT: The maximum number of dynamic ARP entries for slot 2 reached.
日志说明	形式一： 指定slot学到的动态ARP表项数达到最大值 形式二： 指定chassis内slot上学到的动态ARP表项数达到最大值
处理建议	无需处理

## 6.9 ARP\_ENTRY\_CONFLICT

日志内容	The software entry for [STRING] on [STRING] and the hardware entry did not have the same [STRING].
参数解释	<p>\$1: IP地址</p> <p>\$2: VPN实例名。如果该ARP属于公网，显示为the public network</p> <p>\$3: 不一致的表项参数类型</p> <ul style="list-style-type: none"> <li>• MAC address: MAC 地址</li> <li>• output interface: ARP 表项的出接口</li> <li>• output port : ARP 表项的出端口</li> <li>• outermost layer VLAN ID: 第一层 VLAN 标签</li> <li>• second outermost layer VLAN ID: 第二层 VLAN 标签</li> <li>• VSI index: VSI 索引</li> <li>• link ID: VSI 出链路标识符</li> </ul>
日志等级	6
举例	<p>ARP/6/ARP_ENTRY_CONFLICT: The software entry for 1.1.1.1 on the VPN a and the hardware entry did not have the same MAC address, output port, VSI index, and link ID.</p> <p>ARP/6/ARP_ENTRY_CONFLICT: The software entry for 1.1.1.2 on the public network and the hardware entry did not have the same MAC address, output port, VSI index, and link ID.</p>
日志说明	ARP软件表项与硬件表项不一致，比如ARP表项的出接口
处理建议	不需要处理，ARP会主动重刷硬件表项

## 6.10 ARP\_ENTRY\_ENOUGHRESOURCE

日志内容	<p>Issued the software entry to the driver for IPv4 address [STRING] on VPN instance [STRING].</p> <p>Issued the software entry to the driver for IPv4 address [STRING] on the public network.</p>
参数解释	<p>\$1: IPv4地址</p> <p>\$2: VPN实例名。如果该ARP属于公网，该字段不显示</p>
日志等级	6
举例	<p>ARP/6/ARP_ENTRY_ENOUGHRESOURCE: Issued the software entry to the driver for IPv4 address 10.1.1.1 on VPN instance vpn_1.</p> <p>ARP/6/ARP_ENTRY_ENOUGHRESOURCE: Issued the software entry to the driver for IPv4 address 10.1.1.2 on the public network.</p>
日志说明	使用 <b>arp consistency-check enable</b> 命令开启ARP表项一致性检查功能后，如果根据ARP软件表项刷新驱动硬件表项成功，则输出本日志
处理建议	无

## 6.11 ARP\_ENTRY\_INCONSISTENT

日志内容	Inconsistent software and hardware ARP entries for IPv4 address [STRING] on VPN instance [STRING]. Inconsistent parameters: [STRING]. Inconsistent software and hardware ARP entries for IPv4 address [STRING] on the public network. Inconsistent parameters: [STRING].
参数解释	<p>\$1: IPv4地址</p> <p>\$2: VPN实例名。如果该ARP属于公网，该字段不显示</p> <p>\$3: 不一致的表项参数类型</p> <ul style="list-style-type: none"> <li>• MAC address: MAC 地址</li> <li>• output interface: ARP 表项的出接口</li> <li>• output port : ARP 表项的出端口</li> <li>• outermost layer VLAN ID: 第一层 VLAN 标签</li> <li>• second outermost layer VLAN ID: 第二层 VLAN 标签</li> <li>• VSI index: VSI 索引</li> <li>• link ID: VSI 出链路标识符</li> </ul>
日志等级	6
举例	<p>ARP/6/ARP_ENTRY_INCONSISTENT: Inconsistent software and hardware ARP entries for IPv4 address 10.1.1.1 on VPN instance vpn_1. Inconsistent parameters: MAC address, output port, VSI index, and link ID.</p> <p>ARP/6/ARP_ENTRY_INCONSISTENT: Inconsistent software and hardware ARP entries for IPv4 address 10.1.1.2 on the public network. Inconsistent parameters: MAC address, output port, VSI index, and link ID.</p>
日志说明	使用 <code>arp consistency-check enable</code> 命令开启ARP表项一致性检查功能后，如果设备检测到ARP软件表项与硬件表项不一致（比如ARP表项的出接口），则输出本日志
处理建议	不需要处理，ARP会主动根据ARP软件表项刷新驱动硬件表项

## 6.12 ARP\_ENTRY\_NORESOURCE

日志内容	Not enough hardware resources to issue the software entry to the driver for IPv4 address [STRING] on VPN instance [STRING]. Not enough hardware resources to issue the software entry to the driver for IPv4 address [STRING] on the public network.
参数解释	\$1: IPv4地址 \$2: VPN实例名。如果该ARP属于公网，该字段不显示
日志等级	6
举例	ARP/6/ARP_ENTRY_NORESOURCE: Not enough hardware resources to issue the software entry to the driver for IPv4 address 10.1.1.1 on VPN instance vpn_1. ARP/6/ARP_ENTRY_NORESOURCE: Not enough hardware resources to issue the software entry to the driver for IPv4 address 10.1.1.2 on the public network.
日志说明	使用 <code>arp consistency-check enable</code> 命令开启ARP表项一致性检查功能后，当ARP软件表项下发驱动时，如果驱动没有足够的ARP硬件表项资源，则输出此日志
处理建议	不需要处理，ARP会主动根据ARP软件表项刷新驱动硬件表项

## 6.13 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

## 6.14 ARP\_LOCALPROXY\_ENABLE\_FAILED

日志内容	Failed to enable local proxy ARP on interface [STRING].
参数解释	\$1: 接口名称
日志等级	4
举例	ARP/4/ARP_LOCALPROXY_ENABLE_FAILED: -MDC=1-Slot=2; Failed to enable local proxy ARP on interface VSI-interface 1.
日志说明	VSI虚接口下开启ARP本地代理失败。主控板设置成功、非主控板设置失败的情况下在相应非主控板打印
处理建议	<b>8.</b> 检查设备相应单板是否支持本功能; <b>9.</b> 确认设备的硬件资源是否充足

## 6.15 ARP\_PKTQUE\_ALERT

日志内容	The current size of the ARP_PKT queue has reached [UINT32]. Please check the network environment.
参数解释	\$1: ARP报文队列长度
日志等级	6
举例	ARP/6/ARP_PKTQUE_ALERT: The current size of ARP_PKT queue has reached 4096. Please check the network environment.
日志说明	当上送CPU的ARP报文队列长度超过4K时，系统将每隔60秒输出一次日志信息进行提示
处理建议	请检查异常报文来源

## 6.16 ARP\_RATE\_EXCEEDED

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

## 6.17 ARP\_RATELIMIT\_NOTSUPPORT

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

## 6.18 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

## 6.19 ARP\_SENDER\_MAC\_INVALID

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

## 6.20 ARP\_SENDER\_SMACCONFLICT

日志内容	Packet was discarded because its sender MAC address was the MAC address of the receiving interface. Interface: [STRING], sender IP: [STRING], target IP: [STRING].
参数解释	\$1: 接口名 \$2: 发送端IP地址 \$3: 目标IP地址
日志等级	6
举例	ARP/6/ ARP_SENDER_SMACCONFLICT: Packet discarded for the sender MAC address is the same as the receiving interface. Interface: GigabitEthernet1/0/1 sender IP: 1.1.2.2 target IP: 1.1.2.1,
日志说明	设备从接口GigabitEthernet1/0/1接收到的ARP报文中的源MAC和设备的MAC地址冲突
处理建议	无需处理



## 6.21 ARP\_SENDER\_SMACCONFLICT\_VSI

日志内容	Packet was discarded because its sender MAC address was the MAC address of the receiving interface. Interface: [STRING], sender IP: [STRING], target IP: [STRING], VSI index: [UINT32], link ID: [UINT32].
参数解释	\$1: 接口名 \$2: 发送端IP地址 \$3: 目标IP地址 \$4: VSI索引 \$5: link ID
日志等级	6
举例	ARP/6/ ARP_SENDER_SMACCONFLICT_VSI: Packet discarded for the sender MAC address is the same as the receiving interface. Interface: VSI3 sender IP: 1.1.2.2 target IP: 1.1.2.1, VSI Index: 2, Link ID: 0
日志说明	设备从VSI接口3接收到的ARP报文中的源MAC和设备的MAC地址冲突
处理建议	无需处理

## 6.22 ARP\_SRC\_MAC\_FOUND\_ATTACK

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

## 6.23 ARP\_SUP\_ENABLE\_FAILED

日志内容	Failed to enable ARP flood suppression on VSI [STRING].
参数解释	\$1: VSI名称
日志等级	4
举例	ARP/4/ARP_SUP_ENABLE_FAILED: -MDC=1; Failed to enable ARP flood suppression on VSI vna.
日志说明	在VSI内开启ARP泛洪抑制功能失败。本日志打印间隔时间为不低于2s, 若配置下发过快, 部分日志信息将不能输出
处理建议	<ol style="list-style-type: none"><li>1. 检查设备是否支持本功能;</li><li>2. 确认设备的硬件资源是否足够</li></ol>

## 6.24 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

## 6.25 ARP\_THRESHOLD\_REACHED

日志内容	The alarm threshold for dynamic ARP entry learning was reached on interface [STRING].
参数解释	\$1: 接口名称
日志等级	4
举例	ARP/4/ARP_THRESHOLD_REACHED: The alarm threshold for dynamic ARP entry learning was reached on interface GigabitEthernet1/0/1
日志说明	接口GigabitEthernet1/0/1学习的动态ARP表项个数到达了告警门限值
处理建议	检查该接口学习这么多ARP表项是否合理, 网络内是否存在攻击源

## 6.26 ARP\_USER\_DUPLICATE\_IPADDR\_DETECT

日志内容	Detected a user IP address conflict. New user (MAC [STRING], SVLAN [STRING], CVLAN [STRING]) on interface [STRING] and old user (MAC [STRING], SVLAN [STRING], CVLAN [STRING]) on interface [STRING] were using the same IP address [IPADDR].
参数解释	\$1: 新用户的MAC地址 \$2: 新用户所在的外层VLAN \$3: 新用户所在的内层VLAN \$4: 连接新用户的接口名称 \$5: 旧用户的MAC地址 \$6: 旧用户所在的外层VLAN \$7: 旧用户所在的内层VLAN \$8: 连接旧用户的接口名称 \$9: 终端用户的IP地址
日志等级	6
举例	ARP/6/ARP_USER_DUPLICATE_IPADDR_DETECT: Detected a user IP address conflict. New user (MAC 0010-2100-01e1, SVLAN 100, CVLAN 10) on interface GigabitEthernet1/0/1 and old user (MAC 0120-1e00-0102, SVLAN 100, CVLAN 10) on interface GigabitEthernet1/0/1 were using the same IP address 192.168.1.1.
日志说明	ARP检测到终端用户间IP地址冲突，某个新用户的IP地址和某个旧用户的IP地址冲突
处理建议	排查所有终端用户的IP地址，解决IP地址冲突问题

## 6.27 ARP\_USER\_MOVE\_DETECT

日志内容	Detected a user (IP address [IPADDR], MAC address [STRING]) moved to another interface. Before user move: interface [STRING], SVLAN [STRING], CVLAN [STRING]. After user move: interface [STRING], SVLAN [STRING], CVLAN [STRING].
参数解释	\$1: 迁移用户的IP地址 \$2: 迁移用户的MAC地址 \$3: 迁移前接口名称 \$4: 迁移前用户所在的外层VLAN \$5: 迁移前用户所在的内层VLAN \$6: 迁移后接口名称 \$7: 迁移后用户所在的外层VLAN \$8: 迁移后用户所在的内层VLAN
日志等级	6
举例	ARP/6/ARP_USER_MOVE_DETECT: Detected a user (IP address 192.168.1.1, MAC address 0010-2100-01e1) moved to another interface. Before user move: interface GigabitEthernet1/0/1, SVLAN 100, CVLAN 10. After user move: interface GigabitEthernet1/0/2, SVLAN 100, CVLAN 10.
日志说明	ARP检测到终端用户发生接口迁移动作
处理建议	使用 <b>display arp user-move record</b> 命令查看终端用户迁移信息，检查迁移是否合理

## 6.28 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 GigabitEthernet1/0/1, sourced from 0015-E944-A947.
日志说明	ARP检测到重复地址 接口收到ARP报文的发送端IP地址与该接口的IP地址重复
处理建议	修改IP地址配置

## 6.29 DUPIP

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

## 6.30 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 GigabitEthernet1/0/1, sourced from 0015-E944-A947.
日志说明	收到ARP报文中的发送端IP与VRRP虚拟IP地址冲突
处理建议	修改IP地址配置

# 7 ATK

本节介绍 ATK 模块输出的日志信息。

## 7.1 ATK\_ICMP\_ADDRMASK\_REQ

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

## 7.2 ATK\_ICMP\_ADDRMASK\_REQ\_RAW

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

## 7.3 ATK\_ICMP\_ADDRMASK\_REQ\_RAW\_SZ

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

## 7.4 ATK\_ICMP\_ADDRMASK\_REQ\_SZ

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



## 7.5 ATK\_ICMP\_ADDRMASK\_RPL

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

## 7.6 ATK\_ICMP\_ADDRMASK\_RPL\_RAW

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

## 7.7 ATK\_ICMP\_ADDRMASK\_RPL\_RAW\_SZ

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

## 7.8 ATK\_ICMP\_ADDRMASK\_RPL\_SZ

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

## 7.9 ATK\_ICMP\_ECHO\_REQ

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

## 7.10 ATK\_ICMP\_ECHO\_REQ\_RAW

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

## 7.11 ATK\_ICMP\_ECHO\_REQ\_RAW\_SZ

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

## 7.12 ATK\_ICMP\_ECHO\_REQ\_SZ

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

## 7.13 ATK\_ICMP\_ECHO\_RPL

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



## 7.14 ATK\_ICMP\_ECHO\_RPL\_RAW

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

## 7.15 ATK\_ICMP\_ECHO\_RPL\_RAW\_SZ

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

## 7.16 ATK\_ICMP\_ECHO\_RPL\_SZ

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

## 7.17 ATK\_ICMP\_FLOOD

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

## 7.18 ATK\_ICMP\_FLOOD\_SZ

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

## 7.19 ATK\_ICMP\_INFO\_REQ

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

## 7.20 ATK\_ICMP\_INFO\_REQ\_RAW

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

## 7.21 ATK\_ICMP\_INFO\_REQ\_RAW\_SZ

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

## 7.22 ATK\_ICMP\_INFO\_REQ\_SZ

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

## 7.23 ATK\_ICMP\_INFO\_RPL

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

## 7.24 ATK\_ICMP\_INFO\_RPL\_RAW

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

## 7.25 ATK\_ICMP\_INFO\_RPL\_RAW\_SZ

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

## 7.26 ATK\_ICMP\_INFO\_RPL\_SZ

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



## 7.27 ATK\_ICMP\_LARGE

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

## 7.28 ATK\_ICMP\_LARGE\_RAW

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

## 7.29 ATK\_ICMP\_LARGE\_RAW\_SZ

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

## 7.30 ATK\_ICMP\_LARGE\_SZ

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

## 7.31 ATK\_ICMP\_PARAPROBLEM

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

## 7.32 ATK\_ICMP\_PARAPROBLEM\_RAW

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

## 7.33 ATK\_ICMP\_PARAPROBLEM\_RAW\_SZ

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

## 7.34 ATK\_ICMP\_PARAPROBLEM\_SZ

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

## 7.35 ATK\_ICMP\_PINGOFDEATH

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	\$1: 入接口名称 \$2: 源IP地址 \$3: DS-Lite Tunnel对端地址 \$4: 目的IP地址 \$5: VPN名称 \$6: 动作类型 \$7: 攻击开始时间 \$8: 攻击结束时间 \$9: 攻击次数
日志等级	3
举例	ATK/3/ATK_ICMP_PINGOFDEATH: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，标志位设置为最后一块并且(IP offset * 8) + (IP data len) > 65535 的 ICMP报文数超过1，聚合后触发日志
处理建议	无

## 7.36 ATK\_ICMP\_PINGOFDEATH\_RAW

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

## 7.37 ATK\_ICMP\_PINGOFDEATH\_RAW\_SZ

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

## 7.38 ATK\_ICMP\_PINGOFDEATH\_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	\$1: 入域名称 \$2: 源IP地址 \$3: DS-Lite Tunnel对端地址 \$4: 目的IP地址 \$5: VPN名称 \$6: 动作类型 \$7: 攻击开始时间 \$8: 攻击结束时间 \$9: 攻击次数
日志等级	3
举例	ATK/3/ATK_ICMP_PINGOFDEATH_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=-; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=-; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，标志位设置为最后一块并且(IP offset * 8) + (IP data length) > 65535 的 ICMP报文数超过1，聚合后触发日志
处理建议	无



## 7.39 ATK\_ICMP\_REDIRECT

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

## 7.40 ATK\_ICMP\_REDIRECT\_RAW

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

## 7.41 ATK\_ICMP\_REDIRECT\_RAW\_SZ

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

## 7.42 ATK\_ICMP\_REDIRECT\_SZ

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

## 7.43 ATK\_ICMP\_SMURF

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

## 7.44 ATK\_ICMP\_SMURF\_RAW

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

## 7.45 ATK\_ICMP\_SMURF\_RAW\_SZ

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

## 7.46 ATK\_ICMP\_SMURF\_SZ

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

## 7.47 ATK\_ICMP\_SOURCEQUENCH

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

## 7.48 ATK\_ICMP\_SOURCEQUENCH\_RAW

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

## 7.49 ATK\_ICMP\_SOURCEQUENCH\_RAW\_SZ

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



## 7.50 ATK\_ICMP\_SOURCEQUENCH\_SZ

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

## 7.51 ATK\_ICMP\_TIMEEXCEED

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

## 7.52 ATK\_ICMP\_TIMEEXCEED\_RAW

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

## 7.53 ATK\_ICMP\_TIMEEXCEED\_RAW\_SZ

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

## 7.54 ATK\_ICMP\_TIMEEXCEED\_SZ

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

## 7.55 ATK\_ICMP\_TRACEROUTE

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

## 7.56 ATK\_ICMP\_TRACEROUTE\_RAW

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

## 7.57 ATK\_ICMP\_TRACEROUTE\_RAW\_SZ

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

## 7.58 ATK\_ICMP\_TRACEROUTE\_SZ

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

## 7.59 ATK\_ICMP\_TSTAMP\_REQ

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

## 7.60 ATK\_ICMP\_TSTAMP\_REQ\_RAW

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

## 7.61 ATK\_ICMP\_TSTAMP\_REQ\_RAW\_SZ

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



## 7.62 ATK\_ICMP\_TSTAMP\_REQ\_SZ

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

## 7.63 ATK\_ICMP\_TSTAMP\_RPL

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

## 7.64 ATK\_ICMP\_TSTAMP\_RPL\_RAW

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

## 7.65 ATK\_ICMP\_TSTAMP\_RPL\_RAW\_SZ

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

## 7.66 ATK\_ICMP\_TSTAMP\_RPL\_SZ

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

## 7.67 ATK\_ICMP\_TYPE

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

## 7.68 ATK\_ICMP\_TYPE\_RAW

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

## 7.69 ATK\_ICMP\_TYPE\_RAW\_SZ

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

## 7.70 ATK\_ICMP\_TYPE\_SZ

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

## 7.71 ATK\_ICMP\_UNREACHABLE

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



## 7.72 ATK\_ICMP\_UNREACHABLE\_RAW

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

## 7.73 ATK\_ICMP\_UNREACHABLE\_RAW\_SZ

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

## 7.74 ATK\_ICMP\_UNREACHABLE\_SZ

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

## 7.75 ATK\_ICMPV6\_DEST\_UNREACH

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

## 7.76 ATK\_ICMPV6\_DEST\_UNREACH\_RAW

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

## 7.77 ATK\_ICMPV6\_DEST\_UNREACH\_RAW\_SZ

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

## 7.78 ATK\_ICMPV6\_DEST\_UNREACH\_SZ

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

## 7.79 ATK\_ICMPV6\_ECHO\_REQ

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

## 7.80 ATK\_ICMPV6\_ECHO\_REQ\_RAW

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

## 7.81 ATK\_ICMPV6\_ECHO\_REQ\_RAW\_SZ

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

## 7.82 ATK\_ICMPV6\_ECHO\_REQ\_SZ

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

## 7.83 ATK\_ICMPV6\_ECHO\_RPL

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

## 7.84 ATK\_ICMPV6\_ECHO\_RPL\_RAW

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

## 7.85 ATK\_ICMPV6\_ECHO\_RPL\_RAW\_SZ

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

## 7.86 ATK\_ICMPV6\_ECHO\_RPL\_SZ

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



## 7.87 ATK\_ICMPV6\_FLOOD

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

## 7.88 ATK\_ICMPV6\_FLOOD\_SZ

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

## 7.89 ATK\_ICMPV6\_GROUPQUERY

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

## 7.90 ATK\_ICMPV6\_GROUPQUERY\_RAW

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

## 7.91 ATK\_ICMPV6\_GROUPQUERY\_RAW\_SZ

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

## 7.92 ATK\_ICMPV6\_GROUPQUERY\_SZ

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

## 7.93 ATK\_ICMPV6\_GROUPREDUCTION

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

## 7.94 ATK\_ICMPV6\_GROUPREDUCTION\_RAW

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

## 7.95 ATK\_ICMPV6\_GROUPREDUCTION\_RAW\_SZ

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

## 7.96 ATK\_ICMPV6\_GROUPREDUCTION\_SZ

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

## 7.97 ATK\_ICMPV6\_GROUPREPORT

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

## 7.98 ATK\_ICMPV6\_GROUPREPORT\_RAW

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

## 7.99 ATK\_ICMPV6\_GROUPREPORT\_RAW\_SZ

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

## 7.100 ATK\_ICMPV6\_GROUPREPORT\_SZ

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

## 7.101 ATK\_ICMPV6\_LARGE

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

## 7.102 ATK\_ICMPV6\_LARGE\_RAW

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



## 7.103 ATK\_ICMPV6\_LARGE\_RAW\_SZ

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

## 7.104 ATK\_ICMPV6\_LARGE\_SZ

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

## 7.105 ATK\_ICMPV6\_PACKETTOOBIG

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

## 7.106 ATK\_ICMPV6\_PACKETTOOBIG\_RAW

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

## 7.107 ATK\_ICMPV6\_PACKETTOOBIG\_RAW\_SZ

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

## 7.108 ATK\_ICMPV6\_PACKETTOOBIG\_SZ

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

## 7.109 ATK\_ICMPV6\_PARAPROBLEM

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

## 7.110 ATK\_ICMPV6\_PARAPROBLEM\_RAW

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

## 7.111 ATK\_ICMPV6\_PARAPROBLEM\_RAW\_SZ

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

## 7.112 ATK\_ICMPV6\_PARAPROBLEM\_SZ

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

## 7.113 ATK\_ICMPV6\_TIMEEXCEED

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

## 7.114 ATK\_ICMPV6\_TIMEEXCEED\_RAW

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

## 7.115 ATK\_ICMPV6\_TIMEEXCEED\_RAW\_SZ

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

## 7.116 ATK\_ICMPV6\_TIMEEXCEED\_SZ

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

## 7.117 ATK\_ICMPV6\_TRACEROUTE

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



## 7.118 ATK\_ICMPV6\_TRACEROUTE\_RAW

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

## 7.119 ATK\_ICMPV6\_TRACEROUTE\_RAW\_SZ

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

## 7.120 ATK\_ICMPV6\_TRACEROUTE\_SZ

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

## 7.121 ATK\_ICMPV6\_TYPE

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

## 7.122 ATK\_ICMPV6\_TYPE\_RAW

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

## 7.123 ATK\_ICMPV6\_TYPE\_RAW\_SZ

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

## 7.124 ATK\_ICMPV6\_TYPE\_SZ

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

## 7.125 ATK\_IP\_OPTION

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

## 7.126 ATK\_IP\_OPTION\_RAW

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

## 7.127 ATK\_IP\_OPTION\_RAW\_SZ

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

## 7.128 ATK\_IP\_OPTION\_SZ

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



## 7.129 ATK\_IP4\_ACK\_FLOOD

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

## 7.130 ATK\_IP4\_ACK\_FLOOD\_SZ

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

## 7.131 ATK\_IP4\_DIS\_PORTSCAN

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

## 7.132 ATK\_IP4\_DIS\_PORTSCAN\_SZ

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

## 7.133 ATK\_IP4\_DNS\_FLOOD

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

## 7.134 ATK\_IP4\_DNS\_FLOOD\_SZ

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

## 7.135 ATK\_IP4\_FIN\_FLOOD

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

## 7.136 ATK\_IP4\_FIN\_FLOOD\_SZ

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

## 7.137 ATK\_IP4\_FRAGMENT

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

## 7.138 ATK\_IP4\_FRAGMENT\_RAW

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

## 7.139 ATK\_IP4\_FRAGMENT\_RAW\_SZ

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

## 7.140 ATK\_IP4\_FRAGMENT\_SZ

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

## 7.141 ATK\_IP4\_HTTP\_FLOOD

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

## 7.142 ATK\_IP4\_HTTP\_FLOOD\_SZ

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



## 7.143 ATK\_IP4\_IMPOSSIBLE

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

## 7.144 ATK\_IP4\_IMPOSSIBLE\_RAW

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

## 7.145 ATK\_IP4\_IMPOSSIBLE\_RAW\_SZ

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

## 7.146 ATK\_IP4\_IMPOSSIBLE\_SZ

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

## 7.147 ATK\_IP4\_IPSWEEP

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

## 7.148 ATK\_IP4\_IPSWEEP\_SZ

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

## 7.149 ATK\_IP4\_PORTSCAN

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

## 7.150 ATK\_IP4\_PORTSCAN\_SZ

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

## 7.151 ATK\_IP4\_RST\_FLOOD

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

## 7.152 ATK\_IP4\_RST\_FLOOD\_SZ

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

## 7.153 ATK\_IP4\_SYN\_FLOOD

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

## 7.154 ATK\_IP4\_SYN\_FLOOD\_SZ

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

## 7.155 ATK\_IP4\_SYNACK\_FLOOD

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

## 7.156 ATK\_IP4\_SYNACK\_FLOOD\_SZ

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



## 7.157 ATK\_IP4\_TCP\_ALLFLAGS

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

## 7.158 ATK\_IP4\_TCP\_ALLFLAGS\_RAW

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

## 7.159 ATK\_IP4\_TCP\_ALLFLAGS\_RAW\_SZ

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

## 7.160 ATK\_IP4\_TCP\_ALLFLAGS\_SZ

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

## 7.161 ATK\_IP4\_TCP\_FINONLY

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

## 7.162 ATK\_IP4\_TCP\_FINONLY\_RAW

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

## 7.163 ATK\_IP4\_TCP\_FINONLY\_RAW\_SZ

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

## 7.164 ATK\_IP4\_TCP\_FINONLY\_SZ

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

## 7.165 ATK\_IP4\_TCP\_INVALIDFLAGS

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

## 7.166 ATK\_IP4\_TCP\_INVALIDFLAGS\_RAW

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

## 7.167 ATK\_IP4\_TCP\_INVALIDFLAGS\_RAW\_SZ

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

## 7.168 ATK\_IP4\_TCP\_INVALIDFLAGS\_SZ

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

## 7.169 ATK\_IP4\_TCP\_LAND

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	\$1: 入接口名称 \$2: 源IP地址 \$3: DS-Lite Tunnel对端地址 \$4: 目的IP地址 \$5: VPN名称 \$6: 动作类型 \$7: 攻击开始时间 \$8: 攻击结束时间 \$9: 攻击次数
日志等级	3
举例	ATK/3/ATK_IP4_TCP_LAND: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=-; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=-; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=3.
日志说明	日志聚合开关开启，IPv4源目的地址相同的TCP报文数超过1，聚合后触发日志
处理建议	无

## 7.170 ATK\_IP4\_TCP\_LAND\_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	\$1: 入接口名称 \$2: 源IP地址 \$3: DS-Lite Tunnel对端地址 \$4: 目的IP地址 \$5: VPN名称 \$6: 动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TCP_LAND_RAW: RcvIfName(1023)=Ethernet0/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=-; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=-; Action(1049)=logging.
日志说明	日志聚合开关开启，IPv4源目的地址相同的TCP报文首包触发日志；日志聚合开关关闭，每个IPv4源目的地址相同的TCP报文触发一个日志
处理建议	无



## 7.171 ATK\_IP4\_TCP\_LAND\_RAW\_SZ

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

## 7.172 ATK\_IP4\_TCP\_LAND\_SZ

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

## 7.173 ATK\_IP4\_TCP\_NULLFLAG

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

## 7.174 ATK\_IP4\_TCP\_NULLFLAG\_RAW

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

## 7.175 ATK\_IP4\_TCP\_NULLFLAG\_RAW\_SZ

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

## 7.176 ATK\_IP4\_TCP\_NULLFLAG\_SZ

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

## 7.177 ATK\_IP4\_TCP\_SYNFIN

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

## 7.178 ATK\_IP4\_TCP\_SYNFIN\_RAW

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

## 7.179 ATK\_IP4\_TCP\_SYNFIN\_RAW\_SZ

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

## 7.180 ATK\_IP4\_TCP\_SYNFIN\_SZ

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

## 7.181 ATK\_IP4\_TCP\_WINNUKE

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

## 7.182 ATK\_IP4\_TCP\_WINNUKE\_RAW

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

## 7.183 ATK\_IP4\_TCP\_WINNUKE\_RAW\_SZ

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

## 7.184 ATK\_IP4\_TCP\_WINNUKE\_SZ

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



## 7.185 ATK\_IP4\_TEARDROP

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

## 7.186 ATK\_IP4\_TEARDROP\_RAW

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

## 7.187 ATK\_IP4\_TEARDROP\_RAW\_SZ

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

## 7.188 ATK\_IP4\_TEARDROP\_SZ

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

## 7.189 ATK\_IP4\_TINY\_FRAGMENT

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

## 7.190 ATK\_IP4\_TINY\_FRAGMENT\_RAW

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

## 7.191 ATK\_IP4\_TINY\_FRAGMENT\_RAW\_SZ

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

## 7.192 ATK\_IP4\_TINY\_FRAGMENT\_SZ

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

## 7.193 ATK\_IP4\_UDP\_BOMB

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

## 7.194 ATK\_IP4\_UDP\_BOMB\_RAW

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

## 7.195 ATK\_IP4\_UDP\_BOMB\_RAW\_SZ

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

## 7.196 ATK\_IP4\_UDP\_BOMB\_SZ

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



## 7.197 ATK\_IP4\_UDP\_FLOOD

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

## 7.198 ATK\_IP4\_UDP\_FLOOD\_SZ

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

## 7.199 ATK\_IP4\_UDP\_FRAGGLE

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

## 7.200 ATK\_IP4\_UDP\_FRAGGLE\_RAW

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

## 7.201 ATK\_IP4\_UDP\_FRAGGLE\_RAW\_SZ

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

## 7.202 ATK\_IP4\_UDP\_FRAGGLE\_SZ

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

## 7.203 ATK\_IP4\_UDP\_SNORK

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

## 7.204 ATK\_IP4\_UDP\_SNORK\_RAW

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

## 7.205 ATK\_IP4\_UDP\_SNORK\_RAW\_SZ

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

## 7.206 ATK\_IP4\_UDP\_SNORK\_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	\$1: 入域名称 \$2: 源IP地址 \$3: DS-Lite Tunnel对端地址 \$4: 目的IP地址 \$5: VPN名称 \$6: 动作类型 \$7: 攻击开始时间 \$8: 攻击结束时间 \$9: 攻击次数
日志等级	3
举例	ATK/3/ATK_IP4_UDP_SNORK_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=-; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=-; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=2.
日志说明	日志聚合开关开启, IPv4源端口为7、19或135, 目的端口为135的UDP报文数超过1, 聚合后触发日志
处理建议	无

## 7.207 ATK\_IP6\_ACK\_FLOOD

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

## 7.208 ATK\_IP6\_ACK\_FLOOD\_SZ

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

## 7.209 ATK\_IP6\_DIS\_PORTSCAN

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

## 7.210 ATK\_IP6\_DIS\_PORTSCAN\_SZ

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

## 7.211 ATK\_IP6\_DNS\_FLOOD

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



## 7.212 ATK\_IP6\_DNS\_FLOOD\_SZ

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

## 7.213 ATK\_IP6\_FIN\_FLOOD

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

## 7.214 ATK\_IP6\_FIN\_FLOOD\_SZ

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

## 7.215 ATK\_IP6\_FRAGMENT

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

## 7.216 ATK\_IP6\_FRAGMENT\_RAW

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

## 7.217 ATK\_IP6\_FRAGMENT\_RAW\_SZ

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

## 7.218 ATK\_IP6\_FRAGMENT\_SZ

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

## 7.219 ATK\_IP6\_HTTP\_FLOOD

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

## 7.220 ATK\_IP6\_HTTP\_FLOOD\_SZ

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

## 7.221 ATK\_IP6\_IMPOSSIBLE

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

## 7.222 ATK\_IP6\_IMPOSSIBLE\_RAW

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

## 7.223 ATK\_IP6\_IMPOSSIBLE\_RAW\_SZ

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

## 7.224 ATK\_IP6\_IMPOSSIBLE\_SZ

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

## 7.225 ATK\_IP6\_IPSWEEP

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

## 7.226 ATK\_IP6\_IPSWEEP\_SZ

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

## 7.227 ATK\_IP6\_PORTSCAN

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



## 7.228 ATK\_IP6\_PORTSCAN\_SZ

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

## 7.229 ATK\_IP6\_RST\_FLOOD

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

## 7.230 ATK\_IP6\_RST\_FLOOD\_SZ

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

## 7.231 ATK\_IP6\_SYN\_FLOOD

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

## 7.232 ATK\_IP6\_SYN\_FLOOD\_SZ

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

## 7.233 ATK\_IP6\_SYNACK\_FLOOD

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

## 7.234 ATK\_IP6\_SYNACK\_FLOOD\_SZ

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

## 7.235 ATK\_IP6\_TCP\_ALLFLAGS

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

## 7.236 ATK\_IP6\_TCP\_ALLFLAGS\_RAW

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

## 7.237 ATK\_IP6\_TCP\_ALLFLAGS\_RAW\_SZ

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

## 7.238 ATK\_IP6\_TCP\_ALLFLAGS\_SZ

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

## 7.239 ATK\_IP6\_TCP\_FINONLY

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

## 7.240 ATK\_IP6\_TCP\_FINONLY\_RAW

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

## 7.241 ATK\_IP6\_TCP\_FINONLY\_RAW\_SZ

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

## 7.242 ATK\_IP6\_TCP\_FINONLY\_SZ

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



## 7.243 ATK\_IP6\_TCP\_INVALIDFLAGS

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

## 7.244 ATK\_IP6\_TCP\_INVALIDFLAGS\_RAW

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

## 7.245 ATK\_IP6\_TCP\_INVALIDFLAGS\_RAW\_SZ

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

## 7.246 ATK\_IP6\_TCP\_INVALIDFLAGS\_SZ

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

## 7.247 ATK\_IP6\_TCP\_LAND

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

## 7.248 ATK\_IP6\_TCP\_LAND\_RAW

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

## 7.249 ATK\_IP6\_TCP\_LAND\_RAW\_SZ

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

## 7.250 ATK\_IP6\_TCP\_LAND\_SZ

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

## 7.251 ATK\_IP6\_TCP\_NULLFLAG

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

## 7.252 ATK\_IP6\_TCP\_NULLFLAG\_RAW

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

## 7.253 ATK\_IP6\_TCP\_NULLFLAG\_RAW\_SZ

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

## 7.254 ATK\_IP6\_TCP\_NULLFLAG\_SZ

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

## 7.255 ATK\_IP6\_TCP\_SYNFIN

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

## 7.256 ATK\_IP6\_TCP\_SYNFIN\_RAW

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



## 7.257 ATK\_IP6\_TCP\_SYNFIN\_RAW\_SZ

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

## 7.258 ATK\_IP6\_TCP\_SYNFIN\_SZ

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

## 7.259 ATK\_IP6\_TCP\_WINNUKE

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

## 7.260 ATK\_IP6\_TCP\_WINNUKE\_RAW

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

## 7.261 ATK\_IP6\_TCP\_WINNUKE\_RAW\_SZ

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

## 7.262 ATK\_IP6\_TCP\_WINNUKE\_SZ

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

## 7.263 ATK\_IP6\_UDP\_FLOOD

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

## 7.264 ATK\_IP6\_UDP\_FLOOD\_SZ

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

## 7.265 ATK\_IP6\_UDP\_FRAGGLE

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

## 7.266 ATK\_IP6\_UDP\_FRAGGLE\_RAW

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

## 7.267 ATK\_IP6\_UDP\_FRAGGLE\_RAW\_SZ

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

## 7.268 ATK\_IP6\_UDP\_FRAGGLE\_SZ

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

## 7.269 ATK\_IP6\_UDP\_SNORK

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

## 7.270 ATK\_IP6\_UDP\_SNORK\_RAW

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

## 7.271 ATK\_IP6\_UDP\_SNORK\_RAW\_SZ

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

## 7.272 ATK\_IP6\_UDP\_SNORK\_SZ

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



## 7.273 ATK\_IPOPT\_ABNORMAL

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

## 7.274 ATK\_IPOPT\_ABNORMAL\_RAW

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

## 7.275 ATK\_IPOPT\_ABNORMAL\_RAW\_SZ

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

## 7.276 ATK\_IPOPT\_ABNORMAL\_SZ

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

## 7.277 ATK\_IPOPT\_LOOSESRCROUTE

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

## 7.278 ATK\_IPOPT\_LOOSESRCROUTE\_RAW

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

## 7.279 ATK\_IPOPT\_LOOSESRCROUTE\_RAW\_SZ

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

## 7.280 ATK\_IPOPT\_LOOSESRCROUTE\_SZ

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

## 7.281 ATK\_IPOPT\_RECORDROUTE

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



## 7.282 ATK\_IPOPT\_RECORDROUTE\_RAW

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

## 7.283 ATK\_IPOPT\_RECORDROUTE\_RAW\_SZ

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

## 7.284 ATK\_IPOPT\_RECORDROUTE\_SZ

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

## 7.285 ATK\_IPOPT\_ROUTEALERT

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

## 7.286 ATK\_IPOPT\_ROUTEALERT\_RAW

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

## 7.287 ATK\_IPOPT\_ROUTEALERT\_RAW\_SZ

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

## 7.288 ATK\_IPOPT\_ROUTEALERT\_SZ

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

## 7.289 ATK\_IPOPT\_SECURITY

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



## 7.290 ATK\_IPOPT\_SECURITY\_RAW

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

## 7.291 ATK\_IPOPT\_SECURITY\_RAW\_SZ

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

## 7.292 ATK\_IPOPT\_SECURITY\_SZ

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

## 7.293 ATK\_IPOPT\_STREAMID

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

## 7.294 ATK\_IPOPT\_STREAMID\_RAW

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

## 7.295 ATK\_IPOPT\_STREAMID\_RAW\_SZ

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

## 7.296 ATK\_IPOPT\_STREAMID\_SZ

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

## 7.297 ATK\_IPOPT\_STRICTSRCROUTE

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



## 7.298 ATK\_IPOPT\_STRICTSRCROUTE\_RAW

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

## 7.299 ATK\_IPOPT\_STRICTSRCROUTE\_RAW\_SZ

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

## 7.300 ATK\_IPOPT\_STRICTSRCROUTE\_SZ

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

## 7.301 ATK\_IPOPT\_TIMESTAMP

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

## 7.302 ATK\_IPOPT\_TIMESTAMP\_RAW

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

## 7.303 ATK\_IPOPT\_TIMESTAMP\_RAW\_SZ

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

## 7.304 ATK\_IPOPT\_TIMESTAMP\_SZ

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

## 7.305 ATK\_IPV6\_EXT\_HEADER

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

## 7.306 ATK\_IPV6\_EXT\_HEADER\_RAW

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



## 7.307 ATK\_IPV6\_EXT\_HEADER\_RAW\_SZ

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

## 7.308 ATK\_IPV6\_EXT\_HEADER\_SZ

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

# 8 ATM

本节介绍 ATM 模块输出的日志信息。

## 8.1 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	<ol style="list-style-type: none"><li>1. 使用 <b>display atm pvc-info</b> 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：<ol style="list-style-type: none"><li>2. 如果 Interface State 字段显示为 DOWN<ul style="list-style-type: none"><li>• 使用 <b>display interface atm</b> 命令分别检查本端和对端的 ATM 接口是否被手动 <b>shutdown</b>，若是，可通过在接口上执行 <b>undo shutdown</b> 命令解决该问题</li><li>• 检查接口之间的连线是否插好</li></ul></li><li>3. 如果 OAM State 字段显示为 DOWN<ul style="list-style-type: none"><li>• 当两台路由器直连时：<ul style="list-style-type: none"><li>○ 检查对端接口上创建的 PVC 的 VPI/VCI 是否与本端相同</li><li>○ 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 <b>oam cc sink</b>，对端需配置 <b>oam cc source</b>)</li><li>○ 检查对端的 PVC 是否被手动 <b>shutdown</b>，若是，可通过在 PVC 视图上执行 <b>undo shutdown</b> 命令解决该问题</li><li>○ 检查两端连线是否正确</li></ul></li><li>• 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</li></ul></li><li>4. 如果 PVC State 字段显示为 DOWN，请检查本端的 PVC 是否被手动 <b>shutdown</b>，若是，可通过在 PVC 视图上执行 <b>undo shutdown</b> 命令解决该问题</li></ol></li></ol>

## 8.2 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	无需处理

# 9 BFD

本节介绍 BFD 模块输出的日志信息。

## 9.1 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 <ul style="list-style-type: none"><li>○ 0 (No Diagnostic): 表示无诊断信息</li><li>○ 1 (Control Detection Time Expired): 表示 Ctrl 会话本端检测时间超时, 会话 down</li><li>○ 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</li><li>○ 3 (Neighbor Signaled Session Down): 表示对端通知本端 BFD 会话 down</li><li>○ 7 (Administratively Down): 表示本端系统阻止 BFD 会话的建立</li></ul>
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

## 9.2 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

# 10 BGP

本节介绍 BGP 模块输出的日志信息。

## 10.1 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

## 10.2 BGP\_REACHED\_THRESHOLD

日志内容	BGP.[STRING]: The ratio of the number of routes received from peer [STRING] ([STRING]) to the number of allowed routes [UINT32] has reached the threshold ([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数量 \$5: 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 ratio of the number of routes received from peer 1.1.1.1 (IPv4-UNC) to the number of allowed routes 100 has reached the threshold (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： <ul style="list-style-type: none"><li>允许的最大路由数量</li><li>接收的路由数量占允许的最大路由数量百分比的阈值</li></ul>

## 10.3 BGP\_LOG\_ROUTE\_FLAP

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

## 10.4 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

## 10.5 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

## 10.6 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: <ul style="list-style-type: none"><li>IPv4-UNC public: 表示公网 IPv4 单播路由</li><li>IPv6-UNC public: 表示公网 IPv6 单播路由</li><li>IPv4 private: 表示私网 IPv4 单播路由, VPNv4 路由和嵌套 VPN 路由</li><li>IPv6 private: 表示私网 IPv6 单播路由, VPNv6 路由</li></ul>
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

## 10.7 BGP\_STATE\_CHANGED

日志内容	BGP.[STRING]: [STRING] state has changed from [STRING] to [STRING].
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: 变化前的状态名称 \$4: 变化后的状态名称
日志等级	5
举例	BGP/5/BGP_STATE_CHANGED: BGP.vpn1: 192.99.0.2 state has changed from ESTABLISHED to IDLE.
日志说明	BGP对等体的状态发生变化 此日志信息当BGP对等体从其他状态进入Established状态或者从Established状态进入其他状态时产生
处理建议	如果BGP对等体意外Down，请检查网络是否发生故障或丢包

## 10.8 BGP\_STATE\_CHANGED\_REASON

日志内容	BGP.[STRING]: [STRING] state has changed from [STRING] to [STRING]. ([STRING])
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: 变化前BGP会话的状态 \$4: 变化后BGP会话的状态 \$5: BGP会话断开相关信息： <ul style="list-style-type: none"><li>Reason: BGP 会话断开的原因</li><li>Error code: 发送或者接收的 Notification 错误码/子错误码（TCP 连接失败导致 BGP 会话断开时不显示本字段）</li><li>Local interface: 建立 BGP 会话使用的物理接口（本字段仅在由于接口不通导致直连对等体间的 BGP 会话断开时显示）</li></ul>
日志等级	5
举例	BGP/5/BGP_STATE_CHANGED_REASON: BGP.vpn1: 192.99.0.2 state has changed from ESTABLISHED to IDLE. (Reason: Directly connected physical interface was down, Error code: Send Notificationcode 6/0, Local interface: GigabitEthernet1/0/1)
日志说明	当BGP对等体从Established状态进入其他状态时打印提示信息
处理建议	请根据会话断开的原因检查网络是否发生故障或丢包

# 11 BLS

本节介绍 BLS 模块输出的日志信息。

## 11.1 BLS\_ENTRY\_ADD

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

## 11.2 BLS\_ENTRY\_DEL

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



## 11.3 BLS\_IPV6\_ENTRY\_ADD

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

## 11.4 BLS\_IPV6\_ENTRY\_DEL

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

# 12 CFD

本节介绍 CFD 模块输出的日志信息。

## 12.1 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 0011-2233-4401, SeqNum is 78, RMEP is 12, MD ID is without ID, MA ID is 0.
日志说明	MEP收到交叉连接的CCM报文，该报文包含与本端不同的MA ID或MD ID
处理建议	检查两端MEP的配置。让MEP所属的MD和MA的配置一致，且两端MEP级别相同、方向都相同

## 12.2 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 0011-2233-4401, SeqNum is 21, RMEP is 2, MD ID is 7, MA ID is 1.
日志说明	MEP收到错误的CCM报文，该报文包含错误的MEP ID或生存时间
处理建议	检查CCM配置。让两端的CC检测周期配置一致，并配置远端MEP ID在本端允许的MEP列表中

## 12.3 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

## 12.4 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

# 13 CFGMAN

本节介绍配置管理模块输出的日志信息。

## 13.1 CFGMAN\_ARCHIVE\_SCP\_FAIL

日志内容	Archive configuration to SCP server failed: IP = [STRING], Directory = [STRING], Username = [STRING]
参数解释	\$1: SCP服务器的IP地址 \$2: 备份配置文件在SCP服务器上的保存目录 \$3: 登录SCP服务器的用户名
日志等级	5
举例	CFGMAN/5/CFGMAN_ARCHIVE_SCP_FAIL: Archive configuration to SCP server failed: IP = 192.168.21.21, Directory = /test/, Username = admin
日志说明	设备向SCP服务器保存配置文件失败时，打印此日志信息
处理建议	无

## 13.2 CFGMAN\_CFGCHANGED

日志内容	-EventIndex=[INT32]-CommandSource=[INT32]-ConfigSource=[INT32]-ConfigDestination=[INT32]; Configuration changed.
参数解释	<p><b>\$1:</b> 事件索引，取值范围为1到2147483647</p> <p><b>\$2:</b> 引起配置变化的来源，取值为：</p> <ul style="list-style-type: none"> <li>○ cli: 表示引起配置变化的来源为命令行</li> <li>○ 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</li> <li>○ other: 表示引起配置变化的来源为其它途径</li> </ul> <p><b>\$3:</b> 源配置，取值为：</p> <ul style="list-style-type: none"> <li>○ erase: 配置删除或重命名</li> <li>○ running: 保存正在运行的配置</li> <li>○ commandSource: 拷贝配置文件</li> <li>○ startup: 保存运行配置到下次启动配置文件</li> <li>○ local: 保存运行配置到本地文件</li> <li>○ 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</li> <li>○ hotPlugging: 热插拔板卡导致配置被删除或者失效</li> </ul> <p><b>\$4:</b> 目的配置，取值为：</p> <ul style="list-style-type: none"> <li>○ erase: 配置删除或重命名</li> <li>○ running: 保存正在运行的配置</li> <li>○ commandSource: 拷贝配置文件</li> <li>○ startup: 保存运行配置到下次启动配置文件</li> <li>○ local: 保存运行配置到本地文件</li> <li>○ 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</li> <li>○ hotPlugging: 热插拔板卡导致配置被删除或者失效</li> </ul>
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

### 13.3 CFGMAN\_EXIT\_FROM\_CONFIGURE

日志内容	Line=[STRING], IP address=[STRING], user=[STRING]; Exit from the system view or a feature view to the user view.
参数解释	\$1: 用户线名（如果不涉及该参数，显示为**） \$2: IP地址（如果不涉及该参数，显示为**） \$3: 用户名（如果不涉及该参数，显示为**）
日志等级	5
举例	CFGMAN/5/CFGMAN_EXIT_FROM_CONFIGURE: Line=con0, IP address=**, user=**; Exit from the system view or a feature view to the user view.
日志说明	记录交互模式下用户从系统视图、功能视图退出到用户视图
处理建议	无

## 13.4 CFGMAN\_OPTCOMPLETION

日志内容	-OperateType=[INT32]-OperateTime=[INT32]-OperateState=[INT32]-OperateEndTime=[INT32]; Operation completed.
参数解释	<p><b>\$1:</b> 操作类型，取值为：</p> <ul style="list-style-type: none"> <li>○ <b>running2startup:</b> 将运行配置保存为下次启动配置</li> <li>○ <b>startup2running:</b> 将下次启动配置设置为运行配置</li> <li>○ <b>running2net:</b> 将运行配置保存到网络</li> <li>○ <b>net2running:</b> 将网络上的配置文件上传到设备，并作为当前配置运行</li> <li>○ <b>net2startup:</b> 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</li> <li>○ <b>startup2net:</b> 将下次启动配置文件保存到网络</li> </ul> <p><b>\$2:</b> 操作时间</p> <p><b>\$3:</b> 操作状态，取值为：</p> <ul style="list-style-type: none"> <li>○ <b>InProcess:</b> 正在执行</li> <li>○ <b>success:</b> 执行成功</li> <li>○ <b>InvalidOperation:</b> 无效的操作</li> <li>○ <b>InvalidProtocol:</b> 无效的协议</li> <li>○ <b>InvalidSource:</b> 无效的源文件名</li> <li>○ <b>InvalidDestination:</b> 无效的目的地文件名</li> <li>○ <b>InvalidServer:</b> 无效的服务器地址</li> <li>○ <b>DeviceBusy:</b> 设备繁忙</li> <li>○ <b>InvalidDevice:</b> 设备地址无效</li> <li>○ <b>DeviceError:</b> 设备出错</li> <li>○ <b>DeviceNotWritable:</b> 设备不可写</li> <li>○ <b>DeviceFull:</b> 设备的存储空间不足</li> <li>○ <b>FileOpenError:</b> 文件打开出错</li> <li>○ <b>FileTransferError:</b> 文件传输出错</li> <li>○ <b>ChecksumError:</b> 文件校验和错误</li> <li>○ <b>LowMemory:</b> 没有内存</li> <li>○ <b>AuthFailed:</b> 用户验证失败</li> <li>○ <b>TransferTimeout:</b> 传输超时</li> <li>○ <b>UnknownError:</b> 未知原因</li> <li>○ <b>invalidConfig:</b> 无效配置</li> </ul> <p><b>\$4:</b> 操作结束时间</p>
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

## 13.5 CFG\_SAVE\_FAILED

日志内容	<p>形式一： Failed to save the current configuration.</p> <p>形式二： Failed to save the current configuration on [STRING].</p> <p>形式三： Failed to save the current configuration. Reason: [STRING].</p> <p>形式四： Failed to save the current configuration for [STRING].</p> <p>形式五： Failed to save the current configuration on [STRING]. Reason: [STRING].</p>
参数解释	<p>形式二： \$1: 当Slot仅支持单CPU时，表示Slot所在位置；当Slot支持多CPU时，表示CPU所在位置</p> <p>形式三： \$1: 失败原因，取值包括：</p> <ul style="list-style-type: none"> <li>○ No space available on the device: 磁盘空间不足</li> <li>○ Failed to save the current configuration in binary format: 二进制类型配置文件保存失败</li> <li>○ the memory is insufficient: 内存不足</li> <li>○ Failed to set the next-startup configuration on <i>location</i>: 设置板卡的下次启动配置文件失败。当 Slot 仅支持单 CPU 时，<i>location</i> 表示 Slot 所在位置；当 Slot 支持多 CPU 时，<i>location</i> 表示 CPU 所在位置</li> <li>○ the system is rebooting: 正在重启中</li> <li>○ Operation not supported: 操作不支持</li> <li>○ the memory on the memory file system is insufficient: 内存文件系统空间不足</li> </ul> <p>形式四： \$1: MDC/Context <i>mdc-name/context-name</i></p> <p>形式五： \$1: 当Slot仅支持单CPU时，表示Slot所在位置；当Slot支持多CPU时，表示CPU所在位置 \$2: 失败原因，取值同形式三的失败原因</p>
日志等级	4
举例	CFGMAN/4/CFG_SAVE_FAILED: Failed to save the current configuration because no space available on device.
日志说明	<p>保存当前配置失败时输入本日志，其中：</p> <ul style="list-style-type: none"> <li>• 配置保存失败的原因，原因不明确的提示形式一</li> <li>• 对于形式二，一般在如下情况下输出：由于磁盘读写慢、磁盘损坏等原因，将配置文件备份到备用主控板失败</li> <li>• 不提示板卡表示主用主控板和备用主控板配置保存失败，提示板卡表示指定板卡配置保存失败</li> <li>• MDC/Context 内的配置保存失败，具体信息请登录 MDC/Context，执行 <b>display logbuffer</b> 命令查看</li> </ul>



日志内容	<p>形式一： Failed to save the current configuration.</p> <p>形式二： Failed to save the current configuration on [STRING].</p> <p>形式三： Failed to save the current configuration. Reason: [STRING].</p> <p>形式四： Failed to save the current configuration for [STRING].</p> <p>形式五： Failed to save the current configuration on [STRING]. Reason: [STRING].</p>
处理建议	<ol style="list-style-type: none"> <li>1. 执行 <code>dir</code> 命令查看主用主控板和备用主控板的磁盘空间是否充足</li> <li>2. 执行 <code>copy</code> 命令检查主用主控板和备用主控板的磁盘是否可以正常 Copy 文件</li> <li>3. 执行 <code>display memory</code> 和 <code>display process memory</code> 命令查看内存信息，检查设备内存空间是否充足</li> <li>4. 如果没有发现上述问题，请联系技术支持</li> </ol>

## 13.6 CFG\_SET\_NEXTCFG\_FAILED

日志内容	Failed to set [STRINT] as the [STRING] next-startup file on [STRING].
参数解释	<p>\$1: 文件名</p> <p>\$2: 主备属性，取值包括：</p> <ul style="list-style-type: none"> <li>o main: 表示设置为主用下次启动配置文件</li> <li>o backup: 表示设置为备用下次启动配置文件</li> </ul> <p>\$3: 当Slot仅支持单CPU时，表示Slot所在位置；当Slot支持多CPU时，表示CPU所在位置</p>
日志等级	4
举例	CFGMAN/4/CFG_SET_NEXTCFG_FAILED: Failed to set startup.cfg as the main next-startup file on slot 1.
日志说明	设置下次启动配置文件失败
处理建议	请确认文件是否存在，文件内容是否合法。如果没有发现错误，请记录当时操作，联系技术支持

# 14 CONNLMT

本节介绍连接数限制模块输出的日志信息。

## 14.1 CONNLMT\_IPV4\_OVERLOAD

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

## 14.2 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	<p>\$1: 全局或接口名称</p> <p>\$2: 传输层协议类型</p> <p>\$3: 源IP地址</p> <p>\$4: 目的IP地址</p> <p>\$5: 服务端口号</p> <p>\$6: 源VPN名称</p> <p>\$7: 目的VPN名称</p> <p>\$8: 对端隧道ID</p> <p>\$9: 丢包数</p> <p>\$10: 下限值</p> <p>\$11: 规则ID</p> <p>\$12: Event信息</p>
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)=Reduces 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

## 14.3 CONNLMT\_IPV6\_OVERLOAD

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

## 14.4 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	CONNLM/6/CONNLM_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)=Reduces 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

# 15 DEV

本节介绍 DEV（设备管理）模块输出的日志信息。

## 15.1 AUTOSWITCH\_FAULT

日志内容	[STRING] automatically switches between active and standby, and a fault occurs during the switching.
参数解释	\$1: chassis编号
日志等级	1
举例	DEV/1/AUTO_SWITCH_FAULT: Chassis 1 automatically switches between active and standby, and a fault occurs during the switching, please contact technical support.
日志说明	设备自动发生主备倒换，倒换过程中发生故障
处理建议	<ul style="list-style-type: none"><li>用户可手工重启设备来尝试恢复故障。重启设备前，请执行 <a href="#">javascript:infosearch(3077425)</a> 命令收集并保存诊断信息，以便定位故障</li><li>重启设备后，可执行 <b>display device</b> 命令查看设备状态。如果状态不是 <b>Normal</b>，表示故障未解除，请联系技术支持</li></ul>

## 15.2 AUTOSWITCH\_FAULT\_REBOOT

日志内容	[STRING] automatically switches between active and standby, and a fault occurs during the switching, the device will immediately restart [STRING] to restore the fault.
参数解释	\$1: chassis编号 \$2: chassis编号+slot编号或slot编号
日志等级	1
举例	DEV/1/AUTO_SWITCH_FAULT_REBOOT: Chassis 1 automatically switches between active and standby, and a fault occurs during the switching, the device will immediately restart chassis 1 slot 0 to restore the fault.
日志说明	设备自动发生主备倒换，倒换过程中出现故障，设备会立即自动重启故障单板来恢复故障
处理建议	故障单板重启后，可执行 <b>display device</b> 命令查看单板状态。如果状态不是 <b>Normal</b> ，表示故障未解除，请联系技术支持解决

## 15.3 BOARD\_INSERTED

日志内容	Board was inserted on [STRING], type is unknown.
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_INSERTED: Board was inserted on slot 1, type is unknown.
日志说明	有单板插入设备，但是单板类型未知
处理建议	单板插入设备后，需要一段时间才能完成启动，该段时间内，提示该日志，属于正常情况，无需处理

## 15.4 BOARD\_REBOOT

日志内容	Board is rebooting on [STRING].
参数解释	\$1: chassis编号+slot编号或slot编号
日志等级	5
举例	DEV/5/BOARD_REBOOT: Board is rebooting on slot 1.
日志说明	用户在重启指定slot, 或者指定slot因为异常而重启
处理建议	<ol style="list-style-type: none"><li>1. 检查是否有用户在重启指定 slot</li><li>2. 如果没有用户重启, 等待指定 slot 重新启动后, 通过 display version 命令、对应指定 slot 信息中的 Last reboot reason 字段, 查看重启原因</li><li>3. 如果重启原因为异常重启, 请联系技术支持</li></ol>

## 15.5 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	<ol style="list-style-type: none"><li>1. 检查对应单板是否插紧</li><li>2. 检查对应单板是否损坏</li><li>3. 重新插入单板或更换单板</li><li>4. 重新将设备加入 IRF</li></ol>

## 15.6 BOARD\_RUNNING\_FAULT

日志内容	[STRING] is detected to be faulty.
参数解释	\$1: chassis编号+slot编号或slot编号
日志等级	1
举例	DEV/1/ BOARD_FAULT_REBOOT: Chassis 1 slot 0 is detected to be faulty, please contact technical support.
日志说明	设备运行过程中检测到单板发生故障
处理建议	<ul style="list-style-type: none"><li>• 用户可手工重启故障单板来尝试恢复故障。重启单板前，可以执行 <a href="#">javascript:infosearch(3077425)</a> 命令收集并保存诊断信息，以便定位故障</li><li>• 重启单板后，可执行 <b>display device</b> 命令查看单板状态。如果状态不是 <b>Normal</b>，表示故障未解除，请联系技术支持解决</li></ul>

## 15.7 BOARD\_RUNNING\_FAULT\_REBOOT

日志内容	[STRING] is detected to be faulty, the device will immediately restart [STRING] to recover from the fault.
参数解释	\$1: chassis编号+slot编号或slot编号 \$2: chassis编号+slot编号或slot编号
日志等级	1
举例	DEV/1/ BOARD_RUNNING_FAULT_REBOOT: Chassis 1 slot 0 is detected to be faulty, the device will immediately restart chassis 1 slot 0 to recover from the fault.
日志说明	设备运行过程中检测到单板发生故障，设备会立即重启单板来恢复故障
处理建议	单板自动重启后，可执行 <b>display device</b> 命令查看设备状态。如果状态不是 <b>Normal</b> ，表示故障未解除，请联系技术支持



## 15.8 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： <ul style="list-style-type: none"><li>• 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</li><li>• 单板不能正常工作</li></ul>
处理建议	根据日志产生的情况，处理建议如下： <ul style="list-style-type: none"><li>• 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</li><li>• 对于第二种情况：请联系技术支持</li></ul>

## 15.9 BOARD\_STATE\_NORMAL

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

## 15.10 BOARD\_STATE\_STARTING

日志内容	Board state changed to Starting on [STRING], type is unknown.
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_STATE_STARTING: Board state changed to Starting on slot 1, type is unknown.
日志说明	单板处于启动阶段（正在初始化或者加载软件版本），不能正常工作
处理建议	<ol style="list-style-type: none"><li>1. 查看单板型号和设备型号是否适配</li><li>2. 查看启动文件和设备软件版本以及硬件是否适配</li><li>3. 请联系技术支持</li></ol>

## 15.11 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卡所在的槽位号
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

## 15.12 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	<ol style="list-style-type: none"><li>1. 检查 CF 卡是否插紧</li><li>2. 检查 CF 卡是否损坏</li><li>3. 重新安装 CF 卡或更换 CF 卡</li></ol>

## 15.13 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	<ol style="list-style-type: none"><li>1. 检查是否有用户在重启成员设备</li><li>2. 如果没有用户重启，等待成员设备重新启动后，通过 <code>display version</code> 命令、对应成员设备单板信息中的 <code>Last reboot reason</code> 字段，查看重启原因</li><li>3. 如果重启原因为异常重启，请联系技术支持</li></ol>

## 15.14 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

## 15.15 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	<ol style="list-style-type: none"><li>1. 重启单板尝试恢复</li><li>2. 联系工程师分析解决</li></ol>

## 15.16 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，或风扇被拔出
处理建议	<ol style="list-style-type: none"><li>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</li><li>2. 如果有风扇，检查风扇框是否插紧</li><li>3. 检查风扇框是否损坏</li><li>4. 重新安装风扇框或更换风扇框</li></ol>

## 15.17 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	<ol style="list-style-type: none"><li>1. 根据机房通风系统的风向，选择风向一致的型号的风扇</li><li>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</li></ol>

## 15.18 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

## 15.19 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

## 15.20 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	<ol style="list-style-type: none"><li>1. 使用 <code>display irf</code> 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</li><li>2. 使用 <code>display irf link</code> 查看 IRF 链路信息，确认故障的 IRF 链路</li><li>3. 手工修复状态为 DOWN 的 IRF 链路</li></ol>

## 15.21 MAD\_PROC

日志内容	[STRING] protocol detected MAD conflict: Local health value=[UINT32], Peer health value=[UINT32].
参数解释	<p>\$1: 检测到MAD冲突的协议名称，取值为ARP、ND、LACP、BFD</p> <p>\$2: 本端IRF的健康值</p> <p>\$3: 检测到MAD冲突时对端IRF的检查值</p>
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IRF和对端IRF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

## 15.22 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	<ol style="list-style-type: none"><li>1. 检查电源是否插紧</li><li>2. 检查电源是否损坏</li><li>3. 重新安装电源或更换电源</li></ol>

## 15.23 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

## 15.24 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	<ol style="list-style-type: none"><li>1. 检查电源监控模块是否插紧</li><li>2. 检查电源监控模块是否损坏</li><li>3. 重新安装电源监控模块或更换电源监控模块</li></ol>

## 15.25 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



## 15.26 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Normal
处理建议	无

## 15.27 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Normal
处理建议	无

## 15.28 RPS\_ABSENT

日志内容	形式一： RPS [INT32] is absent. 形式二： Chassis [INT32] RPS [INT32] is absent.
参数解释	形式一： \$1: 冗余电源模块ID 形式二： \$1: chassis编号 \$2: 冗余电源模块ID
日志等级	3
举例	DEV/3/RPS_ABSENT: RPS 1 is absent.
日志说明	冗余电源模块被拔出
处理建议	<ol style="list-style-type: none"><li>1. 检查冗余电源模块是否插紧</li><li>2. 检查冗余电源模块是否损坏</li><li>3. 重新安装冗余电源模块或更换冗余电源模块</li></ol>

## 15.29 RPS\_FAILED

日志内容	形式一： RPS [INT32] failed. 形式二： Chassis [INT32] RPS [INT32] failed.
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	2
举例	DEV/2/RPS_FAILED: RPS 2 failed.
日志说明	冗余电源模块没供电或者故障
处理建议	<ol style="list-style-type: none"><li>1. 检查冗余电源线是否插紧</li><li>2. 检查冗余电源模块是否故障</li><li>3. 对于可插拔的冗余电源模块，请重新安装冗余电源模块或更换冗余电源模块</li></ol>

## 15.30 RPS\_NORMAL

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

## 15.31 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	<ol style="list-style-type: none"><li>1. 如果后续子卡状态可以变为 Normal，则无需处理</li><li>2. 如果子卡一直处于 Falut 状态，则子卡故障，更换子卡</li></ol>

## 15.32 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

## 15.33 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

## 15.34 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	<ol style="list-style-type: none"><li>1. 检查子卡是否插紧</li><li>2. 检查子卡是否损坏</li><li>3. 重新安装子卡或更换子卡</li></ol>

## 15.35 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	<ol style="list-style-type: none"><li>1. 检查是否有用户在重启系统</li><li>2. 如果没有用户重启，等待系统重新启动后，通过 <code>display version</code> 命令显示信息中的 <code>Last reboot reason</code> 字段，查看重启原因</li><li>3. 如果重启原因为异常重启，请联系技术支持</li></ol>

## 15.36 TEMPERATURE\_ALARM

日志内容	<p>形式一： Temperature is greater than the high-temperature alarming threshold on sensor [STRING] [USHOT].</p> <p>形式二： Temperature is greater than the high-temperature alarming threshold on [STRING] sensor [STRING] [USHOT].</p> <p>形式三： Temperature is greater than the high-temperature alarming threshold on [STRING] [STRING] sensor [STRING] [USHOT].</p>
参数解释	<p>形式一： \$1: 传感器类型 \$2: 传感器ID</p> <p>形式二： \$1: slot编号 \$2: 传感器类型 \$3: 传感器ID</p> <p>形式三： \$1: chassis编号 \$2: slot编号 \$3: 传感器类型 \$4: 传感器ID</p>
日志等级	4
举例	DEV/4/TEMPERATURE_ALARM: Temperature is greater than the high-temperature alarming threshold on slot 1 sensor inflow 1.
日志说明	传感器温度超过了严重级（Alarm）高温告警门限。环境温度太高或者风扇异常
处理建议	<ol style="list-style-type: none"> <li>1. 检查环境温度是否过高，保持设备环境正常通风</li> <li>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</li> </ol>

## 15.37 TEMPERATURE\_LOW

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

## 15.38 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



## 15.39 TEMPERATURE\_SHUTDOWN

日志内容	<p>形式一： Temperature is greater than the high-temperature shutdown threshold on sensor [STRING] [INT32]. The slot will be powered off automatically.</p> <p>形式二： Temperature is greater than the high-temperature shutdown threshold on [STRING] sensor [STRING] [INT32]. The slot will be powered off automatically.</p> <p>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.</p>
参数解释	<p>形式一： \$1: 传感器类型 \$2: 传感器ID</p> <p>形式二： \$1: slot编号 \$2: 传感器类型 \$3: 传感器ID</p> <p>形式三： \$1: chassis编号 \$2: slot编号 \$3: 传感器类型 \$4: 传感器ID</p>
日志等级	2
举例	DEV/2/TEMPERATURE_SHUTDOWN: Temperature is greater than the high-temperature shutdown threshold on slot 1 sensor inflow 1. The slot will be powered off automatically.
日志说明	传感器温度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	<ol style="list-style-type: none"> <li>1. 检查环境温度是否过高，保持设备环境通风正常</li> <li>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</li> </ol>

## 15.40 TEMPERATURE\_WARNING

日志内容	形式一： Temperature is greater than the high-temperature warning threshold on sensor [STRING] [INT32]. 形式二： Temperature is greater than the high-temperature warning threshold on [STRING] sensor [STRING] [INT32]. 形式三： Temperature is greater than the high-temperature warning threshold on [STRING] [STRING] sensor [STRING] [INT32].
参数解释	形式一： \$1: 传感器类型 \$2: 传感器ID 形式二： \$1: slot编号 \$2: 传感器类型 \$3: 传感器ID 形式三： \$1: chassis编号 \$2: slot编号 \$3: 传感器类型 \$4: 传感器ID
日志等级	4
举例	DEV/4/TEMPERATURE_WARNING: Temperature is greater than the high-temperature warning threshold on slot 1 sensor inflow 1.
日志说明	传感器温度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	<ol style="list-style-type: none"><li>1. 检查环境温度是否过高，保持设备环境通风正常</li><li>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</li></ol>

## 15.41 TIMER\_CREATE\_FAILED\_FIRST

日志内容	The process with PID [UINT] failed to create a timer. Reason: [STRING].
参数解释	<p>\$1: 创建定时器的进程的PID</p> <p>\$2: 最近一次创建定时器失败的原因，取值为：</p> <ul style="list-style-type: none"> <li>Maximum number of timers already reached: 设备允许创建的定时器个数达到最大值</li> </ul>
日志等级	4
举例	DEV/4/TIMER_CREATE_FAILED_FIRST: The process with PID 70 failed to create a timer. Reason: Maximum number of timers already reached.
日志说明	<p>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：</p> <ul style="list-style-type: none"> <li>进程第一次创建定时器失败时立即输出 <code>TIMER_CREATE_FAILED_FIRST</code> 日志</li> <li>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 <code>TIMER_CREATE_FAILED_MORE</code>，<code>TIMER_CREATE_FAILED_MORE</code> 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</li> </ul>
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

## 15.42 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	<p>\$1: 创建定时器的进程的PID</p> <p>\$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</p> <p>\$3: 上次打印日志的时间</p> <p>\$4: 最近一次创建定时器失败的原因，取值为：</p> <ul style="list-style-type: none"> <li>Maximum number of timers already reached: 设备允许创建的定时器个数达到最大值</li> </ul>
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	<p>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：</p> <ul style="list-style-type: none"> <li>进程第一次创建定时器失败时立即输出 <code>TIMER_CREATE_FAILED_FIRST</code> 日志</li> <li>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 <code>TIMER_CREATE_FAILED_MORE</code>，<code>TIMER_CREATE_FAILED_MORE</code> 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</li> </ul>
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

## 15.43 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

# 16 DHCP

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

## 16.1 DHCP\_NORESOURCES

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

## 16.2 DHCP\_NOTSUPPORTED

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

# 17 DHCPD

本节介绍 DHCPD (IPv4 DHCP Relay) 模块输出的日志信息。

## 17.1 DHCPD\_SERVERCHANGE

日志内容	Switched to the server at [IPADDR] (VPN name: [STRING]) because the current server did not respond. Switched to the DHCP server at [IPADDR] (Public network) because the current DHCP server did not respond.
参数解释	\$1: 切换到下一个DHCP服务器的IP地址 \$2: 切换到下一个DHCP服务器的VPN信息 \$3: 切换到下一个DHCP服务器的IP地址, 该服务器处于公网中
日志等级	3
举例	DHCPD/3/DHCPD_SERVERCHANGE: -MDC=1; Switched to the server at 2.2.2.2 ( VPN name: 1 ) because the current server did not respond.
日志说明	因为DHCP中继无法从当前的DHCP服务器得到应答, 所以DHCP中继切换到下一台指定VPN内或公网内的DHCP服务器申请IP地址
处理建议	无需处理

## 17.2 DHCPD\_SWITCHMASTER

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

# 18 DHCPD

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

## 18.1 DHCP\_SERVER\_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	DHCP/5/DHCP_SERVER_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 0000-0000-905a) from p1 pool.
日志说明	IPv4 DHCP服务器为IPv4 DHCP客户端分配一个ipv4地址租约
处理建议	无

## 18.2 DHCP\_SERVER\_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	DHCP/5/DHCP_SERVER_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

## 18.3 DHCP\_SERVER\_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	DHCP_SERVER/5/DHCP_SERVER_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 0000-0000-905a).
日志说明	IPv4 DHCP服务器为IPv4 DHCP客户端续约
处理建议	无

## 18.4 DHCP\_SERVER\_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	DHCP_SERVER/4/DHCP_SERVER_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

## 18.5 DHCP\_SERVER\_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	DHCP/5/DHCP_SERVER_RECLAIM_IP: DHCP server reclaimed a p1 pool's lease(IP 1.0.0.91, lease 86400 seconds), which is allocated for the DHCP client (MAC 0000-0000-905a).
日志说明	IPv4 DHCP服务器回收一个分配给IPv4 DHCP客户端的地址租约
处理建议	无

## 18.6 DHCP\_SERVER\_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	DHCP/5/DHCP_SERVER_VERIFY_CLASS: Illegal DHCP client-PacketType=DHCPDISCOVER-ClientAddress=0000-5e01-0104;
日志说明	IPv4 DHCP服务器对客户端报文白名单验证不通过
处理建议	确认该DHCP客户端是否合法

# 19 DHCP6

本节介绍 DHCP6 (IPv6 DHCP server) 模块输出的 日志信息。



## 19.1 DHCPV6\_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	DHCPV6/5/DHCPV6_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

## 19.2 DHCPV6\_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	DHCPV6/5/DHCPV6_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

## 19.3 DHCP6\_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	DHCP6/5/DHCP6_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

## 19.4 DHCP6\_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	DHCP6/5/DHCP6_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

## 19.5 DHCP6\_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	DHCP6/5/DHCP6_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

## 19.6 DHCP6\_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	DHCP6/4/DHCP6_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

## 19.7 DHCP6\_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	DHCP6/5/DHCP6_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

## 19.8 DHCP6\_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	DHCP6/5/DHCP6_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

# 20 DHCPSP4

本节介绍 DHCPSP4 模块输出的日志信息。

## 20.1 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

## 20.2 DHCPSP4\_UNTRUSTED\_SERVER

日志内容	Detected reply packet from untrusted server. Server info: IPaddress = [IPADDR], MACaddress = [MAC], Interface = [STRING].
参数解释	\$1: 非信任DHCP服务器的IP地址 \$2: 非信任DHCP服务器的MAC地址 \$3: 连接非信任DHCP服务器的接口名称
日志等级	4
举例	DHCPSP4/4/DHCPSP4_UNTRUSTED_SERVER: Detected reply packet from untrusted server. Server Info: IPaddress = 192.168.1.1, MACaddress = 78a0-7aa4-0307, Interface = GigabitEthernet1/0/1.
日志说明	DHCP Snooping检测到非信任DHCP服务器的应答报文，丢弃该报文并生成包含非信任DHCP服务器的IP地址、MAC地址和连接接口名称信息的日志
处理建议	根据日志信息的IP地址和MAC地址等信息定位和处理非信任DHCP服务器

# 21 DHCPSP6

本节介绍 DHCPSP6 模块输出的 日志信息。

## 21.1 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

# 22 DIAG

本节介绍 Diagnostic 模块输出的日志信息。

## 22.1 CPU\_MINOR\_RECOVERY

日志内容	CPU usage recovered to normal state.
参数解释	无
日志等级	5
举例	DIAG/5/CPU_MINOR_THRESHOLD: CPU usage recovered to normal state.
日志说明	当设备处于CPU低级别告警状态，并且采样值小于或等于恢复门限时，解除CPU低级别告警状态，CPU使用率恢复到正常
处理建议	根据提示信息操作设备，合理使用CPU资源

## 22.2 CPU\_MINOR\_THRESHOLD

日志内容	<p>CPU usage is in minor alarm state.  CPU usage: [UINT]% in last 1 minute.  CPU usage thresholds:  Minor: [UINT]%  Severe: [UINT]%  Recovery: [UINT]%  Process info:  JID PID PRI State FDs HH:MM:SS CPU Name  [UINT] [UINT] [UINT] [CHAR] [UINT] [CHAR] [CHAR] [CHAR]  Core states:  ID Idle User Kernel Interrupt Busy  CPU[UINT] [CHAR] [CHAR] [CHAR] [CHAR] [CHAR]</p>
参数解释	<ul style="list-style-type: none"> <li>• 整个系统中 CPU 利用率的统计信息： <ul style="list-style-type: none"> <li>○ \$1: 过去 1 分钟内统计的 CPU 利用率</li> <li>○ \$2: 低级别告警门限</li> <li>○ \$3: 高级别告警门限</li> <li>○ \$4: 告警恢复门限</li> </ul> </li> <li>• 整个系统中 CPU 利用率最高的前 5 个进程的信息： <ul style="list-style-type: none"> <li>○ \$5: 进程 JID</li> <li>○ \$6: 进程 PID</li> <li>○ \$7: 进程的优先级</li> <li>○ \$8: 进程的状态</li> <li>○ \$9: 进程文件句柄</li> <li>○ \$10: 进程启动时长</li> <li>○ \$11: 进程的 CPU 占用率</li> <li>○ \$12: 进程名</li> </ul> </li> <li>• 整个系统中 CPU 利用率最高的前 5 个核的信息： <ul style="list-style-type: none"> <li>○ \$13: 核 ID</li> <li>○ \$14: 空闲时间</li> <li>○ \$15: 用户态进程占用的时间</li> <li>○ \$16: 内核线程占用的时间</li> <li>○ \$17: 中断占用的时间</li> <li>○ \$18: 运行时间</li> </ul> </li> </ul>
日志等级	4
举例	<p>DIAG/4/CPU_MINOR_THRESHOLD: CPU usage is in minor alarm state.  CPU usage: 3% in last 1 minute.  CPU usage thresholds:  Minor: 1%  Severe: 2%  Recovery: 0%  Process info:  JID PID PRI State FDs HH:MM:SS CPU Name</p>

日志内容	<p>CPU usage is in minor alarm state.  CPU usage: [UINT]% in last 1 minute.  CPU usage thresholds:  Minor: [UINT]%  Severe: [UINT]%  Recovery: [UINT]%  Process info:  JID PID PRI State FDs HH:MM:SS CPU Name  [UINT] [UINT] [UINT] [CHAR] [UINT] [CHAR] [CHAR] [CHAR]  Core states:  ID Idle User Kernel Interrupt Busy  CPU[UINT] [CHAR] [CHAR] [CHAR] [CHAR] [CHAR]</p>
	<pre> 108398 108398 120 S 36 00:00:0 12.58% snmpd 52 52 102 S 0 00:01:2 2.58% [DRV_FWD] 371 371 120 S 95 00:18:5 0.17% pppd 90 90 120 R 18 00:12:0 0.34% diagd 109 109 119 S 41 00:11:1 0.00% vbrd Core states: ID Idle User Kernel Interrupt Busy CPU0 98.61% 0.24% 0.62% 0.53% 1.39% CPU1 99.88% 0.00% 0.03% 0.09% 0.12%</pre>
日志说明	当CPU使用率的采样值从小于/等于变成大于低级别告警门限时，设备进入CPU低级别告警状态，并定期输出该日志，直到CPU低级别告警状态解除
处理建议	根据提示信息操作设备，合理使用CPU资源

## 22.3 CPU\_SEVERE\_RECOVERY

日志内容	CPU usage severe alarm removed.
参数解释	无
日志等级	5
举例	DIAG/5/CPU_RECOVERY: CPU usage severe alarm removed.
日志说明	当设备处于CPU高级别告警状态，并且采样值小于或等于低级别告警门限时，解除CPU高级别告警状态，输出该日志
处理建议	无



## 22.4 CPU\_SEVERE\_THRESHOLD

日志内容	<p>CPU usage is in severe alarm state.  CPU usage: [UINT]% in last 1 minute.  CPU usage thresholds:  Minor: [UINT]%  Severe: [UINT]%  Recovery: [UINT]%  Process info:  JID PID PRI State FDs HH:MM:SS CPU Name  [UINT] [UINT] [UINT] [CHAR] [UINT] [CHAR] [CHAR] [CHAR]  Core states:  ID Idle User Kernel Interrupt Busy  CPU[UINT] [CHAR] [CHAR] [CHAR] [CHAR] [CHAR]</p>
参数解释	<ul style="list-style-type: none"> <li>• 整个系统中 CPU 利用率的统计信息： <ul style="list-style-type: none"> <li>○ \$1: 过去 1 分钟内统计的 CPU 利用率</li> <li>○ \$2: 低级别告警门限</li> <li>○ \$3: 高级别告警门限</li> <li>○ \$4: 告警恢复门限</li> </ul> </li> <li>• 整个系统中 CPU 利用率最高的前 5 个进程的信息： <ul style="list-style-type: none"> <li>○ \$5: 进程 JID</li> <li>○ \$6: 进程 PID</li> <li>○ \$7: 进程的优先级</li> <li>○ \$8: 进程的状态</li> <li>○ \$9: 进程文件句柄</li> <li>○ \$10: 进程启动时长</li> <li>○ \$11: 进程的 CPU 占用率</li> <li>○ \$12: 进程名</li> </ul> </li> <li>• 整个系统中 CPU 利用率最高的前 5 个核的信息： <ul style="list-style-type: none"> <li>○ \$13: 核 ID</li> <li>○ \$14: 空闲时间</li> <li>○ \$15: 用户态进程占用的时间</li> <li>○ \$16: 内核线程占用的时间</li> <li>○ \$17: 中断占用的时间</li> <li>○ \$18: 运行时间</li> </ul> </li> </ul>
日志等级	3
举例	<p>DIAG/3/CPU_THRESHOLD: CPU usage is in severe alarm state.  CPU usage: 3% in last 1 minute.  CPU usage thresholds:  Minor: 1%  Severe: 2%  Recovery: 0%  Process info:  JID PID PRI State FDs HH:MM:SS CPU Name</p>

日志内容	<p>CPU usage is in severe alarm state.  CPU usage: [UINT]% in last 1 minute.  CPU usage thresholds:  Minor: [UINT]%  Severe: [UINT]%  Recovery: [UINT]%  Process info:  JID PID PRI State FDs HH:MM:SS CPU Name  [UINT] [UINT] [UINT] [CHAR] [UINT] [CHAR] [CHAR] [CHAR]  Core states:  ID Idle User Kernel Interrupt Busy  CPU[UINT] [CHAR] [CHAR] [CHAR] [CHAR] [CHAR]</p>
	<pre>108398 108398 120 S 36 00:00:0 12.58% snmpd 52 52 102 S 0 00:01:2 2.58% [DRV_FWD] 371 371 120 S 95 00:18:5 0.17% pppd 90 90 120 R 18 00:12:0 0.34% diagd 109 109 119 S 41 00:11:1 0.00% vbrd</pre> <p>Core states:  ID Idle User Kernel Interrupt Busy  CPU0 98.61% 0.24% 0.62% 0.53% 1.39%  CPU1 99.88% 0.00% 0.03% 0.09% 0.12%</p>
日志说明	当CPU使用率的采样值从小于/等于变成大于高级别告警门限时，设备进入CPU高级别告警状态，并定期输出该日志，直到CPU高级别告警状态解除
处理建议	请使用 <b>display current-configuration   include "monitor cpu-usage"</b> 命令查看CPU的告警门限，如果门限设置不合适，请使用 <b>monitor cpu-usage</b> 命令修改

## 22.5 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

## 22.6 DIAG\_FD\_UPLIMIT\_REACHED

日志内容	FD number upper limit already reached: Process name=[STRING], PID=[INTEGER].
参数解释	\$1: 进程的名称 \$2: 进程的ID
日志等级	4
举例	DIAG/4/DIAG_FD_UPLIMIT_REACHED: FD number upper limit already reached: Process name=snmpd, PID=244.
日志说明	进程已使用的FD个数已经达到上限
处理建议	无

## 22.7 DIAG\_FD\_UPLIMIT\_TO\_REACH

日志内容	Number of FDs is about to reach the upper limit: Process name=[STRING], PID=[INTEGER].
参数解释	\$1: 进程的名称 \$2: 进程的ID
日志等级	4
举例	DIAG/4/DIAG_FD_UPLIMIT_TO_REACH: Number of FDs is about to reach the upper limit. Process name=snmpd, PID=244.
日志说明	进程已使用的FD个数即将达到上限
处理建议	无

## 22.8 MEM\_ALERT

日志内容	<pre> 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] </pre>
参数解释	<ul style="list-style-type: none"> <li>• 整个系统中内存的统计信息： <ul style="list-style-type: none"> <li>○ \$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</li> <li>○ \$2: 整个系统已用的物理内存大小</li> <li>○ \$3: 整个系统可用的物理内存大小</li> <li>○ \$4: 多个进程共享的物理内存总额</li> <li>○ \$5: 已使用的文件缓冲区的大小</li> <li>○ \$6: 高速缓冲寄存器已使用的内存大小</li> </ul> </li> <li>• 应用程序对内存的使用情况： <ul style="list-style-type: none"> <li>○ \$7: <code>-/+ Buffers/Cache:used = Mem:Used – Mem:Buffers – Mem:Cached</code>，表示应用程序已用的物理内存大小</li> <li>○ \$8: <code>-/+ Buffers/Cache:free = Mem:Free + Mem:Buffers + Mem:Cached</code>，表示应用程序可用的物理内存大小</li> </ul> </li> <li>• 交换分区的使用信息： <ul style="list-style-type: none"> <li>○ \$9: 交换分区的总大小</li> <li>○ \$10: 已用的交换分区的大小</li> <li>○ \$11: 可用的交换分区的大小</li> </ul> </li> <li>• Low memory 的使用情况： <ul style="list-style-type: none"> <li>○ \$12: Low memory 中内存的大小</li> <li>○ \$13: Low memory 中已用内存的大小</li> <li>○ \$14: Low memory 中可用内存的大小</li> </ul> </li> </ul>
日志等级	4
举例	<pre> 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 </pre>
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	<ol style="list-style-type: none"> <li>1. 请使用 <code>display memory-threshold</code> 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 <code>memory-threshold</code> 命令修改</li> </ol>

日志内容	<pre> 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] </pre>
	<ol style="list-style-type: none"> <li>2. 检查 ARP、路由表信息，排除设备受到非法攻击可能</li> <li>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</li> </ol>

## 22.9 MEM\_BELOW\_THRESHOLD

日志内容	Memory usage has dropped below [STRING] threshold.
参数解释	<p>\$1: 内存告警门限级别，包括：</p> <ul style="list-style-type: none"> <li>o minor: 一级</li> <li>o severe: 二级</li> <li>o critical: 三级</li> </ul>
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

## 22.10 MEM\_EXCEED\_THRESHOLD

日志内容	Memory [STRING] threshold has been exceeded.
参数解释	<p>\$1: 内存告警门限级别，包括：</p> <ul style="list-style-type: none"> <li>o minor: 一级</li> <li>o severe: 二级</li> <li>o critical: 三级</li> </ul>
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	<ol style="list-style-type: none"> <li>1. 请使用 <code>display memory-threshold</code> 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 <code>memory-threshold</code> 命令修改</li> <li>2. 检查 ARP、路由表信息，排除设备受到非法攻击可能</li> <li>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</li> </ol>

## 22.11 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	设备当前的内存利用率
处理建议	无

# 23 DLDP

本节介绍 DLDP 模块输出的日志信息。

## 23.1 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 <ul style="list-style-type: none"><li>○ AUTHENTICATION PASSWORD: 表示验证字不匹配</li><li>○ AUTHENTICATION TYPE: 表示验证类型不匹配</li><li>○ INTERVAL: 表示通告间隔不匹配</li></ul>
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

## 23.2 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

## 23.3 DLDP\_LINK\_SHUTMODECHG

日志内容	DLDP automatically [STRING] interface [STRING] because the port shutdown mode was changed [STRING].
参数解释	<p>\$1: 接口关闭模式指定的动作</p> <ul style="list-style-type: none"> <li>○ blocked: 表示 DLDP 关闭了端口</li> <li>○ brought up: 表示 DLDP 打开了端口</li> </ul> <p>\$2: 接口名</p> <p>\$3: 接口关闭模式切换指向</p> <ul style="list-style-type: none"> <li>○ from manual to auto: 表示由手动模式切换到自动模式</li> <li>○ from manual to hybrid: 表示由手动模式切换到混合模式</li> <li>○ from hybrid to auto: 表示由混合模式切换到自动模式</li> <li>○ from hybrid to manual: 表示由混合模式切换到手动模式</li> </ul>
日志等级	5
举例	DLDP/5/DLDP_LINK_SHUTMODECHG: DLDP automatically blocked interface Ethernet1/1 because the port shutdown mode was changed from manual to auto.
日志说明	因为DLDP单通关闭模式发生变化，端口被关闭或打开
处理建议	无

## 23.4 DLDP\_LINK\_UNIDIRECTIONAL

日志内容	DLDP detected a unidirectional link on interface [STRING]. [STRING].
参数解释	<p>\$1: 接口名</p> <p>\$2: 接口关闭模式所指定的动作</p> <ul style="list-style-type: none"> <li>○ DLDP automatically blocked the interface: 表示 DLDP 自动关闭了端口</li> <li>○ Please manually shut down the interface: 表示需要用户手动关闭端口</li> <li>○ DLDP automatically shut down the interface. Please manually bring up the interface: 表示 DLDP 自动关闭了端口，需要用户手动打开端口</li> </ul>
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

## 23.5 DLDP\_NEIGHBOR\_AGED

日志内容	A neighbor on interface [STRING] was deleted because the neighbor was aged. The neighbor's system MAC is [MAC], and the port index is [UINT16].
参数解释	\$1: 接口名 \$2: MAC地址 \$3: 接口索引
日志等级	5
举例	DLDP/5/DLDP_NEIGHBOR_AGED: A neighbor on interface Ethernet1/1 was deleted because the neighbor was aged. The neighbor's system MAC is 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

## 23.6 DLDP\_NEIGHBOR\_CONFIRMED

日志内容	A neighbor was confirmed on interface [STRING]. The neighbor's system MAC is [MAC], and the port index is [UINT16].
参数解释	\$1: 接口名 \$2: MAC地址 \$3: 接口索引
日志等级	6
举例	DLDP/6/DLDP_NEIGHBOR_CONFIRMED: A neighbor was confirmed on interface Ethernet1/1. The neighbor's system MAC is 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



## 23.7 DLDP\_NEIGHBOR\_DELETED

日志内容	A neighbor on interface [STRING] was deleted because a [STRING] packet arrived. The neighbor's system MAC is [MAC], and the port index is [UINT16].
参数解释	\$1: 接口名 \$2: 报文类型 <ul style="list-style-type: none"><li>DISABLE: 表示收到了 Disable 报文</li><li>LINKDOWN: 表示收到了 LinkDown 报文</li></ul> \$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

# 24 DOT1X

本节介绍 802.1X（DOT1X）模块输出的日志信息。

## 24.1 DOT1X\_CONFIG\_NOTSUPPORT

日志内容	802.1X is not supported on interface [STRING].
参数解释	\$1: 接口名
日志等级	3
举例	DOT1X/3/DOT1X_CONFIG_NOTSUPPORT: 802.1X is not supported on interface GigabitEthernet1/0/1.
日志说明	接口不支持802.1X特性
处理建议	无

## 24.2 DOT1X\_LOGIN\_FAILURE

日志内容	-IfName=[STRING]-MACAddr=[STRING]-VLANID=[STRING]-Username=[STRING] -ErrCode=[STRING]; User failed 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 \$6: 用户802.1X认证失败的原因: <ul style="list-style-type: none"><li>o MAC address authorization failed: 授权 MAC 地址失败</li><li>o VLAN authorization failed: 授权 VLAN 失败</li><li>o VSI authorization failed: 授权 VSI 失败</li><li>o ACL authorization failed: 授权 ACL 失败</li><li>o User profile authorization failed: 授权 User Profile 失败</li><li>o URL authorization failed: 授权 URL 失败</li><li>o Microsegment authorization failed: 授权微分段失败</li></ul>
日志等级	6
举例	DOT1X/6/DOT1X_LOGIN_FAILURE: -IfName=GigabitEthernet1/0/1-MACAddr=0000-0001-0020-VLANID=2-Username=aaa- ErrCode=5; User failed 802.1X authentication. Reason: ACL authorization failed.
日志说明	用户802.1X认证失败
处理建议	查看失败原因并修改相关配置

## 24.3 DOT1X\_LOGIN\_SUCC

日志内容	-IfName=[STRING]-MACAddr=[STRING]-AccessVLANID=[STRING]-AuthorizationVLAN ID=[STRING]-Username=[STRING]; User passed 802.1X authentication and came online.
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=0010-8400- 22b9-AccessVLANID=444-AuthorizationVLANID=444-Username=aaa; User passed 802.1X authentication and came online.
日志说明	802.1X用户认证成功
处理建议	无

## 24.4 DOT1X\_LOGIN\_SUCC (in open mode)

日志内容	-IfName=[STRING]-MACAddr=[STRING]-VLANID=[STRING]-Username=[STRING]; The user that failed 802.1X authentication passed open authentication and came online.
参数解释	\$1: 接口名 \$2: MAC地址 \$3: VLAN ID \$4: 用户名
日志等级	6
举例	DOT1X/6/DOT1X_LOGIN_SUCC:-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9-VLANID=444-Username=00-10-84-00-22-b9; The user that failed 802.1X authentication passed open authentication and came online.
日志说明	802.1X认证失败但通过开放认证模式认证成功
处理建议	无

## 24.5 DOT1X\_LOGOFF

日志内容	-IfName=[STRING]-MACAddr=[STRING]-VLANID=[STRING]-Username=[STRING]-Err Code=[STRING]; 802.1X user was logged off.
参数解释	\$1: 接口名 \$2: MAC地址 \$3: VLAN ID \$4: 用户名 \$5: 错误码，包括如下取值： <ul style="list-style-type: none"><li>1: 客户端主动下线。可能原因为：<ul style="list-style-type: none"><li>客户端主动发送 logoff 报文下线</li><li>IP 电话 PC 口掉线</li></ul></li></ul>
日志等级	6
举例	DOT1X/6/DOT1X_LOGOFF:-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9- VLANID=444-Username=aaa-ErrCode=1; 802.1X user was logged off.
日志说明	802.1X用户正常下线
处理建议	无

## 24.6 DOT1X\_LOGOFF (in open mode)

日志内容	-IfName=[STRING]-MACAddr=[STRING]-VLANID=[STRING]-Username=[STRING]-ErrCode=[STRING]; 802.1X open user was logged off.
参数解释	\$1: 接口名 \$2: MAC地址 \$3: VLAN ID \$4: 用户名 \$5: 错误码
日志等级	6
举例	DOT1X/6/DOT1X_LOGOFF:-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9-VLANID=444-Username=aaa-ErrCode=1; 802.1X open user was logged off.
日志说明	802.1X open用户正常下线
处理建议	无

## 24.7 DOT1X\_LOGOFF\_ABNORMAL

日志内容	-IfName=[STRING]-MACAddr=[STRING]-VLANID=[STRING]-Username=[STRING]-ErrCode=[STRING]; 802.1X user was logged off abnormally.
参数解释	<p>\$1: 接口名</p> <p>\$2: MAC地址</p> <p>\$3: VLAN ID</p> <p>\$4: 用户名</p> <p>\$5: 错误码，包括如下取值：</p> <ul style="list-style-type: none"> <li>• 2: 端口状态错误。可能原因为： <ul style="list-style-type: none"> <li>○ 设备向服务器发送授权请求或者获取授权信息失败</li> <li>○ 进程重启或者主备倒换平滑在线用户时，端口 down 或者 deactive</li> <li>○ 生效的授权 VLAN 不在端口允许的 VLAN 列表里</li> <li>○ 接口上使能 802.1X SmartOn 功能，将未通过认证的用户踢下线</li> </ul> </li> <li>• 3: 目前不支持这种失败类型</li> <li>• 4: 用户重认证失败</li> <li>• 5: 设备强制去授权。可能原因为： <ul style="list-style-type: none"> <li>○ 授权处理失败</li> <li>○ 上线用户数超过最大值</li> <li>○ 全局关闭 OPEN 认证模式，OPEN 用户下线</li> <li>○ 关闭 802.1X 功能，用户下线</li> <li>○ 响应 MAC-VLAN 关闭事件，用户下线</li> <li>○ 执行 reset dot1x access-user 命令强制用户下线</li> </ul> </li> <li>• 6: 端口重启。目前不支持这种失败类型</li> <li>• 7: 用户平滑过程中，执行如下操作导致用户下线： <ul style="list-style-type: none"> <li>○ 关闭 802.1X 功能</li> <li>○ 执行 dot1x port-method 命令修改端口的接入控制方式</li> <li>○ 执行 dot1x port-control 命令修改设置端口的授权状态</li> </ul> </li> <li>• 8: 用户名或密码错误，或者服务器端没有配置设备信息</li> <li>• 9: 设备未收到客户端的握手报文</li> <li>• 10: 闲置切断。原因可能为用户在下线检测周期内没有流量，设备强制用户下线</li> <li>• 11: 限制用户在线时长（通过服务器下发的 session timeout 字段来设置）的切断。原因可能为 802.1X 会话超时导致设备强制用户下线</li> <li>• 12: 服务器发起的强制用户下线。原因可能为： <ul style="list-style-type: none"> <li>○ 在服务器端强制指定的用户下线</li> <li>○ 服务器通过 session control 功能强制用户下线</li> </ul> </li> <li>• 13: 实时计费失败</li> <li>• 14: 缺省错误，原因可能为： <ul style="list-style-type: none"> <li>○ MAC 绑定处理失败</li> <li>○ 认证成功后，清除操作 VLAN（Guest VLAN、Auth-Fail VLAN 和 Critical VLAN）失败</li> <li>○ 计费失败</li> <li>○ 处理 IPCIM 事件后重授权失败</li> </ul> </li> </ul>

日志内容	-IfName=[STRING]-MACAddr=[STRING]-VLANID=[STRING]-Username=[STRING]-ErrCode=[STRING]; 802.1X user was logged off abnormally.
日志等级	6
举例	DOT1X/6/DOT1X_LOGOFF_ABNORMAL:-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9-VLANID=444-Username=aaa-ErrCode=11; 802.1X user was logged off abnormally.
日志说明	802.1X用户异常下线
处理建议	查看异常下线原因或进行后续操作

## 24.8 DOT1X\_LOGOFF\_ABNORMAL (in open mode)

日志内容	-IfName=[STRING]-MACAddr=[STRING]-VLANID=[STRING]-Username=[STRING]-ErrCode=[STRING]; 802.1X open user was logged off abnormally.
参数解释	\$1: 接口名 \$2: MAC地址 \$3: VLAN ID \$4: 用户名 \$5: 错误码
日志等级	6
举例	DOT1X/6/DOT1X_LOGOFF_ABNORMAL:-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9-VLANID=444-Username=aaa-ErrCode=11; 802.1X open user was logged off abnormally.
日志说明	802.1X open用户异常下线
处理建议	查看异常下线原因或进行后续操作

## 24.9 DOT1X\_MACBINDING\_EXIST

日志内容	-IfName=[STRING]-MACAddr=[STRING]-VLANID=[STRING]-Username=[STRING]; MAC address was already bound to interface [STRING].
参数解释	\$1: 用户接入的接口名 \$2: MAC地址 \$3: VLAN ID \$4: 用户名 \$5: 已绑定MAC地址的接口名
日志等级	6
举例	DOT1X/6/DOT1X_MACBINDING_EXIST: -IfName=GigabitEthernet1/0/1-MACAddr=0000-0001-0020-VLANID=2-Username=aaa; MAC address was already bound to interface GigabitEthernet1/0/3.
日志说明	用户MAC地址已绑定在其它端口，用户无法上线
处理建议	在其它端口取消MAC地址绑定

## 24.10 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

## 24.11 DOT1X\_NOTENOUGH\_EADFREEMSEG\_RES

日志内容	Failed to assign a rule for free microsegment [microsegment-id] on interface [STRING] due to lack of ACL resources.
参数解释	\$1: 微分段ID \$2: 接口名
日志等级	3
举例	DOT1X/3/DOT1X_NOTENOUGH_EADFREEMSEG_RES: Failed to assign a rule for free microsegment 1 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，设备在接口上下发免认证微分段失败
处理建议	暂不使能802.1X，之后尝试重新使能802.1X

## 24.12 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

## 24.13 DOT1X\_NOTENOUGH\_EADMACREDIR\_RES

日志内容	Failed to assign a rule for redirecting HTTP packets with source MAC address [MAC] on interface [STRING].
参数解释	\$1: HTTP报文源MAC地址 \$2: 接口名
日志等级	3
举例	DOT1X/3/DOT1X_NOTENOUGH_EADMACREDIR_RES: Failed to assign a rule for redirecting HTTP packets with source MAC address 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



## 24.14 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

## 24.15 DOT1X\_NOTENOUGH\_ENABLEDOT1X\_RES

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

## 24.16 DOT1X\_PEXAGG\_NOMEMBER\_RES

日志内容	Failed to enable 802.1X on interface [STRING] because the Layer 2 extended-link aggregate interface does not have member ports.
参数解释	\$1: 接口名
日志等级	3
举例	DOT1X/3/DOT1X_PEXAGG_NOMEMBER_RES: Failed to enable 802.1X on interface Bridge-Aggregation100 because the Layer 2 extended-link aggregate interface does not have member ports.
日志说明	因为PEX二层聚合口不存在成员口，不能配置接口的802.1X特性
处理建议	暂不使能802.1X，PEX二层聚合口添加成员口后重新使能802.1X

## 24.17 DOT1X\_SMARTON\_FAILURE

日志内容	-IfName=[STRING]-MACAddr=[STRING]; User failed SmartOn authentication because [STRING].
参数解释	\$1: 接口名 \$2: MAC地址 \$3: 失败原因, 包括如下取值: <ul style="list-style-type: none"><li>the password was wrong.: 密码错误</li><li>the switch ID was wrong.: Switch ID 错误</li></ul>
日志等级	6
举例	DOT1X/6/DOT1X_SMARTON_FAILURE:-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9; User failed SmartOn authentication because the password is mismatched.
日志说明	SmartOn认证失败, 及其原因
处理建议	根据失败原因修改相关配置

## 24.18 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

# 25 DRNI

本节介绍 DRNI 模块输出的日志信息。

## 25.1 DRNI\_AUTORECOVERY\_TIMEOUT

日志内容	The reload delay timer timed out. Please check configuration of the DR system.
参数解释	无
日志等级	4
举例	DRNI/4/DRNI_AUTORECOVERY_TIMEOUT: The reload delay timer timed out. Please check configuration of the DR system.
日志说明	DR系统自动恢复定时器超时，DR系统仅一台设备启动或DR系统出现双主情况
处理建议	<ul style="list-style-type: none"><li>• 检查对端 DR 设备是否正常启动</li><li>• 检查 IPL 和 Keepalive 链路是否正常</li><li>• 检查自动恢复定时器配置值是否过小</li></ul>

## 25.2 DRNI\_GLBCHECK\_CONSISTENCY

日志内容	Finished global type [UINT16] configuration consistency check. No inconsistency exists.
参数解释	\$1: 全局配置的类型，取值为： <ul style="list-style-type: none"><li>• 1: 表示全局配置类型 1</li><li>• 2: 表示全局配置类型 2</li></ul>
日志等级	6
举例	DRNI/6/DRNI_GLBCHECK_CONSISTENCY: Finished global type 1 configuration consistency check. No inconsistency exists.
日志说明	分布式聚合全局配置一致性检查结果一致
处理建议	无

## 25.3 DRNI\_GLBCHECK\_INCONSISTENCY

日志内容	Detected global type [UINT16] configuration inconsistency.
参数解释	\$1: 全局配置的类型, 取值为: <ul style="list-style-type: none"><li>• 1: 表示全局配置类型 1</li><li>• 2: 表示全局配置类型 2</li></ul>
日志等级	6
举例	DRNI/6/DRNI_GLBCHECK_INCONSISTENCY: Detected global type 1 configuration inconsistency.
日志说明	分布式聚合全局配置一致性检查结果不一致
处理建议	<ul style="list-style-type: none"><li>• Type 1 类型的全局配置不一致, 通过 <code>display drni consistency</code> 命令查看两端设备配置信息, 修改配置为一致</li><li>• Type 2 类型的全局配置不一致, 建议两端设备配置为一致</li></ul>

## 25.4 DRNI\_IFCHECK\_CONSISTENCY

日志内容	Finished DR interface [STRING] type [UINT16] configuration consistency check. No inconsistency exists.
参数解释	\$1: 接口名称 \$2: 接口配置的类型, 取值为: <ul style="list-style-type: none"><li>• 1: 表示接口配置类型 1</li><li>• 2: 表示接口配置类型 2</li></ul>
日志等级	6
举例	DRNI/6/DRNI_IFCHECK_CONSISTENCY: Finished DR interface Bridge-Aggregation2 type 1 configuration consistency check. No inconsistency exists.
日志说明	分布式聚合接口配置一致性接口检查结果一致
处理建议	无

## 25.5 DRNI\_IFCHECK\_INCONSISTENCY

日志内容	Detected type [UINT16] configuration inconsistency on interface [STRING].
参数解释	\$1: 接口配置的类型, 取值为: <ul style="list-style-type: none"><li>• 1: 表示接口配置类型 1</li><li>• 2: 表示接口配置类型 2</li></ul> \$2: 接口名称
日志等级	6
举例	DRNI/6/DRNI_IFCHECK_INCONSISTENCY: Detected type 1 configuration inconsistency on interface Bridge-Aggregation2.
日志说明	分布式聚合接口配置一致性检查不一致
处理建议	<ul style="list-style-type: none"><li>• Type 1 类型的接口配置不一致, 通过 <code>display drni consistency</code> 命令查看两端设备配置信息, 修改配置为一致</li><li>• Type 2 类型的接口配置不一致, 建议两端设备配置为一致</li></ul>

## 25.6 DRNI\_IFEVENT\_DR\_BIND

日志内容	Interface [STRING] was assigned to DR group [UINT32].
参数解释	\$1: 二层聚合接口 \$2: 分布式聚合组编号
日志等级	6
举例	DRNI/6/DRNI_IFEVENT_DR_BIND: Interface Bridge-Aggregation1 was assigned to DR group 1.
日志说明	聚合接口加入分布式聚合组, 触发该日志的原因为用户设置
处理建议	无

## 25.7 DRNI\_IFEVENT\_DR\_GLOBALDOWN

日志内容	The state of DR group [UINT32] changed to down.
参数解释	\$1: DR组编号
日志等级	6
举例	DRNI/6/DRNI_IFEVENT_DR_GLOBALDOWN: The state of DR group 2 changed to down.
日志说明	DR组状态变为DOWN, 触发该日志的原因为两台DR设备上同一DR组的DR接口的成员端口都变为未选中状态
处理建议	检查DR设备的系统配置, 系统优先级、系统MAC地址、系统编号是否已配置且一致

## 25.8 DRNI\_IFEVENT\_DR\_GLOBALUP

日志内容	The state of DR group [UINT32] changed to up.
参数解释	\$1: DR组编号
日志等级	6
举例	DRNI/6/DRNI_IFEVENT_DR_GLOBALUP: The state of DR group 2 changed to up.
日志说明	DR组状态变为UP, 触发该日志的原因为两台DR设备上同一DR组的DR接口中第一次有成员端口变为被选中状态
处理建议	无

## 25.9 DRNI\_IFEVENT\_DR\_MAC\_CHANGE

日志内容	Local DR interface [STRING]'s system MAC address changed to [STRING]. Please ensure that the configuration is consistent with that of the peer DR interface.
参数解释	\$1: 二层聚合接口 \$2: 系统MAC地址
日志等级	6
举例	DRNI/6/DRNI_IFEVENT_DR_MAC_CHANGE: Local DR interface Bridge-Aggregation1's system MAC address changed to 2-2-2. Please ensure that the configuration is consistent with that of the peer DR interface.
日志说明	用户修改DR接口系统MAC地址
处理建议	无

## 25.10 DRNI\_IFEVENT\_DR\_NOSELECTED

日志内容	Local DR interface [STRING] in DR group [UINT32] does not have Selected member ports because [STRING].
参数解释	<p>\$1: 二层聚合接口            \$2: DR组编号            \$3: DR口DOWN的原因</p> <ul style="list-style-type: none"> <li>the aggregate interface went down. Please check the aggregate link status: 由于DR接口对应的聚合接口DOWN导致DR接口DOWN, 请检查聚合接口链路状态</li> <li>no peer DR interface was detected. Please check peer DR interface configuration: 由于未检测到对端DR接口导致的DR接口DOWN, 请检查对端DR设备的配置情况</li> <li>of configuration consistency check failure. Please check the type 1 configuration of the DR member devices for inconsistencies: 由于配置一致性检查失败导致的DR接口DOWN, 请检查DR设备的Type 1配置情况</li> <li>it was removed from a DR group. Please reconfigure the DR interface settings as needed: 由于聚合接口取消配置为DR接口, 导致DR接口DOWN, 请根据需求重新配置DR接口</li> </ul>
日志等级	6
举例	DRNI/6/DRNI_IFEVENT_DR_NOSELECTED: Local DR interface Bridge-Aggregation1 in DR group 2 does not have Selected member ports because no peer DR interface was detected. Please check peer DR interface configuration.
日志说明	本端DR接口对应的聚合组内无选中端口
处理建议	检查聚合组成员端口配置或者线缆连接情况

## 25.11 DRNI\_IFEVENT\_DR\_PEERBIND

日志内容	An aggregate interface on the peer DR device was assigned to DR group [UINT32].
参数解释	\$1: DR组编号
日志等级	6
举例	DRNI/6/DRNI_IFEVENT_DR_PEERBIND: An aggregate interface on the peer DR device was assigned to DR group 1.
日志说明	对端DR设备的聚合接口加入分布式聚合组, 触发该日志的原因为用户设置
处理建议	无

## 25.12 DRNI\_IFEVENT\_DR\_PEERUNBIND

日志内容	An aggregate interface on the peer DR device was removed from DR group [UINT32].
参数解释	\$1: DR组编号
日志等级	6
举例	DRNI/6/DRNI_IFEVENT_DR_PEERUNBIND: An aggregate interface on the peer DR device was removed from DR group 1.
日志说明	对端DR设备的聚合接口退出DR组，触发该日志的原因为用户设置
处理建议	无

## 25.13 DRNI\_IFEVENT\_DR\_PEER\_NOSELECTED

日志内容	Peer DR interface in DR group [UINT32] does not have Selected member ports.
参数解释	\$1: DR组编号
日志等级	6
举例	DRNI/6/DRNI_IFEVENT_DR_PEER_NOSELECTED: Peer DR interface in DR group 10 does not have Selected member ports.
日志说明	对端DR接口对应的聚合组内无选中端口
处理建议	检查对端聚合组成员端口配置或者线缆连接情况

## 25.14 DRNI\_IFEVENT\_DR\_PEER\_SELECTED

日志内容	Peer DR interface in DR group [UINT32] has Selected member ports.
参数解释	\$1: DR组编号
日志等级	6
举例	DRNI/6/DRNI_IFEVENT_DR_PEER_SELECTED: Peer DR interface in DR group 10 has Selected member ports.
日志说明	对端DR接口对应的聚合组内存在选中端口
处理建议	无



## 25.15 DRNI\_IFEVENT\_DR\_PRIORITY\_CHANGE

日志内容	DR interface [STRING]'s system priority changed to [UINT16]. Please ensure that the configuration is consistent with that of the peer DR interface.
参数解释	\$1: 二层聚合接口 \$2: 新的系统优先级
日志等级	6
举例	DRNI/6/DRNI_IFEVENT_PRIORITY_CHANGE: DR interface Bridge-Aggregation1's system priority changed to 564. Please ensure that the configuration is consistent with that of the peer DR interface.
日志说明	用户修改DR接口的系统优先级
处理建议	无

## 25.16 DRNI\_IFEVENT\_DR\_SELECTED

日志内容	Local DR interface [STRING] in DR group [UINT32] has Selected member ports.
参数解释	\$1: 二层聚合接口 \$2: DR组编号
日志等级	6
举例	DRNI/6/DRNI_IFEVENT_DR_SELECTED: Local DR interface Bridge-Aggregation1 in DR group 2 has Selected member ports.
日志说明	DR接口对应的聚合组内存在选中端口
处理建议	无

## 25.17 DRNI\_IFEVENT\_DR\_UNBIND

日志内容	Interface [STRING] was removed from DR group [UINT32].
参数解释	\$1: 二层聚合接口 \$2: DR组编号
日志等级	6
举例	DRNI/6/DRNI_IFEVENT_DR_UNBIND: Interface Bridge-Aggregation1 was removed from DR group 1.
日志说明	聚合接口退出DR组，触发该日志的原因为用户设置
处理建议	无

## 25.18 DRNI\_IFEVENT\_IPP\_BIND

日志内容	Interface [STRING] was configured as IPP [UINT16].
参数解释	\$1: 二层聚合接口 \$2: IPP口编号
日志等级	6
举例	DRNI/6/DRNI_IFEVENT_IPP_BIND: Interface Bridge-Aggregation1 was configured as IPP 1.
日志说明	聚合接口配置为IPP口，触发该日志的原因为用户设置
处理建议	无

## 25.19 DRNI\_IFEVENT\_IPP\_DOWN

日志内容	IPP [STRING] went down because [STRING].
参数解释	<p>\$1: 二层聚合接口</p> <p>\$2: IPP口DOWN的原因和处理建议</p> <ul style="list-style-type: none"> <li>the aggregate interface went down. Please check the aggregate link status: 由于 IPP 接口所在的聚合接口 DOWN 导致 IPP 接口 DOWN，请检查聚合接口的链路状态</li> <li>the tunnel interface went down. Please check the tunnel link status: 由于 IP 接口所在的 Tunnel 接口 DOWN 导致 IPP 接口 DOWN，请检查 Tunnel 接口的链路状态</li> <li>no DRCPDUs were received. Please check the devices' DRCPDU transmission and reception status: 由于接收不到有效 DRCP 报文导致的 IPP 口 DOWN，请检查两端 DRCP 报文收发状态</li> <li>the peer failed to receive DRCPDUs. Please check the devices' DRCPDU transmission and reception status: 由于对端设备接收不到有效 DRCP 报文导致的 IPP 口 DOWN，请检查两端 DRCP 报文收发状态</li> <li>the IPP role of the interface was removed. Please reconfigure an interface as the IPP: 由于接口取消配置为 IPP 口，导致 IPP 口 DOWN，请重新配置 IPP 口</li> </ul>
日志等级	6
举例	DRNI/6/DRNI_IFEVENT_IPP_DOWN: IPP Bridge-Aggregation1 went down because the tunnel interface went down. Please check the tunnel link status.
日志说明	IPP口变为DOWN
处理建议	<ul style="list-style-type: none"> <li>检查 DR 设备的系统配置，系统优先级、系统 MAC 地址、系统编号、认证密码、序列号校验功能状态，是否已配置且一致</li> <li>检查配置为 IPP 口的二层聚合接口状态</li> </ul>

## 25.20 DRNI\_IFEVENT\_IPP\_UNBIND

日志内容	Configuration for IPP [UINT16] was removed from interface [STRING].
参数解释	\$1: IPP口编号 \$2: 二层聚合接口
日志等级	6
举例	DRNI/6/DRNI_IFEVENT_IPP_UNBIND: Configuration for IPP 1 was removed from interface Bridge-Aggregation1.
日志说明	删除IPP口，触发该日志的原因为用户设置
处理建议	无

## 25.21 DRNI\_IFEVENT\_IPP\_UP

日志内容	IPP [STRING] came up.
参数解释	\$1: 二层聚合接口
日志等级	6
举例	DRNI/6/DRNI_IFEVENT_IPP_UP: IPP Bridge-Aggregation1 came up.
日志说明	IPP口变为UP状态，触发该日志的原因为DR系统两端能正常收发DRCP协议报文
处理建议	无

## 25.22 DRNI\_IPP\_BLOCK

日志内容	The status of IPP [STRING] changed to blocked.
参数解释	\$1: 二层聚合接口
日志等级	6
举例	DRNI/6/DRNI_IPP_BLOCK: The status of IPP Bridge-Aggregation20 changed to blocked.
日志说明	IPP口变为阻塞状态，该状态下IPP口仅能收发协议报文，不能收发数据报文。触发该日志的原因为当设备有角色且IPP口down时，IPP口变为阻塞状态
处理建议	<ul style="list-style-type: none"><li>检查 IPL 连接线缆是否正常</li><li>检查 IPL 两端配置是否一致</li></ul>

## 25.23 DRNI\_IPP\_UNBLOCK

日志内容	The status of IPP [STRING] changed to unblocked.
参数解释	\$1: 二层聚合接口
日志等级	6
举例	DRNI/6/DRNI_IPP_UNBLOCK: The status of IPP Bridge-Aggregation20 changed to unblocked.
日志说明	IPP口变为非阻塞状态，该状态下IPP口可以正常收发协议报文和数据报文。触发该日志的原因因为当设备有角色且IPP口up时，IPP口变为非阻塞状态
处理建议	无

## 25.24 DRNI\_KEEPLIVEINTERVAL\_MISMATCH

日志内容	Keepalive interval on the local DR device is different from that on the neighbor.
参数解释	无
日志等级	6
举例	DRNI/6/DRNI_KEEPLIVEINTERVAL_MISMATCH: Keepalive interval on the local DR device is different from that on the neighbor.
日志说明	DR系统两端的Keepalive报文发包间隔配置的不一致，会导致一端快速超时，出现误检测，触发该日志的原因因为DR系统两端配置的Keepalive报文发包间隔不一致
处理建议	将DR系统两端的Keepalive报文发包间隔配置一致

## 25.25 DRNI\_KEEPAVIVELINK\_DOWN

日志内容	Keepalive link went down because [STRING].
参数解释	<p>\$1: Keepalive链路故障原因和处理建议</p> <ul style="list-style-type: none"><li>keepalive IP address was not configured. Please configure keepalive IP address: 由于未配置 Keepalive 报文的 IP 地址导致的 Keepalive 链路 DOWN, 请先配置 Keepalive 报文的 IP 地址</li><li>the device failed to send keepalive packets. Please check Layer 3 reachability to the peer: 由于本端发送报文失败导致的 Keepalive 链路文 DOWN, 请检查三层路由是否可达</li><li>the local keepalive timeout timer expired. Please check the keepalive packet transmission and reception status at the two ends: 由于本端接收报文超时导致的 Keepalive 链路 DOWN, 请检查两端 Keepalive 报文收发状态</li><li>the peer keepalive timeout timer expired. Please check the keepalive packet transmission and reception status at the two ends: 由于对端接收报文超时导致的 Keepalive 链路 DOWN, 请检查两端 Keepalive 报文收发状态</li></ul>
日志等级	6
举例	DRNI/6/DRNI_KEEPAVIVELINK_DOWN: Keepalive link went down because the local keepalive timeout timer expired. Please check the keepalive packet transmission and reception status at the two ends.
日志说明	Keepalive链路变为DOWN状态
处理建议	<ul style="list-style-type: none"><li>检查设备角色</li><li>检查 DR 设备的 Keepalive 配置, 两端源 IP、目的 IP 是否匹配</li><li>检查所选取的三层链路状态</li></ul>

## 25.26 DRNI\_KEEPAVIVELINK\_UP

日志内容	Keepalive link came up.
参数解释	无
日志等级	6
举例	DRNI/6/DRNI_KEEPAVIVELINK_UP: Keepalive link came up.
日志说明	KEEPAVIVELINK链路变为UP状态, 触发该日志的原因因为DR系统两端能正常收发Keepalive协议报文
处理建议	无

## 25.27 DRNI\_DEVICE\_MADDOWN

日志内容	[STRING] will change to the DRNI MAD DOWN state because [STRING].
参数解释	<p>\$1: 设备下发DRNI MAD DOWN的接口范围</p> <ul style="list-style-type: none"> <li>○ All service interfaces not excluded from the DRNI MAD DOWN action: 设备上所有不是 DRNI MAD 保留口的接口</li> <li>○ All service interfaces included in the DRNI MAD DOWN action: 设备上所有属于 DRNI MAD include 的接口</li> <li>○ All new service interfaces not excluded from the DRNI MAD DOWN : 设备上所有新加入且不是 DRNI MAD 保留口的接口</li> <li>○ All new service interfaces included in the DRNI MAD DOWN action: 设备上所有新加入且属于 DRNI MAD include 的接口</li> </ul> <p>\$2: 设备下发DRNI MAD DOWN的原因和处理建议</p> <ul style="list-style-type: none"> <li>○ the device is Initializing. Please set up the DR system first: 设备正处于初始化状态, 请先建立 DR 系统</li> <li>○ the IPL went down and the keepalive link remains up. Please check the IPL settings on both ends of the IPL: 由于 IPL 链路故障但 Keepalive 链路状态是 up 的, 请检查分布式聚合设备两端 IPL 配置</li> <li>○ the IPL came up. Please wait for the data restoration delay timer to expire: 由于 IPL 恢复工作, 请等待延迟恢复定时器超时</li> <li>○ the IPL and all DR interfaces went down. Please first check the IPL settings on both ends of the IPL: 由于 IPL 和设备上所有 DR 接口故障, 设备无法正常工作, 请先检查两端设备 IPL 配置</li> </ul>
日志等级	4
举例	DRNI/4/DRNI_DEVICE_MADDOWN: All service interfaces not excluded from the DRNI MAD DOWN action will change to the DRNI MAD DOWN state because the IPL went down and the keepalive link remains up. Please check the IPL settings on both ends of the IPL.
日志说明	不同原因触发设备进行DRNI MAD检测时, 设备会根据触发原因和当前配置关闭相应业务接口
处理建议	检查IPL两端配置

## 25.28 DRNI\_DEVICE\_MADRECOVERY

日志内容	All service interfaces on the device will be recovered from the DRNI MAD DOWN state.
参数解释	无
日志等级	4
举例	DRNI/4/DRNI_DEVICE_MADRECOVERY: All service interfaces on the device will be recovered from the DRNI MAD DOWN state.
日志说明	设备将会开启所有处于DRNI MAD DOWN状态的业务接口
处理建议	无

## 25.29 DRNI\_SYSEVENT\_DEVICEROLE\_CHANGE

日志内容	Device role changed from [STRING] to [STRING] for [STRING].
参数解释	<p>\$1: 旧的设备角色, Primary、Secondary或None \$2: 新的设备角色, Primary、Secondary或None \$3: 角色变化原因:</p> <ul style="list-style-type: none"><li>DR system initialization: DR 系统初始化</li><li>IPL down and all DR interfaces down: IPL 故障时, 所有 DR 接口处于 down 状态</li><li>IPL and keepalive link down: IPL 和 Keepalive 链路均故障</li><li>IPL calculation: 本端设备角色通过 IPL 计算</li><li>IPL down and role calculation based on keepalive link: IPL 故障时, 本端设备角色通过 Keepalive 链路计算</li></ul>
日志等级	6
举例	DRNI/6/DRNI_SYSEVENT_DEVICEROLE_CHANGE: Device role changed from Secondary to Primary for IPL calculation.
日志说明	DR设备角色变化及触发原因
处理建议	无

## 25.30 DRNI\_SYSEVENT\_MAC\_CHANGE

日志内容	System MAC address changed from [STRING] to [STRING].
参数解释	<p>\$1: 旧的系统MAC \$2: 新的系统MAC</p>
日志等级	6
举例	DRNI/6/DRNI_SYSEVENT_MAC_CHANGE: System MAC address changed from 1-1-1 to 2-2-2.
日志说明	分布式聚合系统MAC变化, 触发该日志的原因为用户设置
处理建议	无

## 25.31 DRNI\_SYSEVENT\_MODE\_CHANGE

日志内容	The device's working mode changed to [STRING].
参数解释	\$1: 设备工作模式 <ul style="list-style-type: none"><li>DR system: DR 系统</li><li>standalone: 独立工作</li></ul>
日志等级	6
举例	DRNI/6/DRNI_SYSEVENT_MODE_CHANGE: The device's working mode changed to standalone.
日志说明	DR设备工作模式变化，触发原因为DR系统分裂或者合并
处理建议	无

## 25.32 DRNI\_SYSEVENT\_NUMBER\_CHANGE

日志内容	System number changed from [STRING] to [STRING].
参数解释	\$1: 旧的系统编号 \$2: 新的系统编号
日志等级	6
举例	DRNI/6/DRNI_SYSEVENT_NUMBER_CHANGE: System number changed from 1 to 2.
日志说明	分布式聚合系统编号变化，触发该日志的原因为用户设置
处理建议	无

## 25.33 DRNI\_SYSEVENT\_PRIORITY\_CHANGE

日志内容	System priority changed from [UINT16] to [UINT16].
参数解释	\$1: 旧的系统优先级 \$2: 新的系统优先级
日志等级	6
举例	DRNI/6/DRNI_SYSEVENT_PRIORITY_CHANGE: System priority changed from 123 to 564.
日志说明	分布式聚合系统优先级改变，触发该日志的原因为用户设置
处理建议	无



## 25.34 DRNI\_VMAC\_INEFFECTIVE

日志内容	Failed to assign virtual MAC address [STRING] to interface [STRING]. Cause: [STRING].
参数解释	\$1: 虚拟MAC地址 \$2: 接口名称, 目前仅支持VLAN接口和LoopBack接口 \$3: 失败原因, 目前仅包括硬件资源不足
日志等级	3
举例	DRNI/3/DRNI_VMAC_INEFFECTIVE: Failed to assign virtual MAC address 0001-0001-0001 to interface Vlan-interface10. Cause: Insufficient hardware resources.
日志说明	在接口下配置DRNI虚拟IP地址和虚拟MAC地址时, 由于硬件资源不足, 导致添加虚拟MAC地址失败
处理建议	无

# 26 DRVPLAT

## 26.1 DRVPLAT

### 26.1.1 DRVPLAT/4/DrvDebug

日志内容	The (undo) cut-through enable command requires a reboot to take effect.
参数解释	无
日志等级	4
举例	DRVPLAT/4/DrvDebug: -Slot=1; The (undo) cut-through enable command requires a reboot to take effect.
日志说明	配置cut-through enable或undo cut-through enable命令后, 必须保存配置并重启设备才能生效
处理建议	保存配置并重启设备

## 26.1.2 DRVPLAT/4/DrvDebug

日志内容	The device will reboot because the chip temperature is [UINT32] degrees, exceeding the overtemperature reboot threshold of [UINT32] degrees.
参数解释	\$1: 当前芯片温度 \$2: 过温重启门限
日志等级	4
举例	DRVPLAT/4/DrvDebug: The device will reboot because the chip temperature is 128 degrees, exceeding the overtemperature reboot threshold of 122 degrees.
日志说明	检测到芯片温度超过过温重启门限122度，当前芯片温度为128度，设备重启
处理建议	检查设备风扇模块是否正常

## 26.2 DRVDEBUGMOD\_BSP

### 26.2.1 DRVPLAT/3/DrvDebug

日志内容	I2c read need to retry, p1= [STRING], p2 = [STRING], times: [STRING]
参数解释	\$1: 总线地址 \$2: 设备地址 \$3: 重试次数 其中times 参数最大为3，即如果出现3代表通过总共4次访问均失败，如果小于3，可忽略
日志等级	3
举例	DRVPLAT/3/DrvDebug: I2c read need to retry, p1=0x52, p2 = 0x20, times: 0 在读eeprom（0x52为eeprom的I2C 总线地址）的地址0x20时，出现错误，需要重试
日志说明	I2C总线读操作过程中出现错误，需要重试
处理建议	如果出现times : 3代表通过总共4次访问均失败，请联系技术支持 如果小于3，可忽略

## 26.2.2 DRVPLAT/3/DrvDebug

日志内容	I2c write need to retry, p1 = [STRING], p2 = [STRING], times: [STRING]
参数解释	\$1: 总线地址 \$2: 设备地址 \$3: 重试次数 其中times 参数最大为3, 即如果出现3代表通过总共4次访问均失败, 如果小于3, 可忽略
日志等级	3
举例	DRVPLAT/3/DrvDebug: I2c write need to retry, p1=0x52, p2 = 0x20, times: 0 在写eeprom (0x52为eeprom的I2C 总线地址) 的地址0x20时, 出现错误, 需要重试
日志说明	I2C总线写操作过程中出现错误, 需要重试
处理建议	如果出现times : 3代表通过总共4次访问均失败, 请联系技术支持 如果小于3, 可忽略

## 26.2.3 DRVPLAT/3/DrvDebug

日志内容	I2C Stop,bus is busy!
参数解释	无参数
日志等级	3
举例	无参数变化, 不举例
日志说明	提示I2C总线忙
处理建议	请联系技术支持

## 26.2.4 DRVPLAT/3/DrvDebug

日志内容	I2c Start, read state retry!
参数解释	无参数
日志等级	3
举例	无参数变化, 不举例
日志说明	提示I2C总线发送Start命令后, 发送完成状态寄存器一直未显示发送完成
处理建议	请忽略

### 26.2.5 DRVPLAT/3/DrvDebug

日志内容	I2c Start, write cmd retry!
参数解释	无参数
日志等级	3
举例	无参数变化，不举例
日志说明	I2C总线发送start命令后，程序判断波形未发出，进行重试操作
处理建议	请忽略

### 26.2.6 DRVPLAT/3/DrvDebug

日志内容	There is no i2c device ack!
参数解释	无参数
日志等级	3
举例	无参数变化，不举例
日志说明	提示当写数据时I2C总线中断过程错误，并给出进程号和I2C设备地址
处理建议	请联系技术支持

### 26.2.7 DRVPLAT/3/DrvDebug

日志内容	I2c Read, transmit state retry! i = [STRING].
参数解释	\$1: I2C读取数据的第几个字节出现了错误。状态寄存器一直显示未完成，程序会进行重试 注：驱动代码中，一次I2C读操作可以读取多个字节
日志等级	3
举例	DRVPLAT/3/DrvDebug: I2c Read, transmit state retry! i = 2. 一次读多个字节，读取第3个（i是从0开始计数的）的时候出现了错误
日志说明	提示当读数据时，I2C总线一直处于未完成状态，并给出第几个字节出现错误
处理建议	程序会自行重试，请忽略

## 26.2.8 DRVPLAT/3/DrvDebug

日志内容	I2c Write, transmit state retry! i =[STRING].
参数解释	参数解释 \$1: I2C写入数据的第几个字节出现了错误。状态寄存器一直显示未完成，程序会进行重试 注：驱动代码中，一次I2C写操作可以写入多个字节
日志等级	3
举例	DRVPLAT/3/DrvDebug: I2c Write, transmit state retry! i = 2. 一次写多个字节，写入第3个（i是从0开始计数的）的时候出现了错误
日志说明	提示当读数据时I2C总线中断过程错误，并给出进程号和I2C设备地址
处理建议	程序会自行重试，请忽略

## 26.2.9 DRVPLAT/3/DrvDebug

日志内容	I2c write no ack count = [STRING].. i = [STRING]..
参数解释	\$1: 本次写操作写入字节总数 \$2: 写入第几个出现了未收到ACK的错误
日志等级	3
举例	DRVPLAT/3/DrvDebug: I2c write no ack count = 3.. i = 2..
日志说明	提示写入总共3个字节，第3个（i是从0开始计数的）出现了错误
处理建议	程序会自行重试，请忽略

## 26.2.10 DRVPLAT/3/DrvDebug

日志内容	I2C read or write! DevAddr = [STRING], WR = [STRING], len = [STRING], num = [STRING], i = [STRING]
参数解释	\$1: 设备的总线地址 \$2: 0, 指写操作; 1, 指读操作 \$3: 一次读/写字节数 \$4: 一次操作发送I2C start的次数 \$5: 读/写第几个字节的时候出现了错误
日志等级	3
举例	DRVPLAT/3/DrvDebug: I2C read or write! DevAddr = 0x52, WR = 1, len = 3, num = 2, i = 2 eeprom（0x52为eeprom设备地址），读操作，一次读取3个字节，发送了2个start，在第3个字节出现了错误
日志说明	提示I2C总线访问失败，打印参数方便问题定位
处理建议	程序会自行重试，请忽略

### 26.2.11 DRVPLAT/3/DrvDebug

日志内容	I2C stop! DevAddr = [STRING], WR = [STRING], len = [STRING], num = [STRING], i = [STRING]
参数解释	\$1: 设备的总线地址 \$2: 0, 指写操作; 1, 指读操作 \$3: 一次读/写字节数 \$4: 一次操作发送I2C start的次数 \$5: 读/写第几个字节的时候出现了错误
日志等级	3
举例	DRVPLAT/3/DrvDebug: I2C stop! DevAddr = 0x52, WR = 1, len = 3, num = 2, i = 2 eeprom (0x52为eeprom设备地址), 读操作, 一次读取3个字节, 发送了2个start, 在第3个字节出现了错误
日志说明	提示I2C总线发送stop命令失败, 打印参数方便问题定位
处理建议	程序会自行重试, 请忽略

### 26.2.12 DRVPLAT/3/DrvDebug

日志内容	PCA9548 sel, write need to retry, present try times is [STRING],.
参数解释	其中times 参数最大为3, 即如果出现3代表通过总共4次访问均失败, 如果小于3, 可忽略
日志等级	3
举例	DRVPLAT/3/DrvDebug: PCA9548 sel, write need to retry, present try times is 0,.
日志说明	提示I2C选通器件9548选通第一次访问失败, 需要重试
处理建议	如果出现times : 3代表通过总共4次访问均失败, 请联系技术支持 如果小于3, 可忽略

### 26.2.13 DRVPLAT/3/DrvDebug

日志内容	I2c logic select is error.
参数解释	无参数
日志等级	3
举例	无参数变化, 不举例
日志说明	提示通过CPLD逻辑选通I2C通道失败 注: 有些元器件需要通过逻辑选通I2C通道, 例如光模块
处理建议	请联系技术支持

## 26.3 DRVDEBUGMOD\_DEVM

### 26.3.1 DRVPLAT/2/DrvDebug

日志内容	The device doesn't support the subcard in subslot [UINT32].
参数解释	\$1: 子卡槽位号
日志等级	2
举例	DRVPLAT/2/DrvDebug: The device doesn't support the subcard in subslot 1.
日志说明	本设备不支持该槽位的子卡
处理建议	请联系技术支持

### 26.3.2 DRVPLAT/2/DrvDebug

日志内容	This device do not support this kind of board!
参数解释	无
日志等级	2
举例	DRVPLAT/2/DrvDebug: This device do not support this kind of board!
日志说明	本设备不支持这种类型的单板
处理建议	请联系技术支持

### 26.3.3 DRVPLAT/2/DrvDebug

日志内容	Warning: Standby board on chassis [UINT32]slot [UINT32]is not compatible with master board, Standby board type is [UINT32].
参数解释	\$1: 设备在IRF中的成员编号 \$2: 备用主控板槽位号 \$3: 备用主控板的板类型
日志等级	2
举例	DRVPLAT/2/DrvDebug: Warning: Standby board on chassis1slot 4 is not compatible with master board, Standby board type is 1.0.
日志说明	IRF模式下，备用主控板与全局主控板类型不匹配
处理建议	请联系技术支持

### 26.3.4 DRVPLAT/2/DrvDebug

日志内容	Warning: Standby board on slot [UINT32] is not compatible with master board, Standby board type is [UINT32].
参数解释	\$1: 备用主控板槽位号 \$2: 备用主控板的板类型
日志等级	2
举例	DRVPLAT/2/DrvDebug: Warning: Standby board on slot 4 is not compatible with master board, Standby board type is 1.0.
日志说明	独立运行模式下，备用主控板和主控板的类型不匹配
处理建议	请联系技术支持

### 26.3.5 DRVPLAT/2/DrvDebug

日志内容	Warning: The LPU board on chassis [UINT32] slot [UINT32] is not compatible with MPU board, its board type is [UINT32].
参数解释	\$1: 设备在IRF中的成员编号 \$2: 业务板槽位号 \$3: 业务板的板类型
日志等级	2
举例	DRVPLAT/2/DrvDebug: Warning: The LPU board on chassis 1 slot 1 is not compatible with MPU board, its board type is 3.0..
日志说明	IRF模式下，业务板和全局主控板的类型不匹配
处理建议	请联系技术支持



### 26.3.6 DRVPLAT/2/DrvDebug

日志内容	Warning: The LPU board on slot [UINT32] is not compatible with MPU board, its board type is [UINT32].
参数解释	\$1: 业务板槽位号 \$2: 业务板的板类型
日志等级	2
举例	DRVPLAT/2/DrvDebug: The LPU board on slot 1 is not compatible with MPU board, its board type is 3.0.
日志说明	独立运行模式下，业务板和全局主控板的类型不匹配
处理建议	请联系技术支持

### 26.3.7 DRVPLAT/2/DrvDebug

日志内容	The software version is not compatible with the hardware.
参数解释	无
日志等级	2
举例	DRVPLAT/2/DrvDebug: The software version is not compatible with the hardware.
日志说明	加载的软件和硬件不匹配
处理建议	请联系技术支持

### 26.3.8 DRVPLAT/4/DrvDebug

日志内容	Board state changed to Fault on slot [UINT32], type is unknown.
参数解释	\$1: 单板所在的槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: Board state changed to Fault on slot 3, type is unknown.
日志说明	单板插入时出现此日志属于正常，运行正常的单板检测到故障会打印此信息
处理建议	请联系技术支持

## 26.4 DRVDEBUGMOD\_GOLD

### 26.4.1 DRVPLAT/2/DrvDebug

日志内容	WARNING: interface [STRING] link down
参数解释	\$1: 接口号
日志等级	2
举例	DRVPLAT/2/DrvDebug: WARNING: interface GigabitEthernet 1/0/1 link down
日志说明	接口链路失效
处理建议	<ol style="list-style-type: none"><li>1. 检查是否是网线没插好或直接重新插拔一下网线</li><li>2. 更换网线来检查网线是否正常</li><li>3. 更换本端设备端口（如果条件允许，推荐使用其它槽位的同类型单板）来检查故障是否排除</li><li>4. 更换对端设备端口（如果条件允许，推荐使用其它槽位的同类型单板）来检查故障是否排除</li><li>5. 如上述步骤故障仍未解决，请联系技术支持</li></ol>

### 26.4.2 DRVPLAT/2/DrvDebug

日志内容	WARNING: Local Slot [UINT32] update port info for GOLD failed, while port monitor enable!
参数解释	\$1: 单板所在的槽位号
日志等级	2
举例	DRVPLAT/2/DrvDebug: WARNING: Local Slot 5 update port info for GOLD failed, while port monitor enable!
日志说明	端口监控使能时更新GOLD端口信息失败
处理建议	请联系技术支持

### 26.4.3 DRVPLAT/2/DrvDebug

日志内容	Chassis [UINT32] Slot [UINT32] Unit [UINT32] Port [UINT32] error frame detected!
参数解释	\$1: 设备在IRF中的成员编号 \$2: 单板所在的槽位号 \$3: 单板上的芯片编号 \$4: 单板上的端口编号
日志等级	2
举例	DRVPLAT/2/DrvDebug: Chassis=1-Slot=5; Chassis 1 Slot 5 Unit 0 Port 1 error frame detected!
日志说明	端口检测到错误帧
处理建议	请联系技术支持

### 26.4.4 DRVPLAT/4/DrvDebug

日志内容	WARNING: Unit=[UINT32],Port=[UINT32] has FCS errors, please check.
参数解释	\$1: 芯片编号 \$2: 端口编号
日志等级	4
举例	DRVPLAT/4/DrvDebug: WARNING: Unit=0,Port=1 has FCS errors, please check.
日志说明	端口检测到FCS（frame check sequence,帧校验）错误
处理建议	请联系技术支持

### 26.4.5 DRVPLAT/4/DrvDebug

日志内容	WARNING: interface [STRING] has FCS errors, please check.
参数解释	\$1: 接口号
日志等级	4
举例	DRVPLAT/4/DrvDebug: -MDC=1;WARNING: interface GigabitEthernet 1/0/1 has FCS errors, please check.
日志说明	接口检测到FCS（frame check sequence,帧校验）错误
处理建议	请联系技术支持

## 26.4.6 DRVPLAT/4/DrvDebug

日志内容	WARNING: Chassis [UINT32] Slot [UINT32] Unit [UINT32] Port [UINT32] has FCS errors, please check.
参数解释	\$1: 设备在IRF中的成员编号 \$2: 单板所在的槽位号 \$3: 单板上的芯片编号 \$4: 单板上的端口编号
日志等级	4
举例	DRVPLAT/4/DrvDebug: -MDC=1-Chassis=1-Slot=5;WARNING: Chassis 1 Slot 5 Unit 0 Port 1 has FCS errors, please check.
日志说明	单板端口检测到FCS（frame check sequence,帧校验）错误
处理建议	请联系技术支持

## 26.4.7 DRVPLAT/4/DrvDebug

日志内容	WARNING: Chassis [UINT32] slot [UINT32] is isolated already. Maybe caused by the hardware failure, please remove and check it.
参数解释	\$1: 设备在IRF中的成员编号 \$2: 单板所在的槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: -MDC=1-Chassis=1-Slot=5;WARNING: Chassis 1 slot 5 is isolated already. Maybe caused by the hardware failure, please remove and check it.
日志说明	可能由于硬件错误导致某单板被隔离，请移除该单板并检查
处理建议	请移除该单板并联系技术支持

## 26.4.8 DRVPLAT/4/DrvDebug

日志内容	WARNING: Slot [UINT32] is isolated already. Maybe caused by the hardware failure, please remove and check it.
参数解释	\$1: 单板所在的槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: -MDC=1;WARNING: Slot 5 is isolated already. Maybe caused by the hardware failure, please remove and check it.
日志说明	可能由于硬件错误导致某单板被隔离，请移除该单板并检查
处理建议	请移除该单板并联系技术支持

## 26.4.9 DRVPLAT/4/DrvDebug

日志内容	Chassis [UINT32] slot [UINT32] has a hardware error, will be rebooted. Please check it.
参数解释	\$1: 设备在IRF中的成员编号 \$2: 单板所在的槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: Chassis 1 slot 2 has a hardware error, will be rebooted. Please check it.
日志说明	检测到单板的硬件存在故障，此故障单板将被自动重启
处理建议	<ul style="list-style-type: none"><li>若自动重启后单板仍然故障，且自动重启次数达到 3 次，单板将被自动隔离，</li><li>单板被自动隔离后，请联系技术支持</li></ul>

## 26.4.10 DRVPLAT/4/DrvDebug

日志内容	Slot [UINT32] has a hardware error, will be rebooted. Please check it.
参数解释	\$1: 单板所在的槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: Slot 2 has a hardware error, will be rebooted. Please check it.
日志说明	检测到单板的硬件存在故障，此故障单板将被自动重启
处理建议	<ul style="list-style-type: none"><li>若自动重启后单板仍然故障，且自动重启次数达到 3 次，单板将被自动隔离，</li><li>单板被自动隔离后，请联系技术支持</li></ul>

## 26.4.11 DRVPLAT/4/DrvDebug

日志内容	Chassis [UINT32] slot [UINT32] maybe have a hardware error, will be isolated. Please check it.
参数解释	\$1: 设备在IRF中的成员编号 \$2: 单板所在的槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: Chassis 1 slot 2 maybe have a hardware error, will be isolated. Please check it.
日志说明	检测到单板的硬件存在故障，此故障单板将被自动隔离
处理建议	请移除该单板并联系技术支持

## 26.4.12 DRVPLAT/4/DrvDebug

日志内容	Slot [UINT32] maybe have a hardware error, will be isolated. Please check it.
参数解释	\$1: 单板所在的槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: Slot 2 maybe have a hardware error, will be isolated. Please check it.
日志说明	检测到单板的硬件存在故障，此故障单板将被自动隔离
处理建议	请移除该单板并联系技术支持

## 26.5 DRVDEBUGMOD\_L3

### 26.5.1 DRVPLAT/4/DrvDebug

日志内容	BFD multi-hop not support Vpn. LD[UINT]
参数解释	\$1: 本端BFD鉴别值
日志等级	4
举例	DRVPLAT/4/DrvDebug: -MDC=1;BFD multi-hop not support Vpn. LD[4600].
日志说明	本设备BFD逐跳会话不支持VPN
处理建议	请删除VPN内BFD逐跳会话相关配置

### 26.5.2 DRVPLAT/4/DrvDebug

日志内容	No enough acl resources.
参数解释	无
日志等级	4
举例	DRVPLAT/4/DrvDebug: -MDC=1; No enough acl resources.
日志说明	使能DHCP Snooping时下发规则发现无资源
处理建议	请联系技术支持

### 26.5.3 DRVPLAT/4/DrvDebug

日志内容	The product can't support vrrp load-balance mode.
参数解释	无
日志等级	4
举例	DRVPLAT/4/DrvDebug: -MDC=1; The product can't support vrrp load-balance mode.
日志说明	不支持VRRPE模式
处理建议	不要配置VRRP负载分担模式

### 26.5.4 DRVPLAT/4/DrvDebug

日志内容	-Chassis=[INT32]-Slot=[INT32]; Tunnel[INT32] might not function properly on this device
参数解释	\$1: 设备在IRF中的成员编号 \$2: 单板所在的槽位号 \$3: Tunnel接口编号
日志等级	4
举例	DRVPLAT/4/DrvDebug: -Chassis=1-Slot=3; Tunnel1 might not function properly on this device
日志说明	创建的Tunnel接口数量超过规格数量时打印该日志
处理建议	1. 关闭其它多余的状态正常的 Tunnel 接口 2. 请联系技术支持

### 26.5.5 DRVPLAT/4/DrvDebug

日志内容	-Chassis=[INT32]-Slot=[INT32]; Tunne[INT32] recovered on this device
参数解释	\$1: 设备在IRF中的成员编号 \$2: 单板所在的槽位号 \$3: Tunnel接口编号
日志等级	4
举例	DRVPLAT/4/DrvDebug: -Chassis=2-Slot=4; Tunnel1 recovered on this device
日志说明	Tunnel接口恢复正常
处理建议	无

## 26.6 DRVDEBUGMOD\_PORT

### 26.6.1 DRVPLAT/4/DrvDebug

日志内容	The link status of port [STRING] is abnormal and the port is shut down.
参数解释	\$1: 本地端口名称
日志等级	4
举例	DRVPLAT/4/DrvDebug: The link status of port Ten-GigabitEthernet1/1/4 is abnormal and the port is shut down.
日志说明	链路异常，硬件检测到端口频繁UP/DOWN，将端口关闭
处理建议	<ul style="list-style-type: none"><li>• 检查对端设备是否发生故障。如是请解决对端设备故障问题，如若否，请执行下一步</li><li>• 检查链路两端介质是否故障。如是请更换介质，如若否，请联系技术支持</li><li>• 排查故障后，请对端口执行 shutdown/undo shutdown 操作</li></ul>

### 26.6.2 DRVPLAT/4/DrvDebug

日志内容	The port up-mode configuration exists on port [STRING]. Please remove the configuration, and then install the GE transceiver module.
参数解释	\$1: 本地端口名称
日志等级	4
举例	DRVPLAT/4/DrvDebug: The port up-mode configuration exists on port Ten-GigabitEthernet1/1/4. Please remove the configuration, and then install the GE transceiver module.
日志说明	10G端口若有port up-mode的配置，请取消之后，再插入GE光模块
处理建议	<ul style="list-style-type: none"><li>• 检查当前端口是否存在 port up-mode 的配置；如是，请执行下一步</li><li>• 拔掉当前端口插入的 GE 光模块，然后在当前端口执行 undo port up-mode 的操作</li><li>• 再在该端口上插 GE 光模块</li></ul>



## 26.7 DRVDEBUGMOD\_POWERFAN

### 26.7.1 DRVPLAT/2/DrvDebug

日志内容	Fan Fault! Chassis [UINT32] Frame [UINT32] fan [UINT32] speed < 500(R.P.M). FanState is [UINT32]. (0:ABSENT, 1:NORMAL, 2:FAIL.)
参数解释	\$1: 设备在IRF中的成员编号 \$2: 风扇框所在槽位号 \$3: 风扇编号 \$4: 风扇的状态
日志等级	2
举例	DRVPLAT/2/DrvDebug: Fan Fault! Chassis 1 Frame 0 fan 1 speed < 500(R.P.M). FanState is 2. (0:ABSENT, 1:NORMAL, 2:FAIL.)
日志说明	IRF模式下，风扇发生故障，风扇速度小于500转/每分钟
处理建议	使用 <b>display fan</b> 检查风扇状态 <ul style="list-style-type: none"><li>若风扇状态为 <b>fault</b>，请重新拔插风扇框，如果还不能恢复，请联系技术支持</li><li>若风扇状态为 <b>normal</b>，请联系技术支持</li></ul>

### 26.7.2 DRVPLAT/2/DrvDebug

日志内容	Fan Fault! Frame [UINT32] fan [UINT32] speed < 500(R.P.M). FanState is [UINT32]. (0:ABSENT, 1:NORMAL, 2:FAIL.)
参数解释	\$1: 风扇框所在槽位号 \$2: 风扇编号 \$3: 风扇的状态
日志等级	2
举例	DRVPLAT/2/DrvDebug: Fan Fault! Frame 0 fan 1 speed < 500(R.P.M). FanState is 2. (0:ABSENT, 1:NORMAL, 2:FAIL.)
日志说明	独立运行模式下，风扇发生故障，风扇速度小于500转/每分钟
处理建议	使用 <b>display fan</b> 检查风扇状态 <ul style="list-style-type: none"><li>若风扇状态为 <b>fault</b>，请重新拔插风扇框，如果还不能恢复，请联系技术支持</li><li>若风扇状态为 <b>normal</b>，请联系技术支持</li></ul>

### 26.7.3 DRVPLAT/2/DrvDebug

日志内容	Fan Adjusting failed! Chassis [UINT32] Frame [UINT32] fan [UINT32] speed is [UINT32] (R.P.M), is too low! FanState is [UINT32]. (0:ABSENT, 1:NORMAL, 2:FAIL.)
参数解释	\$1: 设备在IRF中的成员编号 \$2: 风扇框所在槽位号 \$3: 风扇编号 \$4: 风扇转速 \$5: 风扇状态
日志等级	2
举例	DRVPLAT/2/DrvDebug: Fan Adjusting failed! Chassis 1 Frame 0 fan 1 speed is 1124(R.P.M), is too low! FanState is 2. (0:ABSENT, 1:NORMAL, 2:FAIL.)
日志说明	风扇当前的转速比实际设置的风扇模式下的最小转速低
处理建议	<ul style="list-style-type: none"><li>• 当使用 <b>debug sysm fan</b> 命令，将风扇模式配置为 high 时，提示一次，属于正常现象，无需处理</li><li>• 其他情况，请使用 <b>display fan</b> 检查风扇状态：<ul style="list-style-type: none"><li>◦ 若风扇状态为 <b>fault</b>，请尝试拔插风扇框</li><li>◦ 若风扇状态为 <b>normal</b>，请过 2 分钟再看日志是否存在。如果不是，表示风扇已经自动调速，无需处理；如果是，请联系技术支持</li></ul></li></ul>

### 26.7.4 DRVPLAT/2/DrvDebug

日志内容	Fan Adjusting failed! Frame [UINT32] fan [UINT32] speed is [UINT32] (R.P.M), is too low! FanState is [UINT32]. (0:ABSENT, 1:NORMAL, 2:FAIL.)
参数解释	\$1: 风扇框所在槽位号 \$2: 风扇编号 \$3: 风扇转速 \$4: 风扇状态
日志等级	2
举例	DRVPLAT/2/DrvDebug: Fan Adjusting failed! Frame 0 fan 1 speed is 1124(R.P.M), is too low! FanState is 2. (0:ABSENT, 1:NORMAL, 2:FAIL.)
日志说明	风扇当前的转速比实际设置的风扇模式下的最小转速低
处理建议	<ul style="list-style-type: none"><li>• 当使用 <b>debug sysm fan</b> 命令，将风扇模式配置为 high 时，提示一次，属于正常现象，无需处理</li><li>• 其他情况，请使用 <b>display fan</b> 检查风扇状态：<ul style="list-style-type: none"><li>◦ 若风扇状态为 <b>fault</b>，请尝试拔插风扇框</li><li>◦ 若风扇状态为 <b>normal</b>，请过 2 分钟再看日志是否存在。如果不是，表示风扇已经自动调速，无需处理；如果是，请联系技术支持</li></ul></li></ul>

## 26.7.5 DRVPLAT/2/DrvDebug

日志内容	Fan Adjusting failed! Chassis [UINT32] Frame [UINT32] fan [UINT32] speed is [UINT32] (R.P.M), is too high!
参数解释	\$1: 设备在IRF中的成员编号 \$2: 风扇框所在槽位号 \$3: 风扇编号 \$4: 风扇转速
日志等级	2
举例	DRVPLAT/2/DrvDebug: Fan Adjusting failed! Chassis 1 Frame 0 fan 1 speed is 3524(R.P.M), is too high!
日志说明	风扇当前的转速比实际设置的风扇模式下的最大转速高
处理建议	<ul style="list-style-type: none"> <li>• 当使用 <b>debug sysm fan [fan-id] [section-id]</b>命令，将风扇模式配置为 low 或 auto 时，提示一次，属于正常现象，无需处理</li> <li>• 其他情况，请使用 <b>display fan</b> 检查风扇状态： <ul style="list-style-type: none"> <li>○ 若风扇状态为 <b>fault</b>，请尝试拔插风扇框</li> <li>○ 若风扇状态为 <b>normal</b>，请过 2 分钟再看日志是否一直存在。如果不是，表示风扇已经自动调速，无需处理；如果是，请联系技术支持</li> </ul> </li> </ul>

## 26.7.6 DRVPLAT/2/DrvDebug

日志内容	Fan Adjusting failed! Frame [UINT32] fan [UINT32] speed is [UINT32] (R.P.M), is too high!
参数解释	\$1: 风扇框所在槽位号 \$2: 风扇编号 \$3: 风扇转速
日志等级	2
举例	DRVPLAT/2/DrvDebug: Fan Adjusting failed! Frame 0 fan 1 speed is 3524(R.P.M), is too high!
日志说明	风扇当前的转速比实际设置的风扇模式下的最大转速高
处理建议	<ul style="list-style-type: none"> <li>• 当使用 <b>debug sysm fan [fan-id] [section-id]</b>命令，将风扇模式配置为 low 或 auto 时，提示一次，属于正常现象，无需处理</li> <li>• 其他情况，请使用 <b>display fan</b> 检查风扇状态： <ul style="list-style-type: none"> <li>○ 若风扇状态为 <b>fault</b>，请尝试拔插风扇框</li> <li>○ 若风扇状态为 <b>normal</b>，请过 2 分钟再看日志是否一直存在。如果不是，表示风扇已经自动调速，无需处理；如果是，请联系技术支持</li> </ul> </li> </ul>

### 26.7.7 DRVPLAT/2/DrvDebug

日志内容	Fan Changed OK! Frame [UINT32] fan [UINT32] speed is [UINT32](R.P.M), is OK!
参数解释	\$1: 风扇框所在槽位号 \$2: 风扇编号 \$3: 风扇转速
日志等级	2
举例	DRVPLAT/2/DrvDebug: Fan Changed OK! Frame 1 fan 1 speed is 2000(R.P.M), is OK!
日志说明	风扇当前的转速正常
处理建议	无需处理

### 26.7.8 DRVPLAT/2/DrvDebug

日志内容	Power [UINT32] is removed.
参数解释	\$1: 电源编号
日志等级	2
举例	DRVPLAT/2/DrvDebug: Power 2 is removed.
日志说明	电源被拔出
处理建议	无需处理

### 26.7.9 DRVPLAT/2/DrvDebug

日志内容	Warning: Not enough power to power on board chassis [UINT32] slot [UINT32]. Board power is [UINT32]w, system available power is [UINT32]w.
参数解释	\$1: 设备在IRF中的成员编号 \$2: 单板所在的槽位号 \$3: 单板正常运行所需功率 \$4: 系统可用功率
日志等级	2
举例	DRVPLAT/2/DrvDebug: Chassis=1-Slot=5;Warning: Not enough power to power on board chassis 1 slot 5. Board power is 225w, system available power is 130w.
日志说明	系统可用功率不足导致没有足够的功率给单板上电
处理建议	使用 <b>display power</b> 检查系统电源模块状态是否有模块状态为 <b>fault</b> <ul style="list-style-type: none"><li>如有, 请重新插拔电源模块, 并确保电源模块安装到位。如已安装到位, 故障仍存在, 请检查电源及先电源线是否可以正常工作。如不能正常工作, 请更换; 如可以正常工作, 请联系技术支持</li><li>如无, 请增加系统电源模块</li></ul>

## 26.7.10 DRVPLAT/2/DrvDebug

日志内容	Warning: Not enough power to power on board slot [UINT32]. Board power is [UINT32]w, system available power is [UINT32]w.
参数解释	\$1: 单板所在的槽位号 \$2: 单板正常运行所需功率 \$3: 系统可用功率（取值为0）
日志等级	2
举例	DRVPLAT/2/DrvDebug: Warning: Not enough power to power on board slot 5. Board power is 225w, system available power is 130w.
日志说明	系统可用功率不足导致没有足够的功率给单板上电
处理建议	使用 <b>display power</b> 检查系统电源模块状态是否有模块状态为 <b>fault</b> <ul style="list-style-type: none"> <li>如有，请重新插拔电源模块，并确保电源模块安装到位。如已安装到位，故障仍存在，请检查电源及先电源线是否可以正常工作。如不能正常工作，请更换；如可以正常工作，请联系技术支持</li> <li>如无，请增加系统电源模块</li> </ul>

## 26.7.11 DRVPLAT/2/DrvDebug

日志内容	Warning: Not enough power on chassis [UINT32], system available power is [UINT32]w.
参数解释	\$1: 设备在IRF中的成员编号 \$2: 系统可用功率（取值为0）
日志等级	2
举例	DRVPLAT/2/DrvDebug: Warning: Not enough power on chassis 1, system available power is 0w.
日志说明	当系统可用功率为0时，每3分钟打印一次
处理建议	使用 <b>display power</b> 检查系统电源模块状态是否有模块状态为 <b>fault</b> <ul style="list-style-type: none"> <li>如有，请重新插拔电源模块，并确保电源模块安装到位。如已安装到位，故障仍存在，请检查电源及先电源线是否可以正常工作。如不能正常工作，请更换；如可以正常工作，请联系技术支持</li> <li>如无，请增加系统电源模块</li> </ul>

## 26.7.12 DRVPLAT/2/DrvDebug

日志内容	Warning: Not enough power on the device, system available power is [UINT32]w.
参数解释	\$1: 系统可用功率
日志等级	2
举例	DRVPLAT/2/DrvDebug: Warning: Not enough power on the device, system available power is 0w.
日志说明	当系统可用功率为0时，每3分钟打印一次
处理建议	<p>使用<b>display power</b>检查系统电源模块状态是否有模块状态为<b>fault</b></p> <ul style="list-style-type: none"> <li>如有，请重新插拔电源模块，并确保电源模块安装到位。如已安装到位，故障仍存在，请检查电源及电源线是否可以正常工作。如不能正常工作，请更换；如可以正常工作，请联系技术支持</li> <li>如无，请增加系统电源模块</li> </ul>

## 26.7.13 DRVPLAT/2/DrvDebug

日志内容	Warning: Power [UINT32] differs from power [UINT32] in types! Power [UINT32] : [STRING]. Power [UINT32] : [STRING].
参数解释	\$1、\$2、\$3、\$5: 电源编号 \$4、\$6: 电源类型
日志等级	2
举例	DRVPLAT/2/DrvDebug: Power 1 differs from power 2 in types! Power 1 : PSR1400-D. Power 2 : PSR1400-12D1.
日志说明	当电源类型不一致时打印此日志
处理建议	观察打印的 2 个电源的类型是否一致， 如果不一致，请更换电源类型 如果一致，请联系技术支持

### 26.7.14 DRVPLAT/2/DrvDebug

日志内容	Only one power module is installed in power frame [UINT32] Power [UINT32]-[UCHAR] : [STRING]
参数解释	\$1、\$2: 电源的编号 \$3: 子电源在电源框内的编号 \$4: 电源的类型
日志等级	2
举例	DRVPLAT/2/DrvDebug: Only one power module is installed in power frame 1.
日志说明	电源框内只有一个电源正常工作
处理建议	及时插入子电源

### 26.7.15 DRVPLAT/2/DrvDebug

日志内容	Warning: Only one power [UINT32] exist ! Power [UINT32] : [STRING]
参数解释	\$1、\$2: 电源的编号 \$3: 电源的类型
日志等级	2
举例	DRVPLAT/2/DrvDebug: Warning:Only one power 1 exist ! Power 1: PSR1400-D.
日志说明	设备只有一个电源在位
处理建议	及时插入电源

### 26.7.16 DRVPLAT/2/DrvDebug

日志内容	Hotspot [UINT32] in chassis [UINT32] slot [UINT32] read [UINT32]. The temperature exceeded the shutdown threshold and the card is being shut down.
参数解释	\$1: 热点传感器编号 \$2: 设备在IRF中的成员编号 \$3: 单板所在的槽位号 \$4: 温度值
日志等级	2
举例	DRVPLAT/2/DrvDebug: Hotspot 1 in chassis 1 slot 1 read 111. The temperature exceeded the shutdown threshold and the card is being shut down.
日志说明	IRF模式下，单板热点温度超过温度传感器的温度门限
处理建议	请查看风扇运行是否正常

### 26.7.17 DRVPLAT/2/DrvDebug

日志内容	Hotspot [UINT32] in slot [UINT32] read [UINT32]. The temperature exceeded the shutdown threshold and the card is being shut down.
参数解释	\$1: 热点传感器编号 \$2: 单板所在的槽位号 \$3: 温度值
日志等级	2
举例	DRVPLAT/2/DrvDebug: Hotspot 1 in slot 1 read 111. The temperature exceeded the shutdown threshold and the card is being shut down.
日志说明	独立运行模式下，单板热点温度超过温度传感器的温度门限
处理建议	请查看风扇运行是否正常

### 26.7.18 DRVPLAT/2/DrvDebug

日志内容	temp is high in power [UINT32]
参数解释	\$1: 电源的编号
日志等级	2
举例	DRVPLAT/2/DrvDebug: temp is high in power 1
日志说明	电源内部温度过高
处理建议	及时检查电源，避免出现电源损坏

### 26.7.19 DRVPLAT/2/DrvDebug

日志内容	fan is faulty in power [UINT32]
参数解释	\$1: 电源的编号
日志等级	2
举例	DRVPLAT/2/DrvDebug: fan is faulty in power 1.
日志说明	电源内部风扇坏掉
处理建议	及时检查电源，避免电源出现损坏



### 26.7.20 DRVPLAT/2/DrvDebug

日志内容	Chassis [UINT32]: The number of redundant PSU changed: insufficient.
参数解释	\$1: 设备在IRF中的成员编号
日志等级	2
举例	DRVPLAT/2/DrvDebug: Warning: The number of redundant PSU changed: insufficient.
日志说明	设备的冗余功率减少
处理建议	及时插入电源, 避免出现功率不足

### 26.7.21 DRVPLAT/2/DrvDebug

日志内容	The number of redundant PSU changed: insufficient.
参数解释	无
日志等级	2
举例	DRVPLAT/2/DrvDebug: Warning: The number of redundant PSU changed: insufficient.
日志说明	设备的冗余功率减少
处理建议	及时插入电源, 避免出现功率不足

### 26.7.22 DRVPLAT/2/DrvDebug

日志内容	Chassis [UINT32]: The number of redundant PSU changed: sufficient.
参数解释	\$1: 设备在IRF中的成员编号
日志等级	2
举例	DRVPLAT/2/DrvDebug: Warning: Chassis 1: The number of redundant PSU changed: sufficient.
日志说明	设备的冗余功率恢复
处理建议	无需处理

## 26.7.23 DRVPLAT/2/DrvDebug

日志内容	The number of redundant PSU changed: sufficient.
参数解释	无
日志等级	2
举例	DRVPLAT/2/DrvDebug: Warning: The number of redundant PSU changed: sufficient.
日志说明	设备的冗余功率恢复
处理建议	无需处理

## 26.7.24 DRVPLAT/2/DrvDebug

日志内容	The power modules in power frame [UINT32] are of different models. Power[UINT32]-[UCHAR]: [STRING]. Power[UINT32]-[UCHAR]: [STRING].
参数解释	\$1 、 \$2、 \$5: 电源框框号 \$3 、 \$6: 子电源的编号 \$4 、 \$7: 子电源的型号
日志等级	2
举例	DRVPLAT/2/DrvDebug: Warning: The power modules in power frame 1 are of different models. Power1-A: PSR1200-D. Power1-B: PSR1200-A.
日志说明	电源框内出现混插
处理建议	及时更换子电源避免出现混插导致系统不稳定

## 26.8 DRVDEBUGMOD\_QACL

### 26.8.1 DRVPLAT/4/DrvDebug

日志内容	WARNING: This command need reboot device.
参数解释	无
日志等级	4
举例	DRVPLAT/4/DrvDebug: -MDC=1;WARNING: This command need reboot device.
日志说明	因配置Cut Through功能，需要重启设备才能使之生效
处理建议	重启设备

## 26.8.2 DRVPLAT/4/DrvDebug

日志内容	WARNING: Current switch-mode is different with that being configured System, reboot board [INT] to update switch-mode.
参数解释	\$1: 槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: -MDC=1;WARNING: WARNING: Current switch-mode is different with that being configured System, reboot board 5 to update switch-mode.
日志说明	检测到Switch-Mode错误，全局主配置与本地配置不一致，需要重启对应单板已保持一致
处理建议	请联系技术支持

## 26.9 DRVDEBUGMOD\_STACK

### 26.9.1 DRVPLAT/2/DrvDebug

日志内容	The software version is not compatible with the hardware.
参数解释	无
日志等级	2
举例	DRVPLAT/2/DrvDebug: The software version is not compatible with the hardware.
日志说明	该设备的软件版本和硬件不匹配
处理建议	检查设备的软件版本和硬件是否配套： <ul style="list-style-type: none"><li>• 若配套，则可能是硬件存在故障，请联系技术人员处理</li><li>• 若不配套，则请更换软件版本</li></ul>

## 26.9.2 DRVPLAT/2/DrvDebug

日志内容	Hotspot [STRING] in slot [STRING] read [STRING]. The temperature exceeded the shutdown threshold and the card is being shut down.
参数解释	\$1: 热点传感器编号 \$2: 单板所在的槽位号 \$3: 温度值
日志等级	2
举例	DRVPLAT/2/DrvDebug: Hotspot 1 in slot 0 read 125. The temperature exceeded the shutdown threshold and the card is being shut down.
日志说明	热点温度超过温度传感器的断电门限，热点所在单板即将被断电
处理建议	<ol style="list-style-type: none"><li>1. 请使用 <b>display fan</b> 命令检查所有风扇状态：<ul style="list-style-type: none"><li>• 若风扇状态为 <b>absent</b>，请检查风扇框是否安装到位，风扇是否插稳，风扇恢复正常后，为单板上电请执行步骤 2</li><li>• 若风扇状态为 <b>fault</b>，请尝试拔插风扇框或者更换新风扇，如果不能恢复请联系技术支持，若风扇恢复正常，为单板上电请执行步骤 2</li><li>• 若所有风扇状态为 <b>normal</b>，为单板上电请执行步骤 2</li></ul></li><li>2. 更换插入新的正常单板，或者等过温的单板温度降下来，然后拔插该单板使该单板上电</li></ol>

## 26.9.3 DRVPLAT/2/DrvDebug

日志内容	Hotspot [STRING] in chassis [STRING] slot [STRING] read [STRING]. The temperature exceeded the shutdown threshold and the card is being shut down.
参数解释	\$1: 热点传感器编号 \$2: 设备在IRF中的成员编号 \$3: 单板所在的槽位号 \$4: 温度值
日志等级	2
举例	DRVPLAT/2/DrvDebug: Hotspot 1 in chassis 1 slot 0 read 125. The temperature exceeded the shutdown threshold and the card is being shut down.
日志说明	热点温度超过温度传感器的断电门限，热点所在单板即将被断电
处理建议	<ol style="list-style-type: none"><li>1. 请使用 <b>display fan</b> 命令检查所有风扇状态：<ul style="list-style-type: none"><li>• 若风扇状态为 <b>absent</b>，请检查风扇框是否安装到位，风扇是否插稳，风扇恢复正常后，为单板上电请执行步骤 2</li><li>• 若风扇状态为 <b>fault</b>，请尝试拔插风扇框或者更换新风扇，如果不能恢复请联系技术支持，若风扇恢复正常，为单板上电请执行步骤 2</li><li>• 若所有风扇状态为 <b>normal</b>，为单板上电请执行步骤 2</li></ul></li><li>2. 更换插入新的正常单板，或者等过温的单板温度降下来，然后拔插该单板使该单板上电</li></ol>

## 26.9.4 DRVPLAT/4/DrvDebug

日志内容	The MPU in slot [UINT32] failed to obtain the card status in slot [UINT32].
参数解释	\$1: 主控板所在槽位号 \$2: 单板槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: The MPU in slot 0 failed to obtain the card status in slot 2.
日志说明	主控板不能正确读取指定slot的单板状态信息
处理建议	请联系技术支持

## 26.9.5 DRVPLAT/4/DrvDebug

日志内容	The MPU in chassis [UINT32] slot [UINT32] failed to obtain the card status in chassis [UINT32] slot [UINT32].
参数解释	\$1: 设备在IRF中的成员编号 \$2: 主控板所在槽位号 \$3: 设备在IRF中的成员编号 \$4: 单板所在槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: The MPU in chassis 1 slot 0 failed to obtain the card status in chassis 1 slot 2.
日志说明	主控板不能正确读取指定slot的单板状态信息
处理建议	请联系技术支持

## 26.9.6 DRVPLAT/4/DrvDebug

日志内容	The port up-mode configuration exists on port [STRING]. Please remove the configuration, and then install the GE transceiver module.
参数解释	\$1: 本地端口名称
日志等级	4
举例	DRVPLAT/4/DrvDebug: The port up-mode configuration exists on port Ten-GigabitEthernet3/0/49. Please remove the configuration, and then install the GE transceiver module.
日志说明	光口被强制开启后，如果10GE光口插入光电转换模块、1000M光模块，流量不能正常转发
处理建议	<ol style="list-style-type: none"><li>1. 如要继续使用强制开启光口功能，请拔掉当前端口上的光电转换模块、1000M光模块</li><li>2. 如不继续使用强制开启光口功能，需要使用光电转换模块、1000M光模块，则请先拔掉当前10GE光口的上述光模块，然后在端口上执行 <code>undo port up-mode</code> 操作，再次在该端口上插入上述光模块</li></ol>

## 26.9.7 DRVPLAT/4/DrvDebug

日志内容	The port [STRING] has been changed to inactive status, please check.
参数解释	\$1: IRF物理端口号
日志等级	4
举例	DRVPLAT/4/DrvDebug: The port Ten1/1/0/25 has been changed to inactive status, please check.
日志说明	提示端口状态转变为非激活状态
处理建议	<ol style="list-style-type: none"><li>1. 检查光模块是否插紧</li><li>2. 如果光模块已经插紧，请联系技术支持</li></ol>

## 26.9.8 DRVPLAT/4/DrvDebug

日志内容	The port [STRING] has been changed to active status.
参数解释	\$1: IRF物理端口号
日志等级	4
举例	DRVPLAT/4/DrvDebug: The port Ten1/1/0/25 has been changed to active status.
日志说明	提示端口状态转变为激活状态
处理建议	无需处理

### 26.9.9 DRVPLAT/4/DrvDebug

日志内容	The port [STRING] can't receive irf pkt and has been changed to inactive status, please check.
参数解释	\$1: IRF物理端口号
日志等级	4
举例	DRVPLAT/4/DrvDebug: The port Ten1/1/0/25 can't receive irf pkt and has been changed to inactive status, please check.
日志说明	指定端口不能接收IRF协议报文，并且端口已经转变成非激活状态
处理建议	<ol style="list-style-type: none"><li>1. 检查光模块是否插紧</li><li>2. 如果光模块已经插紧，请联系技术支持</li></ol>

### 26.9.10 DRVPLAT/4/DrvDebug

日志内容	The port [STRING] can't receive irf pkt, please check.
参数解释	\$1: IRF物理端口号
日志等级	4
举例	DRVPLAT/4/DrvDebug: The port Ten1/1/0/25 can't receive irf pkt, please check.
日志说明	指定端口不能接收IRF协议报文
处理建议	<ol style="list-style-type: none"><li>1. 检查光模块是否插紧</li><li>2. 如果光模块已经插紧，请联系技术支持</li></ol>

## 26.9.11 DRVPLAT/4/DrvDebug

日志内容	Port [STRING] Connect fail, Reason: [STRING], please check.
参数解释	<p>\$1: IRF物理端口号 \$2: 失败原因 具体原因有:</p> <ul style="list-style-type: none"> <li>• MemberID is the same</li> <li>• IRF-Port is the same</li> <li>• LoopBack</li> <li>• Check timeout</li> <li>• Fiber Connect Error</li> <li>• Topo Invalid</li> <li>• Peer Notify</li> <li>• The settings for the Layer 2 and Layer 3 multicast table capacity mode are different on this card and the peer card on the neighboring member device.</li> <li>• Other reason</li> </ul>
日志等级	4
举例	DRVPLAT/4/DrvDebug: Port Ten1/1/0/25 Connect fail, Reason: Check timeout, please check.
日志说明	提示端口连接失败，给出失败原因
处理建议	<ol style="list-style-type: none"> <li>1. 如果原因为“MemberID is the same”，请修改成 IRF 成员设备的编号为不同值</li> <li>2. 如果原因为“IRF-Port is the same”，请修改一端的 IRF 端口号，保证 IRF 链路两端一端为 IRF-Port1，另一端为 IRF-Port2</li> <li>3. 如果原因为“LoopBack”，请取消 IRF 物理端口上的环回设置</li> <li>4. 如果原因为“Check timeout”，请检查两端 IRF 物理端口上的配置是否正确，一般是一侧连接 IRF 物理端口一侧连接普通业务口导致</li> <li>5. 如果原因为“Fiber Connect Error”，请检查两端的 IRF 物理端口是否在一条 IRF 链路上，并检查 IRF 链路是否正常，IRF 物理端口上的配置是否正确</li> <li>6. 如果原因为“Topo Invalid”，请检查设备连接</li> <li>7. 如果原因为“Peer Notify”，请插拔对端端口的光模块尝试恢复</li> <li>8. 如果原因为“The settings for the Layer 2 and Layer 3 multicast table capacity mode are different on this card and the peer card on the neighboring member device”，请使用 <b>switch-mode</b> 命令将业务板的工作模式和代理模式配置成一致。</li> <li>9. 如果原因为“Other reason”，请联系技术支持</li> </ol>



### 26.9.12 DRVPLAT/4/DrvDebug

日志内容	The max-ecmp-num configuration should be the same on devices in one IRF. Please check it on the neighbor device connected to IRF-port [STRING]
参数解释	\$1: IRF端口号
日志等级	4
举例	DRVPLAT/4/DrvDebug: The max-ecmp-num configuration should be the same on devices in one IRF. Please check it on the neighbor device connected to IRF-port 2
日志说明	在一个IRF中，各个成员设备的最大等价路由数配置必须相同
处理建议	请使用 <b>display max-ecmp-num</b> 命令检查并通过 <b>max-ecmp-num</b> 命令修改各个成员设备的最大等价路由数配置相同

### 26.9.13 DRVPLAT/4/DrvDebug

日志内容	The device vendor must be the same for all member devices in one IRF fabric. Please check the vendor of the neighbor device connected to IRF-port [STRING].
参数解释	\$1: IRF端口号
日志等级	4
举例	DRVPLAT/4/DrvDebug: The device vendor must be the same for all member devices in one IRF fabric. Please check the vendor of the neighbor device connected to IRF-port [STRING].
日志说明	在一个IRF中，各个成员设备的公司品牌必须相同
处理建议	请使用相同公司品牌的交换机组建IRF

### 26.9.14 DRVPLAT/4/DrvDebug

日志内容	DeviceInfo must be the same in one IRF. DeviceInfo: [STRING], PeerDeviceInfo: [STRING].
参数解释	\$1: 本端设备类型 \$2: 对端设备类型
日志等级	4
举例	DRVPLAT/4/DrvDebug: DeviceInfo must be the same in one IRF. DeviceInfo: S12600G, PeerDeviceInfo: S8600XG.
日志说明	本系列交换机仅能与相同系列的交换机之间建立IRF
处理建议	请使用相同系列的交换机组建IRF

## 26.9.15 DRVPLAT/4/DrvDebug

日志内容	The product can't support stack mode.
参数解释	无
日志等级	4
举例	DRVPLAT/4/DrvDebug: The product can't support stack mode.
日志说明	本产品不支持切换成IRF模式
处理建议	请选择支持IRF模式的设备组建

## 26.9.16 DRVPLAT/4/DrvDebug

日志内容	The Systemworking mode configuration should be the same on devices in one IRF. Please check it on the neighbor device connected to IRF-port [STRING].
参数解释	\$1: IRF端口号
日志等级	4
举例	DRVPLAT/4/DrvDebug: The Systemworking mode configuration should be the same on devices in one IRF. Please check it on the neighbor device connected to IRF-port 2.
日志说明	在一个IRF中，各个成员设备的工作模式配置必须相同
处理建议	请用 <b>display system-working-mode</b> 命令检查并通过 <b>system-working-mode</b> 命令修改各个成员设备的工作模式相同

## 26.10 DRVDEBUGMOD\_SWFA

### 26.10.1 DRVPLAT/4/DrvDebug

日志内容	Board fault: chassis [UINT32] slot [UINT32], please check it.
参数解释	\$1: 设备在IRF中的成员编号。独立运行模式下，值为0 \$2: 单板所在的槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: Board fault: chassis 1 slot 10, please check it.
日志说明	检测到单板的硬件存在故障
处理建议	<ol style="list-style-type: none"><li>1. 请使用 <b>reboot</b> 命令重启或插拔故障的单板</li><li>2. 请更换故障的单板</li><li>3. 请联系技术支持</li></ol>

## 26.10.2 DRVPLAT/4/DrvDebug

日志内容	Board fault: chassis [UINT32] slot [UINT32] or chassis [UINT32] slot [UINT32], please check them.
参数解释	\$1、\$3: 设备在IRF中的成员编号。独立运行模式下，值为0 \$2、\$4: 单板所在的槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: Board fault: chassis 1 slot 11 or chassis 1 slot 9, please check them.
日志说明	检测到两块单板中有一块单板的硬件存在故障，但无法确认是哪一块单板
处理建议	<ol style="list-style-type: none"><li>1. 请使用 <b>reboot</b> 命令逐块重启或插拔提示有故障的单板</li><li>2. 请逐块更换提示有故障的单板</li><li>3. 请联系技术支持</li></ol>

## 26.10.3 DRVPLAT/4/DrvDebug

日志内容	Chassis [UINT32] slot [UINT32] will be isolated, please check it.
参数解释	\$1: 设备在IRF中的成员编号。独立运行模式下，值为0 \$2: 单板所在的槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: Chassis 1 slot 2 will be isolated, please check it.
日志说明	检测到单板的硬件存在故障，此故障单板将被隔离。隔离后，单板将一直处于Fault状态
处理建议	<ol style="list-style-type: none"><li>1. 请重新拔插或更换提示有故障的单板</li><li>2. 请联系技术支持</li></ol>

## 26.11 DRVDEBUGMOD\_SYSM

### 26.11.1 DRVPLAT/4/DrvDebug

日志内容	The device does not support board in chassis [UINT32] slot [UINT32] ,type is unknown(0x[UINT32]), Please check.
参数解释	\$1: 设备在IRF中的成员编号 \$2: 单板所在的槽位号 \$3: 单板类型值
日志等级	4
举例	DRVPLAT/4/DrvDebug: Chassis=1-Slot=5;The device does not support board in chassis 1 slot 5 ,type is unknown(0x108), Please check.
日志说明	IRF模式下，提示设备不支持该单板
处理建议	请联系技术支持

### 26.11.2 DRVPLAT/4/DrvDebug

日志内容	The device does not support board in slot [UINT32] ,type is unknown(0x[UINT32]), Please check.
参数解释	\$1: 单板所在的槽位号 \$2: 单板类型值
日志等级	4
举例	DRVPLAT/4/DrvDebug: The device does not support board in slot 5 ,type is unknown(0x108), Please check.
日志说明	独立运行模式下，提示设备不支持该单板
处理建议	请联系技术支持

### 26.11.3 DRVPLAT/4/DrvDebug

日志内容	The service module in slot [UINT32] failed to start up because it does not support the current multicast forwarding mode.
参数解释	\$1: 业务板所在槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: The service module in slot 2 failed to start up because it does not support the current multicast forwarding mode.
日志说明	指定槽位上的业务板不支持当前配置的组播转发模式
处理建议	<ul style="list-style-type: none"><li>• 修改设备的组播转发模式为标准模式，并重启设备</li><li>• 更换该槽位的业务板为支持组播转发模式的业务板</li></ul>

#### 26.11.4 DRVPLAT/4/DrvDebug

日志内容	The service module in slot [UINT32] on chassis [UINT32] failed to start up because the service module does not support the current multicast forwarding mode.
参数解释	\$1: 设备在IRF中的成员编号 \$2: 业务板所在槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: The service module in slot 2 on chassis 1 failed to start up because the service module does not support the current multicast forwarding mode.
日志说明	指定槽位上的业务板不支持当前配置的组播转发模式
处理建议	<ul style="list-style-type: none"><li>• 修改设备的组播转发模式为标准模式，并重启设备</li><li>• 更换该槽位的业务板为支持组播转发模式的业务板</li></ul>

#### 26.11.5 DRVPLAT/4/DrvDebug

日志内容	The service module in chassis [UINT32] slot [UINT32] failed to start because the current fabric-mode does not support the service module. Please change the fabric-mode.
参数解释	\$1: 设备在IRF中的成员编号 \$2: 业务板所在槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: The service module in chassis 1 slot 3 failed to start because the current fabric-mode does not support the service module. Please change the fabric-mode.
日志说明	当前配置的fabric-mode不支持指定槽位上的业务板，请更换转发模式
处理建议	<ul style="list-style-type: none"><li>• 修改设备的转发模式</li><li>• 更换指定槽位的业务板为当前转发模式支持的业务板</li></ul>

## 26.11.6 DRVPLAT/4/DrvDebug

日志内容	The service module in chassis [UINT32] slot [UINT32] failed to start because it is not compatible with the switching fabric modules.
参数解释	\$1: 设备在IRF中的成员编号 \$2: 业务板所在槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: The service module in chassis 2 slot 5 failed to start because it is not compatible with the switching fabric modules.
日志说明	插入的业务板与当前的交换网板不匹配，请更换业务板或交换网板。
处理建议	<ul style="list-style-type: none"><li>• 更换当前交换网板匹配的业务板</li><li>• 更换当前业务板匹配的交换网板</li></ul>

## 26.11.7 DRVPLAT/4/DrvDebug

日志内容	The service module in slot [UINT32] failed to start because it is not compatible with the switching fabric modules.
参数解释	\$1: 业务板所在槽位号
日志等级	4
举例	DRVPLAT/4/DrvDebug: The service module in slot 5 failed to start because it is not compatible with the switching fabric modules.
日志说明	插入的业务板与当前的交换网板不匹配，请更换业务板或交换网板。
处理建议	<ul style="list-style-type: none"><li>• 更换当前交换网板匹配的业务板</li><li>• 更换当前业务板匹配的交换网板</li></ul>

## 26.11.8 DRVPLAT/2/DrvDebug

日志内容	No switching fabric modules are present. For the system to work correctly, verify that at least one fabric module is available and operating correctly.
参数解释	无
日志等级	2
举例	DRVPLAT/2/DrvDebug: -MDC=1; No switching fabric modules are present. For the system to work correctly, verify that at least one fabric module is available and operating correctly.
日志说明	以下情况会出现此日志： <ul style="list-style-type: none"><li>• 业务板启动时，检查到网板槽位上都没有安装网板</li><li>• 网板都拔出</li></ul>
处理建议	<ol style="list-style-type: none"><li>1. 请确认设备的网板槽位上是否有网板在位。如果没有，请至少在一个网板槽位上插入交换网板；如果有，请检查交换网板是否安装到位</li><li>2. 请联系技术支持</li></ol>

## 26.11.9 DRVPLAT/4/DrvDebug

日志内容	The fabric mode configuration should be the same on devices in one IRF. Please check it on the neighbor device connected to IRF-port [STRING].
参数解释	\$1: IRF端口号
日志等级	4
举例	DRVPLAT/4/DrvDebug: -MDC=1; The fabric mode configuration should be the same on devices in one IRF. Please check it on the neighbor device connected to IRF-port 2.
日志说明	在一个IRF中，各个成员设备的转发配置必须相同
处理建议	请用 <b>display fabric-mode</b> 命令检查并通过 <b>fabric-mode</b> 命令修改各个成员设备的工作模式相同

## 26.12 DRVDEBUGMOD\_VLAN

### 26.12.1 DRVPLAT/4/DrvDebug

日志内容	[STRING]: Some VLAN interfaces might not function properly on this device.
参数解释	\$1: 创建的VLAN接口
日志等级	4
举例	DRVPLAT/4/DrvDebug: -Chassis=1-Slot=6; Vlan-interface1000: Some VLAN interfaces might not function properly on this device.
日志说明	在框式设备上创建VLAN接口时超出最大范围提示
处理建议	在规格范围内创建，删除超规格的 VLAN 接口

# 27 EDEV

本节介绍扩展设备管理模块输出的日志信息。

## 27.1 ALARM\_IN\_REMOVED

日志内容	Alarm removed on the alarm-in port [UNIT].
参数解释	\$1: 表示告警输入端口的编号
日志等级	5
举例	EDEV/5/ALARM_IN_REMOVED: Alarm removed on the alarm-in port 1.
日志说明	某个告警输入接口的告警信号已解除，恢复到正常状态
处理建议	无

## 27.2 ALARM\_IN\_REPORTED

日志内容	Alarm reported on the alarm-in port [UNIT].
参数解释	\$1: 表示告警输入端口的编号
日志等级	5
举例	EDEV/5/EDEV_ALARM_IN_REPORTED: Alarm reported on the alarm-in port 1.
日志说明	某个告警输入接口收到告警信号
处理建议	检查和告警输入接口相连的设备，确认该邻居设备是否发生异常



## 27.3 EDEV\_BOOTROM\_UPDATE\_FAILED

日志内容	Failed to execute the bootrom update command.
参数解释	无
日志等级	5
举例	EDEV/5/EDEV_BOOTROM_UPDATE_FAILED: -IPAddr=192.168.79.1-User=**; Failed to execute the bootrom update command.
日志说明	用户执行 <b>bootrom update</b> 命令将文件系统中的BootWare程序加载到BootWare的Normal区，操作失败
处理建议	请根据提示信息采取相应措施

## 27.4 EDEV\_BOOTROM\_UPDATE\_SUCCESS

日志内容	Executed the bootrom update command successfully.
参数解释	无
日志等级	5
举例	EDEV/5/EDEV_BOOTROM_UPDATE_SUCCESS: -IPAddr=192.168.79.1-User=**; Executed the bootrom update command successfully.
日志说明	用户执行 <b>bootrom update</b> 命令将文件系统中的BootWare程序加载到BootWare的Normal区，操作成功
处理建议	无

## 27.5 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: <ul style="list-style-type: none"><li>o primary 表示备份组中 primary 节点处理业务</li><li>o secondary 表示备份组中 secondary 节点处理业务</li></ul>
日志等级	5
举例	EDEV/5/EDEV_FAILOVER_GROUP_STATE_CHANGE: -MDC=1; Status of stateful failover group 123 with ID 0 changed to primary.
日志说明	备份组的状态发生了变化
处理建议	无

# 28 eMDI

本节介绍 eMDI 模块输出的日志信息。

## 28.1 EMDI\_INDICATOR\_OVER\_THRES

日志内容	[STRING] alarm for instance [USHORT] was triggered: Value=[UINT32]/100000, Threshold=[UINT32]/100000, SuppressionTimes=[UCHAR].
参数解释	<p>\$1: 监控指标类型，取值为：</p> <ul style="list-style-type: none"><li>○ RTP-LR: RTP 报文的丢包率</li><li>○ RTP-SER: RTP 报文的乱序率</li><li>○ DPLR: TCP 报文的下游丢包率</li><li>○ UPLR: TCP 报文的上游丢包率</li></ul> <p>\$2: 实例ID</p> <p>\$3: 监控指标值</p> <p>\$4: 监控指标设定的阈值</p> <p>\$5: 监控指标设定的告警抑制次数</p>
日志等级	5
举例	EMDI/5/EMDI_INDICATOR_OVER_THRES: RTP-LR alarm for instance 100 was triggered: Value=150/100000, Threshold=100/100000, SuppressionTimes=3.
日志说明	eMDI监控指标连续多次达到告警阈值
处理建议	<ul style="list-style-type: none"><li>● 执行 <b>display emdi statistics</b> 命令，查看实例的统计信息</li><li>● 结合多个设备的实例的统计信息，进行故障定界</li></ul>

## 28.2 EMDI\_INDICATOR\_OVER\_THRES\_RESUME

日志内容	[STRING] alarm for instance [USHORT] was removed: Value=[UINT32]/100000, Threshold=[UINT32]/100000, SuppressionTimes=[UCHAR].
参数解释	<p>\$1: 监控指标类型，取值为：</p> <ul style="list-style-type: none"> <li>○ RTP-LR: RTP 报文的丢包率</li> <li>○ RTP-SER: RTP 报文的乱序率</li> <li>○ DPLR: TCP 报文的下游丢包率</li> <li>○ UPLR: TCP 报文的上游丢包率</li> </ul> <p>\$2: 实例ID</p> <p>\$3: 监控指标值</p> <p>\$4: 监控指标设定的阈值</p> <p>\$5: 监控指标设定的告警抑制次数</p>
日志等级	5
举例	EMDI/5/EMDI_INDICATOR_OVER_THRES_RESUME: RTP-LR alarm for instance 100 was removed: Value=50/100000, Threshold=100/100000, SuppressionTimes=3.
日志说明	eMDI监控指标连续多次低于告警阈值，监控指标恢复
处理建议	无

## 28.3 EMDI\_INSTANCE\_CONFLICT\_FLOW

日志内容	The flow (SrcIP=[STRING], SrcPort=[USHORT], DstIP=[STRING], DstPort=[USHORT], Protocol=[STRING]) to be bound to a dynamic instance overlaps with the flow bound to instance [USHORT].
参数解释	<p>\$1: 流的源IP地址</p> <p>\$2: 流的源端口号</p> <p>\$3: 流的目的IP地址</p> <p>\$4: 流的目的端口号</p> <p>\$5: 流的协议类型</p> <ul style="list-style-type: none"> <li>○ tcp</li> <li>○ udp</li> </ul> <p>\$6: 已绑定了冲突数据流的实例ID</p>
日志等级	5
举例	EMDI/5/EMDI_INSTANCE_CONFLICT_FLOW: The flow (SrcIP=10.0.0.1, SrcPort=10, DstIP=20.0.0.1, DstPort=20, Protocol=tcp) to be bound to a dynamic instance overlaps with the flow bound to instance 1.
日志说明	为动态实例配置的流与已存在实例中的流冲突
处理建议	请删除已存在的冲突配置

## 28.4 EMDI\_INSTANCE\_EXCEED

日志内容	Maximum number of running instances on [STRING] already reached.
参数解释	\$1: chassis编号+slot编号、slot编号或device
日志等级	5
举例	EMDI/5/EMDI_INSTANCE_EXCEED: Maximum number of running instances on slot 1 already reached.
日志说明	正在运行的实例已经达到了单板规格最大值
处理建议	如果想继续启动一些实例，请先停止一些该板上不必要的实例

## 28.5 EMDI\_INSTANCE\_SAME\_FLOW

日志内容	The flow to be bound to a dynamic instance was already bound to instance [USHORT]: SrcIP=[STRING], SrcPort=[USHORT], DstIP=[STRING], DstPort=[USHORT], Protocol=[STRING].
参数解释	\$1: 已绑定了冲突数据流的实例ID \$2: 流的源IP地址 \$3: 流的源端口号 \$4: 流的目的IP地址 \$5: 流的目的端口号 \$6: 流的协议类型 <ul style="list-style-type: none"><li>o tcp</li><li>o udp</li></ul>
日志等级	5
举例	EMDI/5/EMDI_INSTANCE_SAME_FLOW: The flow to be bound to a dynamic instance was already bound to instance 1: SrcIP=10.0.0.1, SrcPort=10, DstIP=20.0.0.1, DstPort=20, Protocol= tcp.
日志说明	为动态实例配置的流与已存在实例中的流相同
处理建议	请删除已存在的冲突配置

# 29 EPA

本节介绍 EPA 模块输出的日志信息。

## 29.1 EPA\_ENDPOINT\_ONLINE

日志内容	Detected the association of an endpoint (device ID [STRING], MAC address [STRING]) on interface [STRING] in VLAN [UINT16].
参数解释	\$1: 连接终端的那台设备的桥MAC \$2: 终端的MAC地址 \$3: 终端上线接口 \$4: 终端所属的VLAN
日志等级	6
举例	EPA/6/EPA_ENDPOINT_ONLINE: Detected the association of an endpoint (device ID a4c2-d4ad-0200, MAC address 12c2-d4ed-0200) on interface GigabitEthernet1/0/1 in VLAN 1.
日志说明	监控到终端上线
处理建议	无

## 29.2 EPA\_ENDPOINT\_OFFLINE

日志内容	Detected the disassociation of an endpoint (device ID [STRING], MAC address [STRING]) on interface [STRING] in VLAN [UINT16].
参数解释	\$1: 连接终端的那台设备的桥MAC \$2: 终端的MAC地址 \$3: 终端上线接口 \$4: 终端所属的VLAN
日志等级	6
举例	EPA/6/EPA_ENDPOINT_OFFLINE: Detected the disassociation of an endpoint (device ID a4c2-d4ad-0200, MAC address 12c2-d4ed-0200) on interface GigabitEthernet1/0/1 in VLAN 1.
日志说明	监控到终端下线
处理建议	无

## 29.3 EPA\_DEVICETYPE\_CHANGE

日志内容	Cleared EPA monitor rule configurations. Reason: Device type changed from [STRING] to [STRING].
参数解释	\$1: 切换前的设备类型: <ul style="list-style-type: none"><li>○ TM: SmartMC 网络中的管理设备</li><li>○ TC: SmartMC 网络中的成员设备</li><li>○ Self-managed: 非 SmartMC 网络中的设备</li></ul> \$2: 切换后的设备类型
日志等级	6
举例	EPA/6/EPA_DEVICETYPE_CHANGE: Cleared EPA monitor rule configurations. Reason: Device type changed from TC to Self-managed.
日志说明	因为设备类型切换，EPA监控规则被完全清除
处理建议	无

# 30 ERPS

本节介绍 ERPS 模块输出的日志信息。

## 30.1 ERPS\_IPP\_CHECK

日志内容	An ERPS ring member port can't be configured as an IPP port.
参数解释	无
日志等级	6
举例	ERPS/6/ERPS_IPP_CHECK: An ERPS ring member port can't be configured as an IPP port.
日志说明	ERPS环端口不支持配置为IPP口
处理建议	无

## 30.2 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	4
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

# 31 ETH

本节介绍 ETH 模块输出的日志信息。

## 31.1 ETH\_SET\_MAC\_FAILED

日志内容	Failed to set the MAC address [STRING] on [STRING].
参数解释	\$1: MAC地址 \$2: 接口名称
日志等级	5
举例	ETH/5/ETH_SET_MAC_FAILED: Failed to set the MAC address 0001-0001-0001 on GigabitEthernet1/0/1.
日志说明	在配置恢复、IRF分裂、新单板插入情况下，由于接口的MAC地址和设备桥MAC地址的高36位不一致，设置接口的MAC地址失败
处理建议	重新配置合适的接口MAC地址

# 32 ETHDRNI

本节介绍 ETHDRNI 模块输出的日志信息。

## 32.1 ETHDRNI\_MAC\_INEFFECTIVE

日志内容	ETHDRNI failed to add the MAC address of [STRING]. Cause: [STRING].
参数解释	\$1: 接口名称 \$2: 出现错误的原因
日志等级	3
举例	ETHDRNI/3/ETHDRNI_MAC_INEFFECTIVE: ETHDRNI failed to add the MAC address of Vlan-interface20. Cause: Insufficient hardware resources.
日志说明	ETHDRNI添加VLAN接口的MAC地址失败
处理建议	联系管理员确定操作失败的根因并解决

# 33 ETHOAM

本节介绍 ETHOAM 模块输出的日志信息。

## 33.1 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

## 33.2 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



### 33.3 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

### 33.4 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

### 33.5 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

## 33.6 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

## 33.7 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

## 33.8 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

### 33.9 ETHOAM\_ENTER\_LOOPBACK\_CTRLING

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_CTRLING: 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

### 33.10 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

### 33.11 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

## 33.12 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

## 33.13 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

## 33.14 ETHOAM\_LOCAL\_ERROR\_SYMBOL

日志内容	An errored symbol event occurred on local interface [string].
参数解释	\$1: 接口名称
日志等级	4
举例	ETHOAM/4/ETHOAM_LOCAL_ERROR_SYMBOL: An errored symbol event occurred on local interface Ethernet1/0/1.
日志说明	本端产生错误信号事件
处理建议	本端收到错误信号，检查一下本端和对端之间的链路是否正常

## 33.15 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

## 33.16 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

## 33.17 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

## 33.18 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 <b>oam remote-loopback start</b> 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 <b>oam remote-loopback start</b> 命令

## 33.19 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

## 33.20 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

## 33.21 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

## 33.22 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

## 33.23 ETHOAM\_QUIT\_LOOPBACK\_CTRLING

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

## 33.24 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

## 33.25 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

## 33.26 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



### 33.27 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

### 33.28 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

### 33.29 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

### 33.30 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

### 33.31 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

### 33.32 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

## 34 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。

## 34.1 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

## 34.2 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

## 34.3 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

## 34.4 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


# 35 EVIISIS

本节介绍 EVI IS-IS 模块输出的日志信息。

## 35.1 EVIISIS\_LICENSE\_EXPIRED

日志内容	The EVIISIS feature is being disabled, because its license has expired.
参数解释	无
日志等级	3
举例	EVIISIS/3/EVIISIS_LICENSE_EXPIRED: The EVIISIS feature is being disabled, because its license has expired.
日志说明	EVIISIS的License已经过期
处理建议	请更换有效的Licence

## 35.2 EVIISIS\_LICENSE\_EXPIRED\_TIME

日志内容	The EVIISIS feature will be disabled in [ULONG] days.
参数解释	\$1: 功能还可使用的天数
日志等级	5
举例	EVIISIS/5/EVIISIS_LICENSE_EXPIRED_TIME: The EVIISIS feature will be disabled in 2 days.
日志说明	<p>EVIISIS的License不可用，EVIISIS功能将在2天后失效</p> <p> 说明</p> <p>主备倒换后新的主控板上没有可用的 EVI License，会启动 30 天临时可用定时器</p>
处理建议	若要继续使用EVIISIS功能，请准备新的License

## 35.3 EVIISIS\_LICENSE\_UNAVAILABLE

日志内容	The EVIISIS feature has no available license.
参数解释	无
日志等级	3
举例	EVIISIS/3/EVIISIS_LICENSE_UNAVAILABLE: The EVIISIS feature has no available license.
日志说明	进程启动时，没有找到EVIISIS对应的License
处理建议	请为EVIISIS安装有效的Licence

## 35.4 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 <ul style="list-style-type: none"><li>o up: 表示邻居关系已建立, 可以正常工作</li><li>o initializing: 表示初始状态</li><li>o down: 表示邻居关系结束</li></ul>
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

# 36 FCLINK

本节介绍 FCLINK 模块输出的日志信息。

## 36.1 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

## 36.2 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

# 37 FCOE

本节介绍 FCOE 模块输出的日志信息。

## 37.1 FCOE\_\_LAGG\_BIND\_ACTIVE

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

## 37.2 FCOE\_\_LAGG\_BIND\_DEACTIVE

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

## 37.3 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

# 38 FCZONE

本节介绍 FCZONE 模块输出的日志信息。



## 38.1 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	<p>不同情况下扩散失败的处理建议如下：</p> <ul style="list-style-type: none"><li>• 如果是激活 Zone set 命令 <code>zoneset activate</code> 触发的扩散，需要分别在 Fabric 中各交换机上通过 <code>display current-configuration</code> 命令查看 VSAN 内的激活 Zone set 的配置，若配置不一致，则通过 <code>zoneset activate</code> 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</li><li>• 如果是完全扩散命令 <code>zoneset distribute</code> 触发的扩散，需要分别在 Fabric 中各交换机上通过 <code>display current-configuration</code> 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 <code>zoneset distribute</code> 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</li><li>• 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 <code>display zone status</code> 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 <code>zoneset distribute</code> 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</li></ul>

## 38.2 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

### 38.3 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

### 38.4 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 <b>display current-configuration</b> 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 <b>shutdown</b> 和 <b>undo shutdown</b> 命令，触发重新发起合并

### 38.5 FCZONE\_ISOLATE\_CLEAR\_ALLVSAN

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

## 38.6 FCZONE\_ISOLATE\_CLEAR\_VSAN

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

## 38.7 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 <b>display current-configuration</b> 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 <b>shutdown</b> 和 <b>undo shutdown</b> 命令触发两台交换机重新发起合并

# 39 FGROUP

本节介绍 Flow Group 模块输出的日志信息。

## 39.1 FLOWGROUP\_APPLY\_FAIL

日志内容	Failed to apply flow group [STRING]. Reason: [STRING]
参数解释	\$1: Flow Group的ID \$2: 失败原因 <ul style="list-style-type: none"><li>○ The operation is not supported.: 操作不支持</li><li>○ Not enough resources to complete the operation.: 资源不足</li></ul>
日志等级	4
举例	FGROUP/4/FLOWGROUP_APPLY_FAIL: Failed to apply flow group 1. Reason: The operation is not supported.
日志说明	<ul style="list-style-type: none"><li>● 不支持配置, 导致应用 Flow Group 失败</li><li>● 资源不足, 导致应用 Flow Group 失败</li></ul>
处理建议	请根据失败原因, 修改或删除Flow Group的相关配置

## 39.2 FLOWGROUP\_MODIFY\_FAIL

日志内容	Failed to modify flow group [STRING]. Reason: [STRING]
参数解释	\$1: Flow Group的ID \$2: 失败原因 <ul style="list-style-type: none"><li>○ The operation is not supported.: 操作不支持</li><li>○ Not enough resources to complete the operation.: 资源不足</li></ul>
日志等级	4
举例	FGROUP/4/FLOWGROUP_MODIFY_FAIL: Failed to modify flow group 1. Reason: The operation is not supported.
日志说明	<ul style="list-style-type: none"><li>● 不支持配置, 导致修改 Flow Group 失败</li><li>● 资源不足, 导致修改 Flow Group 失败</li></ul>
处理建议	如果是资源不足导致修改失败, 请检查并删除设备上不必要的配置, 以节约资源

# 40 FIB

本节包含 FIB 日志消息。

## 40.1 FIB\_FILE

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

## 40.2 FIB\_PREFIX\_ENOUGHRESOURCE

日志内容	Issued the software entry to the driver for IP address [STRING] and mask length [UINT32] on VPN instance [STRING]. Issued the software entry to the driver for IP address [STRING] and mask length [UINT32] on the public network.
参数解释	\$1: IPv4地址或者IPv6地址 \$2: 掩码长度或者前缀长度 \$3: VPN实例名。如果该FIB属于公网，该字段不显示
日志等级	6
举例	FIB/6/FIB_PREFIX_ENOUGHRESOURCE: Issued the software entry to the driver for IP address 10.1.1.1 and mask length 32 on VPN instance vpn_1. FIB/6/FIB_PREFIX_ENOUGHRESOURCE: Issued the software entry to the driver for IP address 10::2 and mask length 128 on the public network.
日志说明	使用 <b>fib consistency-check enable</b> 命令开启IPv4 FIB表项一致性检查功能，或者使用 <b>ipv6 fib consistency-check enable</b> 命令开启IPv6 FIB表项一致性检查功能后，如果FIB重刷硬件表项成功，则输出此日志
处理建议	不需要处理

## 40.3 FIB\_PREFIX\_INCONSISTENT

日志内容	Inconsistent software and hardware FIB entries for IP address [STRING] and mask length [UINT32] on VPN instance [STRING]. Inconsistent parameters: [STRING]. Inconsistent software and hardware FIB entries for IP address [STRING] and mask length [UINT32] on the public network. Inconsistent parameters: [STRING].
参数解释	\$1: IPv4地址或IPv6地址 \$2: 掩码长度或者前缀长度 \$3: VPN实例名。如果该FIB属于公网，该字段不显示 \$4: 不一致的表项参数类型 <ul style="list-style-type: none"><li>○ next hop: 下一跳地址</li><li>○ mpls label: MPLS 标签</li><li>○ adjacent-table: 邻接表</li><li>○ micro-segment ID: 微分段 ID</li></ul>
日志等级	6
举例	FIB/6/FIB_PREFIX_INCONSISTENT: Inconsistent software and hardware FIB entries for IP address 10.1.1.1 and mask length 32 on VPN instance vpn_1. Inconsistent parameters: next hop, mpls label, adjacent-table and micro-segment ID. FIB/6/FIB_PREFIX_INCONSISTENT: Inconsistent software and hardware FIB entries for IP address 10::2 and mask length 128 on the public network. Inconsistent parameters: next hop, mpls label, adjacent-table and micro-segment ID.
日志说明	使用 <b>fib consistency-check enable</b> 命令开启IPv4 FIB表项一致性检查功能，或者 <b>ipv6 fib consistency-check enable</b> 开启IPv6 FIB表项一致性检查功能后，如果设备检测到FIB软件表项与硬件表项不一致（比如FIB表项的下一跳地址），则输出本日志
处理建议	不需要处理，FIB会主动重刷硬件表项

## 40.4 FIB\_PREFIX\_NORESOURCE

日志内容	Not enough hardware resources to issue the software entry to the driver for IP address [STRING] and mask length [UINT32] on VPN instance [STRING]. Not enough hardware resources to issue the software entry to the driver for IP address [STRING] and mask length [UINT32] on the public network.
参数解释	\$1: IPv4地址或者IPv6地址 \$2: 掩码长度或者前缀长度 \$3: VPN实例名。如果该FIB属于公网，该字段不显示
日志等级	6
举例	FIB/6/FIB_PREFIX_NORESOURCE: Not enough hardware resources to issue the software entry to the driver for IP address 10.1.1.1 and mask length 32 on VPN instance vpn_1. FIB/6/FIB_PREFIX_NORESOURCE: Not enough hardware resources to issue the software entry to the driver for IP address 10::2 and mask length 128 on the public network.
日志说明	使用 <b>fib consistency-check enable</b> 命令开启IPv4 FIB表项一致性检查功能，或者 <b>ipv6 fib consistency-check enable</b> 开启IPv6 FIB表项一致性检查功能后，当FIB软件表项下发驱动时，驱动没有足够的FIB硬件表项资源，则输出此日志
处理建议	不需要处理，FIB会主动重刷硬件表项

## 40.5 FIB\_VN\_ENOUGHRESOURCE

日志内容	Issued the following [UINT32] software FIB entries to the driver: Entry for IP address [STRING] and mask length [UINT32] on VPN instance [STRING]. Issued the following [UINT32] software FIB entries to the driver: Entry for IP address [STRING] and mask length [UINT32] on the public network.
参数解释	\$1: FIB表项数量 \$2: IPv4地址或者IPv6地址 \$3: 掩码长度或者前缀长度 \$4: VPN实例名。如果该FIB属于公网，该字段不显示。
日志等级	6
举例	FIB/6/FIB_VN_ENOUGHRESOURCE: Issued the following 1 software FIB entries to the driver: Entry for IP address 10.1.1.1 and mask length 32 on VPN instance vpn_1. FIB/6/FIB_PREFIX_ENOUGHRESOURCE: Issued the following 1 software FIB entries to the driver: Entry for IP address 10::2 and mask length 128 on the public network.
日志说明	使用 <b>fib consistency-check enable</b> 命令开启IPv4 FIB表项一致性检查功能，或者 <b>ipv6 fib consistency-check enable</b> 开启IPv6 FIB表项一致性检查功能后，如果虚拟下一跳表项重刷硬件表项成功，则输出此日志，提示用户哪些FIB表项恢复
处理建议	不需要处理

## 40.6 FIB\_VN\_INCONSISTENT

日志内容	<p>Inconsistent software and hardware entries for the following [UINT32] FIB entries. Inconsistent parameters: [STRING].</p> <p>Entry for IP address [STRING] and mask length [UINT32] on VPN instance [STRING].</p> <p>Inconsistent software and hardware entries for the following [UINT32] FIB entries. Inconsistent parameters: [STRING].</p> <p>Entry for IP address [STRING] and mask length [UINT32] on the public network.</p>
参数解释	<p>\$1: FIB表项个数</p> <p>\$2: 不一致的表项参数类型</p> <ul style="list-style-type: none"> <li>○ next hop: 下一跳地址</li> <li>○ mpls label: MPLS 标签</li> <li>○ max ECMP number: 最大等价路由条数</li> <li>○ output tunnel interface: 隧道出接口</li> </ul> <p>\$3: IPv4地址或者IPv6地址</p> <p>\$4: 掩码长度或者前缀长度</p> <p>\$5: VPN实例名。如果该FIB属于公网，该字段不显示</p>
日志等级	6
举例	<p>FIB/6/FIB_VN_INCONSISTENT: Inconsistent software and hardware entries for the following 1 FIB entries. Inconsistent parameters: next hop and mpls label.</p> <p>Entry for IP address 10.1.1.1 and mask length 32 on VPN instance vpn_1.</p> <p>FIB/6/FIB_VN_INCONSISTENT: Inconsistent software and hardware entries for the following 1 FIB entries. Inconsistent parameters: next hop and mpls label.</p> <p>Entry for IP address 10::2 and mask length 128 on the public network.</p>
日志说明	<p>使用<b>fib consistency-check enable</b>命令开启IPv4 FIB表项一致性检查功能，或者<b>ipv6 fib consistency-check enable</b>开启IPv6 FIB表项一致性检查功能后，如果设备检测到FIB虚拟下一跳软件表项与硬件表项不一致（比如FIB虚拟下一跳表项的下一跳地址），则输出本日志，提示用户哪些FIB表项失效</p>
处理建议	不需要处理，FIB会主动重刷硬件表项



## 40.7 FIB\_VN\_NORESOURCE

日志内容	Not enough hardware resources to issue the following [UINT32] software FIB entries to the driver: Entry for IP address [STRING] and mask length [UINT32] on VPN instance [STRING]. Not enough hardware resources to issue the following [UINT32] software FIB entries to the driver: Entry for IP address [STRING] and mask length [UINT32] on the public network.
参数解释	\$1: FIB表项数量 \$2: IPv4地址或者IPv6地址 \$3: 掩码长度或者前缀长度 \$4: VPN实例名。如果该FIB属于公网，该字段不显示
日志等级	6
举例	FIB/6/FIB_VN_NORESOURCE: Not enough hardware resources to issue the following 1 software FIB entries to the driver: Entry for IP address 10.1.1.1 and mask length 32 on VPN instance vpn_1. FIB/6/FIB_VN_NORESOURCE: Not enough hardware resources to issue the following 1 software FIB entries to the driver: Entry for IP address 10::2 and mask length 128 on the public network.
日志说明	使用 <b>fib consistency-check enable</b> 命令开启IPv4 FIB表项一致性检查功能，或者 <b>ipv6 fib consistency-check enable</b> 开启IPv6 FIB表项一致性检查功能后，当虚拟下一跳软件表项下发驱动时，如果驱动没有足够的硬件表项资源，则输出此日志，提示用户哪些FIB表项失效
处理建议	不需要处理，FIB会主动重刷硬件表项

# 41 FILTER

本节介绍 FILTER 模块输出的日志信息。

## 41.1 FILTER\_EXECUTION\_ICMP

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

## 41.2 FILTER\_EXECUTION\_ICMPV6

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

## 41.3 FILTER\_IPV4\_EXECUTION

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

## 41.4 FILTER\_IPV6\_EXECUTION

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

# 42 FIPSNG

本节介绍 FIP Snooping 模块输出的日志信息。

## 42.1 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

## 42.2 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

# 43 FS

本节介绍 FS（File System）模块输出的日志信息。

## 43.1 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_UNFORMATTED_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

# 44 FTP

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

## 44.1 FTP\_ACL\_DENY

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

## 44.2 FTPD\_AUTHOR\_FAILED

日志内容	Authorization failed for user [ STRING ]@[ STRING ].
参数解释	\$1: 用户名 \$2: 用户IP地址
日志等级	4
举例	FTP/4/FTPD_AUTHOR_FAILED: Authorization failed for user admin@10.11.115.63.
日志说明	FTP用户授权失败
处理建议	请检查是否配置该用户支持FTP服务

## 44.3 FTP\_REACH\_SESSION\_LIMIT

日志内容	FTP client [ STRING ] failed to log in. The current number of FTP sessions is [ NUMBER ]. The maximum number allowed is ([ NUMBER ]).
参数解释	\$1: FTP客户端IP地址 \$2: 当前的FTP会话数 \$3: 设备允许建立的FTP会话数
日志等级	6
举例	FTP/6/FTP_REACH_SESSION_LIMIT: FTP client 1.1.1.1 failed to log in. The current number of FTP sessions is 10. The maximum number allowed is (10).
日志说明	FTP登录用户达到上限。该日志在FTP服务端检测到登录客户端数达到上限时输出
处理建议	<ul style="list-style-type: none"><li>请使用 <b>display current-configuration   include session-limit</b> 命令查看设备当前允许的FTP最大登录用户数(如果执行该<b>display</b>命令后没有显示,则表示使用的是缺省配置)</li><li>根据需要使用 <b>aaa session-limit</b> 命令配置允许的FTP最大登录用户数</li></ul>

# 45 gRPC

本节介绍 gRPC 模块输出的日志信息。

## 45.1 GRPC\_LOGIN

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

## 45.2 GRPC\_LOGIN\_FAILED

日志内容	[STRING] from [STRING] login failed. 或 [STRING] from [STRING] login failed. [STRING]
参数解释	\$1: 用户名 \$2: 客户端地址 \$3: 失败原因，取值为Number of the gRPC sessions reached the limit.
日志等级	4
举例	GRPC/4/GRPC_LOGIN_FAILED: user from 127.0.0.1 login failed. GRPC/4/GRPC_LOGIN_FAILED: user from 127.0.0.1 login failed. Number of the gRPC sessions reached the limit.
日志说明	用户登录失败
处理建议	<ol style="list-style-type: none"><li>1. 如果未显示失败原因，请检查是否已配置用户，以及用户名和密码是否正确</li><li>2. 如果显示 gRPC 会话到达数量上限，请减少 gRPC 客户端连接数</li></ol>



## 45.3 GRPC\_LOGOUT

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

## 45.4 GRPC\_SERVER\_FAILED

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

## 45.5 GRPC\_SUBSCRIBE\_EVENT\_FAILED

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

## 45.6 GRPC\_RECEIVE\_SUBSCRIPTION

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

# 46 HA

本节介绍 HA 模块输出的日志信息。

## 46.1 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
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	主用主控板和备用主控板之间的批量备份完成
处理建议	无

## 46.2 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
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	主用主控板和备用主控板之间的批量备份开始
处理建议	无

## 46.3 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
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，如果备用主控板未准备好，则不会进行主备倒换，而是重启备用主控板和主用主控板，并在备用主控板上打印该信息
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

## 46.4 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
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，备用主控板成为主用主控板
处理建议	无

# 47 HLTH

本节介绍 HLTH（健康检测）模块输出的日志信息。

## 47.1 LIPC\_COMM\_FAULTY

日志内容	LIPC [STRING] between [STRING] and [STRING] might be faulty.
参数解释	<p>\$1: 通信类型, 取值包括:</p> <ul style="list-style-type: none"><li>unicast: 表示单播</li><li>broadcast: 表示广播</li><li>topo: 表示拓扑</li></ul> <p>\$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</p> <p>\$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</p>
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 <b>display system health</b> 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

## 47.2 LIPC\_COMM\_RECOVER

日志内容	LIPC [STRING] between [STRING] and [STRING] recovered.
参数解释	<p>\$1: 通信类型, 取值包括:</p> <ul style="list-style-type: none"><li>unicast: 表示单播</li><li>broadcast: 表示广播</li><li>topo: 表示拓扑</li></ul> <p>\$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</p> <p>\$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</p>
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

# 48 HQOS

本节介绍 HQOS (Hierarchical QoS) 模块输出的日志信息。

## 48.1 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

## 48.2 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

## 48.3 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 <b>display qos scheduler-policy diagnosis interface</b> 查看失败的转发节点以及失败原因，之后检查运行配置

## 48.4 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

# 49 HTTPD

本节介绍 HTTPD (HTTP daemon) 模块输出的日志信息。

## 49.1 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

## 49.2 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

## 49.3 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

## 49.4 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

## 49.5 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

## 49.6 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 <code>aaa session-limit</code> 配置允许的Web最大登录用户数

# 50 IFNET

本节介绍接口管理模块输出的日志信息。



## 50.1 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 <b>jumboframe enable [size]</b> 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 <i>size</i> 范围，将聚合接口的 <i>size</i> 配置在该范围内

## 50.2 IF\_BUFFER\_CONGESTION\_CLEAR

日志内容	[STRING] congestion on queue [UINT32] of [STRING] is cleared. [UINT64] packets are discarded.
参数解释	\$1: 接收或发送数据缓冲区，ingress、egress \$2: 队列ID，0~7 \$3: 接口名称 \$4: 丢弃报文数
日志等级	5
举例	IFNET/5/IF_BUFFER_CONGESTION_CLEAR: Ingress congestion on queue 1 of GigabitEthernet1/0/1 is cleared. 1000 packets are discarded.
日志说明	在接口 GigabitEthernet1/0/1 上队列1接收数据缓冲区的拥塞解除。共有1000个报文被丢弃
处理建议	无

## 50.3 IF\_BUFFER\_CONGESTION\_OCCURRENCE

日志内容	[STRING] congestion occurs on queue [INTEGER] of [STRING].
参数解释	\$1: 接收或发送数据缓冲区，ingress、egress \$2: 队列ID，0~7 \$3: 接口名称
日志等级	4
举例	IFNET/4/IF_BUFFER_CONGESTION_OCCURRENCE: Ingress congestion occurs on queue 1 of GigabitEthernet1/0/1.
日志说明	在接口 GigabitEthernet1/0/1 上队列1的接收数据缓冲区发生拥塞
处理建议	检查网络状况

## 50.4 IF\_LINKFLAP\_DETECTED

日志内容	Link flapping was detected on [STRING].
参数解释	\$1: 接口名称
日志等级	3
举例	IFNET/3/IF_LINKFLAP_DETECTED: Link flapping was detected on GigabitEthernet1/0/1.
日志说明	在链路震荡检查时间间隔内，接口状态从UP变为DOWN的次数大于等于链路震荡次数阈值
处理建议	<ol style="list-style-type: none"><li>1. 检查接口（本端或对端）连线是否被频繁插拔</li><li>2. 通过 port link-flap protect enable 命令调整链路震荡检查时间间隔和链路震荡次数阈值</li></ol>

## 50.5 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 Ethernet0/0/0 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

## 50.6 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 Ethernet0/0/0 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	<ol style="list-style-type: none"><li>1. 检查接口（本端或对端）连线是否被频繁插拔</li><li>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</li></ol>

## 50.7 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 Ethernet0/0 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 <b>display interface</b> 命令查看链路层状态, 进一步定位链路层状态为down的原因

## 50.8 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

## 50.9 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 Ethernet0/0 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。.

## 50.10 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 Ethernet6/4/1 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

## 50.11 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 <ul style="list-style-type: none"><li>o <i>lowerlimit%</i></li><li>o <i>lowerlimit pps</i></li><li>o <i>lowerlimit kbps</i></li></ul>
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

## 50.12 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 <ul style="list-style-type: none"><li>○ <i>upperlimit%</i></li><li>○ <i>upperlimit pps</i></li><li>○ <i>upperlimit kbps</i></li></ul>
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

## 50.13 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 <ul style="list-style-type: none"><li>○ <i>upperlimit%</i></li><li>○ <i>upperlimit pps</i></li><li>○ <i>upperlimit kbps</i></li></ul>
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

## 50.14 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 <ul style="list-style-type: none"><li>○ <i>lowerlimit%</i></li><li>○ <i>lowerlimit pps</i></li><li>○ <i>lowerlimit kbps</i></li></ul>
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

## 50.15 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 <b>display interface</b> 命令查看链路层状态, 进一步定位链路层状态为down的原因

## 50.16 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 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

## 50.17 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

# 51 IKE

本节介绍 IKE 模块输出的日志信息。

## 51.1 IKE\_P1\_SA\_ESTABLISH\_FAIL

日志内容	Failed to establish phase 1 SA for the reason of [STRING]. The SA's source address is [STRING], and its destination address is [STRING].
参数解释	<p>\$1: 失败原因:</p> <ul style="list-style-type: none"> <li>○ IKE 提议匹配失败, 显示为: no matching proposal</li> <li>○ ID 信息无效, 显示为: invalid ID information</li> <li>○ 证书不可用, 显示为: unavailable certificate</li> <li>○ 不支持的 DOI, 显示为: unsupported DOI</li> <li>○ 不支持当前应用场景, 显示为: unsupported situation</li> <li>○ IKE 提议语法无效, 显示为: invalid proposal syntax</li> <li>○ SPI 无效, 显示为: invalid SPI</li> <li>○ 协议 ID 错误, 显示为: invalid protocol ID</li> <li>○ 证书无效显示为: invalid certificate</li> <li>○ 认证失败, 显示为: authentication failure</li> <li>○ 信息头错误, 显示为: invalid message header</li> <li>○ 变换载荷 ID 无效, 显示为: invalid transform ID</li> <li>○ 载荷形式错误, 显示为: malformed payload</li> <li>○ 重传超时, 显示为: retransmission timeout</li> <li>○ 配置错误, 显示为: incorrect configuration</li> </ul> <p>\$2: 源地址</p> <p>\$3: 目的地址</p>
日志等级	6
举例	IKE/6/IKE_P1_SA_ESTABLISH_FAIL: Failed to establish phase 1 SA for the reason of no matching proposal. The SA's source address is 1.1.1.1 and its destination address is 2.2.2.2.
日志说明	IKE建立第一阶段SA失败以及失败原因
处理建议	检查本端和对端设备的IKE配置



## 51.2 IKE\_P2\_SA\_ESTABLISH\_FAIL

日志内容	Failed to establish phase 2 SA for the reason of [STRING]. The SA's source address is [STRING], and its destination address is [STRING].
参数解释	<p>\$1: 失败原因:</p> <ul style="list-style-type: none"> <li>○ 密钥信息无效, 显示为: invalid key information</li> <li>○ ID 信息无效, 显示为: invalid ID information</li> <li>○ IKE 提议不可用, 显示为: unavailable proposal</li> <li>○ 不支持的 DOI, 显示为: unsupported DOI</li> <li>○ 不支持当前应用场景, 显示为: unsupported situation</li> <li>○ IKE 提议语法无效, 显示为: invalid proposal syntax</li> <li>○ SPI 无效, 显示为: invalid SPI</li> <li>○ 协议 ID 无效, 显示为: invalid protocol ID</li> <li>○ 哈希信息无效, 显示为: invalid hash information</li> <li>○ 信息头无效, 显示为: invalid message header</li> <li>○ 载荷形式错误, 显示为: malformed payload</li> <li>○ 重传超时, 显示为: retransmission timeout</li> <li>○ 配置错误, 显示为: incorrect configuration</li> </ul> <p>\$2: 源地址</p> <p>\$3: 目的地址</p>
日志等级	6
举例	IKE/6/IKE_P2_SA_ESTABLISH_FAIL: Failed to establish phase 2 SA for the reason of invalid key information. The SA's source address is 1.1.1.1, and its destination address is 2.2.2.2.
日志说明	IKE建立第二阶段SA失败以及失败原因
处理建议	检查本端和对端设备的IKE和IPsec配置

## 51.3 IKE\_P2\_SA\_TERMINATE

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

## 51.4 IKE\_VERIFY\_CERT\_FAIL

日志内容	Failed to verify the peer certificate. Reason: [STRING].
参数解释	<p>\$1: 失败原因:</p> <ul style="list-style-type: none"><li>● 获取颁发者证书失败, 显示为: unable to get issuer certificate.</li><li>● 无法获取证书的 CRL, 显示为: unable to get certificate CRL.</li><li>● 无法解密 CRL 的签名, 显示为: unable to decrypt CRL's signature.</li><li>● 无法解析颁发者的公钥, 显示为: unable to decode issuer public key.</li><li>● 证书签名错误, 显示为: certificate signature failure.</li><li>● CRL 签名失败, 显示为: CRL signature failure.</li><li>● 解密证书签名失败, 显示为: unable to decrypt certificate's signature.</li><li>● 证书尚未生效, 显示为: certificate is not yet valid.</li><li>● 证书已失效, 显示为: certificate has expired.</li><li>● CRL 尚未生效, 显示为: CRL is not yet valid.</li><li>● CRL 已经失效, 显示为: CRL has expired.</li><li>● 证书的起始时间格式错误, 显示为: format error in certificate's notBefore field.</li><li>● 证书的结束时间格式错误, 显示为: format error in certificate's notAfter field.</li><li>● CRL 的上次更新时间格式错误, 显示为: format error in CRL's lastUpdate field.</li><li>● CRL 的下次更新时间格式错误, 显示为: format error in CRL's nextUpdate field.</li><li>● 内存不足, 显示为: out of memory.</li><li>● 自签名证书, 显示为: self signed certificate.</li><li>● 证书链中存在自签名证书, 显示为: self signed certificate in certificate chain.</li><li>● 获取本地颁发者证书失败, 显示为: unable to get local issuer certificate.</li><li>● 验证首个证书失败, 显示为: unable to verify the first certificate.</li><li>● 证书链过长, 显示为: certificate chain too long.</li><li>● 证书被撤回, 显示为: certificate revoked.</li><li>● 无效的 CA 证书, 显示为: invalid CA certificate.</li><li>● 无效的非 CA 证书, 显示为: invalid non-CA certificate (has CA markings).</li><li>● 超过路径深度约束, 显示为: path length constraint exceeded.</li><li>● 超过代理路径深度约束, 显示为: proxy path length constraint exceeded.</li><li>● 代理证书不通过, 请设置合适的标记, 显示为: proxy certificates not allowed, please set the appropriate flag.</li><li>● 不支持的证书用途, 显示为: unsupported certificate purpose.</li><li>● 证书不被信任, 显示为: certificate not trusted.</li><li>● 证书被拒绝, 显示为: certificate rejected.</li><li>● 证书应用验证失败, 显示为: application verification failure.</li><li>● 证书主题颁发者不匹配, 显示为: subject issuer mismatch.</li><li>● 授权和主题密钥认证人不匹配, 显示为: authority and subject key identifier mismatch.</li><li>● 授权和颁发者序列号不匹配, 显示为: authority and issuer serial number mismatch.</li></ul>

日志内容	Failed to verify the peer certificate. Reason: [STRING].
	<ul style="list-style-type: none"> <li>• 密钥用途不包括证书签名, 显示为: key usage does not include certificate signing.</li> <li>• 获取 CRL 颁发者证书失败, 显示为: unable to get CRL issuer certificate.</li> <li>• 不受控的决定性的扩展, 显示为: unhandled critical extension.</li> <li>• 密钥用途不包括 CRL 签名, 显示为: key usage does not include CRL signing.</li> <li>• 密钥用途不包括数字签名, 显示为: key usage does not include digital signature.</li> <li>• 不受控的决定性的 CRL 扩展, 显示为: unhandled critical CRL extension.</li> <li>• 无效或不一致的证书扩展, 显示为: invalid or inconsistent certificate extension.</li> <li>• 无效或不一致的证书策略扩展, 显示为: invalid or inconsistent certificate policy extension.</li> <li>• 不存在明确的策略, 显示为: no explicit policy.</li> <li>• CRL 范围不同, 显示为: Different CRL scope.</li> <li>• 不支持的扩展特性, 显示为: Unsupported extension feature.</li> <li>• RFC 3779 资源不是父资源的子集, 显示为: RFC 3779 resource not subset of parent's resources.</li> <li>• 被允许的子树违规, 显示为: permitted subtree violation.</li> <li>• 被排除的子树违规, 显示为: excluded subtree violation.</li> <li>• 名字约束的最小和最大范围不支持, 显示为: name constraints minimum and maximum not supported.</li> <li>• 不支持的名字约束类型, 显示为: unsupported name constraint type.</li> <li>• CRL 路径检验失败, 显示为: CRL path validation error.</li> <li>• 不支持的或无效的名字语法, 显示为: unsupported or invalid name syntax.</li> <li>• 不支持的或无效的名字约束语法, 显示为: unsupported or invalid name constraint syntax.</li> <li>• Suite B: 证书版本号无效, 显示为: Suite B: certificate version invalid.</li> <li>• Suite B: 无效的公钥算法, 显示为: Suite B: invalid public key algorithm.</li> <li>• Suite B: 无效的 ECC 曲线, 显示为: Suite B: invalid ECC curve.</li> <li>• Suite B: 无效的签名算法, 显示为: Suite B: invalid signature algorithm.</li> <li>• Suite B: 曲线不被本 LOS 准许, 显示为: Suite B: curve not allowed for this LOS.</li> <li>• Suite B: 不能使用 P-256 给 P-384 签名, 显示为: Suite B: cannot sign P-384 with P-256.</li> <li>• 主机名不匹配, 显示为: Hostname mismatch.</li> <li>• 邮件地址不匹配, 显示为: Email address mismatch.</li> <li>• IP 地址不匹配, 显示为: IP address mismatch.</li> <li>• 无效的证书认证上下文, 显示为: Invalid certificate verification context.</li> <li>• 颁发者证书检查失败, 显示为: Issuer certificate lookup error.</li> <li>• 代理主题名称不规范, 显示为: proxy subject name violation.</li> </ul>
日志等级	6
举例	IKE/6/IKE_VERIFY_CERT_FAIL: Failed to verify the peer certificate. Reason: invalid or inconsistent certificate extension.
日志说明	验证证书失败, 可能原因, 证书格式无效等
处理建议	无

# 52 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。

## 52.1 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

## 52.2 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

## 52.3 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

## 52.4 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

## 52.5 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

## 52.6 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

# 53 iNQA

本节介绍 iNQA (Intelligent Network Quality Analyzer, 智能网络质量分析) 模块输出的日志信息。

## 53.1 INQA\_BWD\_LOSS\_EXCEED

日志内容	Packet loss rate of the backward flow in instance [UINT] exceeded the upper limit.
参数解释	\$1: 实例号
日志等级	5
举例	INQA/5/INQA_BWD_LOSS_EXCEED: Packet loss rate of the backward flow in instance 1 exceeded the upper limit.
日志说明	反向流的丢包率大于丢包超限告警值
处理建议	检查当前组网环境，查看物理线路是否正常

## 53.2 INQA\_BWD\_LOSS\_RECOV

日志内容	Packet loss rate of the backward flow in instance [UINT] recovered.
参数解释	\$1: 实例号
日志等级	6
举例	INQA/6/INQA_BWD_LOSS_RECOV: Packet loss rate of the backward flow in instance 1 recovered.
日志说明	反向流的丢包率恢复到正常状态
处理建议	无

## 53.3 INQA\_DEBUG\_FAIL

日志内容	Setting debugging switch to drive failed.
日志等级	5
举例	INQA/5/INQA_DEBUG_FAIL: Setting debugging switch to drive failed.
日志说明	iNQA Debug开关配置下发驱动失败
处理建议	删除iNQA Debug开关配置，重新配置

## 53.4 INQA\_FLAG\_DIFF

日志内容	Flags of collectors bound with the analyzer instance [UINT] are inconsistent.
参数解释	\$1: Analyzer实例号
日志等级	5
举例	INQA/5/INQA_FLAG_DIFF: Flags of collectors bound with the analyzer instance 1 are inconsistent.
日志说明	Analyzer实例下关联的Collector端配置的染色位不一致
处理建议	检查该Analyzer实例下关联的所有Collector端染色位信息，保证配置一致

## 53.5 INQA\_FLAG\_FAIL

日志内容	Setting coloring bit to drive failed.
日志等级	5
举例	INQA/5/INQA_FLAG_FAIL: Setting coloring bit to drive failed.
日志说明	染色位配置下发驱动失败
处理建议	使用 <b>display qos-acl resource</b> 命令查看设备的 ACL 资源是否足够。如果 ACL 资源不足，请删除暂时无需使用的 ACL 后，再重新配置染色位

## 53.6 INQA\_FLOW\_DIFF

日志内容	Flows of collectors bound with the analyzer instance [UINT] are inconsistent.
参数解释	\$1: Analyzer实例号
日志等级	5
举例	INQA/5/INQA_FLOW_DIFF: Flows of collectors bound with the analyzer instance 1 are inconsistent.
日志说明	Analyzer实例下关联的Collector端发送过来的报文中携带的目标流不一致
处理建议	检查该Analyzer实例下关联的所有Collector端配置的目标流，保证目标流的配置一致

## 53.7 INQA\_FWD\_LOSS\_EXCEED

日志内容	Packet loss rate of the forward flow in instance [UINT] exceeded the upper limit.
参数解释	\$1: 实例号
日志等级	5
举例	INQA/5/INQA_FWD_LOSS_EXCEED: Packet loss rate of the forward flow in instance 1 exceeded the upper limit.
日志说明	正向流的丢包率大于丢包超限告警阈值
处理建议	检查当前组网环境，查看物理线路是否正常

## 53.8 INQA\_FWD\_LOSS\_RECOV

日志内容	Packet loss rate of the forward flow in instance [UINT] recovered.
参数解释	\$1: 实例号
日志等级	6
举例	INQA/6/INQA_FWD_LOSS_RECOV: Packet loss rate of the forward flow in instance 1 recovered.
日志说明	正向流的丢包率恢复到正常状态
处理建议	无

## 53.9 INQA\_INIT\_ERROR

日志内容	Failed to issue the configuration of instance [UINT] to drive because the MPs in the instance are mutually exclusive.
参数	\$1: 实例的编号
日志等级	5
举例	INQA/5/INQA_INIT_ERROR: Failed to issue the configuration of instance 1 to drive because the MPs in the instance are mutually exclusive.
日志说明	由于该实例中MP之间的配置互斥，导致实例配置下发给驱动失败
处理建议	检查实例下的配置，删除冲突配置



## 53.10 INQA\_INST\_FAIL

日志内容	Setting instance [UINT] information to drive failed.
参数解释	\$1: 实例号
日志等级	5
举例	INQA/5/INQA_INST_FAIL: Setting instance 1 information to drive failed.
日志说明	实例配置下发给驱动失败
处理建议	使用 <b>display qos-acl resource</b> 命令查看设备的ACL资源是否足够。如果ACL资源不足，请删除暂时无需使用的ACL后，再重新配置实例

## 53.11 INQA\_INTVL\_DIFF

日志内容	Intervals of collectors bound with analyzer instance [UINT] are inconsistent.
参数解释	\$1: Analyzer实例号
日志等级	5
举例	INQA/5/INQA_INTVL_DIFF: Intervals of collectors bound with analyzer instance 1 are inconsistent.
日志说明	Analyzer实例下关联的Collector端发送过来的报文携带的统计周期值不一致
处理建议	检查该Analyzer实例下关联的所有Collector端配置的统计周期，保持配置一致

## 53.12 INQA\_MP\_NOIF

日志内容	No statistics on MP [UINT]. Reason: [TEXT],
参数	\$1: 无统计信息的原因，取值为： <ul style="list-style-type: none"><li>• The MP does not bound to any interface: MP 没有绑定接口</li><li>• The interface bound with the MP does not exist: MP 绑定的接口不存在</li></ul>
日志等级	5
举例	INQA/5/INQA_MP_NOIF: No statistics on MP 1. Reason: The MP does not bound to any interface.
日志说明	MP上没有统计到数据，原因是MP没有绑定任何接口
处理建议	确定MP绑定接口，接口能正常收发报文

## 53.13 INQA\_NO\_RESOURCE

日志内容	Failed to configure instance [UINT] due to insufficient resources.
参数解释	\$1: 实例号
日志等级	5
举例	INQA/5/INQA_NO_RESOURCE: Failed to configure instance 1 due to insufficient resources.
日志说明	由于ACL表项资源不足，导致iNQA实例配置失败
处理建议	删除当前不需要使用的iNQA实例，或者删除当前不需要使用的ACL，来释放ACL表项资源，再重新配置当前实例

## 53.14 INQA\_NO\_SUPPORT

日志内容	iNQA is not supported in this slot.
日志等级	5
举例	INQA/5/INQA_NO_SUPPORT: iNQA is not supported in this slot.
日志说明	指定slot不支持iNQA功能
处理建议	更换slot，或者将需要测量的流量切换到支持iNQA的slot上

## 53.15 INQA\_SMOOTH\_BEGIN\_FAIL

日志内容	Setting smoothing beginning to kernel failed.
日志等级	5
举例	INQA/5/INQA_SMOOTH_BEGIN_FAIL: Setting smoothing beginning to the kernel failed.
日志说明	iNQA模块通知内核平滑开始，通知失败
处理建议	请联系技术支持人员

## 53.16 INQA\_SMOOTH\_END\_FAIL

日志内容	Setting smoothing ending to kernel failed.
日志等级	5
举例	INQA/5/INQA_SMOOTH_END_FAIL: Setting smoothing ending to kernel failed.
日志说明	iNQA模块通知内核平滑结束，通知失败
处理建议	请联系技术支持人员

# 54 IP6ADDR

本节介绍 IPv6 地址模块输出的日志信息。

## 54.1 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

## 54.2 IP6ADDR\_FUNCTION\_FAIL

日志内容	Failed to enable IPv6 on interface [STRING]. Reason: [STRING].
参数解释	\$1: 接口名 \$2: 使能IPv6功能失败的原因，取值包括： <ul style="list-style-type: none"><li>Insufficient resources: 资源不足</li><li>IPv6 is not supported: 由于设备不支持 IPv6，接口上不支持配置 IPv6 地址</li><li>Unknown error: 未知错误</li></ul>
日志等级	6
举例	IP6ADDR/6/IP6ADDR_FUNCTION_FAIL: Failed to enable IPv6 on interface GigabitEthernet1/0/1. Reason: Insufficient resources.
日志说明	接口通过有状态或无状态方式获取IPv6地址时，或手工指定接口的IPv6地址时，会使能IPv6功能。如果为接口配置IPv6地址失败，即使能IPv6功能失败，则打印此日志。使能IPv6功能失败的原因一般有：资源不足、设备不支持IPv6、未知错误等
处理建议	<ol style="list-style-type: none"><li>1. 如果是因为资源不足，可清理设备内存以释放资源，然后重新执行操作</li><li>2. 如果是未知错误，请联系技术支持</li></ol>

# 55 IP6FW

本节包含 IP6FW（IPv6 Forwarding）日志信息。

## 55.1 IPv6\_MTU\_SET\_DRV\_NOT\_SUPPORT

日志内容	The operation is not supported to set driver IPv6 interface MTU: interface is [STRING], MTU is [UINT32].
参数解释	\$1: 接口名称 \$2: IP MTU值
日志等级	5
举例	IP6FW/5/IPv6_MTU_SET_DRV_NOT_SUPPORT: The operation is not supported to set driver IPv6 interface MTU: interface is GigabitEthernet1/0/1, MTU is 1400.
日志说明	配置接口GigabitEthernet1/0/1上发送IPv6报文的MTU值，配置不支持下驱动
处理建议	<ol style="list-style-type: none"><li>1. 对于硬件转发的设备，无需处理，设备不支持配置接口上发送 IPv6 报文的 MTU</li><li>2. 对于软件转发的设备，请联系技术支持</li></ol>

# 56 IPADDR

本节介绍 IP 地址模块输出的日志信息。

## 56.1 IPADDR\_HA\_EVENT\_ERROR

日志内容	A process failed HA upgrade because [STRING].
------	---

日志内容	A process failed HA upgrade because [STRING].
参数解释	<p>\$1: 进程HA升级失败原因:</p> <ul style="list-style-type: none"> <li>• IPADDR failed the smooth upgrade: 板间平滑失败</li> <li>• IPADDR failed to reupgrade to the master process: 重新升级为主失败</li> <li>• IPADDR stopped to restart the timer: 重启定时器停止</li> <li>• IPADDR failed to upgrade to the master process: 升级为主进程失败</li> <li>• IPADDR failed to restart the upgrade: 重新尝试升级失败</li> <li>• 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</li> <li>• IPADDR failed to create an unicast object: 创建单播失败</li> <li>• IPADDR role switchover failed when the standby process switched to the master process: 备升主时角色转换失败</li> <li>• IPADDR switchover failed when the master process switched to the standby process: 主变备时降级失败</li> <li>• IPADDR HA upgrade failed: HA 升级失败</li> <li>• IPADDR failed to set the interface filtering criteria: 设置接口选择句柄失败</li> <li>• IPADDR failed to register interface events: 注册接口事件失败</li> <li>• IPADDR failed to subscribe port events: 订阅端口事件失败</li> <li>• 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</li> <li>• IRDP failed to open DBM: 打开 DBM 数据库失败</li> <li>• IRDP failed to initiate a connection to the device management module: 向设备管理建立连接失败</li> <li>• 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</li> <li>• IRDP failed to register device management events: 注册设备管理事件失败</li> <li>• IRDP failed to subscribe port events: 订阅协议使能端口事件失败</li> <li>• 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</li> <li>• IRDP failed to set the interface filtering criteria: 设置接口选择句柄失败</li> <li>• IRDP failed to register interface events: 注册接口事件失败</li> <li>• IRDP failed to register network events: 注册网络事件失败</li> <li>• IRDP failed to create the interface control block storage handle: 创建接口控制块存储句柄失败</li> <li>• IRDP failed to create the timer: 创建定时器失败</li> <li>• 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</li> <li>• IRDP failed to set the schedule time for the timer: 设置定时器调度时间失败</li> <li>• IRDP failed to set the timer to unblocked status: 设置定制器为非阻塞失败</li> <li>• IRDP failed to create a timer instance: 创建定时器实例失败</li> </ul>

日志内容	A process failed HA upgrade because [STRING].
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

## 56.2 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

# 57 IPFW

本节包含 IPFW（IP Forwarding）日志信息。

## 57.1 IPFW\_FAILURE

日志内容	The card doesn't support the split horizon forwarding configuration.
参数解释	无
日志等级	5
举例	IPFW/5/IPFW_FAILURE: -MDC=1; The card doesn't support the split horizon forwarding configuration.
日志说明	单板不支持配置转发水平分割
处理建议	<ol style="list-style-type: none"> <li>1. 请确保所属单板支持转发水平分割配置</li> <li>2. 请联系技术支持</li> </ol>

日志内容	Failed to configure split horizon forwarding on the card.
参数解释	无
日志等级	5
举例	IPFW/5/IPFW_FAILURE: -MDC=1; Failed to configure split horizon forwarding on the card.
日志说明	单板配置转发水平分割失败
处理建议	请联系技术支持

## 57.2 IPv4\_MTU\_SET\_DRV\_NOT\_SUPPORT

日志内容	The operation is not supported to set driver IPv4 interface MTU: interface is [STRING], MTU is [UINT32].
参数解释	\$1: 接口名称 \$2: IP MTU值
日志等级	5
举例	IPFW/5/IPv4_MTU_SET_DRV_NOT_SUPPORT: The operation is not supported to set driver IPv4 interface MTU: interface is GigabitEthernet1/0/1, MTU is 1400.
日志说明	配置接口GigabitEthernet1/0/1上发送IPv4报文的MTU值，配置不支持下驱动
处理建议	<ol style="list-style-type: none"> <li>1. 对于硬件转发的设备，无需处理，设备不支持配置接口上发送 IPv4 报文的 MTU</li> <li>2. 对于软件转发的设备，请联系技术支持</li> </ol>

# 58 IPSEC

本节介绍 IPsec 模块输出的日志信息。

## 58.1 IPSEC\_FAILED\_ADD\_FLOW\_TABLE

日志内容	Failed to add flow-table due to [STRING].
参数解释	\$1: 失败原因
日志等级	4
举例	IPSEC/4/IPSEC_FAILED_ADD_FLOW_TABLE: Failed to add flow-table due to no enough resource.
日志说明	添加流表失败，可能原因包括硬件资源不足等
处理建议	对于硬件资源不足情况，请联系技术支持



## 58.2 IPSEC\_PACKET\_DISCARDED

日志内容	IPsec packet discarded, Src IP:[STRING], Dst IP:[STRING], SPI:[UINT32], SN:[UINT32], Cause:[STRING].
参数解释	<p>\$1: 报文的源IP地址</p> <p>\$2: 报文的目的地IP地址</p> <p>\$3: SPI (Security Parameter Index, 安全参数索引)</p> <p>\$4: 报文的序列号</p> <p>\$5: 报文丢弃的原因:</p> <ul style="list-style-type: none"><li>抗重放检测失败, 显示为: Anti-replay checking failed.</li><li>AH 认证失败, 显示为: AH authentication failed.</li><li>ESP 认证失败, 显示为: ESP authentication failed.</li><li>SA 无效, 显示为: Invalid SA.</li><li>ESP 解密失败, 显示为: ESP decryption failed.</li><li>报文的源地址匹配不上 SA, 显示为: Source address of packet does not match the SA.</li><li>没有匹配的 ACL 规则, 显示为: No ACL rule matched.</li></ul>
日志等级	6
举例	IPSEC/6/IPSEC_PACKET_DISCARDED: IPsec packet discarded, Src IP:1.1.1.2, Dest IP:1.1.1.4, SPI:1002, SN:0, Cause:ah authentication failed
日志说明	IPsec报文被丢弃
处理建议	无

## 58.3 IPSEC\_SA\_ESTABLISH

日志内容	Established IPsec SA. The SA's source address is [STRING], destination address is [STRING], protocol is [STRING], and SPI is [UINT32].
参数解释	<p>\$1: IPsec SA的源IP地址</p> <p>\$2: IPsec SA的目的IP地址</p> <p>\$3: IPsec SA使用的安全协议</p> <p>\$4: IPsec SA的SPI</p>
日志等级	6
举例	IPSEC/6/IPSEC_SA_ESTABLISH: Established IPsec SA. The SA's source address is 1.1.1.1, destination address is 2.2.2.2, protocol is AH, and SPI is 2435.
日志说明	IPsec SA创建成功
处理建议	无

## 58.4 IPSEC\_SA\_ESTABLISH\_FAIL

日志内容	Failed to establish IPsec SA for the reason of [STRING]. The SA's source address is [STRING], and its destination address is [STRING].
参数解释	<p>\$1: IPsec SA创建失败的原因:</p> <ul style="list-style-type: none"><li>隧道创建失败, 显示为: Tunnel establishment failure.</li><li>配置不完整, 显示为: Incomplete configuration.</li><li>配置的安全提议无效, 显示为: Unavailable transform set.</li></ul> <p>\$2: 源IP地址</p> <p>\$3: 目的IP地址</p>
日志等级	6
举例	IPSEC/6/IPSEC_SA_ESTABLISH_FAIL: Failed to establish IPsec SA for the reason of creating tunnel failure. The SA's source address is 1.1.1.1, and its destination address is 2.2.2.2.
日志说明	IPsec SA创建失败。触发该日志的原因可能有: 隧道创建失败、配置不完整、或者配置的安全提议无效
处理建议	检查本端和对端设备上的IPsec配置

## 58.5 IPSEC\_SA\_INITINATION

日志内容	Began to establish IPsec SA. The SA's source address is [STRING], and its destination address is [STRING].
参数解释	<p>\$1: IPsec SA的源IP地址</p> <p>\$2: IPsec SA的目的IP地址</p>
日志等级	6
举例	IPSEC/6/IPSEC_SA_INITINATION: Began to establish IPsec SA. The SA's source address is 1.1.1.1, and its destination address is 2.2.2.2.
日志说明	开始创建IPsec SA
处理建议	无

## 58.6 IPSEC\_SA\_TERMINATE

日志内容	The IPsec SA was deleted for the reason of [STRING]. The SA's source address is [STRING], destination address is [STRING], protocol is [STRING], and SPI is [UINT32].
参数解释	<p>\$1: IPsec SA被删除的原因:</p> <ul style="list-style-type: none"><li>SA 空闲超时, 显示为: SA idle timeout.</li><li>执行了 reset 命令, 显示为: <b>reset</b> command executed.</li></ul> <p>\$2: 源IP地址</p> <p>\$3: 目的IP地址</p> <p>\$4: 使用的安全协议</p> <p>\$5: SPI</p>
日志等级	6
举例	IPSEC/6/IPSEC_SA_TERMINATE: The IPsec SA was deleted for the reason of SA idle timeout. The SA's source address is 1.1.1.1, destination address is 2.2.2.2, protocol is ESP, and SPI is 34563.
日志说明	IPsec SA被删除。触发该日志的原因可能有: SA空闲超时或者执行了reset命令
处理建议	无

# 59 IPSG

本节介绍 IPSG (IP Source Guard) 模块输出的日志信息。

## 59.1 IPKG\_ADDENTRY\_ERROR

日志内容	Failed to add an IP source guard binding (IP [STRING], MAC [STRING], and VLAN [UINT16]) on interface [STRING]. [STRING].
参数解释	<p>\$1: IPv4地址或IPv6地址（如果没有指定，则显示N/A）</p> <p>\$2: MAC地址（如果没有指定，则显示为N/A）</p> <p>\$3: VLAN ID（如果没有指定，则显示为无意义值65535）</p> <p>\$4: 接口名称（如果没有指定，则显示为N/A）</p> <p>\$5: 失败原因：</p> <ul style="list-style-type: none"> <li>○ Feature not supported: 特性不支持</li> <li>○ Resources not sufficient: 资源不足</li> <li>○ Maximum number of IPv4 binding entries already reached: IPv4 绑定表项达到最大规格</li> <li>○ Maximum number of IPv6 binding entries already reached: IPv6 绑定表项达到最大规格</li> <li>○ Unknown error: 未知错误</li> </ul>
日志等级	6
举例	IPSG/6/IPKG_ADDENTRY_ERROR: Failed to add an IP source guard binding (IP 1.1.1.1, MAC 0001-0001-0001, and VLAN 1) on interface Vlan-interface1. 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、表项达到最大规格或未知错误
处理建议	<ul style="list-style-type: none"> <li>● 当提示硬件资源不足时，可清理设备内存以释放资源</li> <li>● 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</li> <li>● 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</li> </ul>

## 59.2 IPSG\_ADEXCLUDEDVLAN\_ERROR

日志内容	Failed to add excluded VLANs (start VLAN [UINT16] to end VLAN [UINT16]). [STRING].
参数解释	\$1: Start VLAN (免过滤VLAN的起始VLAN ID) \$2: End VLAN (免过滤VLAN的结束VLAN ID) \$3: 失败原因: <ul style="list-style-type: none"><li>• Feature not supported: 特性不支持</li><li>• Resources not sufficient: 资源不足</li><li>• Unknown error: 未知错误</li></ul>
日志等级	6
举例	IPSG/6/IPSG_ADEXCLUDEDVLAN_ERROR: -MDC=1-Slot=4; Failed to add excluded VLANs (start VLAN 1 to end VLAN 5). Resources not sufficient.
日志说明	下发免过滤VLAN失败, 可能的原因有: 特性不支持、资源不足或未知错误
处理建议	<ul style="list-style-type: none"><li>• 因硬件资源不足而引起的免过滤 VLAN 下发失败, 可清理设备内存以释放资源, 然后重新执行命令下发该配置</li><li>• 当下发免过滤 VLAN 失败原因为未知错误时, 请联系技术支持</li></ul>

## 59.3 IPSG\_ARP\_LOCALMAC\_CONFLICT

日志内容	MAC conflict exists between an ARP entry and a local entry: IP=[STRING], VPN=[STRING], ARPMAC=[STRING], LocalMAC=[STRING].
参数解释	\$1: IP地址 \$2: VPN实例的名称 \$3: ARP表项MAC地址 \$4: 本地绑定表项MAC地址
日志等级	5
举例	IPSG/5/IPSG_ARP_LOCALMAC_CONFLICT: MAC conflict exists between an ARP entry and a local entry: IP=1.1.1.1, VPN=1, ARPMAC=0008-0008-0008, LocalMAC=0008-0008-0009.
日志说明	ARP表项和本地绑定表项的MAC地址冲突。当存在恶意的ARP攻击时, 如果ARP表项和本地绑定表项的IP地址相同, 但两者的MAC地址不同, 则会输出该日志
处理建议	检查ARP表项的来源设备是否存在恶意攻击行为

## 59.4 IPSG\_ARP\_REMOTEMAC\_CONFLICT

日志内容	MAC conflict exists between an ARP entry and a remote entry: IP=[STRING], VPN=[STRING], ARPMAC=[STRING], RemoteMAC=[STRING].
参数解释	\$1: IP地址 \$2: VPN实例的名称 \$3: ARP表项MAC地址 \$4: 远端绑定表项MAC地址
日志等级	5
举例	IPSG/5/IPSG_ARP_REMOTEMAC_CONFLICT: MAC conflict exists between an ARP entry and a remote entry: IP=1.1.1.1, VPN=1, ARPMAC=0008-0008-0008, RemoteMAC=0008-0008-0009.
日志说明	ARP表项和远端绑定表项的MAC地址冲突，有以下情况会输出该日志： <ul style="list-style-type: none"> <li>存在恶意的ARP攻击，设备学习到非法用户的ARP表项与远端绑定表项的IP地址相同，但两者的MAC地址不同</li> <li>远端用户漫游到本地上线，使得设备学习到该漫游用户的ARP表项与远端绑定表项的IP地址相同，但两者的MAC地址不同</li> </ul>
处理建议	<ul style="list-style-type: none"> <li>当存在恶意ARP攻击时，请检查ARP表项的来源设备</li> <li>对于漫游用户本地上线，无需处理</li> </ul>

## 59.5 IPSG\_DELENTY\_ERROR

日志内容	Failed to delete an IP source guard binding (IP [STRING], MAC [STRING], and VLAN [UINT16]) on interface [STRING]. [STRING].
参数解释	\$1: IP地址（如果没有指定，则显示N/A） \$2: MAC地址（如果没有指定，则显示为N/A） \$3: VLAN ID（如果没有指定，则显示为无意义值65535） \$4: 接口名（如果没有指定，则显示为N/A） \$5: 失败原因： <ul style="list-style-type: none"> <li>Feature not supported: 特性不支持</li> <li>Unknown error: 未知错误</li> </ul>
日志等级	6
举例	IPSG/6/IPSG_DELENTY_ERROR: Failed to delete an IP source guard binding (IP 1.1.1.1, MAC 0001-0001-0001, and VLAN 1) on interface Vlan-interface1. Unknown error.
日志说明	删除全局静态IP Source Guard绑定表项失败，可能的原因有：特性不支持或者未知错误
处理建议	<ul style="list-style-type: none"> <li>重新执行命令删除该表项</li> <li>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</li> </ul>

## 59.6 IPSG\_DELEXCLUDEDVLAN\_ERROR

日志内容	Failed to delete excluded VLANs (start VLAN [UINT16] to end VLAN [UINT16]). [STRING].
参数解释	<p>\$1: Start VLAN (免过滤VLAN的起始VLAN ID)</p> <p>\$2: End VLAN (免过滤VLAN的结束VLAN ID)</p> <p>\$3: 失败原因:</p> <ul style="list-style-type: none"> <li>• Feature not supported: 特性不支持</li> <li>• Resources not sufficient: 资源不足</li> <li>• Unknown error: 未知错误</li> </ul>
日志等级	6
举例	IPSG/6/IPSG_DELEXCLUDEDVLAN_ERROR: -MDC=1-Slot=4; Failed to delete excluded VLANs (start VLAN 1 to end VLAN 5). Resources not sufficient.
日志说明	删除免过滤VLAN失败, 可能的原因有: 特性不支持、资源不足或未知错误
处理建议	<ul style="list-style-type: none"> <li>• 因硬件资源不足而引起的删除免过滤 VLAN 失败, 可清理设备内存以释放资源, 然后重新执行命令下发该配置</li> <li>• 当删除免过滤 VLAN 失败原因为未知错误时, 请联系技术支持</li> </ul>

## 59.7 IPSG\_MAC\_CONFLICT

日志内容	MAC conflict exists between a local entry and a remote entry: IP=[STRING], VPN=[STRING], LocalMAC=[STRING], RemoteMAC=[STRING].
参数解释	<p>\$1: IP地址</p> <p>\$2: VPN实例的名称</p> <p>\$3: 本地绑定表项MAC地址</p> <p>\$4: 远端绑定表项MAC地址</p>
日志等级	5
举例	IPSG/5/IPSG_MAC_CONFLICT: MAC conflict exists between a local entry and a remote entry: IP=1.1.1.1, VPN=1, LocalMAC=0008-0008-0008, RemoteMAC=0008-0008-0009.
日志说明	远端绑定表项和本地绑定表项的MAC地址冲突。当本地学习到一个远端绑定表项时, 若该绑定表项的IP地址与本地已有某绑定表项的IP地址相同, 但两者的MAC地址不同, 则会输出该日志
处理建议	无需处理

## 59.8 IPSPG\_ND\_LOCALMAC\_CONFLICT

日志内容	MAC conflict exists between an ND entry and a local entry: IPv6=[STRING], VPN=[STRING], NDMAC=[STRING], LocalMAC=[STRING].
参数解释	\$1: IP地址 \$2: VPN实例的名称 \$3: ND表项MAC地址 \$4: 本地绑定表项MAC地址
日志等级	5
举例	IPSPG/5/IPSPG_ND_LOCALMAC_CONFLICT: MAC conflict exists between an ND entry and a local entry: IPv6=1::1, VPN=1, NDMAC=0008-0008-0008, LocalMAC=0008-0008-0009.
日志说明	ND表项和本地绑定表项的MAC地址冲突。当存在恶意的ND攻击时，如果ND表项和本地绑定表项的IP地址相同，但两者的MAC地址不同，则会输出该日志
处理建议	检查ND表项的来源设备是否存在恶意攻击行为

## 59.9 IPSPG\_ND\_REMOTEMAC\_CONFLICT

日志内容	MAC conflict exists between an ND entry and a remote entry: IPv6=[STRING], VPN=[STRING], NDMAC=[STRING], RemoteMAC=[STRING].
参数解释	\$1: IP地址 \$2: VPN实例的名称 \$3: ND表项MAC地址 \$4: 远端绑定表项MAC地址
日志等级	5
举例	IPSPG/5/IPSPG_ND_REMOTEMAC_CONFLICT: MAC conflict exists between an ND entry and a remote entry: IPv6=1::1, VPN=1, NDMAC=0008-0008-0008, RemoteMAC=0008-0008-0009.
日志说明	ND表项和远端绑定表项的MAC地址冲突，有以下情况会输出该日志： <ul style="list-style-type: none"><li>存在恶意的ND攻击，设备学习到非法用户的ND表项与远端绑定表项的IPv6地址相同，但两者的MAC地址不同</li><li>远端用户漫游到本地上线，使得设备学习到该漫游用户的ND表项与远端绑定表项的IPv6地址相同，但两者的MAC地址不同</li></ul>
处理建议	<ul style="list-style-type: none"><li>当存在恶意ARP攻击时，请检查ND表项的来源设备</li><li>对于漫游用户本地上线，无需处理</li></ul>



## 59.10 IPSG\_IPV4\_ALARMCLEAR

日志内容	The packet dropping rate on [STRING] dropped below [UINT32] pps.
参数解释	\$1: 接口名称 \$2: 告警阈值
日志等级	4
举例	IPSG/4/IPSG_IPV4_ALARMCLEAR: The packet dropping rate on GigabitEthernet1/0/1 dropped below 100 pps.
日志说明	接口上每秒丢弃报文数恢复到告警阈值之内
处理建议	无

## 59.11 IPSG\_IPV4\_ALARMEMERGE

日志内容	The packet dropping rate on [STRING] reached or exceeded [UINT32] pps.
参数解释	\$1: 接口名称 \$2: 告警阈值
日志等级	4
举例	IPSG/4/IPSG_IPV4_ALARMEMERGE: The packet dropping rate on GigabitEthernet1/0/1 reached or exceeded 100 pps.
日志说明	接口上每秒丢弃报文数大于或等于告警阈值
处理建议	检查遭到攻击的接口下的用户是否存在攻击源

## 59.12 IPSG\_IPV6\_ALARMCLEAR

日志内容	The packet dropping rate on [STRING] dropped below [UINT32] pps.
参数解释	\$1: 接口名称 \$2: 告警阈值
日志等级	4
举例	IPSG/4/IPSG_IPV6_ALARMCLEAR: The packet dropping rate on GigabitEthernet1/0/1 dropped below 100 pps.
日志说明	接口上每秒丢弃报文数恢复到告警阈值之内
处理建议	无

## 59.13 IPKG\_IPV6\_ALARMEMERGE

日志内容	The packet dropping rate on [STRING] reached or exceeded [UINT32] pps.
参数解释	\$1: 接口名称 \$2: 告警阈值
日志等级	4
举例	IPKG/4/IPKG_IPV6_ALARMEMERGE: The packet dropping rate on GigabitEthernet1/0/1 reached or exceeded 100 pps.
日志说明	接口上每秒丢弃报文数大于或等于告警阈值
处理建议	检查遭到攻击的接口下是否存在攻击源

# 60 IRDP

本节介绍 IRDP 模块输出的日志信息。

## 60.1 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

# 61 IRF

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

## 61.1 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

## 61.2 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： <ul style="list-style-type: none"><li>• IRF 端口下是否绑定了物理接口</li><li>• 绑定的物理接口是否和对端正确连接</li></ul>

## 61.3 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

## 61.4 IRF\_MEMBERID\_CONFLICT

日志内容	IRF member ID conflict occurred. The ID [UINT32] has been used for another device with CPU-Mac: [STRING].
参数解释	\$1: 设备的成员编号 \$2: 设备的CPU MAC
日志等级	4
举例	IRF/4/IRF_MEMBERID_CONFLICT:-slot = 5; IRF member ID conflict occurred, The ID 5 has been used for another device with CPU-Mac: 000c-29d7-c1ae.
日志说明	在同一广播域中发现跟自己成员编号相同的设备时，打印该日志，提示成员冲突
处理建议	根据提示信息，检查IRF中的成员编号，重新设置新加入设备的成员编号

## 61.5 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

## 61.6 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

## 61.7 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

# 62 ISIS

本节介绍 IS-IS 模块输出的日志信息。

## 62.1 ISIS\_LSP\_CONFLICT

日志内容	ISIS [UINT16], [STRING] LSP, LSPID=[STRING], SeqNum=[HEX], system ID conflict might exist.
参数解释	\$1: 进程ID \$2: IS类型，值为Level-1或Level-2 \$3: LSP ID \$4: LSP序列号
日志等级	5
举例	ISIS/5/ISIS_LSP_CONFLICT: -MDC=1; ISIS 1, Level-1 LSP, LSPID=1111.1111.1111.00-00, SeqNum=0x000045bf, system ID conflict might exist.
日志说明	网络中可能存在System ID冲突
处理建议	检查产生该LSP的设备的System ID是否和其他设备的System ID冲突

## 62.2 ISIS\_MEM\_ALERT

日志内容	ISIS Process received system memory alert [STRING] event.
参数解释	\$1: 内存告警类型
日志等级	5
举例	ISIS/5/ISIS_MEM_ALERT: ISIS Process received system memory alert start event.
日志说明	IS-IS模块收到内存告警信息
处理建议	当超过各级内存门限时，检查系统内存占用情况，对占用内存较多的模块进行调整，尽量释放可用内存

## 62.3 ISIS\_NBR\_CHG

日志内容	IS-IS [UINT16], [STRING] adjacency [STRING] ([STRING]), state changed to [STRING], Reason: [STRING].
参数解释	<p>\$1: IS-IS进程ID</p> <p>\$2: IS-IS邻居等级</p> <p>\$3: 邻居ID</p> <p>\$4: 接口名称</p> <p>\$5: 当前邻居状态, 包括DOWN、UP和INIT</p> <p>\$6: 邻居状态变化原因, 包括:</p> <ul style="list-style-type: none"> <li>• circuit data clean: 邻居状态发生变化时, 清除路由数据, 导致邻居状态变为 down</li> <li>• holdtime expired: 没有收到邻居发送的 Hello 报文, 则认为邻居失效, 将邻居状态置为 down</li> <li>• BFD session down: BFD 检测到链路故障并通知 IS-IS, IS-IS 将邻居状态置为 down</li> <li>• peer reset: 执行 <b>reset isis peer</b> 命令, 导致邻居状态变为 down</li> <li>• circuit ID conflicts: 收到邻居发送的 Hello 报文中, circuit ID 不一致, 导致邻居状态变为 down</li> <li>• P2P peer GR down: GR 恢复过程中, 收到邻居发送的 Hello 报文中没有携带 GR 选项, 导致邻居状态变为 down</li> <li>• 2way-pass: IS-IS 邻居建立成功, 邻居状态变为 UP</li> <li>• 2way-fail: 收到邻居发送的 one-way Hello 报文, 邻居状态变为 INIT</li> </ul>
日志等级	5
举例	ISIS/5/ISIS_NBR_CHG: IS-IS 1, Level-1 adjacency 0000.0000.0001 (GigabitEthernet1/0/1), state changed to DOWN, Reason: circuit data clean.
日志说明	邻居状态发生变化
处理建议	<p>需要关注邻居状态变化原因。当邻居状态变为DOWN或INIT时, 对于不同的邻居状态变化原因的处理建议如下:</p> <ul style="list-style-type: none"> <li>• circuit data clean 的处理建议: <ul style="list-style-type: none"> <li>○ 检查接口状态</li> <li>○ 检查 IS-IS 配置的正确性</li> <li>○ 检查网络连通性</li> </ul> </li> <li>• holdtime expired 的处理建议为, 确认是否收到了邻居发送的 Hello 报文</li> <li>• BFD session down 的处理建议为, 检查与邻居的连通性</li> <li>• peer reset 的处理建议为, 检查是否执行了 <b>reset isis peer</b> 命令</li> <li>• circuit ID conflicts 的处理建议为, 检查邻居是否反复修改了使能 IS-IS 的接口</li> <li>• P2P peer GR down 的处理建议为, 检查邻居设备是否支持 GR 能力</li> <li>• 2way-fail 的处理建议: <ul style="list-style-type: none"> <li>○ 检查是否执行了 <b>reset isis peer</b> 命令</li> <li>○ 确认是否收到了邻居发送的 Hello 报文</li> <li>○ 检查两端的认证配置是否一致</li> </ul> </li> </ul>

# 63 ISSU

本节介绍 ISSU 模块输出的日志信息。

## 63.1 ISSU\_LOAD\_FAILED

日志内容	Failed to execute the issu load command.
参数解释	无
日志等级	5
举例	ISSU/5/ISSU_LOAD_FAILED: -IPAddr=192.168.79.1-User=**; Failed to execute the issu load command.
日志说明	用户执行 <b>issu load</b> 命令进行ISSU升级，操作失败
处理建议	请根据提示信息采取相应措施

## 63.2 ISSU\_LOAD\_SUCCESS

日志内容	Executed the issu load command successfully.
参数解释	无
日志等级	5
举例	ISSU/5/ISSU_LOAD_SUCCESS: -IPAddr=192.168.79.1-User=**; Executed the issu load command successfully.
日志说明	用户执行 <b>issu load</b> 命令进行ISSU升级，操作成功
处理建议	无

## 63.3 ISSU\_PROCESSWITCHOVER

日志内容	Switchover completed. The standby process became the active process.
参数解释	无
日志等级	5
举例	ISSU/5/ISSU_PROCESSWITCHOVER: Switchover completed. The standby process became the active process.
日志说明	用户执行 <b>issu run switchover</b> 进行主备倒换完成，备进程已升级为主进程
处理建议	无



## 63.4 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 <b>issu rollback</b> 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

# 64 L2PT

本节介绍 L2PT 模块输出的日志信息。

## 64.1 L2PT\_ADD\_GROUPMEMBER\_FAILED

日志内容	Failed to add [STRING] as a member to the VLAN tunnel group for [STRING].
参数解释	\$1: 接口名称 \$2: 协议类型
日志等级	4
举例	L2PT/4/L2PT_ADD_GROUPMEMBER_FAILED: Failed to add GigabitEthernet2/0/1 as a member to the VLAN tunnel group for STP.
日志说明	接口加入协议的VLAN Tunnel组播组失败
处理建议	无

## 64.2 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

## 64.3 L2PT\_ENABLE\_DROP\_FAILED

日志内容	Failed to enable [STRING] packet drop on [STRING].
参数解释	\$1: 协议类型 \$2: 接口名称
日志等级	4
举例	L2PT/4/L2PT_ENABLE_DROP_FAILED: Failed to enable STP packet drop on GigabitEthernet2/0/1.
日志说明	接口上使能L2PT Drop功能失败
处理建议	无

## 64.4 L2PT\_SET\_MULTIMAC\_FAILED

日志内容	Failed to set a tunnel destination MAC address to [MAC].
参数解释	\$1: MAC地址
日志等级	4
举例	L2PT/4/L2PT_SET_MULTIMAC_FAILED: Failed to set a tunnel destination MAC address to 010f-e200-0003.
日志说明	配置BPDU Tunnel报文的的目的MAC地址失败
处理建议	无

# 65 L2TPV2

本节介绍 L2TPV2 模块输出的日志信息。

## 65.1 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

## 65.2 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 <b>reset l2tp tunnel</b> 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

# 66 L2VPN

本节介绍 L2VPN 模块输出的日志信息。

## 66.1 L2VPN\_ARP\_MOBILITY\_SUPPRESS (public instance)

日志内容	ARP (IP [STRING], MAC [STRING]) was suppressed in the public instance due to frequent ARP mobility events.
参数解释	\$1: IP地址 \$2: MAC地址
日志等级	4
举例	L2VPN/4/L2VPN_ARP_MOBILITY_SUPPRESS: ARP (IP 10.1.1.1, MAC 0001-0001-0001) was suppressed in the public instance due to frequent ARP mobility events.
日志说明	开启ARP反复迁移抑制功能后，ARP迁移频率超过限制，抑制该ARP迁移
处理建议	ARP迁移频率过高的原因可能是网络中存在IP地址冲突。请检查网络中的IP地址配置，避免IP地址冲突

## 66.2 L2VPN\_ARP\_MOBILITY\_SUPPRESS (VPN instance)

日志内容	ARP (IP [STRING], MAC [STRING]) was suppressed in VPN instance [STRING] due to frequent ARP mobility events.
参数解释	\$1: IP地址 \$2: MAC地址 \$3: VPN实例名称
日志等级	4
举例	L2VPN/4/L2VPN_ARP_MOBILITY_SUPPRESS: ARP (IP 10.1.1.1, MAC 0001-0001-0001) was suppressed in VPN instance vpna due to frequent ARP mobility events.
日志说明	开启ARP反复迁移抑制功能后，ARP迁移频率超过限制，抑制该ARP迁移
处理建议	ARP迁移频率过高的原因可能是网络中存在IP地址冲突。请检查网络中的IP地址配置，避免IP地址冲突

## 66.3 L2VPN\_ARP\_MOBILITY\_UNSUPPRESS (public instance)

日志内容	ARP (IP [STRING], MAC [STRING]) was unsuppressed in the public instance.
参数解释	\$1: IP地址 \$2: MAC地址 \$3: VPN实例名称
日志等级	4
举例	L2VPN/4/L2VPN_ARP_MOBILITY_UNSUPPRESS: ARP (IP 10.1.1.1, MAC 0001-0001-0001) was unsuppressed in the public instance.
日志说明	执行 <b>undo evpn route arp-mobility suppress</b> 命令后，解除指定ARP的迁移抑制，可以向远端通告该ARP信息
处理建议	无

## 66.4 L2VPN\_ARP\_MOBILITY\_UNSUPPRESS (VPN instance)

日志内容	ARP (IP [STRING], MAC [STRING]) was unsuppressed in VPN instance [STRING].
参数解释	\$1: IP地址 \$2: MAC地址 \$3: VPN实例名称
日志等级	4
举例	L2VPN/4/L2VPN_ARP_MOBILITY_UNSUPPRESS: ARP (IP 10.1.1.1, MAC 0001-0001-0001) was unsuppressed in VPN instance vpna.
日志说明	执行 <b>undo evpn route arp-mobility suppress</b> 命令后，解除指定ARP的迁移抑制，可以向远端通告该ARP信息
处理建议	无

## 66.5 L2VPN\_MAC\_MOBILITY\_SUPPRESS

日志内容	MAC address [STRING] was suppressed in VSI [STRING] due to frequent MAC mobility events.
参数解释	\$1: MAC地址 \$2: VSI名称
日志等级	4
举例	L2VPN/4/L2VPN_MAC_MOBILITY_SUPPRESS: MAC address 0001-0001-0001 was suppressed in VSI vpna due to frequent MAC mobility events.
日志说明	开启MAC地址反复迁移抑制功能后，MAC地址迁移频率超过限制，抑制该MAC地址迁移
处理建议	MAC地址迁移频率过高的原因可能是网络中存在MAC地址冲突。请检查网络中的MAC地址配置，避免MAC地址冲突

## 66.6 L2VPN\_MAC\_MOBILITY\_UNSUPPRESS

日志内容	MAC address [STRING] was unsuppressed in VSI [STRING].
参数解释	\$1: MAC地址 \$2: VSI名称
日志等级	4
举例	L2VPN/4/L2VPN_MAC_MOBILITY_UNSUPPRESS: MAC address 0001-0001-0001 was unsuppressed in VSI vpna.
日志说明	执行 <b>undo evpn route mac-mobility suppress</b> 命令后，解除指定MAC地址的迁移抑制，可以向远端通告该MAC地址
处理建议	无

## 66.7 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： <ul style="list-style-type: none"><li>• 新接收到一个远端 Site ID 和本端 Site ID 相同</li><li>• 新配置本端 Site ID 和已接收到的一个远端 Site ID 相同</li></ul>
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

## 66.8 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

## 66.9 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

## 66.10 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

## 66.11 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： <ul style="list-style-type: none"><li>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</li><li>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</li></ul>
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

## 66.12 L2VPN\_MLAG\_AC\_CONFLICT

日志内容	The dynamic AC created for Ethernet service instance [INT32] on interface [STRING] causes a conflict.
参数解释	\$1: 以太网服务实例编号 \$2: 以太网服务实例所在的接口
日志等级	4
举例	L2VPN/4/L2VPN_MLAG_AC_CONFLICT: The dynamic AC created for Ethernet service instance 10 on interface Bridge-Aggregation 5 causes a conflict.
日志说明	EVPN支持分布式聚合组网中，IPL链路由隧道切换为聚合链路时，根据不同的静态AC生成的动态AC相互冲突
处理建议	删除引发冲突的动态AC对应的静态AC，再重新配置静态AC，并为AC指定合理的报文匹配规则

## 66.13 PROCESS

日志内容	The EVPN global MAC address is a reserved MAC.
参数解释	无
日志等级	7
举例	L2VPN/7/PROCESS: The EVPN global MAC address is a reserved MAC.
日志说明	配置的EVPN全局MAC地址为当前设备的预留MAC地址
处理建议	修改EVPN全局MAC地址

# 67 LAGG

本节介绍 LAGG 模块输出的日志信息。



## 67.1 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 FGE1/0/50 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

## 67.2 LAGG\_AUTO\_AGGREGATION

日志内容	Failed to assign automatic assignment-enabled interface [STRING] to an aggregation group. Please check the configuration on the interface.
参数解释	\$1: 端口名称
日志等级	6
举例	LAGG/6/LAGG_AUTO_AGGREGATON: Failed to assign automatic assignment-enabled interface FGE1/0/1 to an aggregation group. Please check the configuration on the interface.
日志说明	开启自动聚合功能后，由于以下原因导致接口无法加入聚合组： <ul style="list-style-type: none"><li>该接口的属性类配置和聚合接口不同</li><li>该接口上存在不能加入聚合组的配置</li></ul>
处理建议	<ul style="list-style-type: none"><li>修改对应接口上的属性类配置，以保证和聚合接口一致</li><li>删除对应接口上与加入聚合组互斥的功能</li></ul>

## 67.3 LAGG\_INACTIVE\_AICFG

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the port and the aggregate interface had 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 FGE1/0/50 of aggregation group BAGG1 changed to the inactive state, because the port and the aggregate interface had 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

## 67.4 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 FGE1/0/50 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

## 67.5 LAGG\_INACTIVE\_CONFIGURATION

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the link aggregation configuration of the port was 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 FGE1/0/50 of aggregation group BAGG1 changed to the inactive state, because the link aggregation configuration of the port was 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	建议用户检查端口配置的兼容性和正确性

## 67.6 LAGG\_INACTIVE\_DUPLEX

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the duplex mode of the port was different from that of 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 FGE1/0/50 of aggregation group BAGG1 changed to the inactive state, because the duplex mode of the port was different from that of 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

## 67.7 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 prevented it from being Selected.
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 FGE1/0/50 of aggregation group BAGG1 changed to the inactive state, because of the port's hardware restriction prevented it from being Selected.
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	将端口移出聚合组

## 67.8 LAGG\_INACTIVE\_IFCFG\_DEFAULT

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because no LACPDU was received by 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_IFCFG_DEFAULT: Member port FGE1/0/50 of aggregation group BAGG1 changed to the inactive state, because no LACPDU was received by the reference port.
日志说明	由于聚合组内参考端口没有收到对端的LACPDU，该成员端口变为去激活状态
处理建议	检查对端是否发送LACPDU

## 67.9 LAGG\_INACTIVE\_IFCFG\_LOOPPORT

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the reference port received its own LACPDUs.
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_IFCFG_LOOPPORT: Member port FGE1/0/50 of aggregation group BAGG1 changed to the inactive state, because the reference port received its own LACPDUs.
日志说明	由于聚合组内参考端口收到自己的LACPDU，该成员端口变为去激活状态
处理建议	检查设备是否存在环路

## 67.10 LAGG\_INACTIVE\_IFCFG\_NONAGG

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the link of the port was not aggregatable.
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_IFCFG_NONAGG: Member port FGE1/0/50 of aggregation group BAGG1 changed to the inactive state, because the link of the port was not aggregatable.
日志说明	由于聚合组内端口所在链路不可聚合，该成员端口变为去激活状态
处理建议	修改端口配置

## 67.11 LAGG\_INACTIVE\_KEY\_INVALID

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the port's operational key was invalid.
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_KEY_INVALID: Member port FGE1/0/50 of aggregation group BAGG1 changed to the inactive state, because the port's operational key was invalid.
日志说明	由于聚合组内成员端口操作Key无效，该成员端口变为去激活状态
处理建议	重新配置端口，保证配置符合聚合要求

## 67.12 LAGG\_INACTIVE\_LOWER\_LIMIT

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the number of Selected ports was 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 FGE1/0/50 of aggregation group BAGG1 changed to the inactive state, because the number of Selected ports was 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

## 67.13 LAGG\_INACTIVE\_NODEREMOVE

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the card that hosts the port was absent.
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_NODEREMOVE: Member port FGE1/0/50 of aggregation group BAGG1 changed to the inactive state, because the card that hosts the port was absent.
日志说明	由于聚合组内端口所在单板被拔出，该成员端口变为去激活状态
处理建议	检查接口所在板是否已插入

## 67.14 LAGG\_INACTIVE\_OPERSTATE

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the peer port did not have the Synchronization flag.
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_OPERSTATE: Member port FGE1/0/50 of aggregation group BAGG1 changed to the inactive state, because the peer port did not have the Synchronization flag.
日志说明	由于聚合组对端成员端口所在链路未处于同步状态，本端成员端口变为去激活状态
处理建议	检查对端发送的LACPDU

## 67.15 LAGG\_INACTIVE\_PARTNER

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the link aggregation configuration of its peer port was 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 FGE1/0/50 of aggregation group BAGG1 changed to the inactive state, because the link aggregation configuration of its peer port was 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

## 67.16 LAGG\_INACTIVE\_PARTNER\_KEY\_WRONG

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the operational key of the peer port was different from that of 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_PARTNER_KEY_WRONG: Member port FGE1/0/50 of aggregation group BAGG1 changed to the inactive state, because the operational key of the peer port was different from that of the reference port.
日志说明	由于聚合组对端操作Key与参考端口不一致, 本端成员端口变为去激活状态
处理建议	修改对端计算操作Key的参数与参考端口一致

## 67.17 LAGG\_INACTIVE\_PARTNER\_MAC\_WRONG

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the system MAC address of the peer port was different from that of the peer port for 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_PARTNER_MAC_WRONG: Member port FGE1/0/50 of aggregation group BAGG1 changed to the inactive state, because the system MAC address of the peer port was different from that of the peer port for the reference port.
日志说明	由于聚合组对端系统MAC地址与参考端口的对端端口不一致, 本端成员端口变为去激活状态
处理建议	保证两侧聚合系统的系统MAC地址一致

## 67.18 LAGG\_INACTIVE\_PARTNER\_NONAGG

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the link of the peer port was not aggregatable.
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_NONAGG: Member port FGE1/0/50 of aggregation group BAGG1 changed to the inactive state, because the link of the peer port was not aggregatable.
日志说明	由于聚合组内对端端口所在链路不可聚合，本端成员端口变为去激活状态
处理建议	修改对端端口配置

## 67.19 LAGG\_INACTIVE\_PARTNER\_RDIRHANDLE

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because link-aggregation traffic redirection was triggered on the peer 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_PARTNER_RDIRHANDLE: Member port FGE1/0/50 of aggregation group BAGG1 changed to the inactive state, because link-aggregation traffic redirection was triggered on the peer port.
日志说明	由于聚合组对端端口触发聚合重定向功能，本端成员端口变为去激活状态
处理建议	修改对端端口配置

## 67.20 LAGG\_INACTIVE\_PHYSTATE

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the physical or line protocol 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_PHYSTATE: Member port FGE1/0/50 of aggregation group BAGG1 changed to the inactive state, because the physical or line protocol state of the port was 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

## 67.21 LAGG\_INACTIVE\_PORT\_DEFAULT

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the port had not received LACPDU.
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_PORT_DEFAULT: Member port FGE1/0/50 of aggregation group BAGG1 changed to the inactive state, because the port had not received LACPDU.
日志说明	由于聚合组内成员端口未收到LACPDU, 该成员端口变为去激活状态
处理建议	检查对端是否发送LACPDU

## 67.22 LAGG\_INACTIVE\_RDIRHANDLE

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because link-aggregation traffic redirection was triggered on the local 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_RDIRHANDLE: Member port FGE1/0/50 of aggregation group BAGG1 changed to the inactive state, because link-aggregation traffic redirection was triggered on the local port.
日志说明	由于聚合组本端端口触发聚合重定向功能, 该成员端口变为去激活状态
处理建议	修改端口配置

## 67.23 LAGG\_INACTIVE\_REDUNDANCY

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the port was in secondary state in a redundancy group.
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_REDUNDANCY: Member port FGE1/0/50 of aggregation group BAGG1 changed to the inactive state, because the port was in secondary state in a redundancy group.
日志说明	由于聚合组内端口处于冗余备份状态, 该成员端口变为去激活状态
处理建议	冗余组节点中使本端端口处于工作状态



## 67.24 LAGG\_INACTIVE\_RESOURCE\_INSUFICIE

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because hardware resources were not enough.
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 FGE1/0/50 of aggregation group BAGG1 changed to the inactive state, because hardware resources were not enough.
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

## 67.25 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 was different from that of 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_SPEED: Member port FGE1/0/50 of aggregation group BAGG1 changed to the inactive state, because the speed configuration of the port was different from that of the reference port.
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

## 67.26 LAGG\_INACTIVE\_STANDBY

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the port was in Standby 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_INACTIVE_STANDBY: Member port FGE1/0/50 of aggregation group BAGG1 changed to the inactive state, because the port was in Standby state.
日志说明	由于聚合组内端口处于standby状态，该成员端口变为去激活状态
处理建议	等待一段时间再查看成员端口状态，确认是否处于选中状态，如果处于非选中状态，则根据 <b>display link-aggregation troubleshooting</b> 命令定位非选中原因及处理建议

## 67.27 LAGG\_INACTIVE\_UPPER\_LIMIT

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the number of Selected ports had 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 FGE1/0/50 of aggregation group BAGG1 changed to the inactive state, because the number of Selected ports had 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

## 67.28 LAGG\_SELECTPORT\_INCONSISTENT

日志内容	The maximum number of Selected ports for [STRING] on PEXs is inconsistent with that on the parent fabric. Please reconfigure this setting.
参数解释	\$1: 聚合接口编号
日志等级	4
举例	LAGG/4/LAGG_SELECTPORT_INCONSISTENT: The maximum number of Selected ports for Route-Aggregation1 on PEXs is inconsistent with that on the parent fabric. Please reconfigure this setting.
日志说明	PEX设备上聚合组中选中端口数超过了父设备上聚合组的最大选中端口数，需要用户重新配置。触发该日志的原因可能有：以太网接口加入或退出聚合组
处理建议	用户重新配置父设备上聚合组的最大选中端口数或减少PEX设备上聚合组的选中端口，使得父设备与PEX设备的最大选中端口数保持一致

# 68 LDP

本节介绍 LDP 模块输出的日志信息。

## 68.1 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： <b>1.</b> 如果配置了 LDP LSR ID，则 LDP 的 LSR ID 为此命令配置的值 <b>2.</b> 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 <b>display mpls ldp parameter</b> 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

## 68.2 LDP\_SESSION\_CHG

日志内容	Session ([STRING], [STRING]) is [STRING].
参数解释	<p>\$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</p> <p>\$2: VPN实例名。如果该会话属于公网, 显示为public instance</p> <p>\$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</p>
日志等级	5
举例	<p>LDP/5/LDP_SESSION_CHG: Session (22.22.22.2:0, public instance) is up.</p> <p>LDP/5/LDP_SESSION_CHG: Session (22.22.22.2:0, VPN instance: vpn1) is down (hello hold timer expired).</p>
日志说明	会话状态改变了
处理建议	<p>当会话状态是up时, 无</p> <p>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</p> <p>会话失败原因包括:</p> <ul style="list-style-type: none"> <li>• interface not operational: 接口不可用</li> <li>• MPLS disabled on interface: 接口已取消使能 MPLS</li> <li>• LDP disabled on interface: 接口已取消使能 LDP</li> <li>• LDP auto-configure disabled on interface: 接口已取消使能 LDP 自动配置功能</li> <li>• VPN instance changed on interface: 接口所属的 VPN 实例已更改</li> <li>• LDP instance deleted: LDP 实例已删除</li> <li>• 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</li> <li>• L2VPN disabled targeted peer: L2VPN 注销 targeted peer</li> <li>• TE tunnel disabled targeted peer: TE 隧道注销 targeted peer</li> <li>• session protection disabled targeted peer: 会话保护注销 targeted peer</li> <li>• process deactivated: LDP 进程降级</li> <li>• failed to receive the initialization message: 未收到初始化信息</li> <li>• graceful restart reconnect timer expired: 平滑重启重连时间超时</li> <li>• failed to recover adjacency by NSR: NSR 恢复邻接关系失败</li> <li>• failed to upgrade session by NSR: NSR 升级会话失败</li> <li>• closed the GR session: GR 会话关闭</li> <li>• keepalive hold timer expired: keepalive 保持时间超时</li> <li>• adjacency hold timer expired: 邻接关系保持时间超时</li> <li>• session reset manually: 手动重启会话</li> <li>• TCP connection down: TCP 连接断开</li> <li>• received a fatal notification message : 收到致命的通知信息</li> <li>• internal error: 内部错误</li> <li>• memory in critical state: 内存达到 critical 状态</li> <li>• transport address changed on interface: 接口上的传输地址更改</li> </ul>

## 68.3 LDP\_SESSION\_GR

日志内容	Session ([STRING], [STRING]): ([STRING]).
参数解释	<p>\$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</p> <p>\$2: VPN实例名。如果该会话属于公网, 显示为public instance</p> <p>\$3: 会话平滑重启的状态, 取值包括:</p> <ul style="list-style-type: none"><li>Start reconnection: 启动会话重连</li><li>Reconnection failed: 会话重连失败</li><li>Start recovery: 会话重连成功, 进入标签通告恢复过程</li><li>Recovery completed: 会话恢复全过程完成</li></ul>
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

## 68.4 LDP\_SESSION\_SP

日志内容	Session ([STRING], [STRING]): ([STRING]).
参数解释	<p>\$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</p> <p>\$2: VPN实例名。如果该会话属于公网, 显示为public instance</p> <p>\$3: 会话保护状态, 取值包括:</p> <ul style="list-style-type: none"><li>Hold up the session: 保持会话, 等待 Link hello 邻接关系恢复</li><li>Session recovered successfully: Link hello 邻接关系恢复成功</li><li>Session recovery failed: Link hello 邻接关系恢复失败</li></ul>
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

# 69 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。

## 69.1 LIPC\_CHECKDOWN

日志内容	The quality of the link is poor. Owner=[STRING], VRF=[INTEGER], local address/port=[INTEGER]/[INTEGER], remote address/port=[INTEGER]/[INTEGER].
参数解释	\$1: 建立该LIPC链接的进程的名称 \$2: LIPC链接所属的VPN \$3: LIPC链接的四元组信息之本地节点的LIP地址 \$4: LIPC链接的四元组信息之本地节点端口号 \$5: LIPC链接的四元组信息之对端节点的LIP地址 \$6: LIPC链接的四元组信息之对端节点端口号
日志等级	4
举例	LIPC/4/LIPC_CHECKDOWN: The quality of the link is poor. Owner=1, VRF=0, local address/port=0/20415, remote address/port=8/10515.
日志说明	进程在需要进行内部通信时，会自动建立LIPC链接。LIPC STCP模块会自动按周期检测这些LIPC链接的质量。当LIPC链接的质量不佳，输出该日志
处理建议	无，系统会自动尝试修复质量不佳的LIPC链接，如果修复失败，系统会自动关闭该LIPC链接

## 69.2 LIPC\_MTCP\_CHECK

日志内容	Data stays in the receive buffer for an over long time. Owner=[STRING], VRF=[INTEGER], Group=[INTEGER], MID=[INTEGER].
参数解释	\$1: 进程的名称 \$2: LIPC链接所属的VPN \$3: LIPC链接的组播组号 \$4: LIPC链接的组播组的成员ID
日志等级	4
举例	LIPC/4/LIPC_MTCP_CHECK: Data stays in the receive buffer for an over long time. Owner=fsd, VRF=0, Group=134, MID=10001.
日志说明	进程在需要进行内部通信时，会自动建立LIPC链接，LIPC MTCP模块会给进程分配接收缓存区。LIPC MTCP模块会自动按周期检测这些缓冲区是否有数据未被进程收走。如果进程长时间未来“接收缓存区”取数据，则表示数据有积压，进程可能运行异常
处理建议	该日志用于协助开发人员定位，用户无需处理

## 69.3 LIPC\_STCP\_CHECK

日志内容	Data stays in the receive buffer for an over long time. Owner=[STRING], VRF=[INTEGER], local address/port=[INTEGER]/[INTEGER], remote address/port=[INTEGER]/[INTEGER].
参数解释	\$1: 进程的名称 \$2: LIPC链接所属的VPN \$3: LIPC链接的四元组信息之本地节点的LIP地址 \$4: LIPC链接的四元组信息之本地节点端口号 \$5: LIPC链接的四元组信息之对端节点的LIP地址 \$6: LIPC链接的四元组信息之对端节点端口号
日志等级	4
举例	LIPC/4/LIPC_STCP_CHECK: Data stays in the receive buffer for an over long time. Owner=fsd, VRF=0, local address/port=8/10515, remote address/port=0/20415.
日志说明	进程在需要进行内部通信时，会自动建立LIPC链接，LIPC STCP模块会给进程分配接收缓存区。LIPC STCP模块会自动按周期检测这些缓冲区是否有数据未被进程收走。如果进程长时间未来“接收缓存区”取数据，则表示数据有积压，进程可能运行异常
处理建议	该日志用于协助开发人员定位，用户无需处理

## 69.4 LIPC\_SUDP\_CHECK

日志内容	Data stays in the receive buffer for an over long time. Owner=[STRING], VRF=[INTEGER], local address/port=[INTEGER]/[INTEGER], remote address/port=[INTEGER]/[INTEGER].
参数解释	\$1: 进程的名称 \$2: LIPC链接所属的VPN \$3: LIPC链接的四元组信息之本地节点的LIP地址 \$4: LIPC链接的四元组信息之本地节点端口号 \$5: LIPC链接的四元组信息之对端节点的LIP地址 \$6: LIPC链接的四元组信息之对端节点端口号
日志等级	4
举例	LIPC/4/LIPC_SUDP_CHECK: Data stays in the receive buffer for an over long time. Owner=snmpd, VRF=0, local address/port=0/10525, remote address/port=32768/0.
日志说明	进程在需要进行内部通信时，会自动建立LIPC链接，LIPC SUDP模块会给进程分配接收缓存区。LIPC SUDP模块会自动按周期检测这些缓冲区是否有数据未被进程收走。如果进程长时间未来“接收缓存区”取数据，则表示数据有积压，进程可能运行异常
处理建议	该日志用于协助开发人员定位，用户无需处理

## 69.5 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

# 70 LLDP

本节介绍 LLDP 模块输出的日志信息。

## 70.1 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



## 70.2 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

## 70.3 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

## 70.4 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

## 70.5 LLDP\_NEIGHBOR\_PROTECTION\_BLOCK

日志内容	The status of port [STRING] changed to blocked ([STRING]) for the [STRING] agent.
参数解释	\$1: 接口名称 \$2: 接口保护类型，aging或validation \$3: 代理类型
日志等级	4
举例	LLDP/4/LLDP_NEIGHBOR_PROTECTION_BLOCK: -MDC=1; -ifDescr=GigabitEthernet1/0/1; The status of port GigabitEthernet1/0/1 changed to blocked (aging) for the nearest bridge agent.
日志说明	当接口阻塞时，打印本信息，并且说明阻塞原因
处理建议	<ul style="list-style-type: none"><li>当接口保护类型是 aging 时：检查链路状态，或者检查两端 LLDP 的接收和发送状态</li><li>当接口保护类型是 validation 时：检查收到报文的 Chassis ID subtype、Chassis ID 和 Port ID subtype、Port ID 值与配置的邻居识别信息是否一致</li></ul>

## 70.6 LLDP\_NEIGHBOR\_PROTECTION\_DOWN

日志内容	The status of port [STRING] changed to down (aging) for the [STRING] agent.
参数解释	\$1: 接口名称 \$2: 代理类型
日志等级	4
举例	LLDP/4/LLDP_NEIGHBOR_PROTECTION_DOWN: -MDC=1; -ifDescr=GigabitEthernet1/0/1; The status of port GigabitEthernet1/0/1 changed to down (aging) for the nearest bridge agent.
日志说明	当端口接收报文超时关闭端口时，打印本信息，并且说明DOWN原因
处理建议	当接口保护类型是aging时：检查链路状态，或者检查两端LLDP的接收和发送状态

## 70.7 LLDP\_NEIGHBOR\_PROTECTION\_UNBLOCK

日志内容	The status of port [STRING] changed to unblocked for the [STRING] agent.
参数解释	\$1: 接口名称 \$2: 代理类型
日志等级	4
举例	LLDP/4/LLDP_NEIGHBOR_PROTECTION_UNBLOCK: -MDC=1; -ifDescr=GigabitEthernet1/0/1; The status of port GigabitEthernet1/0/1 changed to unblocked for the nearest bridge agent.
日志说明	当接口由阻塞状态转换为非阻塞状态时，打印本信息
处理建议	无

## 70.8 LLDP\_NEIGHBOR\_PROTECTION\_UP

日志内容	The status of port [STRING] changed to up for the [STRING] agent.
参数解释	\$1: 接口名称 \$2: 代理类型
日志等级	4
举例	LLDP/4/LLDP_NEIGHBOR_PROTECTION_UP: -MDC=1; -ifDescr=GigabitEthernet1/0/1; The status of port GigabitEthernet1/0/1 changed to up for the nearest bridge agent.
日志说明	当接口由DOWN状态转换为UP状态时，打印本信息
处理建议	无

## 70.9 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

## 70.10 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

# 71 LOAD

本节介绍 LOAD 模块输出的日志信息。

## 71.1 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

## 71.2 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	<ol style="list-style-type: none"><li>1. 使用 <code>display boot-loader</code> 命令查看单板使用的下次启动软件包</li><li>2. 使用 <code>dir</code> 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</li><li>3. 如果仍不能解决，请联系工程师</li></ol>

## 71.3 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

# 72 LOGIN

本节介绍 LOGIN（登录管理）模块输出的日志信息。

## 72.1 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

## 72.2 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

# 73 LPDT

本节介绍 LPDT 模块输出的日志信息。

## 73.1 LPDT\_LOOPED

日志内容	A loop was detected on [STRING].
参数解释	\$1: 接口名
日志等级	4
举例	LPDT/4/LPDT_LOOPED: A loop was detected on GigabitEthernet1/0/1.
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

## 73.2 LPDT\_RECOVERED

日志内容	All loops were removed on [STRING].
参数解释	\$1: 接口名
日志等级	5
举例	LPDT/5/LPDT_RECOVERED: All loops were removed on GigabitEthernet1/0/1.
日志说明	接口检测到所有VLAN的环路都消除时，环路检测模块会生成该信息
处理建议	无需处理

## 73.3 LPDT\_VLAN\_LOOPED

日志内容	A loop was detected on [STRING] in VLAN [UINT16].
参数解释	\$1: 接口名 \$2: VLAN ID
日志等级	4
举例	LPDT/4/LPDT_VLAN_LOOPED: A loop was detected on GigabitEthernet1/0/1 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

## 73.4 LPDT\_VLAN\_RECOVERED

日志内容	A loop was removed on [STRING] in VLAN [UINT16].
参数解释	\$1: 接口名 \$2: VLAN ID
日志等级	5
举例	LPDT/5/LPDT_VLAN_RECOVERED: A loop was removed on GigabitEthernet1/0/1 in VLAN 1.
日志说明	接口检测到一个VLAN的环路消除时，环路检测模块会生成该信息
处理建议	无需处理

## 73.5 LPDT\_VSI\_LOOPED

日志内容	A loop was detected on VSI [STRING]'s Ethernet service instance srv[UINT8] on [STRING].
参数解释	\$1: VSI名称 \$2: 以太网服务示例编号 \$3: 接口名
日志等级	4
举例	LPDT/4/LPDT_VSI_LOOPED: A loop was detected on VSI 1's Ethernet service instance srv1 on GigabitEthernet1/0/1.
日志说明	接口检测到一个AC口发生环路时，环路检测模块会生成该信息
处理建议	检查该VSI的网络环路

## 73.6 LPDT\_VSI\_RECOVERED

日志内容	All loops were removed from VSI [STRING]'s Ethernet service instance srv[UINT8] on [STRING].
参数解释	\$1: VSI名称 \$2: 以太网服务示例编号 \$3: 接口名
日志等级	5
举例	LPDT/5/LPDT_VSI_RECOVERED: All loops were removed from VSI 1's Ethernet service instance srv1 on GigabitEthernet1/0/1.
日志说明	接口检测到一个AC口所有的环路消除时，环路检测模块会生成该信息
处理建议	无需处理



## 73.7 LPDT\_VSI\_BLOCKFAIL

日志内容	Failed to block [STRING] that hosts VSI [STRING]'s Ethernet service instance srv[UINT8] because of insufficient resources.
参数解释	\$1: 接口名 \$2: VSI名称 \$3: 以太网服务示例编号
日志等级	5
举例	LPDT/5/LPDT_VSI_BLOCKFAIL: Failed to block GigabitEthernet1/0/1 that hosts VSI 1's Ethernet service instance srv1 because of insufficient resources.
日志说明	触发环路检测保护动作后，将端口设置为阻塞失败时生成该信息
处理建议	手工处理产生环路的接口

# 74 LS

本节包含本地服务器日志信息。

## 74.1 LOCALSVR\_PROMPTED\_CHANGE\_PWD

日志内容	Please change the password of [STRING] [STRING], because [STRING].
参数解释	<p><b>\$1:</b> 密码类型</p> <ul style="list-style-type: none"><li>device management user: 设备管理用户</li><li>user line: 用户线</li><li>user line class: 用户线类</li></ul> <p><b>\$2:</b> 用户名/用户线编号/用户线类型</p> <p><b>\$3:</b> 提醒修改密码原因</p> <ul style="list-style-type: none"><li>the current password is a weak-password: 密码是弱密码</li><li>the current password is the default password: 密码是缺省密码</li><li>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</li><li>the password had expired: 密码已经老化</li></ul>
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： <ul style="list-style-type: none"><li>认证方式为 scheme 时，请修改用户的本地密码</li><li>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</li></ul>

## 74.2 LS\_ADD\_USER\_TO\_GROUP

日志内容	Admin [STRING] added user [STRING] to group [STRING].
参数解释	<p><b>\$1:</b> 管理员名</p> <p><b>\$2:</b> 用户名</p> <p><b>\$3:</b> 用户组名</p>
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

## 74.3 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 <ul style="list-style-type: none"><li>• 用户没有找到</li><li>• 密码认证失败</li><li>• 用户未上线</li><li>• 接入类型不匹配</li><li>• 绑定属性失败</li><li>• 用户在黑名单</li></ul>
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

## 74.4 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

## 74.5 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

## 74.6 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

## 74.7 LS\_PWD\_ADDBLACKLIST

日志内容	User [STRING] at [STRING] was added to the blacklist due to multiple login failures, [STRING].
参数解释	\$1: 用户名 \$2: IP地址 \$3: 结果 <ul style="list-style-type: none"><li>但是可以做其他的尝试</li><li>被永久阻塞</li><li>被临时阻塞指定时间（单位：分钟）</li></ul>
日志等级	4
举例	LS/4/LS_PWD_ADDBLACKLIST: user1 at 192.168.0.22 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

## 74.8 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

## 74.9 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

## 74.10 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

## 74.11 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

## 74.12 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

## 74.13 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

## 74.14 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	<p>\$1: 管理员名 \$2: IP地址 \$3: 用户名 \$4: 失败原因</p> <ul style="list-style-type: none"><li>• old password is incorrect: 旧密码不正确</li><li>• password is too short: 新密码太短</li><li>• 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）</li><li>• 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）</li><li>• password has repeated chars: 密码中包含连续三个或以上的相同字符</li><li>• password contains username: 密码中包含用户名</li><li>• 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）</li><li>• password is in update-wait time: 密码仍在等待更新的时间内</li></ul>
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

## 74.15 LS\_PWD\_MODIFY\_SUCCESS

日志内容	Admin [STRING] from [STRING] modify the password for user [STRING] successfully.
参数解释	<p>\$1: 管理员名 \$2: IP地址 \$3: 用户名</p>
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

## 74.16 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

## 74.17 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

## 74.18 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



## 74.19 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

## 74.20 LS\_USER\_ROLE\_CHANGE

日志内容	Admin [STRING] [STRING] the user role [STRING] for [STRING].
参数解释	\$1: 管理员名 \$2: 添加/删除 \$3: 用户角色 \$4: 用户名
日志等级	4
举例	LS/4/LS_USER_ROLE_CHANGE: Admin admin add user role network-admin for user abcd.
日志说明	管理员修改了用户的用户角色
处理建议	无

# 75 LSPV

本节介绍 LSP 验证模块输出的日志信息。

## 75.1 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

# 76 MAC

本节介绍 MAC 模块输出的日志信息。

## 76.1 MAC\_DRIVER\_ADD\_ENTRY

日志内容	Driver failed to add MAC address entry: MAC address=[STRING], VLAN=[UINT32], State=[UINT32], interface=[STRING].
参数解释	\$1: MAC地址 \$2: VLAN ID \$3: 表项类型编号 \$4: 端口名称
日志等级	4
举例	MAC/4/MAC_DRIVER_ADD_ENTRY: Driver failed to add MAC address entry: MAC address=1-1-1, VLAN=1, State=2, interface=GigabitEthernet1/0/1.
日志说明	在接口GigabitEthernet1/0/1上添加OpenFlow类型MAC地址失败，MAC地址为1-1-1，所属VLAN为VLAN 1
处理建议	无

## 76.2 MAC\_PROTOCOLPKT\_NORES\_GLOBAL

日志内容	The card does not have enough hardware resources to send protocol packets destined for [STRING] to the CPU for [STRING],
参数解释	\$1: MAC地址 \$2: 协议类型
日志等级	5
举例	MAC/5/MAC_PROTOCOLPKT_NORES_GLOBAL: The card does not have enough hardware resources to send protocol packets destined for 0180-C200-000e to the CPU for LLDP.
日志说明	单板硬件资源不足导致协议报文上送CPU失败
处理建议	无

## 76.3 MAC\_PROTOCOLPKT\_NORES\_PORT

日志内容	The card does not have enough hardware resources to send protocol packets destined for [STRING] to the CPU for [STRING] on [STRING].
参数解释	\$1: MAC地址 \$2: 协议类型 \$3: 接口名称
日志等级	5
举例	MAC/5/MAC_PROTOCOLPKT_NORES_PORT: The card does not have enough hardware resources to send protocol packets destined for 0180-C200-000e to the CPU for LLDP on GigabitEthernet2/0/32.
日志说明	单板硬件资源不足导致接口上的协议报文上送CPU失败
处理建议	无

## 76.4 MAC\_PROTOCOLPKT\_NORES\_VLAN

日志内容	The card does not have enough hardware resources to send protocol packets destined for [STRING] to the CPU for [STRING] in VLAN [UINT16].
参数解释	\$1: MAC地址 \$3: 协议类型 \$3: VLAN ID
日志等级	5
举例	MAC/5/MAC_PROTOCOLPKT_NORES_VLAN: The card does not have enough hardware resources to send protocol packets destined for 0180-C200-000e to the CPU for LLDP in VLAN 100.
日志说明	单板硬件资源不足导致VLAN内的协议报文上送CPU失败
处理建议	无

## 76.5 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

## 76.6 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

## 76.7 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

## 76.8 MAC\_VLAN\_LEARNLIMIT\_NORESOURCE

日志内容	The card does not have enough hardware resources to set MAC learning limit for VLAN [UINT16].
参数解释	\$1: VLAN ID
日志等级	5
举例	MAC/5/MAC_VLAN_LEARNLIMIT_NORESOURCE: The card does not have enough hardware resources to set MAC learning limit for VLAN 100.
日志说明	单板硬件资源不足导致无法配置VLAN内允许学习的最大MAC地址数量
处理建议	无

## 76.9 MAC\_VLAN\_LEARNLIMIT\_NOTSUPPORT

日志内容	The card does not support setting MAC learning limit for VLAN [UINT16].
参数解释	\$1: VLAN ID
日志等级	5
举例	MAC/5/ MAC_VLAN_LEARNLIMIT_NOTSUPPORT: The card does not support setting MAC learning limit for VLAN 100.
日志说明	单板不支持配置VLAN内允许学习的最大MAC地址数量
处理建议	无

# 77 MACA

本节介绍 MAC 地址认证模块输出的日志信息。

## 77.1 MACA\_ENABLE\_NOT\_EFFECTIVE

日志内容	MAC authentication is enabled but is not effective on interface [STRING].
参数解释	\$1: 接口名
日志等级	3
举例	MACA/3/MACA_ENABLE_NOT_EFFECTIVE: MAC authentication is enabled but is not effective on interface Ethernet3/1/2.
日志说明	MAC地址认证配置在接口上不生效，因为该接口不支持MAC地址认证
处理建议	关闭接口上的MAC地址认证

## 77.2 MACA\_LOGIN\_FAILURE

日志内容	-IfName=[STRING]-MACAddr=[STRING]-VLANID=[STRING]-Username=[STRING]-UsernameFormat=[STRING]; User failed MAC authentication. Reason: [STRING].
参数解释	<p>\$1: 接口名 \$2: MAC地址 \$3: VLAN ID \$4: 用户名 \$5: 用户名格式 \$6: 失败原因</p> <ul style="list-style-type: none"><li>• MAC address authorization failed: 授权 MAC 地址失败</li><li>• VLAN authorization failed: 授权 VLAN 失败</li><li>• VSI authorization failed: 授权 VSI 失败</li><li>• ACL authorization failed: 授权 ACL 失败</li><li>• User profile authorization failed: 授权 User Profile 失败</li><li>• URL authorization failed: 授权 URL 失败</li><li>• Microsegment authorization failed: 授权微分段失败</li><li>• Authentication process failed: 认证失败</li></ul>
日志等级	6
举例	MACA/6/MACA_LOGIN_FAILURE: -IfName=GigabitEthernet1/0/1-MACAddr=0000-0000-0001-VLANID=1-Username=0000-0000-0001-UsernameFormat=MAC address; User failed MAC authentication. Reason: VLAN authorization failed.
日志说明	用户MAC地址认证失败
处理建议	查看失败原因并修改相关配置

## 77.3 MACA\_LOGIN\_FAILURE (EAD)

日志内容	-IfName=[STRING]-MACAddr=[STRING]-VLANID=[STRING]-Username=[STRING]-UsernameFormat=[STRING]; User failed MAC authentication. Reason: [STRING]. Can't trigger MAC authentication for the user before the EAD user entry ages out.
参数解释	<p>\$1: 接口名            \$2: MAC地址            \$3: VLAN ID            \$4: 用户名            \$5: 用户名格式            \$6: 失败原因</p> <ul style="list-style-type: none"> <li>• MAC address authorization failed: 授权 MAC 地址失败</li> <li>• VLAN authorization failed: 授权 VLAN 失败</li> <li>• VSI authorization failed: 授权 VSI 失败</li> <li>• ACL authorization failed: 授权 ACL 失败</li> <li>• User profile authorization failed: 授权 User Profile 失败</li> <li>• URL authorization failed: 授权 URL 失败</li> <li>• Authentication process failed: 认证失败</li> </ul>
日志等级	6
举例	MACA/6/MACA_LOGIN_FAILURE: -IfName=GigabitEthernet1/0/1-MACAddr=0000-0000-0001-VLANID=1-Username=0000-0000-0001-UsernameFormat=MAC address; User failed MAC authentication. Reason: VLAN authorization failed. Can't trigger MAC authentication for the user before the EAD user entry ages out.
日志说明	用户MAC地址认证失败，在EAD表项老化之前，用户无法再次触发MAC地址认证
处理建议	查看失败原因并修改相关配置；关闭EAD快速部署功能或删除当前接口上的802.1X配置

## 77.4 MACA\_LOGIN\_SUCC

日志内容	-IfName=[STRING]-MACAddr=[STRING]-AccessVLANID=[STRING]-AuthorizationVLANID=[STRING]-Username=[STRING]-UsernameFormat=[STRING]; User passed MAC authentication and came online.
参数解释	\$1: 接口名 \$2: MAC地址 \$3: 接入VLAN ID \$4: 授权VLAN ID \$5: 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=0010-8400-22b9-AccessVLANID=444-AuthorizationVLANID=444-Username=00-10-84-00-22-b9-UsernameFormat=MAC address; User passed MAC authentication and came online.
日志说明	MAC地址认证成功
处理建议	无

## 77.5 MACA\_LOGIN\_SUCC (in open mode)

日志内容	-IfName=[STRING]-MACAddr=[STRING]-VLANID=[STRING]-Username=[STRING]-UsernameFormat=[STRING]; The user that failed MAC authentication passed open authentication and came online.
参数解释	\$1: 接口名 \$2: MAC地址 \$3: VLAN ID \$4: 用户名 \$5: 用户名格式
日志等级	6
举例	MACA/6/MACA_LOGIN_SUCC:-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9-VLANID=444-Username=00-10-84-00-22-b9-UsernameFormat=MAC address; The user that failed MAC authentication passed open authentication and came online.
日志说明	MAC地址认证失败但通过开放认证模式成功上线
处理建议	无



## 77.6 MACA\_LOGOFF

日志内容	-IfName=[STRING]-MACAddr=[STRING]-VLANID=[STRING]-Username=[STRING]-UsernameFormat=[STRING]; MAC authentication user was logged off.
参数解释	\$1: 接口名 \$2: MAC地址 \$3: VLAN ID \$4: 用户名 \$5: 用户名格式
日志等级	6
举例	MACA/6/MACA_LOGOFF:-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9-VLANID=444-Username=00-10-84-00-22-b9-UsernameFormat=MAC address; MAC authentication user was logged off.
日志说明	MAC地址认证用户下线
处理建议	查看下线原因或进行后续操作

## 77.7 MACA\_LOGOFF (in open mode)

日志内容	-IfName=[STRING]-MACAddr=[STRING]-VLANID=[STRING]-Username=[STRING]-UsernameFormat=[STRING]; MAC authentication open user was logged off.
参数解释	\$1: 接口名 \$2: MAC地址 \$3: VLAN ID \$4: 用户名 \$5: 用户名格式
日志等级	6
举例	MACA/6/MACA_LOGOFF:-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9-VLANID=444-Username=00-10-84-00-22-b9-UsernameFormat=MAC address; MAC authentication open user was logged off.
日志说明	MAC地址认证open用户下线
处理建议	查看下线原因或进行后续操作

# 78 MACSEC

本节介绍 MAC Security 模块输出的日志信息。

## 78.1 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

## 78.2 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

## 78.3 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

## 78.4 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

## 78.5 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： <ul style="list-style-type: none"><li>• MKA 会话由明文通信切换为密文通信</li><li>• 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</li></ul>
处理建议	无

## 78.6 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： <ul style="list-style-type: none"><li>• 使能 MKA 功能后，有新的可用 CAK</li><li>• 用户重建 MKA 会话</li><li>• 协商会话失败的接口收到新的 MKA 报文</li></ul>
处理建议	无

## 78.7 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： <ul style="list-style-type: none"><li>• 用户删除或重建了接口的 MKA 会话</li><li>• MKA 会话所在链路故障</li></ul>
处理建议	使用 <b>display mka session</b> 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

## 78.8 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： <ul style="list-style-type: none"><li>• MKA 会话由密文通信切换为明文通信</li><li>• 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</li></ul>
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

# 79 MBFD

本节介绍 MPLS BFD 模块输出的日志信息。

## 79.1 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

# 80 MBUF

本节介绍 MBUF 模块输出的日志信息。

## 80.1 MBUF\_DATA\_BLOCK\_CREATE\_FAIL

日志内容	Failed to create an MBUF data block because of insufficient memory. Failure count: [UINT32].
参数解释	\$1: 失败次数
日志等级	2
举例	MBUF/2/MBUF_DATA_BLOCK_CREATE_FAIL: Failed to create an MBUF data block because of insufficient memory. Failure count: 128.
日志说明	当申请MBUF数据块失败时，输出该日志。为避免该日志输出过于频繁，本次申请MBUF数据块失败距上次申请MBUF数据块失败间隔大于等于一分钟时，才会输出该日志
处理建议	<ol style="list-style-type: none"><li>4. 在 Probe 视图下执行 <code>display system internal kernel memory pool   include mbuf</code> 命令查询已申请的 MBUF 数据块的数量</li><li>5. 在系统视图下执行 <code>display memory</code> 命令查询系统内存总量</li><li>6. 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</li></ol> <ul style="list-style-type: none"><li>• 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</li><li>• 如果是，则继续通过 Probe 视图下的 <code>display system internal mbuf socket statistics</code> 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<ul style="list-style-type: none"><li>◦ 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</li><li>◦ 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</li></ul></li></ul>

# 81 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。

## 81.1 MDC\_CREATE

日志内容	MDC [UINT16] was created.
参数解释	\$1: MDC的编号
日志等级	5
举例	MDC/5/MDC_CREATE: MDC 2 was created.
日志说明	MDC成功创建
处理建议	无

## 81.2 MDC\_CREATE\_ERR

日志内容	Failed to create MDC [UINT16] for insufficient resources.
参数解释	\$1: MDC的编号
日志等级	5
举例	MDC/5/MDC_CREATE_ERR: -Slot=1; Failed to create MDC 2 for insufficient resources.
日志说明	备用主控板启动时会从主用主控板获取所有已创建的MDC的信息，并在备用主控板创建同样的MDC。如果备用主控板因为资源限制无法创建该MDC，则输出此日志信息。MDC进驻备用主控板失败，无法在该备用主控板上提供服务
处理建议	<ol style="list-style-type: none"><li>1. 使用 <code>display mdc resource</code> 命令查询新插入的备用主控板的 CPU、内存空间和磁盘空间</li><li>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</li><li>3. 使用 <code>undo mdc</code> 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</li></ol>

## 81.3 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

## 81.4 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: 取值为MDC或Context \$2: MDC或Context的编号 \$3: 内核事件的阶段 \$4: 内核事件阶段对应的函数的地址 \$5: 所用时间
日志等级	4
举例	MDC/4/MDC_KERNEL_EVENT_TOOLONG: -slot=1; MDC 2 kernel event in sequence 0x4fe5 function 0xff245e failed to finish within 15 minutes.
日志说明	某内核事件在长时间内未完成
处理建议	<ol style="list-style-type: none"><li>1. 重启单板，尝试恢复</li><li>2. 联系工程师分析解决</li></ol>

## 81.5 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

## 81.6 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



## 81.7 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

## 81.8 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

## 81.9 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

## 81.10 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: <ul style="list-style-type: none"><li>o updating 表示正在给 MDC 分配接口板, 即对 MDC 执行 location 命令</li><li>o stopping 表示 MDC 正在停止, 即 MDC 正在执行 undo mdc start 命令</li><li>o inactive 表示 MDC 处于未启动状态</li><li>o starting 表示 MDC 正在启动中, 即对 MDC 正在执行 mdc start 命令</li><li>o active 表示 MDC 正常运行</li></ul>
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

# 82 MFIB

本节介绍组播转发模块输出的日志信息。

## 82.1 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

## 82.2 MFIB\_MTI\_NO\_ENOUGH\_RESOURCE

日志内容	Failed to create [STRING] because of insufficient resources.
参数解释	\$1: MTunnel名称
日志等级	5
举例	MFIB/5/MFIB_MTI_NO_ENOUGH_RESOURCE: Failed to create MTunnel129 because of insufficient resources.
日志说明	组播隧道资源不足导致隧道创建失败
处理建议	无

# 83 MGROUP

本节主要介绍与镜像组相关的日志消息。

## 83.1 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

## 83.2 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

## 83.3 MGROUP\_RESTORE\_GROUP\_FAIL

日志内容	Failed to restore configuration for mirroring group [UINT16], because [STRING]
参数解释	\$1: 镜像组编号 \$2: 恢复镜像组配置失败的原因 <ul style="list-style-type: none"><li>monitor resources are insufficient: 镜像资源不足</li></ul>
日志等级	3
举例	MGROUP/3/MGROUP_RESTORE_GROUP_FAIL: Failed to restore configuration for mirroring group 1, because monitor resources are insufficient.
日志说明	设备启动后，因为镜像资源不足，导致镜像组的配置恢复失败
处理建议	流镜像和端口镜像使用相同的镜像资源。当设备整机重启时，优先恢复流镜像配置，再恢复端口镜像配置。请删除不需要的镜像配置释放资源，然后重新配置恢复失败的镜像组

## 83.4 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

## 83.5 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

# 84 MOD

本节介绍 MOD 模块输出的日志信息。

## 84.1 MOD\_ENABLE\_FAIL

日志内容	Failed to enable MOD Function. Reason: [STRING]
参数解释	<b>\$1:</b> 失败原因 <ul style="list-style-type: none"><li>○ The sampling function is not supported.: 采样功能不支持</li><li>○ The sampler has been used by another function.: 采样器被其他功能引用</li></ul>
日志等级	4
举例	MOD/4/MOD_ENABLE_FAIL: Failed to enable MOD function. Reason: The sampling function is not supported.
日志说明	开启MOD功能失败
处理建议	关闭MOD的采样功能

## 84.2 MOD\_MODIFY\_FAIL

日志内容	Failed to modify MOD parameters. Reason: [STRING]
参数解释	<b>\$1:</b> 失败原因 <ul style="list-style-type: none"><li>○ The sampling function is not supported.: 采样功能不支持</li><li>○ The sampler has been used by another function.: 采样器被其他功能引用</li></ul>
日志等级	4
举例	MOD/4/MOD_MODIFY_FAIL: Failed to modify MOD parameters. Reason: The sampling function is not supported.
日志说明	修改MOD参数失败
处理建议	关闭MOD的采样功能

# 85 MPLS

本节介绍 MPLS 模块输出的日志信息。

## 85.1 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

## 85.2 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

# 86 MTLK

本节介绍 Monitor Link 模块输出的日志信息。

## 86.1 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 <ul style="list-style-type: none"><li>○ down: 故障</li><li>○ up: 正常</li></ul>
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

# 87 NAT

本节介绍 NAT 模块输出的日志信息。

## 87.1 NAT\_ADDR\_BIND\_CONFLICT

日志内容	Failed to activate NAT configuration on interface [STRING], because global IP addresses already bound to another service card.
参数解释	\$1: 接口名称
日志等级	4
举例	NAT/4/NAT_ADDR_BIND_CONFLICT: Failed to activate NAT configuration on interface Ethernet0/0/2, because global IP addresses already bound to another service card.
日志说明	配置中的外网地址绑定指定业务板时发现其已经绑定到其他业务板上，则触发该日志
处理建议	如果有多个接口引用了相同的外网地址，则这些接口必须指定同一块业务板进行NAT处理。请使用 <b>display nat all</b> 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



## 87.2 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

## 87.3 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	<ul style="list-style-type: none"><li>• 对于硬件资源不足情况，请联系技术支持</li><li>• 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</li></ul>

## 87.4 NAT\_FLOW

日志内容	<pre>Protocol(1001)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];NATSrcIPAddr(1005)=[IPADDR];NATSrcPort(1006)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];NATDstIPAddr(1009)=[IPADDR];NATDstPort(1010)=[UINT16];InitPktCount(1044)=[UINT32];InitByteCount(1046)=[UINT32];RplyPktCount(1045)=[UINT32];RplyByteCount(1047)=[UINT32];RcvVPNInstance(1042)=[STRING];SndVPNInstance(1043)=[STRING];RcvDSLiteTunnelPeer(1040)=[STRING];SndDSLiteTunnelPeer(1041)=[STRING];BeginTime_e(1013)=[STRING];EndTime_e(1014)=[STRING];Event(1048)=[UNIT16][STRING];</pre>
参数解释	<p>\$1: 协议类型</p> <p>\$2: 源IP地址</p> <p>\$3: 源端口号</p> <p>\$4: 转换后的源IP地址</p> <p>\$5: 转换后的源端口号</p> <p>\$6: 目的IP地址</p> <p>\$7: 目的端口号</p> <p>\$8: 转换后的目的IP地址</p> <p>\$9: 转换后的目的端口号</p> <p>\$10: 入方向的报文总数</p> <p>\$11: 入方向的字节总数</p> <p>\$12: 出方向的报文总数</p> <p>\$13: 出方向的字节总数</p> <p>\$14: 源VPN名称</p> <p>\$15: 目的VPN名称</p> <p>\$16: 源DS-Lite Tunnel</p> <p>\$17: 目的DS-Lite Tunnel</p> <p>\$18: 创建会话的时间</p> <p>\$19: 会话删除时间</p> <p>\$20: 日志类型</p> <p>\$21: 日志类型描述信息, 包括:</p> <ul style="list-style-type: none"> <li>• Session created: NAT 会话创建日志</li> <li>• Active flow threshold: 流量或时间阈值日志</li> <li>• Normal over: 正常流结束, 会话删除日志</li> <li>• Aged for timeout: 会话老化删除日志</li> <li>• Aged for reset or config-change: 通过配置删除会话日志</li> <li>• Other: 其他原因删除会话日志, 如由其他模块删除</li> </ul>
日志等级	6
举例	<pre>NAT/6/NAT_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;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;</pre>

日志内容	Protocol(1001)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];NATSrcIPAddr(1005)=[IPADDR];NATSrcPort(1006)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];NATDstIPAddr(1009)=[IPADDR];NATDstPort(1010)=[UINT16];InitPktCount(1044)=[UINT32];InitByteCount(1046)=[UINT32];RplyPktCount(1045)=[UINT32];RplyByteCount(1047)=[UINT32];RcvVPNInstance(1042)=[STRING];SndVPNInstance(1043)=[STRING];RcvDSLiteTunnelPeer(1040)=[STRING];SndDSLiteTunnelPeer(1041)=[STRING];BeginTime_e(1013)=[STRING];EndTime_e(1014)=[STRING];Event(1048)=[UINT16][STRING];
日志说明	<ul style="list-style-type: none"> <li>• 创建、删除 NAT 会话时会发送该日志</li> <li>• NAT 会话过程中会定时发送该日志</li> <li>• NAT 会话的流量或时间达到指定的阈值时会发送该日志</li> </ul>
处理建议	无

## 87.5 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

## 87.6 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 <ul style="list-style-type: none"><li>NAT addresses already bound to another service card: NAT 地址已经绑定到其他业务板</li><li>NAT service is not supported on this service card: 指定业务板不支持 NAT 业务</li><li>the hardware resources are not enough: 硬件资源不足</li><li>unknown error: 未知错误</li></ul> 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 <ul style="list-style-type: none"><li>NAT addresses already bound to another service card: NAT 地址已经绑定到其他业务板</li><li>NAT service is not supported on this service card: 指定业务板不支持 NAT 业务</li><li>the hardware resources are not enough: 硬件资源不足</li><li>unknown error: 未知错误</li></ul>
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	<ul style="list-style-type: none"><li>如果提示 NAT 地址已经绑定到其他业务板，则使用 <code>display nat all</code> 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</li><li>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</li></ul>

# 88 ND

本节介绍 ND 模块输出的日志信息。

## 88.1 ND\_COMMONPROXY\_ENABLE\_FAILED

日志内容	Failed to enable common ND proxy on interface [STRING].
参数解释	\$1: 接口名称
日志等级	4
举例	ND/4/ND_COMMONPROXY_ENABLE_FAILED: -MDC=1-Slot=2; Failed to enable common ND proxy on interface Vlan-interface 1.
日志说明	接口下开启普通ND代理失败。如果非主控板的接口下开启普通ND代理失败，则在对应的接口板上打印该日志信息
处理建议	<ul style="list-style-type: none"><li>• 检查设备相应单板是否支持本功能</li><li>• 确认设备的硬件资源是否充足</li></ul>

## 88.2 ND\_CONFLICT

日志内容	[STRING] is inconsistent.
参数解释	\$1: 配置类型 <ul style="list-style-type: none"><li>• M_FLAG: 被管理地址配置标志位</li><li>• O_FLAG: 其他信息配置标志位</li><li>• CUR_HOP_LIMIT: 跳数限制</li><li>• REACHABLE TIME: 保持邻居可达状态的时间</li><li>• NS INTERVAL: 邻居请求消息间隔</li><li>• MTU: 发布链路的 MTU</li><li>• PREFIX VALID TIME: 前缀的有效存活时间</li><li>• PREFIX PREFERRED TIME: 前缀用于无状态地址配置的优选项的存活时间</li></ul>
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

## 88.3 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

## 88.4 ND\_ENTRY\_ENOUGHRESOURCE

日志内容	Issued the software entry to the driver for IPv6 address [STRING] on VPN instance [STRING]. Issued the software entry to the driver for IPv6 address [STRING] on the public network.
参数解释	\$1: IPv6地址 \$2: VPN实例名。如果该ND属于公网，该字段不显示
日志等级	6
举例	ND/6/ND_ENTRY_ENOUGHRESOURCE: Issued the software entry to the driver for IPv6 address 10::1 on VPN instance vpn_1. ND/6/ND_ENTRY_ENOUGHRESOURCE: Issued the software entry to the driver for IPv6 address 10::2 on the public network.
日志说明	使用 <b>ipv6 nd consistency-check enable</b> 命令开启ND表项一致性检查功能后，如果ND重刷硬件表项成功，则输出此日志
处理建议	无

## 88.5 ND\_ENTRY\_INCONSISTENT

日志内容	Inconsistent software and hardware ND entries for IPv6 address [STRING] on VPN instance [STRING]. Inconsistent parameters: [STRING]. Inconsistent software and hardware ND entries for IPv6 address [STRING] on the public network. Inconsistent parameters: [STRING].
参数解释	\$1: IPv6地址 \$2: VPN实例名。如果该ND属于公网，该字段不显示 \$3: 不一致的表项参数类型 <ul style="list-style-type: none"> <li>○ MAC address: MAC 地址</li> <li>○ output interface: ND 表项的出接口</li> <li>○ output port : ND 表项的出端口</li> <li>○ outermost layer VLAN ID: 第一层 VLAN 标签</li> <li>○ second outermost layer VLAN ID: 第二层 VLAN 标签</li> <li>○ VSI index: VSI 索引</li> <li>○ link ID: VSI 出链路标识符</li> </ul>
日志等级	6
举例	ND/6/ND_ENTRY_INCONSISTENT: Inconsistent software and hardware ND entries for IPv6 address 10::1 on VPN instance vpn_1. Inconsistent parameters: MAC address, output port, VSI index, and link ID. ND/6/ND_ENTRY_INCONSISTENT: Inconsistent software and hardware ND entries for IPv6 address 10::2 on the public network. Inconsistent parameters: MAC address, output port, VSI index, and link ID.
日志说明	使用 <b>ipv6 nd consistency-check enable</b> 命令开启ND表项一致性检查功能后，如果设备检测到ND软件表项与硬件表项不一致（比如ND表项的出接口），则输出本日志
处理建议	不需要处理，ND会主动根据ND软件表项刷新驱动硬件表项

## 88.6 ND\_ENTRY\_NORESOURCE

日志内容	Not enough hardware resources to issue the software entry to the driver for IPv6 address [STRING] on VPN instance [STRING]. Not enough hardware resources to issue the software entry to the driver for IPv6 address [STRING] on the public network.
参数解释	\$1: IPv6地址 \$2: VPN实例名。如果该ND属于公网，该字段不显示
日志等级	6
举例	ND/6/ND_ENTRY_NORESOURCE: Not enough hardware resources to issue the software entry to the driver for IPv6 address 10::1 on VPN instance vpn_1. ND/6/ND_ENTRY_NORESOURCE: Not enough hardware resources to issue the software entry to the driver for IPv6 address 10::2 on the public network.
日志说明	使用 <b>ipv6 nd consistency-check enable</b> 命令开启ND表项一致性检查功能后，当ND软件表项下发驱动时，驱动没有足够的ND硬件表项资源，则输出此日志
处理建议	不需要处理，ND会主动根据ND软件表项刷新驱动硬件表项

## 88.7 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

## 88.8 ND\_LOCALPROXY\_ENABLE\_FAILED

日志内容	Failed to enable local ND proxy on interface [STRING].
参数解释	\$1: 接口名称
日志等级	4
举例	ND/4/ND_LOCALPROXY_ENABLE_FAILED: -MDC=1-Slot=2; Failed to enable local ND proxy on interface Vlan-interface 1.
日志说明	接口下开启本地ND代理失败。如果非主控板的接口下开启本地ND代理失败，则在对应的接口板上打印该日志信息
处理建议	<ul style="list-style-type: none"><li>• 检查设备相应单板是否支持本功能</li><li>• 确认设备的硬件资源是否充足</li></ul>



## 88.9 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 0002-0002-0001 was inconsistent with link-layer address 0002-0002-0002.
日志说明	<b>ipv6 nd mac-check enable</b> 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 <b>ipv6 nd check log enable</b> 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

## 88.10 ND\_NETWORKROUTE\_DUPLICATE

日志内容	Prefix [STRING] of the IPv6 ND network route matches different ports: [STRING] and [STRING].
参数解释	\$1: IPv6地址前缀 \$2: 接口名称 \$3: 接口名称
日志等级	5
举例	ND/5/ND_NETWORKROUTE_DUPLICATE: Prefix 120::/70 of the IPv6 ND network route matches different ports: GigabitEthernet1/0/1 and GigabitEthernet1/0/2.
日志说明	使用 <b>ipv6 nd route-direct prefix convert-length</b> 命令配置匹配指定IPv6前缀的ND表项生成网段路由的前缀长度后，如果根据不同的ND表项（与邻居相连的二层端口不同、但是与邻居相连的接口所属的VLAN相同）生成相同的网段路由，则输出本日志
处理建议	检查网络配置，根据实际需求修改网络配置

## 88.11 ND\_RAGUARD\_DROP

日志内容	Dropped RA messages with the source IPv6 address [STRING] on interface [STRING]. [STRING] messages dropped in total on the interface.
参数解释	\$1: 被丢弃报文的源IPv6地址 \$2: 丢弃报文的端口名 \$3: 该端口已丢弃的报文总数
日志等级	4
举例	ND/4/ND_RAGUARD_DROP: Dropped RA messages with the source IPv6 address FE80::20 on interface GigabitEthernet1/0/1. 20 RA messages dropped in total on the interface.
日志说明	RA Guard检测到攻击，丢弃相应的报文并提示日志信息
处理建议	检查报文源是否合法

## 88.12 ND\_RATE\_EXCEEDED

日志内容	The ND packet rate ([UINT32] pps) exceeded the rate limit ([UINT32] pps) on interface [STRING] in most recent [UINT32] seconds.
参数解释	\$1: ND报文速率 \$2: ND报文限速速率 \$3: 接口名称 \$4: 间隔时间
日志等级	4
举例	ND/4/ND_RATE_EXCEEDED: The ND packet rate (100 pps) exceeded the rate limit (80 pps) on interface GigabitEthernet1/0/1 in most recent 10 seconds.
日志说明	在此前的一段时间内，接口接收ND报文速率超过了接口的ND报文限速值
处理建议	检查发送ND报文的主机是否合法

## 88.13 ND\_RATELIMIT\_NOTSUPPORT

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

## 88.14 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

## 88.15 ND\_SET\_VLAN\_REDIRECT\_NORESOURCE

日志内容	Not enough resources to complete the operation.
参数解释	无
日志等级	6
举例	ND/6/ND_VLAN_REDIRECT_NORESOURCE: Not enough resources to complete the operation.
日志说明	下发VLAN规则失败，原因是驱动资源不足
处理建议	释放设备驱动资源，重新下发

## 88.16 ND\_SNOOPING\_LEARN\_ALARM

日志内容	The total number of ND snooping entries learned in all VLANs reached or exceeded the alarm threshold.
参数解释	无
日志等级	4
举例	ND/4/ND_SNOOPING_LEARN_ALARM: -MDC=1; The total number of ND snooping entries learned in all VLANs reached or exceeded the alarm threshold.
日志说明	所有VLAN学习的总的ND Snooping表项数达到或超过告警阈值
处理建议	检查是否有ND攻击

## 88.17 ND\_SNOOPING\_LEARN\_ALARM\_RECOVER

日志内容	The total number of ND snooping entries learned in all VLANs dropped below the alarm threshold.
参数解释	无
日志等级	4
举例	ND/4/ND_SNOOPING_LEARN_ALARM_RECOVER: -MDC=1; The total number of ND snooping entries learned in all VLANs dropped below the alarm threshold.
日志说明	所有VLAN学习的总的ND Snooping表项数降低到告警阈值以下
处理建议	无

## 88.18 ND\_USER\_DUPLICATE\_IPV6ADDR

日志内容	Detected a user IPv6 address conflict. New user (MAC [STRING], SVLAN [STRING], CVLAN [STRING]) on interface [STRING] and old user (MAC [STRING], SVLAN [STRING], CVLAN [STRING]) on interface [STRING] were using the same IPv6 address [IPV6ADDR].
参数解释	\$1: 新用户的MAC地址 \$2: 新用户所在的外层VLAN \$3: 新用户所在的内层VLAN \$4: 连接新用户的接口名称 \$5: 旧用户的MAC地址 \$6: 旧用户所在的外层VLAN \$7: 旧用户所在的内层VLAN \$8: 连接旧用户的接口名称 \$9: 终端用户的IPv6地址
日志等级	6
举例	ND/6/ND_USER_DUPLICATE_IPV6ADDR: Detected a user IPv6 address conflict. New user (MAC 0010-2100-01e1, SVLAN 100, CVLAN 10) on interface GigabitEthernet1/0/1 and old user (MAC 0120-1e00-0102, SVLAN 100, CVLAN 10) on interface GigabitEthernet1/0/1 were using the same IPv6 address 10::1.
日志说明	使用 <b>ipv6 nd user-ip-conflict record enable</b> 命令开启ND记录终端用户间IPv6地址冲突功能后，如果设备检测到冲突，则输出本日志
处理建议	排查所有终端用户的IPv6地址，解决IPv6地址冲突问题

## 88.19 ND\_USER\_MOVE

日志内容	Detected a user (IPv6 address [IPV6ADDR], MAC address [STRING]) moved to another interface. Before user move: interface [STRING], SVLAN [STRING], CVLAN [STRING]. After user move: interface [STRING], SVLAN [STRING], CVLAN [STRING].
参数解释	\$1: 迁移用户的IPv6地址 \$2: 迁移用户的MAC地址 \$3: 迁移前接口名称 \$4: 迁移前用户所在的外层VLAN \$5: 迁移前用户所在的内层VLAN \$6: 迁移后接口名称 \$7: 迁移后用户所在的外层VLAN \$8: 迁移后用户所在的内层VLAN
日志等级	6
举例	ND/6/ND_USER_MOVE: Detected a user (IPv6 address 10::1, MAC address 0010-2100-01e1) moved to another interface. Before user move: interface GigabitEthernet1/0/1, SVLAN 100, CVLAN 20. After user move: interface GigabitEthernet1/0/2, SVLAN 100, CVLAN 10.
日志说明	使用 <b>ipv6 nd user-move record enable</b> 命令开启ND记录终端用户端口迁移功能后，如果设备检测到终端用户在接口间迁移，则输出本日志
处理建议	使用 <b>display ipv6 nd user-move record</b> 命令查看终端用户端口迁移表项信息，确认迁移是否合理

## 88.20 ND\_USER\_OFFLINE

日志内容	Detected a user (IPv6 address [IPV6ADDR], MAC address [STRING]) was offline from interface [STRING].
参数解释	\$1: 下线用户的IPv6地址 \$2: 下线用户的MAC地址 \$3: 连接下线用户的接口名称
日志等级	6
举例	ND/6/ND_USER_OFFLINE: Detected a user (IPv6 address 10::1, MAC address 0010-2100-01e1) was offline from interface GigabitEthernet1/0/1.
日志说明	使用 <b>ipv6 nd online-offline-log enable</b> 命令开启ND输出终端用户上下线日志功能后，如果设备检测到终端用户下线，则输出本日志
处理建议	无需处理

## 88.21 ND\_USER\_ONLINE

日志内容	Detected a user (IPv6 address [IPV6ADDR], MAC address [STRING]) was online on interface [STRING].
参数解释	\$1: 上线用户的IPv6地址 \$2: 上线用户的MAC地址 \$3: 连接上线用户的接口名称
日志等级	6
举例	ND/6/ND_USER_ONLINE: Detected a user (IPv6 address 10::1, MAC address 0010-2100-01e1) was online on interface GigabitEthernet1/0/1.
日志说明	使用 <code>ipv6 nd online-offline-log enable</code> 命令开启ND输出终端用户上下线日志功能后, 如果设备检测到终端用户上线, 则输出本日志
处理建议	检查上线用户是否是合法用户

# 89 NETCONF

本节介绍 NETCONF 模块输出的日志信息。

## 89.1 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 <ul style="list-style-type: none"><li>如果用户使用 Scheme 方式登录设备, 该值为用户名</li><li>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</li></ul> \$2: 用户IP地址或用户线类型及相对编号 <ul style="list-style-type: none"><li>用户通过 Telnet 或 SSH 登录设备时, 该字段取值为用户的 IP 地址</li><li>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</li></ul> \$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

## 89.2 EDIT-CONFIG

日志内容	<p>User ([STRING], [STRING][STRING])[STRING] operation=[STRING] [STRING] [STRING], result=[STRING]. No attributes.</p> <p>或</p> <p>User ([STRING], [STRING],[STRING]),[STRING] operation=[STRING] [STRING] [STRING], result=[STRING]. Attributes: [STRING].</p>
参数解释	<p><b>\$1:</b> 用户名或用户线类型</p> <ul style="list-style-type: none"> <li>○ 如果用户使用 <b>Scheme</b> 方式登录设备，该值为用户名</li> <li>○ 如果用户使用无认证或 <b>Password</b> 方式登录设备，该值为用户线的类型，例如 VTY</li> </ul> <p><b>\$2:</b> 用户IP地址或用户线类型及相对编号</p> <ul style="list-style-type: none"> <li>○ 用户通过 <b>Telnet</b> 或 <b>SSH</b> 登录设备时，该字段取值为用户的 IP 地址</li> <li>○ 用户通过 <b>Console</b> 或 <b>AUX</b> 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</li> </ul> <p><b>\$3:</b> NETCONF会话的编号，没有则不显示</p> <p><b>\$4:</b> NETCONF请求中的message-id，没有则不显示</p> <p><b>\$5:</b> NETCONF行操作名称</p> <p><b>\$6:</b> 模块和表名称</p> <p><b>\$7:</b> 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</p> <p><b>\$8:</b> 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</p> <p><b>\$9:</b> 属性列信息。仅配置属性列时显示该信息</p>
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	<p>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</p> <p>仅action和set操作支持输入该日志</p>
处理建议	无



## 89.3 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	<ol style="list-style-type: none"><li>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</li><li>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</li></ol>

## 89.4 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

# 90 NQA

本节介绍 NQA 模块输出的日志信息。

## 90.1 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 \$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: <ul style="list-style-type: none"><li>Probe-pass: 表示告警解除, 监控对象恢复到正常状态</li><li>Probe-fail: 表示触发告警, 监控对象处于告警状态</li></ul>
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与上次探测相比发生了变化, 触发告警或者告警解除
处理建议	<ul style="list-style-type: none"><li>如果测试成功, 无需处理</li><li>如果测试失败, 请检查网络环境</li></ul>

## 90.2 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

## 90.3 NQA\_START\_FAILURE

日志内容	NQA entry ([STRING]-[STRING]): [STRING]
参数解释	<p>\$1: NQA测试组的管理员名称</p> <p>\$2: 测试操作的标签</p> <p>\$3: NQA测试下发驱动执行时失败，失败的原因包括：</p> <ul style="list-style-type: none"><li>○ Operation failed due to configuration conflicts: 配置冲突导致下发驱动失败</li><li>○ 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</li><li>○ Operation not supported: 驱动不支持该操作</li><li>○ Not enough resources to complete the operation: 资源不足导致下发驱动失败</li><li>○ Operation failed due to an unknown error: 其他情况导致下发驱动操作失败</li></ul>
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	<ul style="list-style-type: none"><li>• 检查配置参数进行修改并重新启动测试</li><li>• 联系技术支持</li></ul>

## 90.4 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	<p>\$1: 测试会话ID</p> <p>\$2: 统计数据的序列号</p>
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

## 90.5 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	<p>\$1: 测试会话的ID</p> <p>\$2: 阈值告警组编号</p> <p>\$3: 阈值告警类型, 取值包括:</p> <ul style="list-style-type: none"><li>two-way delay: 双向时延阈值告警</li><li>two-way loss: 双向丢包率阈值告警</li><li>two-way jitter: 双向抖动阈值告警</li></ul> <p>\$4: 阈值动作, 取值包括:</p> <ul style="list-style-type: none"><li>upper: 大于等于阈值告警的上限阈值</li><li>lower: 小于等于阈值告警的下限阈值</li></ul> <p>\$5: 日志告警周期</p>
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

## 90.6 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, <b>test-session</b> 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

# 91 NSS

本节介绍 NSS (Session-based NetStream, 基于会话的 NetStream) 模块输出的日志信息。

## 91.1 NSS\_ENABLE\_FAIL

日志内容	Failed to apply the command <b>session-based netstream enable</b> to the driver. Reason: [STRING].
参数解释	\$1: 失败原因 <ul style="list-style-type: none"><li>The operation is not supported: 操作不支持</li><li>The operation conflicts with existing configurations: 与已存在的配置冲突</li></ul>
日志等级	4
举例	NSS/4/NSS_ENABLE_FAIL: Failed to apply the command <b>session-based netstream enable</b> to the driver. Reason: The operation is not supported.
日志说明	<b>session-based netstream enable</b> 命令下发驱动失败
处理建议	<ol style="list-style-type: none"><li>检查 FPGA 子卡是否在位，并重新下发命令</li><li>检查设备上是否配置了 NetStream 或 sFlow（基于会话的 NetStream、NetStream 和 sFlow 三者间存在冲突，同一时间设备仅支持运行其中一种功能）</li></ol>

## 91.2 NSS\_SESSION\_TIMEOUT\_FAIL

日志内容	Failed to apply the command <b>session-based netstream session-timeout</b> to the driver. Reason: [STRING].
参数解释	\$1: 失败原因 <ul style="list-style-type: none"><li>The operation is not supported: 操作不支持</li></ul>
日志等级	4
举例	NSS/4/NSS_SESSION_TIMEOUT_FAIL: Failed to apply the command <b>session-based netstream session-timeout</b> to the driver. Reason: The operation is not supported.
日志说明	<b>session-based netstream session-timeout</b> 命令下发驱动失败
处理建议	检查FPGA子卡是否在位，并重新下发命令

# 92 NTP

本节介绍 NTP 模块输出的日志信息。

## 92.1 NTP\_CLOCK\_CHANGE

日志内容	System clock changed from [STRING] to [STRING], the NTP server's IP address is [STRING].
参数解释	\$1: 起始时间 \$2: 同步后时间 \$3: IP地址
日志等级	5
举例	NTP/5/NTP_CLOCK_CHANGE: System clock changed from 02:12:58:345 12/28/2012 to 02:29:12:879 12/28/2012, the NTP server's IP address is 192.168.30.116.
日志说明	NTP客户端的时间已经和NTP服务器同步
处理建议	无

## 92.2 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	<ul style="list-style-type: none"><li>• NTP 闰秒标识是一个二位数，预报当天最近的分钟里要被插入的闰秒秒数</li><li>• 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</li><li>• 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</li></ul>
处理建议	无

## 92.3 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

## 92.4 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	<ol style="list-style-type: none"><li>1. 检查 NTP 服务器及网络连接</li><li>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</li></ol>

## 92.5 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

# 93 OAP

本节介绍 OAP 模块输出的日志信息。

## 93.1 OAP\_CLIENT\_DEREG

日志内容	OAP client [UINT32] on interface [STRING] deregistered.
参数解释	\$1: Client ID \$2: 接口名称
日志等级	5
举例	OAP/5/OAP_CLIENT_DEREG: OAP client 1 on interface GigabitEthernet1/0/24 deregistered.
日志说明	接口上承载的OAP client已取消注册
处理建议	检查OAP client的登录信息

## 93.2 OAP\_CLIENT\_TIMEOUT

日志内容	OAP client [UINT32] on interface [STRING] timed out.
参数解释	\$1: Client ID \$2: 接口名称
日志等级	4
举例	OAP/4/OAP_CLIENT_TIMEOUT: OAP client 1 on interface GigabitEthernet1/0/24 timed out.
日志说明	接口上承载的OAP client超时
处理建议	检查故障链路

# 94 OBJP

本节介绍 OBJP（对象策略）模块输出的日志信息。

## 94.1 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

## 94.2 OBJP\_ACCELERATE\_NOT\_SUPPORT

日志内容	Failed to accelerate [STRING] object-policy [STRING]. Object-policy acceleration is not supported.
参数解释	\$1: 对象策略版本 \$2: 对象策略名称
日志等级	4
举例	OBJP/4/OBJP_ACCELERATE_NOT_SUPPORT: Failed to accelerate IPv6 object-policy a. The operation is not supported.
日志说明	因系统不支持对象策略加速而导致对象策略加速失败
处理建议	无



## 94.3 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

# 95 OFF

本节介绍 OpenFlow 模块输出的日志信息。

## 95.1 OFF\_ACTIVE

日志内容	Activate openflow instance [UINT16]
参数解释	\$1: 实例ID
日志等级	5
举例	OFF/5/OFF_ACTIVE: Activate openflow instance 1.
日志说明	收到激活OpenFlow实例的命令
处理建议	无

## 95.2 OFF\_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	OFF/4/OFF_ACTIVE_FAILED: Failed to activate instance 1.
日志说明	激活OpenFlow实例失败
处理建议	无

## 95.3 OFF\_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	OFF/5/OFF_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

## 95.4 OFF\_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	OFF/5/OFF_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

## 95.5 OFF\_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, 取值包括smart和standalone
日志等级	4
举例	OFF/4/OFF_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 <b>fail-open mode</b> ), 将回退为缺省模式Secure
处理建议	请联系技术支持

## 95.6 OFF\_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

## 95.7 OFF\_FLOW\_ADD\_ARP\_FAILED

日志内容	Failed to add OpenFlow ARP entry: IPAddr=[STRING], OutIfIndex=[UINT32], MACAddr=[STRING].
参数解释	\$1: ARP表项的IP地址 \$2: ARP表项对应的出接口的索引 \$3: ARP表项的MAC地址
日志等级	5
举例	OFP/5/OFP_FLOW_ADD_ARP_FAILED: Failed to add OpenFlow ARP entry: IPAddr=102.0.1.1, OutIfIndex=605, MACAddr=0002-0300-0002.
日志说明	OpenFlow ARP表项添加失败
处理建议	请联系技术支持

## 95.8 OFF\_FLOW\_ADD\_BUSY

日志内容	The device is busy adding a large number of OpenFlow messages. Please do not reboot the active MPU.
参数解释	无
日志等级	5
举例	OFF/5/OFF_FLOW_ADD_BUSY: The device is busy adding a large number of OpenFlow messages. Please do not reboot the active MPU.
日志说明	设备正忙于添加大量OpenFlow消息，建议不要重启主用主控板，否则可能导致备用主控板重启两次
处理建议	看到这条日志之后，建议避免重启主用主控板

## 95.9 OFF\_FLOW\_ADD\_BUSY\_RECOVER

日志内容	Finished adding a large number of OpenFlow messages.
参数解释	无
日志等级	5
举例	OFF/5/OFF_FLOW_ADD_BUSY_RECOVER: Finished adding a large number of OpenFlow messages.
日志说明	大量OpenFlow消息已完成添加，设备不再处于忙状态
处理建议	无

## 95.10 OFF\_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	OFF/5/OFF_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

## 95.11 OFF\_FLOW\_ADD\_FAILED

日志内容	Openflow instance [UINT16] controller [CHAR]: failed to add flow entry [UINT32],table id [CHAR],because of insufficient resources.
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	OFF/4/OFF_FLOW_ADD_FAILED: Openflow instance 1 controller 0: failed to add flow entry 641,table id 0,because of insufficient resources.
日志说明	由于资源不足，添加流表项失败
处理建议	请联系技术支持

## 95.12 OFF\_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	OFF/4/OFF_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	请联系技术支持

## 95.13 OFF\_FLOW\_ADD\_ND\_FAILED

日志内容	Failed to add OpenFlow ND entry: IPv6Addr=[STRING], OutIfIndex=[UINT32], MACAddr=[STRING].
参数解释	\$1: ND表项的IPv6地址 \$2: ND表项对应的出接口的索引 \$3: ND表项的MAC地址
日志等级	5
举例	OFF/5/OFF_FLOW_ADD_ND_FAILED: Failed to add OpenFlow ND entry: IPv6Addr=1:1::1:1, OutIfIndex=5, MACAddr=1-1-1.
日志说明	OpenFlow ND表项添加失败
处理建议	请联系技术支持

## 95.14 OFF\_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	OFF/5/OFF_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

## 95.15 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

## 95.16 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

## 95.17 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: 2 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

## 95.18 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



## 95.19 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

## 95.20 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

## 95.21 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: 2 flow entries in table 1 of instance 1 were deleted because a tunnel (ifindex 141) in VXLAN 1 was deleted.
日志说明	VXLAN隧道被删除导致多个流表项被删除
处理建议	无

## 95.22 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

## 95.23 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

## 95.24 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

## 95.25 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

## 95.26 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

## 95.27 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

## 95.28 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

## 95.29 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

## 95.30 OFF\_FLOW\_UPDATE\_FAILED

日志内容	OpenFlow instance [UINT16] table [CHAR]: failed to update or synchronize flow entry [UINT32].
参数解释	\$1: 实例ID \$2: 流表ID \$3: 流表项ID
日志等级	4
举例	OFF/4/OFF_FLOW_SMOOTH_FAILED: OpenFlow instance 1 table 0: failed to update or synchronize flow entry 10000.
日志说明	主备倒换时，新主用主控板更新流表项失败 设备插入新接口板时，接口板同步主控板的流表项失败 IRF中主从设备倒换时，新主设备更新流表项失败 IRF中加入新成员设备时，成员设备同步主设备的流表项失败
处理建议	删除下发失败的流表项

## 95.31 OFF\_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	OFF/5/OFF_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

## 95.32 OFF\_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	OFF/4/OFF_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	请联系技术支持

## 95.33 OFF\_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	OFF/5/OFF_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

## 95.34 OFF\_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	OFF/5/OFF_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

## 95.35 OFF\_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	OFF/4/OFF_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

## 95.36 OFF\_GROUP\_REFRESH\_FAILED

日志内容	Openflow instance [STRING]:Failed to refresh group [STRING].
参数解释	\$1: 实例ID \$2: Group表项ID
日志等级	4
举例	OFF/4/OFF_GROUP_REFRESH_FAILED: Openflow instance 1:Failed to refresh group 1.
日志说明	控制器成功下发Group表项到设备后，设备因为拔出/插入接口板或删除/重新创建接口，需要刷新该Group表项中某些bucket的接口信息，但是由于硬件资源不足或设备异常，刷新Group表项失败
处理建议	请联系技术支持

## 95.37 OFF\_GROUP\_ROLLBACK\_FAILED

日志内容	Openflow instance [STRING]:Failed to roll back group [STRING].
参数解释	\$1: 实例ID \$2: Group表项ID
日志等级	4
举例	OFF/4/OFF_GROUP_ROLLBACK_FAILED: Openflow instance 1:Failed to roll back group 1.
日志说明	控制器修改设备的Group表项失败时，设备需要将该Group表项回退到修改前状态，但是由于硬件资源不足或设备异常，回退Group表项失败
处理建议	请联系技术支持



## 95.38 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

## 95.39 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	请联系技术支持

## 95.40 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

## 95.41 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

## 95.42 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

## 95.43 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

## 95.44 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

## 95.45 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

## 95.46 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

## 95.47 OFP\_SMARTGROUP\_BIND

日志内容	Bind target [UINT32] to program [UINT32] by flow ID map [UINT32].
参数解释	<p>\$1: Target ID \$2: Program ID \$3: Flow ID Map, 代表一到多个Flow ID</p> <ul style="list-style-type: none"> <li>本参数以十进制数显示,其对应二进制值的各bit从右到左分别代表Flow ID 0~Flow ID 31, bit 值为 1 表示取该位对应的 Flow ID。例如, Flow ID Map 值 7 对应的二进制数 00000000 00000000 00000000 00000111 表示取 Flow ID 0、Flow ID 1、Flow ID 2</li> <li>取值为 0 时, 表示所有 Flow ID</li> </ul>
日志等级	5
举例	OFP/5/OFP_SMARTGROUP_BIND: Bind target 1 to program 2 by flow ID map 7.
日志说明	<p>收到控制器消息, 准备将指定Target ID和Flow ID的Target Group表项与指定Program ID和Flow ID的Program Group表项进行绑定。其中, Flow ID由Flow ID Map提供</p> <p>本日志对应的操作中, 同一Target Group表项只能绑定到一个Program Group表项</p> <p>上述举例中的日志信息表示设备执行了如下操作:</p> <ul style="list-style-type: none"> <li>将 Target ID 为 1、Flow ID 为 0 的 Target Group 表项绑定到 Program ID 为 2、Flow ID 为 0 的 Program Group 表项</li> <li>将 Target ID 为 1、Flow ID 为 1 的 Target Group 表项绑定到 Program ID 为 2、Flow ID 为 1 的 Program Group 表项</li> <li>将 Target ID 为 1、Flow ID 为 2 的 Target Group 表项绑定到 Program ID 为 2、Flow ID 为 2 的 Program Group 表项</li> </ul>
处理建议	无

## 95.48 OFP\_SMARTGROUP\_BIND\_FAILED

日志内容	Failed to bind target [UINT32] to program [UINT32] by flow ID map [UINT32].
参数解释	<p>\$1: Target ID \$2: Program ID \$3: Flow ID Map, 代表一到多个Flow ID</p> <ul style="list-style-type: none"> <li>本参数以十进制数显示,其对应二进制值的各bit从右到左分别代表Flow ID 0~Flow ID 31, bit 值为 1 表示取该位对应的 Flow ID。例如, Flow ID Map 值 7 对应的二进制数 00000000 00000000 00000000 00000111 表示取 Flow ID 0、Flow ID 1、Flow ID 2</li> <li>取值为 0 时, 表示所有 Flow ID</li> </ul>
日志等级	4
举例	OFP/4/OFP_SMARTGROUP_BIND_FAILED: Failed to bind target 1 to program 2 by flow ID map 7.
日志说明	对Target Group表项的绑定操作失败
处理建议	请联系技术支持人员

## 95.49 OFF\_SMARTGROUP\_NEW\_BIND

日志内容	Bind target [UINT32] to program [UINT32] by flow ID map [UINT32].
参数解释	<p>\$1: Target ID \$2: Program ID \$3: Flow ID Map, 代表一到多个Flow ID</p> <ul style="list-style-type: none"> <li>本参数以十进制数显示,其对应二进制值的各bit从右到左分别代表Flow ID 0~Flow ID 31, bit 值为 1 表示取该位对应的 Flow ID。例如, Flow ID Map 值 7 对应的二进制数 00000000 00000000 00000000 00000111 表示取 Flow ID 0、Flow ID 1、Flow ID 2</li> <li>取值为 0 时, 表示所有 Flow ID</li> </ul>
日志等级	5
举例	OFFP/5/OFP_SMARTGROUP_NEW_BIND: Bind target 1 to program 2 by flow ID map 7.
日志说明	<p>收到控制器消息, 准备将指定Target ID和Flow ID的Target Group表项绑定到指定Program ID和Flow ID的Program Group表项。其中, Flow ID由Flow ID Map提供</p> <p>上述举例中的日志信息表示设备执行了如下操作:</p> <ul style="list-style-type: none"> <li>将 Target ID 为 1、Flow ID 为 0 的 Target Group 表项绑定到 Program ID 为 2、Flow ID 为 0 的 Program Group 表项</li> <li>将 Target ID 为 1、Flow ID 为 1 的 Target Group 表项绑定到 Program ID 为 2、Flow ID 为 1 的 Program Group 表项</li> <li>将 Target ID 为 1、Flow ID 为 2 的 Target Group 表项绑定到 Program ID 为 2、Flow ID 为 2 的 Program Group 表项</li> </ul>
处理建议	无

## 95.50 OFF\_SMARTGROUP\_NEW\_BIND\_FAILED

日志内容	Failed to bind target [UINT32] to program [UINT32] by flow ID map [UINT32].
参数解释	<p>\$1: Target ID \$2: Program ID \$3: Flow ID Map, 代表一到多个Flow ID</p> <ul style="list-style-type: none"> <li>本参数以十进制数显示,其对应二进制值的各bit从右到左分别代表Flow ID 0~Flow ID 31, bit 值为 1 表示取该位对应的 Flow ID。例如, Flow ID Map 值 7 对应的二进制数 00000000 00000000 00000000 00000111 表示取 Flow ID 0、Flow ID 1、Flow ID 2</li> <li>取值为 0 时, 表示所有 Flow ID</li> </ul>
日志等级	4
举例	OFFP/4/OFP_SMARTGROUP_NEW_BIND_FAILED: Failed to bind target 1 to program 2 by flow ID map 7.
日志说明	对Target Group表项的绑定操作失败
处理建议	请联系技术支持人员

## 95.51 OFF\_SMARTGROUP\_REBIND

日志内容	Unbind target [UINT32] from program [UINT32] and bind target [UINT32] to program [UINT32] by flow ID map [UINT32].
参数解释	<p>\$1: Target ID</p> <p>\$2: Program ID</p> <p>\$3: Target ID</p> <p>\$4: Program ID</p> <p>\$5: Flow ID Map, 代表一到多个Flow ID</p> <ul style="list-style-type: none"> <li>○ 本参数以十进制数显示, 其对应二进制值的各 bit 从右到左分别代表 Flow ID 0~Flow ID 31, bit 值为 1 表示取该位对应的 Flow ID。例如, Flow ID Map 值 7 对应的二进制数 00000000 00000000 00000000 00000111 表示取 Flow ID 0、Flow ID 1、Flow ID 2</li> <li>○ 取值为 0 时, 表示所有 Flow ID</li> </ul>
日志等级	5
举例	OFF/5/OFF_SMARTGROUP_REBIND: Unbind target 1 from program 1 and bind target 1 to program 2 by flow ID map 7.
日志说明	<p>收到控制器消息, 准备将指定Target ID和Flow ID的Target Group表项与指定Program ID和Flow ID的Program Group表项解除绑定, 并将这些Target Group表项绑定到新的Program Group表项。其中, Flow ID由Flow ID Map提供</p> <p>上述举例中的日志信息表示设备执行了如下操作:</p> <ul style="list-style-type: none"> <li>○ 将 Target ID 为 1、Flow ID 为 0 的 Target Group 表项与 Program ID 为 1、Flow ID 为 0 的 Program Group 表项解除绑定, 再绑定到 Program ID 为 2、Flow ID 为 0 的 Program Group 表项</li> <li>○ 将 Target ID 为 1、Flow ID 为 1 的 Target Group 表项与 Program ID 为 1、Flow ID 为 1 的 Program Group 表项解除绑定, 再绑定到 Program ID 为 2、Flow ID 为 1 的 Program Group 表项</li> <li>○ 将 Target ID 为 1、Flow ID 为 2 的 Target Group 表项与 Program ID 为 1、Flow ID 为 2 的 Program Group 表项解除绑定, 再绑定到 Program ID 为 2、Flow ID 为 2 的 Program Group 表项</li> </ul>
处理建议	无

## 95.52 OFF\_SMARTGROUP\_REBIND\_FAILED

日志内容	Failed to unbind target [UINT32] from program [UINT32] and bind target [UINT32] to program [UINT32] by flow ID map [UINT32].
参数解释	<p>\$1: Target ID</p> <p>\$2: Program ID</p> <p>\$3: Target ID</p> <p>\$4: Program ID</p> <p>\$5: Flow ID Map, 代表一到多个Flow ID</p> <ul style="list-style-type: none"> <li>○ 本参数以十进制数显示, 其对应二进制值的各 bit 从右到左分别代表 Flow ID 0~Flow ID 31, bit 值为 1 表示取该位对应的 Flow ID。例如, Flow ID Map 值 7 对应的二进制数 00000000 00000000 00000000 00000111 表示取 Flow ID 0、Flow ID 1、Flow ID 2</li> <li>○ 取值为 0 时, 表示所有 Flow ID</li> </ul>
日志等级	4
举例	OFF/4/OFP_SMARTGROUP_REBIND_FAILED: Failed to unbind target 1 from program 1 and bind target 1 to program 2 by flow ID map 7.
日志说明	对Target Group表项的重新绑定操作失败
处理建议	请联系技术支持人员

## 95.53 OFF\_SMARTGROUP\_UNBIND

日志内容	Unbind target [UINT32] from program [UINT32] by flow ID map [UINT32].
参数解释	<p>\$1: Target ID</p> <p>\$2: Program ID</p> <p>\$3: Flow ID Map, 代表一到多个Flow ID</p> <ul style="list-style-type: none"> <li>○ 本参数以十进制数显示, 其对应二进制值的各 bit 从右到左分别代表 Flow ID 0~Flow ID 31, bit 值为 1 表示取该位对应的 Flow ID。例如, Flow ID Map 值 7 对应的二进制数 00000000 00000000 00000000 00000111 表示取 Flow ID 0、Flow ID 1、Flow ID 2</li> <li>○ 取值为 0 时, 表示所有 Flow ID</li> </ul>
日志等级	5
举例	OFF/5/OFP_SMARTGROUP_UNBIND: Unbind target 1 from program 2 by flow ID map 7.
日志说明	收到控制器消息, 准备将指定Target ID和Flow ID的Target Group表项与指定Program ID和Flow ID的Program Group表项解除绑定。其中, Flow ID由Flow ID Map提供
处理建议	无

## 95.54 OFP\_SMARTGROUP\_UNBIND\_FAILED

日志内容	Failed to unbind target [UINT32] from program [UINT32] by flow ID map [UINT32].
参数解释	<p>\$1: Target ID</p> <p>\$2: Program ID</p> <p>\$3: Flow ID Map, 代表一到多个Flow ID</p> <ul style="list-style-type: none"> <li>○ 本参数以十进制数显示, 其对应二进制值的各 bit 从右到左分别代表 Flow ID 0~Flow ID 31, bit 值为 1 表示取该位对应的 Flow ID。例如, Flow ID Map 值 7 对应的二进制数 00000000 00000000 00000000 00000111 表示取 Flow ID 0、Flow ID 1、Flow ID 2</li> <li>○ 取值为 0 时, 表示所有 Flow ID</li> </ul>
日志等级	4
举例	OFP/4/OFP_SMARTGROUP_UNBIND_FAILED: Failed to unbind target 1 from program 2 by flow ID map 7.
日志说明	对Target Group表项的解除绑定操作失败
处理建议	请联系技术支持人员

## 95.55 OFP\_TTP\_GROUP\_DEL\_DENY

日志内容	Openflow instance [STRING] controller [CHAR]: Failed to delete TTP group [STRING], XID [HEX]. Reason: The TTP group is used by another TTP group.
参数解释	<p>\$1: 实例ID</p> <p>\$2: 控制器ID</p> <p>\$3: TTP (Table Type Pattern) Group表项ID</p> <p>\$4: XID (Transaction ID, 交互ID)</p>
日志等级	4
举例	OFP/4/OFP_TTP_GROUP_DEL_DENY: Openflow instance 1 controller 0: Failed to delete TTP group 1, XID 0x1. Reason: The TTP group is used by another TTP group.
日志说明	被其他TTP Group表项引用的TTP Group表项不允许被删除
处理建议	请控制器先删除引用TTP Group表项的其他TTP Group表项, 再重试删除操作



## 95.56 PORT\_MOD

日志内容	Port modified. InstanceID =[UINT16], IfIndex =[UINT32], PortDown=[STRING], NoRecv=[STRING], NoFwd=[STRING], NoPktIn=[STRING], Speed=[STRING], Duplex=[STRING].
参数解释	<p>\$1: 实例ID</p> <p>\$2: 接口索引</p> <p>\$3: 接口状态是否设置为down。NoChange表示不改变接口状态， True表示设置接口down， False表示设置接口up</p> <p>\$4: 设置接口不接收报文。NoChange表示不改变接口设置， True表示设置接口不接收报文， False表示设置接口接收报文</p> <p>\$5: 设置接口不发送报文。NoChange表示不改变接口设置， True表示设置接口不发送报文， False表示设置接口发送报文</p> <p>\$6: 设置接口上的报文不上送控制器。NoChange表示不改变接口设置， True表示设置接口的报文不上送控制器， False表示设置接口的报文上送控制器</p> <p>\$7: 设置的接口速率。取值包括Auto、 Error、 10M、 100M、 1G、 10G等。其中Error表示设置的速率不支持。如果取值为空，表示没有设置该参数</p> <p>\$8: 设置的接口双工模式。取值包括Full、 Half、 Auto和Error。其中Error表示设置的双工模式不支持。如果取值为空，表示没有设置该参数</p>
日志等级	5
举例	OFP/5/PORT_MOD: Port modified. InstanceID =1, IfIndex =2, PortDown=True, NoRecv=NoChange, NoFwd=NoChange, NoPktIn=NoChange, Speed=, Duplex=.
日志说明	控制器修改了OpenFlow实例中的接口
处理建议	无

## 95.57 OFP\_RADARDETECTION

日志内容	inIfIndex = [UINT32], packageId = [UINT16], innerTTL = [CHAR], outerTTL = [CHAR].
参数解释	<p>\$1: 报文入接口索引</p> <p>\$2: 报文标记</p> <p>\$3: 报文内层IP头的Time To Live取值</p> <p>\$4: 报文外层IP头的Time To Live取值</p>
日志等级	5
举例	OFP/5/OFP_RADARDETECTION: inIfIndex = 1, packageId = 1, innerTTL = 128, outerTTL = 128.
日志说明	收到用于雷达探测或VM仿真功能的报文
处理建议	无

# 96 OPENSRC (FreeRADIUS)

本节介绍 OPENSRC 模块输出的开源软件 FreeRADIUS 日志信息。

## 96.1 HUP事件

日志内容	[DATE] [TIME] radiusd[UINT32]: [STRING]
参数解释	\$1: 时间 (月日) \$2: 时刻 (时:分:秒) \$3: FreeRADIUS进程ID \$4: HUP事件说明, 详见 <a href="#">表96-1</a>
日志等级	6
举例	OPENSRC/6/SYSLOG: Jan 1 01:14:04 radiusd[427]: Received HUP sign
日志说明	接收到HUP信号, 重新加载用户配置信息 (用户名、用户密码、授权VLAN、授权ACL及用户有效期) 用于认证处理; 收到此HUP信号间隔小于5秒, 忽略
处理建议	请根据HUP事件的详细说明选择相应的处理方式, 详见 <a href="#">表96-1</a>

表96-1 HUP 事件的详细说明列表

HUP 事件	说明	处理建议
Received HUP sign	收到HUP信号	不需要处理
Module: Reloaded module "files"	重新加载模块配置文件	不需要处理
HUP - Files loaded by a module have changed.	收到HUP信号, 完成配置文件加载	不需要处理
Ignoring HUP (less than 5s since last one)	收到此HUP信号间隔小于5秒, 忽略	如果希望5秒内配置的新用户生效, 执行激活命令 <b>radius-server activate</b>

## 96.2 进程重启

日志内容	[DATE] [TIME] radiusd[UIN32]: [STRING]
参数解释	\$1: 日期（月 日） \$2: 时间（时:分:秒） \$3: FreeRADIUS进程ID \$4: 进程重启事件说明
日志等级	6
举例	OPENSRC/6/SYSLOG: Jan 1 02:00:02 radiusd[427]: Signalled to terminate
日志说明	终结当前进程并重新启动
处理建议	请根据进程重启事件的详细说明选择相应的处理方式，详见 <a href="#">表96-2</a>

表96-2 进程重启事件的详细说明列表（日志等级为 6）

进程重启事件	说明	处理建议
Signalled to terminate	收到终结进程信号	不需要处理
Exiting normally	进程关闭	不需要处理
Debugger not attached	进程对应的调试信息开关处于关闭状态	不需要处理
Loaded virtual server <default>	加载虚拟服务器	不需要处理
Loaded virtual server inner-tunnel	加载虚拟服务器内部通道	不需要处理
Loaded virtual server default	加载虚拟服务器默认配置	不需要处理
Ready to process requests	准备开始处理认证报文	不需要处理

## 96.3 进程启动

日志内容	[DATE] [TIME] radiusd[UIN32]: [STRING]
参数解释	\$1: 日期（月 日） \$2: 时间（时:分:秒） \$3: FreeRADIUS进程ID \$4: 进程启动事件说明
日志等级	4
举例	OPENSRC/4/SYSLOG: Jan 1 02:00:03 radiusd[460]: [//etc/raddb/mods-config/attr_filter/access_reject]:11 Check item "FreeRADIUS-Response-Delay" found in filter list for realm "DEFAULT".
日志说明	进程启动时，系统加载默认检查项
处理建议	请根据进程启动的详细说明选择相应的处理方式，详见 <a href="#">表96-3</a>

表96-3 进程启动的详细说明列表（日志等级为 4）

进程启动事件	说明	处理建议
11 Check item "FreeRADIUS-Response-Delay" found in filter list for realm "DEFAULT".	在指定文件中检查默认过滤项 FreeRADIUS-Response-Delay	不需要处理
11 Check item "FreeRADIUS-Response-Delay-USec" found in filter list for realm "DEFAULT".	在指定文件中检查默认过滤项 FreeRADIUS-Response-Delay-USec	不需要处理
Ignoring "sql" (see raddb/mods-available/README.rst)	忽略SQL处理	不需要处理
Ignoring "ldap" (see raddb/mods-available/README.rst)	忽略LDAP处理	不需要处理

## 96.4 用户认证

日志内容	[DATE] [TIME] radiusd[UINT32]: ([UINT32]) [STRING]: [[STRING]] (from client [IPADDR] port [UINT32] cli [MAC])
参数解释	\$1: 日期（月 日） \$2: 时间（时:分:秒） \$3: FreeRADIUS进程ID \$4: 日志编号 \$5: 认证结果 \$6: 用户名 \$7: RADIUS客户端IP地址 \$8: RADIUS客户端端口号 \$9: 用户MAC地址
日志等级	5
举例	OPENSRC/5/SYSLOG: Jan 1 02:06:15 radiusd[460]: (0) Login OK: [test] (from client 7.7.7.7 port 33591297 cli 00-00-00-00-00-02)
日志说明	用户认证成功
处理建议	请根据认证结果的详细说明选择相应的处理方式，详见 <a href="#">表96-4</a>

表96-4 认证结果的详细说明列表

认证结果	说明	处理建议
Login OK	认证成功或共享密钥配置不一致	<ul style="list-style-type: none"> <li>• 如果用户认证成功，则不需要处理</li> <li>• 如果用户认证失败，请检查 RADIUS 客户端和 RADIUS 服务器端的共享密钥是否一致               <ul style="list-style-type: none"> <li>◦ 客户端共享密钥通过 <b>primary</b></li> </ul> </li> </ul>

认证结果	说明	处理建议
		<b>authentication</b> 命令配置 <ul style="list-style-type: none"> <li>服务器端共享密钥通过 <b>radius-server client ip</b> 命令配置</li> </ul>
Login incorrect (pap: Cleartext password does not match "known good" password)	PAP认证密码错误	用户重新输入正确的密码
Login incorrect (chap: Password comparison failed: password is incorrect)	CHAP认证密码错误	用户重新输入正确的密码
Login incorrect (No Auth-Type found: rejecting the user via Post-Auth-Type = Reject)	PAP认证用户名不匹配或802.1X用户配置的认证类型为EAP	<ul style="list-style-type: none"> <li>若是非法用户，则不需要处理</li> <li>若是新增用户，则需要添加本地用户（通过 <b>local-user</b> 命令）</li> <li>检查配置的认证类型是否准确。例如，对于 802.1X 用户可以通过 <b>display dot1x</b> 查看认证类型，并通过 <b>dot1x authentication-method</b> 命令修改认证方式</li> </ul>
Login incorrect (chap: &control: Cleartext-Password is required for authentication)	CHAP认证用户名不匹配	<ul style="list-style-type: none"> <li>若是非法用户，则不需要处理</li> <li>若是新增用户，则需要添加对应的本地用户（通过 <b>local-user</b> 命令）</li> </ul>
Invalid user (expiration: Account expired at 'Jan 1 2013 02:19:00 UTC')	用户存在，但已经失效	<ul style="list-style-type: none"> <li>若是用户账户正常失效，则不需要处理</li> <li>若需要延长用户有效期，则需要修改该本地用户的生效截止日期（通过 <b>validity-datetime</b> 命令）</li> </ul>

日志内容	[DATE] [TIME] radiusd[UINT32]: ([UINT32]) Login incorrect (No Auth-Type found: rejecting the user via Post-Auth-Type = Reject): [[STRING]] (from client [IPADDR] port [UINT32])
参数解释	\$1: 日期（月 日） \$2: 时间（时:分:秒） \$3: FreeRADIUS进程ID \$4: 日志编号 \$5: 用户名 \$6: RADIUS客户端IP地址 \$7: RADIUS客户端端口号
日志等级	5
举例	OPENSRC/5/SYSLOG: Jan 1 02:21:20 radiusd[460]: (16) Login incorrect (No Auth-Type found: rejecting the user via Post-Auth-Type = Reject): [ddd] (from client 7.7.7.7 port 0)
日志说明	不支持Login类型的用户认证
处理建议	不需要处理

日志内容	[DATE] [TIME] radiusd[UINT32]: Ignoring request to auth address * port 1812 bound to server default from unknown client [IPADDR] port [UINT32] proto udp
参数解释	\$1: 日期（月 日） \$2: 时间（时:分:秒） \$3: FreeRADIUS进程ID \$4: RADIUS客户端IP地址 \$5: RADIUS客户端端口号
日志等级	3
举例	OPENSRC/3/SYSLOG: Jan 1 02:31:05 radiusd[548]: Ignoring request to auth address * port 1812 bound to server default from unknown client 7.7.7.7 port 11969 proto udp
日志说明	未知的RADIUS客户端IP地址和端口号，不处理认证请求报文
处理建议	<ul style="list-style-type: none"> <li>若是非法客户端，则不需要处理</li> <li>若是新增客户端，则通过 <code>radius-server client</code> 命令新增对应的 RADIUS 客户端配置</li> </ul>

## 97 OPTMOD

本节介绍 OPTMOD 模块输出的日志信息。

## 97.1 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	<ol style="list-style-type: none"><li>1. display transceiver diagnosis interface 命令查看当前偏置电流值是否已经超过高告警门限</li><li>2. display transceiver alarm interface 命令查看当前是否确实有偏置电流值高的告警</li><li>3. 如果确实超过门限了，模块有问题，更换模块</li></ol>

## 97.2 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	<ol style="list-style-type: none"><li>1. display transceiver diagnosis interface 命令查看当前偏置电流值是否已经超过低告警门限</li><li>2. display transceiver alarm interface 命令查看当前是否确实有偏置电流高的告警</li><li>3. 如果低于低告警门限，模块有问题，更换模块</li></ol>

## 97.3 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

## 97.4 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

## 97.5 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

## 97.6 FIBER\_SFPMODULE\_INVALID

日志内容	[STRING]: This transceiver module is not compatible with the interface card. UNIS does not guarantee the correct operation of the transceiver module. The transceiver module will be invalidated in [UINT32] days. Please replace it with a compatible one as soon as possible.
参数解释	\$1: 端口类型和编号 \$2: 光模块失效天数
日志等级	4
举例	OPTMOD/4/FIBER_SFPMODULE_INVALID: GigabitEthernet1/0/1: This transceiver module is not compatible with the interface card. UNIS does not guarantee the correct operation of the transceiver module. The transceiver module will be invalidated in 3 days. Please replace it with a compatible one as soon as possible.
日志说明	光模块与接口卡不匹配
处理建议	更换光模块



## 97.7 FIBER\_SFPMODULE\_NOWINVALID

日志内容	[STRING]: This is not a supported transceiver for this platform. UNIS does not guarantee the normal operation or maintenance of unsupported transceivers. Please review the platform datasheet on the UNIS web site or contact your UNIS sales rep for a list of supported transceivers.
参数解释	\$1: 端口类型和编号
日志等级	4
举例	OPTMOD/4/FIBER_SFPMODULE_NOWINVALID: GigabitEthernet1/0/1: This is not a supported transceiver for this platform. UNIS does not guarantee the normal operation or maintenance of unsupported transceivers. Please review the platform datasheet on the UNIS web site or contact your UNIS sales rep for a list of supported transceivers.
日志说明	不支持该光模块
处理建议	更换光模块

## 97.8 IO\_ERR

日志内容	[STRING]: The transceiver information I/O failed.
参数解释	\$1: 端口类型和编号
日志等级	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 <b>display transceiver diagnosis interface</b> 或者 <b>display transceiver alarm interface</b> 命令, 如果都显示fail, 则表示光模块故障, 请更换

## 97.9 MOD\_ALM\_OFF

日志内容	[STRING]: [STRING] was removed.
参数解释	\$1: 端口类型和编号 \$2: 故障类型
日志等级	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

## 97.10 MOD\_ALM\_ON

日志内容	[STRING]: [STRING] was detected.
参数解释	\$1: 端口类型和编号 \$2: 故障类型
日志等级	5
举例	OPTMOD/5/MOD_ALM_ON: GigabitEthernet1/0/1: Module_not_ready was detected.
日志说明	检测到光模块一故障
处理建议	执行 <b>display transceiver alarm interface</b> 命令, 如果仍然显示Module not ready, 则表示光模块有问题, 请更换

## 97.11 MODULE\_IN

日志内容	[STRING]: The transceiver is [STRING].
参数解释	\$1: 端口类型和编号 \$2: 光模块类型
日志等级	4
举例	OPTMOD/4/MODULE_IN: GigabitEthernet1/0/1: The transceiver is 1000_BASE_T_AN_SFP.
日志说明	光模块类型。当一光模块插入某端口时, 设备生成此日志信息
处理建议	无

## 97.12 MODULE\_OUT

日志内容	[STRING]: Transceiver absent.
参数解释	\$1: 端口类型和编号
日志等级	4
举例	OPTMOD/4/MODULE_OUT: GigabitEthernet1/0/1: The transceiver is absent.
日志说明	光模块被拔出
处理建议	无

## 97.13 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

## 97.14 RX\_ALM\_OFF

日志内容	[STRING]: [STRING] was removed.
参数解释	\$1: 端口类型和编号 \$2: RX故障类型
日志等级	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

## 97.15 RX\_ALM\_ON

日志内容	[STRING]: [STRING] was detected.
参数解释	\$1: 端口类型和编号 \$2: RX故障类型
日志等级	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 <b>display transceive alarm interface</b> 命令可查看到这个故障，确认是模块问题，更换模块

## 97.16 RX\_POW\_HIGH

日志内容	[STRING]: RX power is high.
参数解释	\$1: 端口类型和编号
日志等级	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	<ol style="list-style-type: none"><li>1. display transceiver diagnosis interface 命令查看功率是否已经超过高告警门限</li><li>2. display transceiver alarm interface 命令查看当前是否确实有功率高的告警</li><li>3. 如果确实超过门限了, 模块有问题, 更换模块</li></ol>

## 97.17 RX\_POW\_LOW

日志内容	[STRING]: RX power is low.
参数解释	\$1: 端口类型和编号
日志等级	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	<ol style="list-style-type: none"><li>1. display transceiver diagnosis interface 命令查看功率是否已经低于低告警门限</li><li>2. display transceiver alarm interface 命令查看当前是否确实有功率低告警</li><li>3. 如果确实低于门限了, 模块有问题, 更换模块</li></ol>

## 97.18 RX\_POW\_NORMAL

日志内容	[STRING]: RX power is normal.
参数解释	\$1: 端口类型和编号
日志等级	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

## 97.19 TEMP\_HIGH

日志内容	[STRING]: Temperature is high.
参数解释	\$1: 端口类型和编号
日志等级	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

## 97.20 TEMP\_LOW

日志内容	[STRING]: Temperature is low.
参数解释	\$1: 端口类型和编号
日志等级	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，如果温度确实过低就调节温度，如果环境温度正常，就是模块故障，更换模块

## 97.21 TEMP\_NORMAL

日志内容	[STRING]: Temperature is normal.
参数解释	\$1: 端口类型和编号
日志等级	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

## 97.22 TX\_ALM\_OFF

日志内容	[STRING]: [STRING] was removed.
参数解释	\$1: 端口类型和编号 \$2: TX故障类型
日志等级	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

## 97.23 TX\_ALM\_ON

日志内容	[STRING]: [STRING] was detected.
参数解释	\$1: 端口类型和编号 \$2: TX故障类型
日志等级	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 <b>display transceive alarm interface</b> 命令可查看到这个故障，确认是模块问题，更换模块

## 97.24 TX\_POW\_HIGH

日志内容	[STRING]: TX power is high.
参数解释	\$1: 端口类型和编号
日志等级	2
举例	OPTMOD/2/TX_POW_HIGH: GigabitEthernet1/0/1: TX power is high.
日志说明	光模块TX功率超过上限
处理建议	<ol style="list-style-type: none"><li>1. <b>display transceive diagnosis interface</b> 命令查看功率是否已经超过高告警门限</li><li>2. <b>display transceive alarm interface</b> 命令查看当前是否确实有功率高告警</li><li>3. 如果确实超过门限了，模块有问题，更换模块</li></ol>

## 97.25 TX\_POW\_LOW

日志内容	[STRING]: TX power is low.
参数解释	\$1: 端口类型和编号
日志等级	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	<ol style="list-style-type: none"><li>1. display transceiver diagnosis interface 命令查看功率是否已经低于低告警门限</li><li>2. display transceiver alarm interface 命令查看当前是否确实有功率低告警</li><li>3. 如果确实低于门限了，模块有问题，更换模块</li></ol>

## 97.26 TX\_POW\_NORMAL

日志内容	[STRING]: TX power is normal.
参数解释	\$1: 端口类型和编号
日志等级	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

## 97.27 TYPE\_ERR

日志内容	[STRING]: The transceiver type is not supported by port hardware.
参数解释	\$1: 端口类型和编号
日志等级	3
举例	OPTMOD/3/TYPE_ERR: GigabitEthernet1/0/1: The transceiver type is not supported by port hardware.
日志说明	端口硬件不支持光模块类型
处理建议	更换光模块

## 97.28 VOLT\_HIGH

日志内容	[STRING]: Voltage is high.
参数解释	\$1: 端口类型和编号
日志等级	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	<ol style="list-style-type: none"><li>1. display transceiver diagnosis interface 命令查看电压是否已经超过高告警门限</li><li>2. display transceiver alarm interface 命令查看当前是否确实有电压高告警</li><li>3. 如果确实超过门限了，模块有问题，更换模块</li></ol>

## 97.29 VOLT\_LOW

日志内容	[STRING]: Voltage is low.
参数解释	\$1: 端口类型和编号
日志等级	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	<ol style="list-style-type: none"><li>1. display transceiver diagnosis interface 命令查看电压是否已经超过低告警门限</li><li>2. display transceiver alarm interface 命令查看当前是否确实有电压低告警</li><li>3. 如果确实超过门限了，模块有问题，更换模块</li></ol>

## 97.30 VOLT\_NORMAL

日志内容	[STRING]: Voltage is normal.
参数解释	\$1: 端口类型和编号
日志等级	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

# 98 OSPF

本节介绍 OSPF 模块输出的日志信息。



## 98.1 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 <b>reset ospf process</b> 命令使新的路由器ID生效

## 98.2 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

## 98.3 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： <ul style="list-style-type: none"><li>• 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</li><li>• 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</li><li>• 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</li><li>• 如果是接口状态变化导致的邻居 down，检查网络连接情况</li></ul>

## 98.4 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

## 98.5 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 12.1.1.2(GigabitEthernet10/1) changed from FULL to DOWN.
日志说明	接口OSPF邻接状态改变
处理建议	当某接口与邻居的状态发生改变时发送该日志，请检查OSPF配置正确性和网络连通性

## 98.6 OSPF\_NBR\_CHG\_REASON

日志内容	<p>OSPF [UINT32] Area [STRING] Router [STRING]([STRING]) CPU usage: [STRING], VPN name: [STRING], IfMTU: [UINT32], Neighbor address: [STRING], NbrID [STRING] changed from [STRING] to [STRING] at [STRING].</p> <p>Last 4 hello packets received at: [STRING]</p> <p>Last 4 hello packets sent at: [STRING]</p>
参数解释	<p>\$1: OSPF进程ID</p> <p>\$2: 区域ID</p> <p>\$3: 路由ID</p> <p>\$4: 接口简名</p> <p>\$5: CPU使用率</p> <p>\$6: VPN名称</p> <p>\$7: 接口MTU大小</p> <p>\$8: 邻居的IP地址</p> <p>\$9: 邻居的路由器ID</p> <p>\$10: 变化前的邻居状态</p> <p>\$11: 变化后的邻居状态和状态变化原因</p> <p>\$12: 邻居状态改变的时间</p> <p>\$13: 邻居状态改变前接收的4个Hello报文的时间</p> <p>\$14: 邻居状态改变前发送的4个Hello报文的时间</p>
日志等级	5
举例	<p>OSPF/5/OSPF_NBR_CHG_REASON: OSPF 1 Area 0.0.0.0 Router 2.2.2.2(GE1/0/1) CPU usage:3.80%, VPN name: a, IfMTU:1500, Neighbor address:10.1.1.2, NbrID:1.1.1.1 changed from Full to Down because OSPF interface parameters changed at 2019-04-01 15:20:57:034.</p> <p>Last 4 hello packets received at:</p> <p>2019-04-01 15:19:46:225</p> <p>2019-04-01 15:19:56:224</p> <p>2019-04-01 15:20:06:225</p> <p>2019-04-01 15:20:16:225</p> <p>Last 4 hello packets sent at:</p> <p>2019-04-01 15:20:22:033</p> <p>2019-04-01 15:20:32:033</p> <p>2019-04-01 15:20:42:032</p> <p>2019-04-01 15:20:52:033</p>
日志说明	接口OSPF邻居状态改变
处理建议	当某接口与邻居的状态发生回退时发送该日志，请检查OSPF配置正确性和网络连通性

## 98.7 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

## 98.8 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 <b>reset ospf process</b> 命令使新的路由器ID生效

## 98.9 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_CONFLICT_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 <b>reset ospf process</b> 命令使新的路由器ID生效

## 98.10 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 <b>reset ospf process</b> 命令使新的路由器ID生效

## 98.11 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

# 99 OSPFV3

本节介绍 OSPFv3 模块输出的日志信息。

## 99.1 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： <ul style="list-style-type: none"><li>• 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</li><li>• 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</li><li>• 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</li><li>• 如果是接口状态变化导致的邻居 down，检查网络连接情况</li></ul>

## 99.2 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

## 99.3 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

## 99.4 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

# 100 PBB

本节介绍 PBB 模块输出的日志信息。



## 100.1 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

# 101 PBR

本节介绍 PBR 模块输出的日志信息。

## 101.1 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： <ul style="list-style-type: none"><li>○ 硬件资源不足</li><li>○ 系统不支持该操作</li><li>○ 硬件资源不足且系统不支持</li></ul>
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

# 102 PCE

本节介绍 PCE 模块输出的日志信息

## 102.1 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: <ul style="list-style-type: none"><li>• TCP connection down: TCP 连接断开</li><li>• received a close message: 收到关闭消息</li><li>• reception of a malformed PCEP message: 收到非法消息</li><li>• internal error: 内部错误</li><li>• memory in critical state: 内存不足</li><li>• dead timer expired: 会话超时</li><li>• process deactivated: PCE 进程去激活</li><li>• remote peer unavailable/untriggered: 对等体失效</li><li>• reception of an unacceptable number of unrecognized PCEP messages: 收到超过限制的未知消息</li><li>• 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</li><li>• PCE address changed: PCE 地址变化</li><li>• initialization failed: 初始化失败</li></ul>
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

# 103 PEX (IRF3.1)

本节介绍 IRF3.1 PEX (Port Extender) 模块输出的日志信息。

## 103.1 PEX\_AUTOCONFIG\_BAGG\_ASSIGNMEMBER

日志内容	[STRING] was assigned to [STRING].
参数解释	\$1: 物理接口名称 \$2: 二层聚合接口名称
日志等级	5
举例	PEX/5/PEX_AUTOCONFIG_BAGG_ASSIGNMEMBER: GigabitEthernet 1/2/0/1 was assigned to Bridge-Aggregation10.
日志说明	父设备运行IRF3.1系统自动配置功能时, 自动将连接PEX的物理接口添加到作为级联接口的聚合组中
处理建议	不需要处理

## 103.2 PEX\_AUTOCONFIG\_BAGG\_CREATE

日志内容	[STRING] was created by the PEX auto-config feature.
参数解释	\$1: 二层聚合接口名称
日志等级	5
举例	PEX/5/PEX_AUTOCONFIG_BAGG_CREATE: Bridge-Aggregation10 was created by the PEX auto-config feature.
日志说明	父设备运行IRF3.1系统自动配置功能时, 自动创建二层聚合接口用来作级联接口
处理建议	不需要处理

## 103.3 PEX\_AUTOCONFIG\_BAGG\_NORESOURCE

日志内容	Not enough resources to create a Layer 2 aggregate interface.
参数解释	无
日志等级	5
举例	PEX/5/PEX_AUTOCONFIG_BAGG_NORESOURCE: Not enough resources to create a Layer 2 aggregate interface.
日志说明	父设备运行IRF3.1系统自动配置功能时, 没有空闲资源创建二层聚合接口
处理建议	删除设备上不需要使用的聚合接口, 释放资源

## 103.4 PEX\_AUTOCONFIG\_BAGG\_REMOVEMEMBER

日志内容	[STRING] was removed from [STRING].
参数解释	\$1: 物理接口名称 \$2: 二层聚合接口名称
日志等级	5
举例	PEX/5/PEX_AUTOCONFIG_BAGG_REMOVEMEMBER: GigabitEthernet 1/2/0/1 was removed from Bridge-Aggregation10.
日志说明	父设备运行IRF3.1系统自动配置功能时,会自动将连接PEX的物理接口添加到作为级联接口的聚合组中。添加端口时,如果检查到该物理接口已经被添加到其他级联接口的聚合组中,则先将该物理接口从其他级联接口的聚合组中删除
处理建议	不需要处理

## 103.5 PEX\_AUTOCONFIG\_CAPABILITY\_ENABLE

日志内容	PEX connection capability was enabled on [STRING] and the interface was assigned to PEX group [UINT32].
参数解释	\$1: 二层聚合接口名称 \$2: PEX组编号
日志等级	5
举例	PEX/5/PEX_AUTOCONFIG_CAPABILITY_ENABLE: PEX connection capability was enabled on Bridge-Aggregation 10 and the interface was assigned to PEX group 1.
日志说明	父设备运行IRF3.1系统自动配置功能时,自动开启连接PEX的二层聚合接口的PEX连接能力,并将该接口加入PEX组中
处理建议	不需要处理

## 103.6 PEX\_AUTOCONFIG\_CASCADELIMIT

日志内容	Failed to assign cascade port [STRING] to PEX group [UINT32]. Reason: Maximum number of cascade ports already reached in the PEX group.
参数解释	\$1: 二层聚合接口名称 \$2: PEX组编号
日志等级	5
举例	PEX/5/PEX_AUTOCONFIG_CASCADELIMIT: Failed to assign cascade port Bridge-Aggregation10 to PEX group1. Reason: Maximum number of cascade ports already reached in the PEX group.
日志说明	父设备运行IRF3.1系统自动配置功能时,检测到PEX组中级联接口的数目已达到上限,无法再将聚合接口加入该PEX组中
处理建议	删除该组中空闲的级联接口,释放资源

## 103.7 PEX\_AUTOCONFIG\_CONNECTION\_ERROR

日志内容	A PEX connected to more than one upper-tier PEXs.
参数解释	无
日志等级	5
举例	PEX/5/PEX_AUTOCONFIG_CONNECTION_ERROR: A PEX connected to more than one upper-tier PEXs.
日志说明	父设备运行IRF3.1系统自动配置功能时,检测到PEX和两台或两台以上上级PEX之间存在物理连接
处理建议	PEX上行链路只能连接到同一台上级PEX,否则可能导致PEX无法上线或上线后功能运行异常。请检查并修改组网连接

## 103.8 PEX\_AUTOCONFIG\_DIFFGROUPNUMBER

日志内容	[STRING] failed to join in PEX group [UINT32]. Reason: Its upper-tier PEX was in PEX group [UINT32]. Please make sure they are in the same PEX group.
参数解释	\$1: 二层聚合接口名称 \$2: PEX组编号 \$3: PEX组编号
日志等级	5
举例	PEX/5/PEX_AUTOCONFIG_DIFFGROUPNUMBER: Bridge-Aggregation10 failed to join in PEX group 1. Reason: Its upper-tier PEX was in PEX group 2. Please make sure they are in the same PEX group.
日志说明	父设备运行IRF3.1系统自动配置功能,开启PEX二层聚合接口连接PEX的能力并将接口加入PEX组时,所指定的PEX组编号与上级PEX所在PEX组编号不同。
处理建议	下级PEX只能与上级PEX加入同一PEX组,请修改配置

## 103.9 PEX\_AUTOCONFIG\_DYNAMICBAGG\_STP

日志内容	[STRING] was automatically set to dynamic aggregation mode and configured as an STP edge port.
参数解释	\$1: 二层聚合接口名称
日志等级	5
举例	PEX/5/PEX_AUTOCONFIG_DYNAMICBAGG_STP: Bridge-Aggregation10 was automatically set to dynamic aggregation mode and configured as an STP edge port.
日志说明	父设备运行IRF3.1系统自动配置功能时,将级联接口自动配置为动态聚合模式并且配置为STP边缘端口。
处理建议	不需要处理

## 103.10 PEX\_AUTOCONFIG\_GROUP\_CREATE

日志内容	PEX group [UINT32] was created.
参数解释	\$1: PEX组编号
日志等级	5
举例	PEX/5/PEX_AUTOCONFIG_GROUP_CREATE: PEX group 1 was created.
日志说明	父设备运行IRF3.1系统自动配置功能时，自动创建PEX组
处理建议	不需要处理

## 103.11 PEX\_AUTOCONFIG\_NONUMBERRESOURCE

日志内容	形式一： No virtual slot numbers are available. 形式二： No virtual chassis numbers are available.
参数解释	无
日志等级	5
举例	PEX/5/PEX_AUTOCONFIG_NONUMBERRESOURCE: No virtual slot numbers are available.
日志说明	父设备运行IRF3.1系统自动配置功能时，没有虚拟槽位号/虚拟框号资源用来分配
处理建议	删除空闲级联接口或在空闲级联接口上取消分配虚拟槽位号/虚拟框号的配置，释放资源

## 103.12 PEX\_AUTOCONFIG\_NOT\_CASCADEPORT

日志内容	[STRING] was already assigned to [STRING], which is an aggregate interface not enabled with PEX connection capability. Please remove [STRING] from [STRING] or use another physical interface to connect the PEX.
参数解释	\$1: 物理接口名称 \$2: 二层聚合接口名称 \$3: 物理接口名称 \$4: 二层聚合接口名称
日志等级	5
举例	PEX/5/PEX_AUTOCONFIG_NOT_CASCADEPORT: GigabitEthernet 1/2/0/1 was already assigned to Bridge-Aggregation10, which is an aggregate interface not enabled with PEX connection capability. Please remove GigabitEthernet 1/2/0/1 from Bridge-Aggregation10 or use another physical interface to connect the PEX.
日志说明	父设备运行IRF3.1系统自动配置功能时，检测到连接PEX的物理接口已经加入到聚合组中，但对对应聚合接口没有开启连接PEX的能力
处理建议	将物理接口从聚合组中退出或更换其他物理接口

## 103.13 PEX\_AUTOCONFIG\_NUMBER\_ASSIGN

日志内容	形式一： Virtual slot number [UINT32] was assigned on [STRING]. 形式二： Virtual chassis number [UINT32] was assigned on [STRING].
参数解释	形式一： \$1: 虚拟槽位号 \$2: 二层聚合接口名称 形式二： \$1: 虚拟框号 \$2: 二层聚合接口名称
日志等级	5
举例	PEX/5/PEX_AUTOCONFIG_NUMBER_ASSIGN: Virtual slot number 100 was assigned on Bridge-Aggregation 10.
日志说明	父设备运行IRF3.1系统自动配置功能时，在连接PEX的二层聚合接口上，自动为PEX分配虚拟槽位号/虚拟框号
处理建议	不需要处理

## 103.14 PEX\_LLDP\_DISCOVER

日志内容	Discover peer device on interface [STRING]: MAC=STRING, priority=UINT32.
参数解释	\$1: 接口名称 \$2: 对端MAC地址 \$3: PEX设备上行口的优先级
日志等级	5
举例	PEX/5/PEX_LLDP_DISCOVER: Discover peer device on interface Ten-GigabitEthernet1/0/1: MAC=20f4-9cb6-0100, priority=0.
日志说明	父设备或PEX设备通过LLDP协议发现对端
处理建议	正常状态，无需任何处理

## 103.15 PEX\_MEMBERID\_EXCEED

日志内容	To use the IRF fabric connected to interface [STRING] as a PEX, the IRF member ID must be in the range of 1 to 4.
参数解释	\$1: 接口名称
日志等级	4
举例	PEX/4/PEX_MEMBERID_EXCEED: To use the IRF fabric connected to interface Bridge-Aggregation1 as a PEX, the IRF member ID must be in the range of 1 to 4.
日志说明	设备作为PEX加入IRF3.1系统时，PEX设备的IRF成员编号必须在1~4范围以内
处理建议	请检查PEX设备的IRF成员编号是否在1~4范围之内。如果不是，用户可登录PEX设备，用 <b>irf member renumber</b> 命令修改PEX设备的成员编号

## 103.16 PEX\_PECSP\_OPEN\_RCVD

日志内容	Received a CSP Open message on interface [STRING].
参数解释	\$1: 接口名称
日志等级	5
举例	PEX/5/PEX_PECSP_OPEN_RCVD: Received a CSP Open message on interface Bridge-Aggregation1.
日志说明	接口收到PE CSP协议的OPEN报文，表示对端请求建立连接。如果双方均能在发送请求后60秒内接收到对端回复的OPEN报文，则父设备和PEX之间的连接建立成功
处理建议	正常状态，无需任何处理



## 103.17 PEX\_PECSP\_OPEN\_SEND

日志内容	Sent a CSP Open message on interface [STRING].
参数解释	\$1: 接口名称
日志等级	5
举例	PEX/5/PEX_PECSP_OPEN_SEND: Sent a CSP Open message on interface Bridge-Aggregation1.
日志说明	父设备级联口或PEX设备上行口发送PE CSP协议的OPEN报文，表示请求与对方建立连接。如果双方均能在发送请求后60秒内接收到对端回复的OPEN报文，则父设备和PEX之间的连接建立成功
处理建议	正常状态，无需任何处理

## 103.18 PEX\_PECSP\_TIMEOUT

日志内容	PE CSP timed out on interface [STRING].
参数解释	\$1: 接口名称
日志等级	4
举例	PEX/4/PEX_PECSP_TIMEOUT: PE CSP timed out on interface Bridge-Aggregation1.
日志说明	PE CSP协议超时，PEX设备和父设备无法建立连接
处理建议	请检查父设备和PEX之间链路和IRF3.1相关配置

# 104 PFILTER

本节介绍报文过滤模块输出的日志信息。

## 104.1 PFILTER\_GLB\_RES\_CONFLICT

日志内容	Failed to apply or refresh [STRING] ACL [UINT] to the [STRING] direction globally. [STRING] ACL [UINT] has already been applied globally.
参数解释	\$1: ACL版本 \$2: ACL编号 \$3: 流量方向 \$4: ACL类型 \$5: ACL编号
日志等级	3
举例	PFILTER/3/PFILTER_GLB_RES_CONFLICT: Failed to apply or refresh IPv6 ACL 2000 to the inbound direction globally. IPv6 ACL 3000 has already been applied globally.
日志说明	IPv4、IPv6、MAC类型的ACL在某方向上全局应用了，系统无法在此方向上全局应用或更新相同类型的ACL规则
处理建议	删除相同类型的ACL

## 104.2 PFILTER\_GLB\_IPV4\_DACT\_NO\_RES

日志内容	Failed to apply or refresh the IPv4 default action to the [STRING] direction globally. The resources are insufficient.
参数解释	\$1: 流量方向
日志等级	3
举例	PFILTER/3/PFILTER_GLB_IPV4_DACT_NO_RES: Failed to apply or refresh the IPv4 default action to the inbound direction globally. The resources are insufficient.
日志说明	因硬件资源不足，系统无法在某个方向上全局应用或更新IPv4缺省动作
处理建议	使用 <b>display qos-acl resource</b> 命令检查硬件资源使用情况

## 104.3 PFILTER\_GLB\_IPV4\_DACT\_UNK\_ERR

日志内容	Failed to apply or refresh the IPv4 default action to the [STRING] direction globally.
参数解释	\$1: 流量方向
日志等级	3
举例	PFILTER/3/PFILTER_GLB_IPV4_DACT_UNK_ERR: Failed to apply or refresh the IPv4 default action to the inbound direction globally.
日志说明	因故障导致系统无法在某个方向上全局应用或更新IPv4缺省动作
处理建议	无

## 104.4 PFILTER\_GLB\_IPV6\_DACT\_NO\_RES

日志内容	Failed to apply or refresh the IPv6 default action to the [STRING] direction globally. The resources are insufficient.
参数解释	\$1: 流量方向
日志等级	3
举例	PFILTER/3/PFILTER_GLB_IPV6_DACT_NO_RES: Failed to apply or refresh the IPv6 default action to the inbound direction globally. The resources are insufficient.
日志说明	因硬件资源不足，系统无法在某个方向上全局应用或更新IPv6缺省动作
处理建议	使用display qos-acl resource命令检查硬件资源使用情况

## 104.5 PFILTER\_GLB\_IPV6\_DACT\_UNK\_ERR

日志内容	Failed to apply or refresh the IPv6 default action to the [STRING] direction globally.
参数解释	\$1: 流量方向
日志等级	3
举例	PFILTER/3/PFILTER_GLB_IPV6_DACT_UNK_ERR: Failed to apply or refresh the IPv6 default action to the inbound direction globally.
日志说明	因故障导致系统无法在某个方向上全局应用或更新IPv6缺省动作
处理建议	无

## 104.6 PFILTER\_GLB\_MAC\_DACT\_NO\_RES

日志内容	Failed to apply or refresh the MAC default action to the [STRING] direction globally. The resources are insufficient.
参数解释	\$1: 流量方向
日志等级	3
举例	PFILTER/3/PFILTER_GLB_MAC_DACT_NO_RES: Failed to apply or refresh the MAC default action to the inbound direction globally. The resources are insufficient.
日志说明	因硬件资源不足，系统无法在某个方向上全局应用或更新MAC缺省动作
处理建议	使用display qos-acl resource命令检查硬件资源使用情况

## 104.7 PFILTER\_GLB\_MAC\_DACT\_UNK\_ERR

日志内容	Failed to apply or refresh the MAC default action to the [STRING] direction globally.
参数解释	\$1: 流量方向
日志等级	3
举例	PFILTER/3/PFILTER_GLB_MAC_DACT_UNK_ERR: Failed to apply or refresh the MAC default action to the inbound direction globally.
日志说明	因故障导致系统无法在某个方向上全局应用或更新MAC缺省动作
处理建议	无

## 104.8 PFILTER\_GLB\_NO\_RES

日志内容	Failed to apply or refresh [STRING] ACL [UINT] [STRING] to the [STRING] direction globally. The resources are insufficient.
参数解释	\$1: ACL版本 \$2: ACL编号 \$3: 规则的ID及内容 \$4: 流量方向
日志等级	3
举例	PFILTER/3/PFILTER_GLB_NO_RES: Failed to apply or refresh IPv6 ACL 2000 rule 1 to the inbound direction globally. The resources are insufficient.
日志说明	因硬件资源不足，系统无法在某个方向上全局应用或更新ACL规则
处理建议	使用 <b>display qos-acl resource</b> 命令检查硬件资源使用情况

## 104.9 PFILTER\_GLB\_NOT\_SUPPORT

日志内容	Failed to apply or refresh [STRING] ACL [UINT] [STRING] to the [STRING] direction globally. The ACL is not supported.
参数解释	\$1: ACL版本 \$2: ACL编号 \$3: 规则的ID及内容 \$4: 流量方向
日志等级	3
举例	PFILTER/3/PFILTER_GLB_NOT_SUPPORT: Failed to apply or refresh IPv6 ACL 2000 rule 1 to the inbound direction globally. The ACL is not supported.
日志说明	因系统不支持ACL规则而导致无法在某个方向上全局应用或更新ACL规则
处理建议	检查ACL规则并删除不支持的配置

## 104.10 PFILTER\_GLB\_UNK\_ERR

日志内容	Failed to apply or refresh [STRING] ACL [UINT] [STRING] to the [STRING] direction globally.
参数解释	\$1: ACL版本 \$2: ACL编号 \$3: ACL规则的ID及内容 \$4: 流量方向
日志等级	3
举例	PFILTER/3/PFILTER_GLB_UNK_ERR: Failed to apply or refresh IPv6 ACL 2000 rule 1 to the inbound direction globally.
日志说明	因故障导致系统无法在某个方向上全局应用或更新ACL
处理建议	无

## 104.11 PFILTER\_IF\_IPV4\_DACT\_NO\_RES

日志内容	Failed to apply or refresh the IPv4 default action to the [STRING] direction of interface [STRING]. The resources are insufficient.
参数解释	\$1: 流量方向 \$2: 接口名称
日志等级	3
举例	PFILTER/3/PFILTER_IF_IPV4_DACT_NO_RES: Failed to apply or refresh the IPv4 default action to the inbound direction of interface Ethernet 3/1/2. The resources are insufficient.
日志说明	因硬件资源不足，系统无法在接口的某个方向上应用或更新IPv4缺省动作
处理建议	使用display qos-acl resource命令检查硬件资源使用情况

## 104.12 PFILTER\_IF\_IPV4\_DACT\_UNK\_ERR

日志内容	Failed to apply or refresh the IPv4 default action to the [STRING] direction of interface [STRING].
参数解释	\$1: 流量方向 \$2: 接口名称
日志等级	3
举例	PFILTER/3/PFILTER_IF_IPV4_DACT_UNK_ERR: Failed to apply or refresh the IPv4 default action to the inbound direction of interface Ethernet 3/1/2.
日志说明	因故障系统无法在接口的某个方向上应用或更新IPv4缺省动作
处理建议	无

## 104.13 PFILTER\_IF\_IPV6\_DACT\_NO\_RES

日志内容	Failed to apply or refresh the IPv6 default action to the [STRING] direction of interface [STRING]. The resources are insufficient.
参数解释	\$1: 流量方向 \$2: 接口名称
日志等级	3
举例	PFILTER/3/PFILTER_IF_IPV6_DACT_NO_RES: Failed to apply or refresh the IPv6 default action to the inbound direction of interface Ethernet 3/1/2. The resources are insufficient.
日志说明	因硬件资源不足，系统无法在接口的某个方向上应用或更新IPv6缺省动作
处理建议	使用 <b>display qos-acl resource</b> 命令检查硬件资源使用情况

## 104.14 PFILTER\_IF\_IPV6\_DACT\_UNK\_ERR

日志内容	Failed to apply or refresh the IPv6 default action to the [STRING] direction of interface [STRING].
参数解释	\$1: 流量方向 \$2: 接口名称
日志等级	3
举例	PFILTER/3/PFILTER_IF_IPV6_DACT_UNK_ERR: Failed to apply or refresh the IPv6 default action to the inbound direction of interface Ethernet 3/1/2.
日志说明	因故障系统无法在接口的某个方向上应用或更新IPv6缺省动作
处理建议	无

## 104.15 PFILTER\_IF\_MAC\_DACT\_NO\_RES

日志内容	Failed to apply or refresh the MAC default action to the [STRING] direction of interface [STRING]. The resources are insufficient.
参数解释	\$1: 流量方向 \$2: 接口名称
日志等级	3
举例	PFILTER/3/PFILTER_IF_MAC_DACT_NO_RES: Failed to apply or refresh the MAC default action to the inbound direction of interface Ethernet 3/1/2. The resources are insufficient.
日志说明	因硬件资源不足，系统无法在接口的某个方向上应用或更新MAC缺省动作
处理建议	使用 <b>display qos-acl resource</b> 命令检查硬件资源使用情况

## 104.16 PFILTER\_IF\_MAC\_DACT\_UNK\_ERR

日志内容	Failed to apply or refresh the MAC default action to the [STRING] direction of interface [STRING].
参数解释	\$1: 流量方向 \$2: 接口名称
日志等级	3
举例	PFILTER/3/PFILTER_IF_MAC_DACT_UNK_ERR: Failed to apply or refresh the MAC default action to the inbound direction of interface Ethernet 3/1/2.
日志说明	因故障系统无法在接口的某个方向上应用或更新MAC缺省动作
处理建议	无

## 104.17 PFILTER\_IF\_NO\_RES

日志内容	Failed to apply or refresh [STRING] ACL [UINT] [STRING] to the [STRING] direction of interface [STRING]. The resources are insufficient.
参数解释	\$1: ACL版本 \$2: ACL编号 \$3: ACL规则的ID及内容 \$4: 流量方向 \$5: 接口名称
日志等级	3
举例	PFILTER/3/PFILTER_IF_NO_RES: Failed to apply or refresh IPv6 ACL 2000 rule 1 to the inbound direction of interface Ethernet 3/1/2. The resources are insufficient.
日志说明	因硬件资源不足，系统无法在接口的某个方向上应用或更新ACL规则
处理建议	使用 <b>display qos-acl resource</b> 命令检查硬件资源使用情况

## 104.18 PFILTER\_IF\_NOT\_SUPPORT

日志内容	Failed to apply or refresh [STRING] ACL [UINT] [STRING] to the [STRING] direction of interface [STRING]. The ACL is not supported.
参数解释	\$1: ACL版本 \$2: ACL编号 \$3: ACL规则的ID及内容 \$4: 流量方向 \$5: 接口名称
日志等级	3
举例	PFILTER/3/PFILTER_IF_NOT_SUPPORT: Failed to apply or refresh IPv6 ACL 2000 rule 1 to the inbound direction of interface Ethernet 3/1/2. The ACL is not supported.
日志说明	因系统不支持ACL规则而导致无法在接口的某个方向上应用或更新ACL规则
处理建议	检查ACL规则并删除不支持的配置

## 104.19 PFILTER\_IF\_RES\_CONFLICT

日志内容	Failed to apply or refresh [STRING] ACL [UINT] to the [STRING] direction of interface [STRING]. [STRING] ACL [UINT] has already been applied to the interface.
参数解释	\$1: ACL版本 \$2: ACL编号 \$3: 流量方向 \$4: 接口名称 \$5: ACL类型 \$6: ACL编号
日志等级	3
举例	PFILTER/3/PFILTER_IF_RES_CONFLICT: Failed to apply or refresh IPv6 ACL 2000 to the inbound direction of interface Ethernet 3/1/2. IPv6 ACL 3000 has already been applied to the interface.
日志说明	IPv4、IPv6、MAC类型的ACL在接口某方向上应用了，系统无法在此方向上应用或更新相同类型的ACL规则
处理建议	删除相同类型的ACL



## 104.20 PFILTER\_IF\_UNK\_ERR

日志内容	Failed to apply or refresh [STRING] ACL [UINT] [STRING] to the [STRING] direction of interface [STRING].
参数解释	\$1: ACL版本 \$2: ACL编号 \$3: ACL规则的ID及内容 \$4: 流量方向 \$5: 接口名称
日志等级	3
举例	PFILTER/3/PFILTER_IF_UNK_ERR: Failed to apply or refresh IPv6 ACL 2000 rule 1 to the inbound direction of interface Ethernet 3/1/2.
日志说明	因故障系统无法在接口的某个方向上应用或更新ACL规则
处理建议	无

## 104.21 PFILTER\_IPV4\_FLOW\_INFO

日志内容	ACL [STRING] [STRING] [STRING] rule [STRING] [STRING]
参数解释	\$1: ACL编号或名称 \$2: 流量方向 \$3: ACL应用的位置 \$4: ACL规则的编号及动作 \$5: ACL规则匹配的首个报文的信息
日志等级	6
举例	PFILTER/6/PFILTER_IPV4_FLOW_INFO: ACL 3000 inbound Ethernet 3/1/2 rule 0 permit tcp 192.168.1.1(1024) -> 192.168.5.1(1024).
日志说明	报文过滤引用的IPv4高级ACL规则匹配的首个报文的信息
处理建议	无

## 104.22 PFILTER\_IPV4\_FLOW\_STATIS

日志内容	ACL [STRING] [STRING] rule [STRING] [STRING], [UINT64] packet(s).
参数解释	\$1: ACL编号或名称 \$2: 流量方向 \$3: ACL规则的编号及动作 \$4: ACL规则匹配的报文的信息 \$5: 匹配的报文个数
日志等级	6
举例	PFILTER/6/PFILTER_IPV4_FLOWLOG_STATIS: ACL 3000 inbound rule 0 permit icmp 192.168.1.1(1024) -> 192.168.5.1(1024), 1000 packets.
日志说明	报文过滤引用的IPv4 高级ACL规则匹配报文的信息和统计信息
处理建议	无

## 104.23 PFILTER\_IPV6\_FLOW\_INFO

日志内容	IPv6 ACL [STRING] [STRING] [STRING] rule [STRING] [STRING]
参数解释	\$1: ACL编号或名称 \$2: 流量方向 \$3: ACL应用的位置 \$4: ACL规则的编号及动作 \$5: ACL规则匹配的首个报文的信息
日志等级	6
举例	PFILTER/6/PFILTER_IPV6_FLOW_INFO: IPv6 ACL 3000 inbound Ethernet 3/1/2 rule 0 permit tcp 0:1020::200:0(0)->0:720::200:0(0).
日志说明	报文过滤引用的IPv6高级ACL规则匹配的首个报文的信息
处理建议	无

## 104.24 PFILTER\_IPV6\_FLOW\_STATIS

日志内容	IPv6 ACL [STRING] [STRING] rule [STRING] [STRING], [UINT64] packet(s).
参数解释	\$1: ACL编号或名称 \$2: 流量方向 \$3: ACL规则的编号及动作 \$4: ACL规则匹配的报文的信息 \$5: 匹配的报文个数
日志等级	6
举例	PFILTER/6/PFILTER_IPV6_FLOWLOG_STATIS: IPv6 ACL 3000 rule 0 permit icmpv6 0:1020::200:0(0)->0:720::200:0(0), 1000 packets.
日志说明	报文过滤引用的IPv6高级ACL规则匹配报文的信息和统计信息
处理建议	无

## 104.25 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应用的位置 \$2: 流量方向 \$3: ACL编号或名称 \$4: ACL规则的编号ID及内容 \$5: ACL规则匹配的报文个数
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	ACL规则在报文过滤日志发送周期结束后匹配的报文个数
处理建议	无

## 104.26 PFILTER\_MAC\_FLOW\_INFO

日志内容	MAC ACL [STRING] [STRING] [STRING] rule [STRING] [STRING]
参数解释	\$1: ACL编号或名称 \$2: 流量方向 \$3: ACL应用的位置 \$4: ACL规则的编号及动作 \$5: ACL规则匹配的首个报文的信息
日志等级	6
举例	PFILTER/6/PFILTER_MAC_FLOW_INFO: MAC ACL 4000 inbound Ethernet 3/1/2 rule 0 permit 0800-2700-9000 -> DC2D-CB1D-0676.
日志说明	报文过滤引用的二层ACL规则匹配的首个报文的信息
处理建议	无

## 104.27 PFILTER\_STATIS\_INFO

日志内容	[STRING] ([STRING]): Packet-filter [UINT32] [STRING] [UINT64] packet(s).
参数解释	\$1: ACL应用的位置 \$2: 流量方向 \$3: ACL编号或名称 \$4: ACL规则的编号及内容 \$5: ACL规则匹配的报文个数
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	ACL规则在报文过滤日志发送周期结束后匹配的报文个数
处理建议	无

## 104.28 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 <b>display qos-acl resource</b> 命令检查硬件资源使用情况

## 104.29 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

## 104.30 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 <b>display qos-acl resource</b> 命令检查硬件资源使用情况

## 104.31 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

## 104.32 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 <b>display qos-acl resource</b> 命令检查硬件资源使用情况

## 104.33 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

## 104.34 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 <b>display qos-acl resource</b> 命令检查硬件资源使用情况

## 104.35 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

## 104.36 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

## 104.37 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

# 105 PIM

本节介绍 PIM 模块输出的日志信息。



## 105.1 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

## 105.2 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

# 106 PING

本节介绍 ping 模块输出的日志信息。

## 106.1 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 <b>ping</b> 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

## 106.2 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 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

# 107 PKG

本节介绍包管理模块输出的日志信息。

## 107.1 PKG\_BOOTLOADER\_FILE\_FAILED

日志内容	Failed to execute the boot-loader file command.
参数解释	无
日志等级	5
举例	PKG/5/PKG_BOOTLOADER_FILE_FAILED: -IPAddr=192.168.79.1-User=**; Failed to execute the boot-loader file command.
日志说明	用户执行boot-loader file命令配置设备下次启动时使用的软件包, 操作失败
处理建议	请根据提示信息采取相应措施

## 107.2 PKG\_BOOTLOADER\_FILE\_SUCCESS

日志内容	Executed the boot-loader file command successfully.
参数解释	无
日志等级	5
举例	PKG/5/PKG_BOOTLOADER_FILE_SUCCESS: -IPAddr=192.168.79.1-User=**; Executed the boot-loader file command successfully.
日志说明	用户执行 <b>boot-loader file</b> 命令配置设备下次启动时使用的软件包，操作成功
处理建议	无

## 107.3 PKG\_INSTALL\_ACTIVATE\_FAILED

日志内容	Failed to execute the install activate command.
参数解释	无
日志等级	5
举例	PKG/5/PKG_INSTALL_ACTIVATE_FAILED: -IPAddr=192.168.79.1-User=**; Failed to execute the install activate command.
日志说明	用户执行 <b>install activate</b> 命令用来激活或查看软件包，操作失败
处理建议	请根据提示信息采取相应措施

## 107.4 PKG\_INSTALL\_ACTIVATE\_SUCCESS

日志内容	Executed the install activate command successfully.
参数解释	无
日志等级	5
举例	PKG/5/PKG_INSTALL_ACTIVATE_SUCCESS: -IPAddr=192.168.79.1-User=**; Executed the install activate command successfully.
日志说明	用户执行 <b>install activate</b> 命令用来激活或查看软件包，操作成功
处理建议	无

# 108 PKI

本节包含 PKI 日志消息。

## 108.1 GET\_CERT\_FROM\_CA\_SERVER\_FAIL

日志内容	Failed to get the CA or RA certificate from the CA server. Reason: [STRING].
参数解释	<p>\$1: 失败原因</p> <ul style="list-style-type: none"><li>• 获取 PKI 的源 IP 地址失败，显示为：failed to get the source IP address of PKI protocol packets.</li><li>• 获取证书链失败，显示为：failed to get the certificate chain.</li><li>• 证书链没有根 CA，显示为：root CA not found in the certificate chain.</li><li>• 验证 CA/RA 证书链失败，显示为：failed to verify the CA/RA certificate chain (%s).</li></ul>
日志等级	5
举例	PKI/5/GET_CERT_FROM_CA_SERVER_FAIL: Failed to get the CA or RA certificate from the CA server. Reason: root CA not found in the certificate chain.
日志说明	命令行从CA服务器获取CA/RA证书时失败
处理建议	无

## 108.2 IMPORT\_CERT\_FAIL

日志内容	Failed to import the certificate. Reason: [STRING].
参数解释	<p>\$1: 失败原因</p> <ul style="list-style-type: none"><li>● 获取颁发者证书失败, 显示为: unable to get issuer certificate.</li><li>● 无法获取证书的 CRL, 显示为: unable to get certificate CRL.</li><li>● 无法解密 CRL 的签名, 显示为: unable to decrypt CRL's signature.</li><li>● 无法解析颁发者的公钥, 显示为: unable to decode issuer public key.</li><li>● 证书签名错误, 显示为: certificate signature failure.</li><li>● CRL 签名失败, 显示为: CRL signature failure.</li><li>● 解密证书签名失败, 显示为: unable to decrypt certificate's signature.</li><li>● 证书尚未生效, 显示为: certificate is not yet valid.</li><li>● 证书已失效, 显示为: certificate has expired.</li><li>● CRL 尚未生效, 显示为: CRL is not yet valid.</li><li>● CRL 已经失效, 显示为: CRL has expired.</li><li>● 证书的起始时间格式错误, 显示为: format error in certificate's notBefore field.</li><li>● 证书的结束时间格式错误, 显示为: format error in certificate's notAfter field.</li><li>● CRL 的上次更新时间格式错误, 显示为: format error in CRL's lastUpdate field.</li><li>● CRL 的下次更新时间格式错误, 显示为: format error in CRL's nextUpdate field.</li><li>● 内存不足, 显示为: out of memory.</li><li>● 自签名证书, 显示为: self signed certificate.</li><li>● 证书链中存在自签名证书, 显示为: self signed certificate in certificate chain.</li><li>● 获取本地颁发者证书失败, 显示为: unable to get local issuer certificate.</li><li>● 验证首个证书失败, 显示为: unable to verify the first certificate.</li><li>● 证书链过长, 显示为: certificate chain too long.</li><li>● 证书被撤回, 显示为: certificate revoked.</li><li>● 无效的 CA 证书, 显示为: invalid CA certificate.</li><li>● 无效的非 CA 证书, 显示为: invalid non-CA certificate (has CA markings).</li><li>● 超过路径深度约束, 显示为: path length constraint exceeded.</li><li>● 超过代理路径深度约束, 显示为: proxy path length constraint exceeded.</li><li>● 代理证书不通过, 请设置合适的标记, 显示为: proxy certificates not allowed, please set the appropriate flag.</li><li>● 不支持的证书用途, 显示为: unsupported certificate purpose.</li><li>● 证书不被信任, 显示为: certificate not trusted.</li><li>● 证书被拒绝, 显示为: certificate rejected.</li><li>● 证书应用验证失败, 显示为: application verification failure.</li><li>● 证书主题颁发者不匹配, 显示为: subject issuer mismatch.</li><li>● 授权和主题密钥认证人不匹配, 显示为: authority and subject key identifier mismatch.</li><li>● 授权和颁发者序列号不匹配, 显示为: authority and issuer serial number mismatch.</li></ul>

日志内容	Failed to import the certificate. Reason: [STRING].
	<ul style="list-style-type: none"> <li>• 密钥用途不包括证书签名, 显示为: key usage does not include certificate signing.</li> <li>• 获取 CRL 颁发者证书失败, 显示为: unable to get CRL issuer certificate.</li> <li>• 不受控的决定性的扩展, 显示为: unhandled critical extension.</li> <li>• 密钥用途不包括 CRL 签名, 显示为: key usage does not include CRL signing.</li> <li>• 密钥用途不包括数字签名, 显示为: key usage does not include digital signature.</li> <li>• 不受控的决定性的 CRL 扩展, 显示为: unhandled critical CRL extension.</li> <li>• 无效或不一致的证书扩展, 显示为: invalid or inconsistent certificate extension.</li> <li>• 无效或不一致的证书策略扩展, 显示为: invalid or inconsistent certificate policy extension.</li> <li>• 不存在明确的策略, 显示为: no explicit policy.</li> <li>• CRL 范围不同, 显示为: Different CRL scope.</li> <li>• 不支持的扩展特性, 显示为: Unsupported extension feature.</li> <li>• RFC 3779 资源不是父资源的子集, 显示为: RFC 3779 resource not subset of parent's resources.</li> <li>• 被允许的子树违规, 显示为: permitted subtree violation.</li> <li>• 被排除的子树违规, 显示为: excluded subtree violation.</li> <li>• 名字约束的最小和最大范围不支持, 显示为: name constraints minimum and maximum not supported.</li> <li>• 不支持的名字约束类型, 显示为: unsupported name constraint type.</li> <li>• CRL 路径检验失败, 显示为: CRL path validation error.</li> <li>• 不支持的或无效的名字语法, 显示为: unsupported or invalid name syntax.</li> <li>• 不支持的或无效的名字约束语法, 显示为: unsupported or invalid name constraint syntax.</li> <li>• Suite B: 证书版本号无效, 显示为: Suite B: certificate version invalid.</li> <li>• Suite B: 无效的公钥算法, 显示为: Suite B: invalid public key algorithm.</li> <li>• Suite B: 无效的 ECC 曲线, 显示为: Suite B: invalid ECC curve.</li> <li>• Suite B: 无效的签名算法, 显示为: Suite B: invalid signature algorithm.</li> <li>• Suite B: 曲线不被本 LOS 准许, 显示为: Suite B: curve not allowed for this LOS.</li> <li>• Suite B: 不能使用 P-256 给 P-384 签名, 显示为: Suite B: cannot sign P-384 with P-256.</li> <li>• 主机名不匹配, 显示为: Hostname mismatch.</li> <li>• 邮件地址簿匹配, 显示为: Email address mismatch.</li> <li>• IP 地址不匹配, 显示为: IP address mismatch.</li> <li>• 无效的证书认证上下文, 显示为: Invalid certificate verification context.</li> <li>• 颁发者证书检查失败, 显示为: Issuer certificate lookup error.</li> <li>• 代理主题名称不规范, 显示为: proxy subject name violation.</li> </ul>
日志等级	5
举例	PKI/5/IMPORT_CERT_FAIL: failed to import the certificate. Reason: invalid CA certificate.
日志说明	执行导入命令时可能的失败, 原因为证书无效等
处理建议	无

### 108.3 REQUEST\_CERT\_FAIL

日志内容	Failed to request certificate of domain [STRING].
参数解释	\$1: PKI域名
日志等级	5
举例	PKI/5/REQUEST_CERT_FAIL: Failed to request certificate of domain abc.
日志说明	为PKI域申请证书失败
处理建议	检查设备和CA服务器的配置和其间的网络

### 108.4 REQUEST\_CERT\_SUCCESS

日志内容	Request certificate of domain [STRING] successfully.
参数解释	\$1: PKI域名
日志等级	5
举例	PKI/5/REQUEST_CERT_SUCCESS: Request certificate of domain abc successfully.
日志说明	为PKI域申请证书成功
处理建议	无



## 108.5 RETRIEVE\_CRL\_FAIL

日志内容	Failed to retrieve the CRL. Reason: [STRING].
参数解释	<p>\$1: 失败原因:</p> <ul style="list-style-type: none"> <li>• 证书请求 URL 未配置, 显示为: certificate request URL is not configured.</li> <li>• 本地证书不存在, 显示为: no local certificate.</li> <li>• 从 RA 服务器获取 CRL 时, RA 证书不存在, 显示为: no RA certificate.</li> <li>• 证书申请的注册受理机构未配置, 显示为: type of certificate request reception authority is not configured.</li> <li>• 获取 PKI 的源 IP 地址失败, 显示为: failed to get the source IP address of PKI protocol packets.</li> <li>• 本地证书和密钥不匹配, 显示为: local certificate and key mismatch.</li> <li>• 获取加密证书失败, 显示为: failed to get the encryption certificate.</li> <li>• 从 CA 获取证书签发者失败, 显示为: failed to get issuer name from CA certificate.</li> <li>• 从 CA 证书获取 CA 证书的序列号失败, 显示为: failed to get serial number from CA certificate.</li> <li>• 解析 URL 失败, 显示为: failed to parse the URL.</li> <li>• 从回应消息中获取 CRL 失败, 显示为: failed to get CRLs from reply.</li> <li>• 从回应消息中获取 CRL 数据失败, 显示为: failed to get CRL data from the reply.</li> <li>• 获取本地颁发者 CA 失败, 显示为: unable to get local issuer certificate.</li> <li>• CRL 签名失败, 显示为: CRL signature failure.</li> <li>• 解码颁发者公钥失败, 显示为: unable to decode issuer public key.</li> <li>• CRL 的上次更新时间格式错误, 显示为: Format error in CRL's lastUpdate field.</li> <li>• CRL 尚未生效, 显示为: CRL is not yet valid.</li> <li>• CRL 的下次更新时间格式错误, 显示为: Format error in CRL's nextUpdate field.</li> <li>• CRL 已经失效, 显示为: CRL has expired.</li> <li>• 获取颁发者证书失败, 显示为: unable to get issuer certificate.</li> <li>• 保存 CRL 到设备失败, 显示为: Failed to save the CRL to the device.</li> <li>• 无法获取证书的 CRL, 显示为: unable to get certificate CRL.</li> <li>• 无法解密 CRL 的签名, 显示为: unable to decrypt CRL's signature</li> </ul>
日志等级	5
举例	PKI/5/RETRIEVE_CRL_FAIL: Failed to retrieve the CRL. Reason: CRL has expired.
日志说明	取回CRL时的失败原因
处理建议	无

## 108.6 VALIDATE\_CERT\_FAIL

日志内容	Failed to validate the certificate. Reason: [STRING].
参数解释	<p>\$1: 失败原因</p> <ul style="list-style-type: none"><li>● 获取颁发者证书失败, 显示为: unable to get issuer certificate.</li><li>● 无法获取证书的 CRL, 显示为: unable to get certificate CRL.</li><li>● 无法解密 CRL 的签名, 显示为: unable to decrypt CRL's signature.</li><li>● 无法解析颁发者的公钥, 显示为: unable to decode issuer public key.</li><li>● 证书签名错误, 显示为: certificate signature failure.</li><li>● CRL 签名失败, 显示为: CRL signature failure.</li><li>● 解密证书签名失败, 显示为: unable to decrypt certificate's signature.</li><li>● 证书尚未生效, 显示为: certificate is not yet valid.</li><li>● 证书已失效, 显示为: certificate has expired.</li><li>● CRL 尚未生效, 显示为: CRL is not yet valid.</li><li>● CRL 已经失效, 显示为: CRL has expired.</li><li>● 证书的起始时间格式错误, 显示为: format error in certificate's notBefore field.</li><li>● 证书的结束时间格式错误, 显示为: format error in certificate's notAfter field.</li><li>● CRL 的上次更新时间格式错误, 显示为: format error in CRL's lastUpdate field.</li><li>● CRL 的下次更新时间格式错误, 显示为: format error in CRL's nextUpdate field.</li><li>● 内存不足, 显示为: out of memory.</li><li>● 自签名证书, 显示为: self signed certificate.</li><li>● 证书链中存在自签名证书, 显示为: self signed certificate in certificate chain.</li><li>● 获取本地颁发者证书失败, 显示为: unable to get local issuer certificate.</li><li>● 验证首个证书失败, 显示为: unable to verify the first certificate.</li><li>● 证书链过长, 显示为: certificate chain too long.</li><li>● 证书被撤回, 显示为: certificate revoked.</li><li>● 无效的 CA 证书, 显示为: invalid CA certificate.</li><li>● 无效的非 CA 证书, 显示为: invalid non-CA certificate (has CA markings).</li><li>● 超过路径深度约束, 显示为: path length constraint exceeded.</li><li>● 超过代理路径深度约束, 显示为: proxy path length constraint exceeded.</li><li>● 代理证书不通过, 请设置合适的标记, 显示为: proxy certificates not allowed, please set the appropriate flag.</li><li>● 不支持的证书用途, 显示为: unsupported certificate purpose.</li><li>● 证书不被信任, 显示为: certificate not trusted.</li><li>● 证书被拒绝, 显示为: certificate rejected.</li><li>● 证书应用验证失败, 显示为: application verification failure.</li><li>● 证书主题颁发者不匹配, 显示为: subject issuer mismatch.</li><li>● 授权和主题密钥认证人不匹配, 显示为: authority and subject key identifier mismatch.</li><li>● 授权和颁发者序列号不匹配, 显示为: authority and issuer serial number mismatch.</li></ul>

日志内容	Failed to validate the certificate. Reason: [STRING].
	<ul style="list-style-type: none"> <li>• 密钥用途不包括证书签名, 显示为: key usage does not include certificate signing.</li> <li>• 获取 CRL 颁发者证书失败, 显示为: unable to get CRL issuer certificate.</li> <li>• 不受控的决定性的扩展, 显示为: unhandled critical extension.</li> <li>• 密钥用途不包括 CRL 签名, 显示为: key usage does not include CRL signing.</li> <li>• 密钥用途不包括数字签名, 显示为: key usage does not include digital signature.</li> <li>• 不受控的决定性的 CRL 扩展, 显示为: unhandled critical CRL extension.</li> <li>• 无效或不一致的证书扩展, 显示为: invalid or inconsistent certificate extension.</li> <li>• 无效或不一致的证书策略扩展, 显示为: invalid or inconsistent certificate policy extension.</li> <li>• 不存在明确的策略, 显示为: no explicit policy.</li> <li>• CRL 范围不同, 显示为: Different CRL scope.</li> <li>• 不支持的扩展特性, 显示为: Unsupported extension feature.</li> <li>• RFC 3779 资源不是父资源的子集, 显示为: RFC 3779 resource not subset of parent's resources.</li> <li>• 被允许的子树违规, 显示为: permitted subtree violation.</li> <li>• 被排除的子树违规, 显示为: excluded subtree violation.</li> <li>• 名字约束的最小和最大范围不支持, 显示为: name constraints minimum and maximum not supported.</li> <li>• 不支持的名字约束类型, 显示为: unsupported name constraint type.</li> <li>• CRL 路径检验失败, 显示为: CRL path validation error.</li> <li>• 不支持的或无效的名字语法, 显示为: unsupported or invalid name syntax.</li> <li>• 不支持的或无效的名字约束语法, 显示为: unsupported or invalid name constraint syntax.</li> <li>• Suite B: 证书版本号无效, 显示为: Suite B: certificate version invalid.</li> <li>• Suite B: 无效的公钥算法, 显示为: Suite B: invalid public key algorithm.</li> <li>• Suite B: 无效的 ECC 曲线, 显示为: Suite B: invalid ECC curve.</li> <li>• Suite B: 无效的签名算法, 显示为: Suite B: invalid signature algorithm.</li> <li>• Suite B: 曲线不被本 LOS 准许, 显示为: Suite B: curve not allowed for this LOS.</li> <li>• Suite B: 不能使用 P-256 给 P-384 签名, 显示为: Suite B: cannot sign P-384 with P-256.</li> <li>• 主机名不匹配, 显示为: Hostname mismatch.</li> <li>• 邮件地址簿匹配, 显示为: Email address mismatch.</li> <li>• IP 地址不匹配, 显示为: IP address mismatch.</li> <li>• 无效的证书认证上下文, 显示为: Invalid certificate verification context.</li> <li>• 颁发者证书检查失败, 显示为: Issuer certificate lookup error.</li> <li>• 代理主题名称不规范, 显示为: proxy subject name violation.</li> </ul>
日志等级	5
举例	PKI/5/VALIDATE_CERT_FAIL: Failed to validate certificate. Reason: Invalid CA certificate.
日志说明	执行验证命令时可能的失败, 原因为证书无效等
处理建议	无

# 109 PKT2CPU

本节包含 PKT2CPU 日志消息。

## 109.1 PKT2CPU\_NO\_RESOURCE

日志内容	-Interface=[STRING]-ProtocolType=[UINT32]-MacAddr=[STRING]; The resources are insufficient. -Interface=[STRING]-ProtocolType=[UINT32]-SrcPort=[UINT32]-DstPort=[UINT32]; The resources are insufficient.
参数解释	\$1: 接口名 \$2: 协议类型 \$3: MAC地址或源端口 \$4: 目的端口
日志等级	4
举例	PKT2CPU/4/PKT2CPU_NO_RESOURCE: -Interface=Ethernet0/0/2-ProtocolType=21-MacAddr=0180-c200-0014; The resources are insufficient.
日志说明	硬件资源不足
处理建议	取消配置

# 110 PKTCPT

本节介绍 PKTCPT（Packet Capture）模块输出的日志信息。

## 110.1 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

## 110.2 PKTCPT\_ALREADY\_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_ALREADY_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

## 110.3 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	<ul style="list-style-type: none"><li>• 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</li><li>• 检查 URL 中域名解析是否成功</li><li>• 检查开启报文捕获服务设备与 FTP 服务器是否可达</li><li>• 检查 FTP 服务器是否上线</li></ul>

## 110.4 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_INVALID_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

## 110.5 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

## 110.6 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

## 110.7 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	<ul style="list-style-type: none"><li>• 若用户不具有写文件权限，请配置写权限</li><li>• 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</li></ul>

## 110.8 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	<ul style="list-style-type: none"><li>• 检查 FTP 服务器是否可达</li><li>• 检查 FTP 服务器是否在线</li></ul>

## 110.9 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	<ul style="list-style-type: none"><li>• 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</li><li>• 绑定新的端口号，重新启动报文捕获功能</li></ul>

## 110.10 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

## 110.11 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	<ul style="list-style-type: none"><li>• 检查是否试图改变 FTP 的工作目录</li><li>• 检查指定 FTP 服务器上文件是否有写权限</li><li>• 检查 FTP 服务器是否下线</li><li>• 检查与 FTP 服务器是否可达</li><li>• 检查 FTP 服务器是否已满</li><li>• 检查报文捕获服务是否退出</li></ul>

## 110.12 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

# 111 PoE

本节介绍 PoE 模块输出的日志信息。



## 111.1 POE\_AI\_CLEAR

日志内容	Clearing all preceding AI configurations on PoE port [STRING]. Reason: The port still cannot supply power to the PD after forced power supply has been enabled on the port.
参数解释	\$1: PoE接口名称
日志等级	6
举例	POE/6/POE_AI_CLEAR: Recover the ai PoE configuration on the PoE port GigabitEthernet1/0/1. Reason: The port still cannot supply power to the PD after forced power supply has been enabled on the port.
日志说明	开启PoE接口强制供电，处于未供电状态，清除之前的所有AI PoE配置
处理建议	请检查PoE接口到PD之间的链路是否存在硬件故障

## 111.2 POE\_AI\_DETECTIONMODE\_NONE

日志内容	Changing the PD detection mode for PoE port [STRING] to none. Reason: The port still cannot supply power to the PD after the PD detection mode has been changed to simple.
参数解释	\$1: PoE接口名称
日志等级	6
举例	POE/6/POE_AI_DETECTIONMODE_NONE: Changing the PD detection mode for PoE port GigabitEthernet1/0/1 to none. Reason: The port still cannot supply power to the PD after the PD detection mode has been changed to simple.
日志说明	修改对PD支持标准的检测方式为简单检测方式仍无法恢复PoE供电，修改对PD支持标准的检测方式为不检测尝试恢复PoE供电
处理建议	无

## 111.3 POE\_AI\_DETECTIONMODE\_SIMPLE

日志内容	Changing the PD detection mode for PoE port [STRING] to simple. Reason: The port still cannot supply power to the PD after non-standard PD detection is enabled.
参数解释	\$1: PoE接口名称
日志等级	6
举例	POE/6/POE_AI_DETECTIONMODE_SIMPLE: Changing the PD detection mode for PoE port GigabitEthernet1/0/1 to <b>simple</b> . Reason: The port still cannot supply power to the PD after non-standard PD detection is enabled.
日志说明	开启接口的非标准PD检测功能仍无法恢复PoE供电，修改对PD支持标准的检测方式为简单检测方式尝试恢复PoE供电
处理建议	无

## 111.4 POE\_AI\_DISCONNECT\_AC

日志内容	Changing from MPS detection to AC detection on PoE port [STRING]. Reason: The port still cannot supply power to the PD after MPS detection is delayed.
参数解释	\$1: PoE接口名称
日志等级	6
举例	POE/6/POE_AI_DISCONNECT_AC: Changing from MPS detection to AC detection on PoE port GigabitEthernet1/0/1. Reason: The port still cannot supply power to the PD after MPS detection is delayed.
日志说明	延迟启动MPS电流检测时间无法恢复PoE接口供电，切换MPS电流检测为AC检测
处理建议	无

## 111.5 POE\_AI\_DISCONNECT\_DELAY

日志内容	Delaying the MPS detection on PoE port [STRING]. Reason: The port has stopped power supply because of MPS current insufficiency.
参数解释	\$1: PoE接口名称
日志等级	6
举例	POE/6/POE_AI_DISCONNECT_DELAY:Delaying the MPS detection on PoE port GigabitEthernet1/0/1. Reason: The port has stopped power supply because of MPS current insufficiency.
日志说明	PoE接口处于供电状态的情况下发生掉电时，系统检测到掉电原因为MPS电流过小导致PSE认为PD已经拔出而关断电压输出，则延迟启动MPS电流检测时间尝试恢复供电
处理建议	无

## 111.6 POE\_AI\_FORCE\_PoE

日志内容	Enabling forced power supply on PoE port [STRING]. Reason: The port still cannot supply power to the PD after the PD detection mode has been changed to none.
参数解释	\$1: PoE接口名称
日志等级	6
举例	POE/6/POE_AI_FORCE_PoE: Enabling forced power supply on PoE port GigabitEthernet1/0/1. Reason: The port still cannot supply power to the PD after the PD detection mode has been changed to none.
日志说明	修改对PD支持标准的检测方式为不检测仍无法恢复PoE供电，开启PoE接口强制供电
处理建议	无

## 111.7 POE\_AI\_HIGH\_INRUSH

日志内容	Increasing the inrush current threshold for PoE port [STRING]. Reason: The port has stopped power supply because of a high inrush current.
参数解释	无
日志等级	6
举例	POE/6/POE_AI_HIGH_INRUSH:Increasing the inrush current threshold for PoE port GigabitEthernet1/0/1. Reason: The port has stopped power supply because of a high inrush current.
日志说明	PoE接口处于供电状态的情况下发生掉电时，系统检测到掉电原因为Inrush冲击电流过大，自动提高Inrush冲击电流阈值允许高冲击电流通过
处理建议	无

## 111.8 POE\_AI\_LEGACY

日志内容	Enabling non-standard PD detection on PoE port [STRING]. Reason: The port cannot supply power to the PD.
参数解释	\$1: PoE接口名称
日志等级	6
举例	POE/6/POE_AI_LEGACY:Enabling non-standard PD detection on PoE port GigabitEthernet1/0/1. Reason: The port cannot supply power to the PD.
日志说明	检测到PoE接口未进入供电状态，开启接口的非标准PD检测功能尝试恢复PoE供电
处理建议	无

## 111.9 POE\_AI\_MAXPOWER

日志内容	Increasing the maximum power of PoE port [STRING] to [UINT32]. Reason: An instant power surge has caused overload self-protection of the port
参数解释	\$1: PoE接口名称 \$2: 最大输出功率值
日志等级	6
举例	POE/6/POE_AI_MAXPOWER:Increasing the maximum power of PoE port GigabitEthernet1/0/1 to 2000. Reason: An instant power surge has caused overload self-protection of the port.
日志说明	PoE接口处于供电状态的情况下发生掉电时，系统检测到掉电原因为瞬间功率过大导致过载保护，提高PoE接口的最大供电功率
处理建议	无

## 111.10 POE\_AI\_RESTART

日志内容	Re-enabling PoE on port [STRING]. Reason: The power consumption of the port is 0.
参数解释	\$1: PoE接口名称
日志等级	6
举例	POE/6/POE_AI_RESTART:Re-enabling PoE on port GigabitEthernet1/0/1. Reason: The power consumption of the port is 0.
日志说明	PoE接口处于供电状态，但功率消耗为0，复位接口的PoE供电功能
处理建议	无

# 112 PORTAL

本节介绍 PORTAL 模块输出的日志信息。

## 112.1 PORTAL\_RULE\_FAILED

日志内容	Failed to assign a portal rule. Reason=[STRING].
参数解释	\$1: Portal规则下发失败的原因
日志等级	4
举例	PORTAL/4/PORTAL_RULE_FAILED: -Slot=10; Failed to assign a portal rule. Reason=Not enough resources.
日志说明	Portal规则下发失败
处理建议	请根据规则下发失败的原因选择相应的处理方式，详见 <a href="#">表112-1</a>

表112-1 规则下发失败原因列表

规则下发失败原因	说明	处理建议
Portal failed to assign a rule to the driver.	规则下发驱动失败	请将相关日志信息保存到本地，并联系UNIS技术支持
Input parameters in the rule are incorrect.	下发驱动的规则的参数有问题	请将相关日志信息保存到本地，并联系UNIS技术支持
The rule already exists.	驱动已经存在该条规则	请将相关日志信息保存到本地，并联系UNIS技术支持
The driver doesn't support rule assignment.	驱动不支持	请确认产品是否支持。如果支持，请保存相关日志信息并联系UNIS技术支持
Not enough resources.	驱动资源不足	使用 <b>display qos-acl resource</b> 命令检查硬件资源使用情况 释放一部分硬件资源

# 113 PORTSEC

本节介绍端口安全模块输出的日志信息。

## 113.1 PORTSEC\_ACL\_FAILURE

日志内容	-IfName=[STRING]-MACAddr=[STRING]; ACL authorization failed because[STRING].
参数解释	<p>\$1: 接口名 \$2: MAC地址 \$3: 下发ACL失败的原因, 包括如下取值:</p> <ul style="list-style-type: none"><li>the specified ACL didn't exist.: 下发的 ACL 不存在</li><li>this type of ACL is not supported.: 不支持此 ACL 类型</li><li>hardware resources were insufficient.: 资源不足</li><li>the specified ACL conflicted with other ACLs applied to the interface.: 下发的 ACL 与接口上应用的其他 ACL 冲突</li><li>the specified ACL didn't contain any rules.: 下发的 ACL 中未包含规则</li><li>unknown error.: 未知原因</li></ul>
日志等级	4
举例	PORTSEC/4/PORTSEC_ACL_FAILURE:-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9; ACL authorization failed because the specified ACL didn't exist.
日志说明	下发授权ACL失败, 及其原因
处理建议	根据失败原因修改配置

## 113.2 PORTSEC\_CAR\_FAILURE

日志内容	-IfName=[STRING]-MACAddr=[STRING]; Failed to assign CAR attributes to driver.
参数解释	\$1: 接口名 \$2: MAC地址
日志等级	5
举例	PORTSEC/5/PORTSEC_CAR_FAILURE:-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9; Failed to assign CAR attributes to driver.
日志说明	下发CAR到驱动失败
处理建议	无

## 113.3 PORTSEC\_CREATEAC\_FAILURE

日志内容	-IfName=[STRING]-VLANID=[STRING]-MACAddr=[STRING]-VSName=[STRING]; Failed to map an Ethernet service instance to the VSI.
参数解释	\$1: 接口名 \$2: VLAN \$3: MAC地址 \$4: VSI 名称
日志等级	3
举例	PORTSEC/3/PORTSEC_CREATEAC_FAILURE:-IfName=GigabitEthernet1/0/4-VLANID=444-MACAddr=0010-8400-22b9-VSName=aaa; Failed to map an Ethernet service instance to the VSI.
日志说明	端口安全模块接收到相关授权信息或者从其子线程模块收到将以以太网服务实例与VSI绑定的信息后，执行该操作，如果操作失败则输出此日志信息
处理建议	使用 <b>display l2vpn vsi</b> 命令查询VSI Name是否存在，如果不存在，请通过 <b>vsi</b> 命令创建对应的VSI

## 113.4 PORTSEC\_LEARNED\_MACADDR

日志内容	-IfName=[STRING]-MACAddr=[STRING]-VLANID=[STRING]; A new MAC address was learned.
参数解释	\$1: 接口名 \$2: MAC地址 \$3: VLAN ID
日志等级	6
举例	PORTSEC/6/PORTSEC_LEARNED_MACADDR:-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9-VLANID=444; A new MAC address was learned.
日志说明	学到一个新的安全MAC地址
处理建议	无

## 113.5 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

## 113.6 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

## 113.7 PORTSEC\_PROFILE\_FAILURE

日志内容	-IfName=[STRING]-MACAddr=[STRING]; Failed to assign a user profile to driver.
参数解释	\$1: 接口名 \$2: MAC地址
日志等级	5
举例	PORTSEC/5/PORTSEC_PROFILE_FAILURE:-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9; Failed to assign a user profile to driver.
日志说明	下发User Profile到驱动失败
处理建议	无

## 113.8 PORTSEC\_URL\_FAILURE

日志内容	-IfName=[STRING]-MACAddr=[STRING]; URL authorization failed because [STRING].
参数解释	\$1: 接口名 \$2: MAC地址 \$3: 下发URL失败的原因 <ul style="list-style-type: none"><li>o this operation was not supported: 不支持授权 URL</li><li>o hardware resources were insufficient: 资源不足</li><li>o parameters were invalid: 参数错误</li><li>o an unknown error existed: 其它错误</li></ul>
日志等级	4
举例	PORTSEC/5/PORTSEC_URL_FAILURE:-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9; URL authorization failed because hardware resources were insufficient.
日志说明	下发授权URL失败
处理建议	根据失败原因修改配置

## 113.9 PORTSEC\_VIOLATION

日志内容	-IfName=[STRING]-MACAddr=[STRING]-VLANID=[STRING]-IfStatus=[STRING]; Intrusion protection was triggered.
参数解释	\$1: 接口名 \$2: MAC地址 \$3: VLAN ID \$4: 接口状态
日志等级	5
举例	PORTSEC/5/PORTSEC_VIOLATION:-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9-VLANID=444-IfStatus=Up; Intrusion protection was triggered.
日志说明	触发入侵检测
处理建议	检查配置情况或改变端口安全模式



## 113.10 PORTSEC\_VLANMACLIMIT

日志内容	-IfName=[STRING]-MACAddr=[STRING]-VLANID=[STRING]; Maximum number of MAC addresses already reached in the VLAN.
参数解释	\$1: 接口名 \$2: MAC地址 \$3: VLAN ID
日志等级	5
举例	PORTSEC/5/PORTSEC_VLANMACLIMIT:-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9-VLANID=444; Maximum number of MAC addresses already reached in the VLAN.
日志说明	VLAN内同时接入的MAC地址数量达到上限，不允许新MAC地址用户接入
处理建议	检查是否存在来自未知源MAC的报文攻击端口

# 114 PPP

本节介绍 PPP 模块输出的日志信息。

## 114.1 IPOOL\_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/IPOOL_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

## 114.2 PPP\_USER\_LOGOFF

日志内容	-UserName=[STRING]-IPAddr=[IPADDR]-IfName=[STRING]-OutVlan=[UINT16]-InVlan=[UINT16]-MACAddr=[MAC]-Reason=[STRING]; User logged off.
参数解释	\$1: 用户名 \$2: IP地址 \$3: 接口名称 \$4: 外层Vlan \$5: 内层Vlan \$6: MAC地址 \$7: 下线原因, 取值请参见 <a href="#">表114-1</a>
日志等级	6
举例	PPP/6/PPP_USER_LOGOFF: -UserName=abc-IPAddr=1.1.1.2-IfName=Route-Aggregation1023.4000-OutVlan=1000-InVlan=4000-MACAddr=0230-0103-5601-Reason=Use request; User logged off.
日志说明	用户下线
处理建议	无

表114-1 下线原因列表

下线原因	说明
User request	用户主动要求终止连接
Lost carrier	协议保活报文丢失。 一般指BAS下一级网络设备（含该设备）到用户设备间的故障。
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
BAS error	由于BAS内部软件处理异常造成的用户掉线
BAS reboot	BAS异常重启前发送断线信息，以进行非管理性的重启
Admin reset	由于管理的需要，暂时中断用户的链接
BAS reboot	BAS异常重启前发送断线信息，以进行非管理性的重启
Admin reset	由于管理的需要，暂时中断用户的链接
BAS request	其它未规定的掉线原因
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
Server command	AAA服务器强制下线
Idle timeout	用户在规定时间内流量没有达到设定值
Account update fail	计费更新失败
Port error	BAS主动检测到用户接入端口的错误
Admin reboot	在重启BAS前，发送断线信息

## 114.3 PPP\_USER\_LOGON\_FAILED

日志内容	-UserName=[STRING]-IPAddr=[IPADDR]-IfName=[STRING]-OutVlan=[UINT16]-InVlan=[UINT16]-MACAddr=[MAC]-Reason=[STRING]; User got online failed.
参数解释	<p>\$1: 用户名</p> <p>\$2: IP地址</p> <p>\$3: 接口名称</p> <p>\$4: 外层Vlan</p> <p>\$5: 内层Vlan</p> <p>\$6: MAC地址</p> <p>\$7: 上线失败原因, 取值请参见<a href="#">表114-2</a></p>
日志等级	5
举例	PPP/5/PPP_USER_LOGON_FAILED: -UserName=abc-IPAddr=1.1.1.2-IfName=Route-Aggregation1023.4000-OutVlan=1000-InVlan=4000-MACAddr=0230-0103-5601-Reason=Authentication failed; User got online failed.
日志说明	用户上线失败
处理建议	<ul style="list-style-type: none"> <li>• 检查用户名和密码是否正确</li> <li>• 检查认证和计费服务器是否工作正常</li> <li>• 检查设备上地址池是否配置正确</li> </ul>

表114-2 上线失败原因列表

上线失败原因	说明
Authentication failed	认证失败
Authorization failed	授权失败
Assign IP failed	分配IP失败
Accounting failed	计费失败

## 114.4 PPP\_USER\_LOGON\_SUCCESS

日志内容	-UserName=[STRING]-IPAddr=[IPADDR]-IfName=[STRING]-OutVlan=[UINT16]-InVlan=[UINT16]-MACAddr=[MAC]; User got online successfully.
参数解释	\$1: 用户名 \$2: IP地址 \$3: 接口名称 \$4: 外层Vlan \$5: 内层Vlan \$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-OutVlan=1000-InVlan=4000-MACAddr=0230-0103-5601; User got online successfully.
日志说明	用户上线成功
处理建议	无

# 115 PTP

本节介绍 PTP 模块输出的日志信息。

## 115.1 PTP\_MASTER\_CLOCK\_CHANGE

日志内容	In PTP instance [UINT16], PTP master clock property changed. (OldMasterClockId=[STRING], CurrentMasterClockId=[STRING], NewSourceIndex=[UINT16], OldSourcePortNum=[UINT16], CurrentSourcePortNum=[UINT16], OldSourcePortName=[STRING], CurrentSourcePortName=[STRING])
参数解释	<p>\$1: PTP实例ID（PTP实例的支持情况与设备型号有关，请以设备实际情况为准）</p> <p>\$2: 原来主时钟ID</p> <p>\$3: 当前主时钟ID</p> <p>\$4: 新的时钟源索引</p> <p>\$5: 曾为本设备提供时钟源的接口编号</p> <p>\$6: 当前为本设备提供时钟源的接口编号</p> <p>\$7: 曾为本设备提供时钟源的接口名称</p> <p>\$8: 当前为本设备提供时钟源的接口名称</p>
日志等级	4
举例	PTP/4/PTP_MASTER_CLOCK_CHANGE: In PTP instance 1, PTP master clock property changed. (OldMasterClockId=000FE2-FFFE-FF0000, CurrentMasterClockId=000FE2-FFFE-FF0000, NewSourceIndex=1, OldSourcePortNum=2, CurrentSourcePortNum=1, OldSourcePortName=GigabitEthernet1/0/2, CurrentSourcePortName=GigabitEthernet1/0/1)
日志说明	<p>主时钟源属性发生改变，原因包括：</p> <ul style="list-style-type: none"> <li>○ PTP 域内的时钟设备属性发生变化，导致出现了优先级更高的时钟源或获取时钟源的路径发生了改变</li> <li>○ 接入了优先级更高的时钟源</li> <li>○ 接收时钟源信号的 PTP 接口所在链路故障或者 PTP 接口 DOWN</li> </ul>
处理建议	<p>使用<b>display ptp interface brief</b>命令查看是否存在PTP接口处于Disabled状态</p> <ul style="list-style-type: none"> <li>● 若存在接口处于 Disabled 状态，则表示该状态为 PTP 协议的错误状态（即检测到错误），接口不处理 PTP 协议报文；收集告警、日志和配置信息，联系技术支持</li> <li>● 若不存在接口处于 Disabled 状态，则查看 PTP 配置信息是否发生改变 <ul style="list-style-type: none"> <li>○ 若 PTP 配置信息发生改变，则恢复配置</li> <li>○ 若 PTP 配置信息未发生改变，则收集告警、日志和配置信息，联系技术支持</li> </ul> </li> </ul>

## 115.2 PTP\_PKTLOST

日志内容	In PTP instance [UINT16], PTP packets were lost. (PortName=[STRING], PktType=[STRING])
参数解释	<p>\$1: PTP实例ID（PTP实例的支持情况与设备型号有关，请以设备实际情况为准）</p> <p>\$2: 接口名称</p> <p>\$3: PTP报文类型，取值包括：</p> <ul style="list-style-type: none"><li>○ Delay_Resp: PTP Delay_Resp 报文</li><li>○ Announce: PTP Announce 报文</li><li>○ Sync: PTP Sync 报文</li><li>○ Pdelay_Resp: PTP Pdelay_Resp 报文</li></ul>
日志等级	4
举例	PTP/4/PTP_PKTLOST: In PTP instance 1, PTP packets were lost. (PortName=GigabitEthernet1/0/1, PktType=Announce)
日志说明	Slave端口检测Announce、Delay_Resp、Sync报文，超过检测时间没有收到报文，则认为报文丢失
处理建议	<p>在打印该日志的PTP从时钟设备上使用<b>display ptp statistics</b>命令查看接收报文统计计数是否增长</p> <ul style="list-style-type: none"><li>● 若增长，则表示链路延时过长导致的超时，无须处理</li><li>● 若不增长，则在 PTP 主时钟设备使用 <b>display ptp statistics</b> 命令查看发送报文统计计数是否增长<ul style="list-style-type: none"><li>○ 若增长，则表示链路故障导致对端超时没收到报文，排除故障恢复链路</li><li>○ 若不增长，则收集告警、日志和配置信息，联系技术支持</li></ul></li></ul>

## 115.3 PTP\_PKTLOST\_RECOVER

日志内容	In PTP instance [UINT16], PTP packets lost were recovered. (PortName=[STRING], PktType=[STRING])
参数解释	<p>\$1: PTP实例ID（PTP实例的支持情况与设备型号有关，请以设备实际情况为准）</p> <p>\$2: 接口名称</p> <p>\$3: PTP报文类型，取值包括：</p> <ul style="list-style-type: none"> <li>○ Delay_Resp: PTP Delay_Resp 报文</li> <li>○ Announce: PTP Announce 报文</li> <li>○ Sync: PTP Sync 报文</li> <li>○ Pdelay_Resp: PTP Pdelay_Resp 报文</li> </ul>
日志等级	4
举例	PTP/4/PTP_PKTLOST_RECOVER: In PTP instance 1, PTP packets lost were recovered. (PortName=GigabitEthernet1/0/1, PktType =Announce)
日志说明	从PTP报文丢失告警状态中恢复正常。只有当Slave端口检测Announce、Delay_Resp、Sync报文超后又重新收到Announce、Delay_Resp报文或者超时时间过长设备自身由从时钟转变为主时钟时，才会打印此日志
处理建议	无

## 115.4 PTP\_PORT\_BMCINFO\_CHANGE

日志内容	In PTP instance [UINT16], PTP BMC info for port [UINT16] changed. (PortName=[STRING], PortSourceId=[STRING], PortSourcePortNum=[UINT16], PortSourceStepsRemoved=[UINT16], CurrentMasterClockId=[STRING])
参数解释	<p>\$1: PTP实例ID（PTP实例的支持情况与设备型号有关，请以设备实际情况为准）</p> <p>\$2: PTP接口索引</p> <p>\$3: PTP接口名称</p> <p>\$4: PTP接口接收到的时钟源ID</p> <p>\$5: PTP接口接收到的时钟源端口号</p> <p>\$6: PTP接口接收到的时钟源跳数</p> <p>\$7: 设备当前主时钟ID</p>
日志等级	5
举例	PTP/5/PTP_PORT_BMCINFO_CHANGE: In PTP instance 1, PTP BMC info for port 1 changed. (PortName=GigabitEthernet1/0/1, PortSourceId=000FE2-FFFE-FF0001, PortSourcePortNum=1, PortSourceStepsRemoved=5, CurrentMasterClockId=000FE2-FFFE-FF0000)
日志说明	PTP接口收到的时钟源ID、时钟源端口号或时钟源跳数等时钟源信息发生变化
处理建议	无

## 115.5 PTP\_PORT\_STATE\_CHANGE

日志内容	In PTP instance [UINT16], PTP port state changed. (IfIndex=[UINT16], PortName=[STRING], PortState=[STRING], OldPortState=[STRING])
参数解释	<p>\$1: PTP实例ID（PTP实例的支持情况与设备型号有关，请以设备实际情况为准）</p> <p>\$2: PTP接口索引</p> <p>\$3: PTP接口名称</p> <p>\$4: PTP接口当前的状态，取值包括：</p> <ul style="list-style-type: none"> <li>○ Master: 接口状态为 Master，对外发布时间信息</li> <li>○ Slave: 接口状态为 Slave，跟踪外部时间信息</li> <li>○ Passive: 接口状态为 Passive（接口收到对端的 Announce 报文后，计算出的状态），不跟踪外部时间信息，也不对外发布时间信息</li> <li>○ Listening: 接口状态为 Listening（接口初始化后，即进入 Listening 状态），不跟踪外部时间信息，也不对外发布时间信息</li> <li>○ Faulty: 接口状态为 Faulty，该状态为 PTP 协议的错误状态（即检测到错误），接口不处理 PTP 协议报文</li> <li>○ Initializing: 接口状态为 Initializing，接口位于初始化状态，接口不处理协议报文</li> <li>○ Premaster: 接口状态为 Premaster，Master 状态前的临时状态</li> <li>○ Disable: 接口状态为 Disabled，接口上 PTP 协议未运行，接口不处理协议报文</li> <li>○ Uncalibrated: 接口状态为 Uncalibrated，Slave 状态前的临时状态</li> </ul> <p>\$5: PTP接口变化前的状态，取值包括：</p> <ul style="list-style-type: none"> <li>○ Master: 接口状态为 Master，对外发布时间信息</li> <li>○ Slave: 接口状态为 Slave，跟踪外部时间信息</li> <li>○ Passive: 接口状态为 Passive（接口收到对端的 Announce 报文后，计算出的状态），不跟踪外部时间信息，也不对外发布时间信息</li> <li>○ Listening: 接口状态为 Listening（接口初始化后，即进入 Listening 状态），不跟踪外部时间信息，也不对外发布时间信息</li> <li>○ Faulty: 接口状态为 Faulty，该状态为 PTP 协议的错误状态（即检测到错误），接口不处理 PTP 协议报文</li> <li>○ Initializing: 接口状态为 Initializing，接口位于初始化状态，接口不处理协议报文</li> <li>○ Premaster: 接口状态为 Premaster，Master 状态前的临时状态</li> <li>○ Disable: 接口状态为 Disabled，接口上 PTP 协议未运行，接口不处理协议报文</li> <li>○ Uncalibrated: 接口状态为 Uncalibrated，Slave 状态前的临时状态</li> </ul>
日志等级	5
举例	PTP/5/PTP_PORT_STATE_CHANGE: In PTP instance 1, PTP port state changed. (IfIndex=1, PortName=GigabitEthernet1/0/1, PortState=Slave, OldPortState=Master)
日志说明	<p>PTP接口状态发生改变，原因包括：</p> <ul style="list-style-type: none"> <li>○ PTP 域内的时钟设备属性发生变化，比如优先级、时钟等级、时钟精度、接口的 NotSlave 属性等</li> <li>○ 接入了优先级更高的时钟源</li> <li>○ PTP 接口所在链路故障或者 PTP 接口 DOWN</li> </ul>
处理建议	<p>使用 <b>display ptp interface brief</b> 命令查看是否存在 PTP 接口处于 Fault 状态</p> <ul style="list-style-type: none"> <li>● 若存在接口处于 Fault 状态，则表示链路故障或接口 DOWN，排除故障恢复链路</li> </ul>



日志内容	In PTP instance [UINT16], PTP port state changed. (IfIndex=[UINT16], PortName=[STRING], PortState=[STRING], OldPortState=[STRING])
	<ul style="list-style-type: none"> <li>● 若不存在接口处于 Fault 状态，则查看 PTP 配置信息是否发生改变 <ul style="list-style-type: none"> <li>○ 若 PTP 配置信息发生改变，则恢复配置</li> <li>○ 若 PTP 配置信息未发生改变，则收集告警、日志和配置信息，联系技术支持</li> </ul> </li> </ul>

## 115.6 PTP\_SRC\_CHANGE

日志内容	In PTP instance [UINT16], PTP clock source property changed. (SourceName=[STRING], Priority1=[UCHAR], Priority2=[UCHAR], ClockClass=[UINT16], ClockAccuracy=[UINT16], ClockSourceType=[STRING])
参数解释	<p>\$1: PTP实例ID（PTP实例的支持情况与设备型号有关，请以设备实际情况为准）</p> <p>\$2: 时钟源，取值包括：</p> <ul style="list-style-type: none"> <li>○ Local: 本地时钟</li> <li>○ Tod1: 第一路 ToD 时钟</li> <li>○ Tod2: 第二路 ToD 时钟</li> </ul> <p>\$3: 第一优先级</p> <p>\$4: 第二优先级</p> <p>\$5: 时钟源的时间等级</p> <p>\$6: 时钟源的时间精度</p> <p>\$7: 最优时钟的时钟类别，取值包括：</p> <ul style="list-style-type: none"> <li>○ Atomic clock: 原子时钟</li> <li>○ GPS: Global Positioning System, 全球定位系统</li> <li>○ Handset: 手持设备</li> <li>○ Internal oscillator: 内部震荡器</li> <li>○ NTP: Network Time Protocol, 网络时间协议</li> <li>○ Other: 其他</li> <li>○ PTP: Precision Time Protocol, 精确时间协议</li> <li>○ Terrestrial radio: 陆基无线电</li> <li>○ Unknown: 未知</li> </ul>
日志等级	5
举例	PTP/5/PTP_SRC_CHANGE: In PTP instance 1, PTP clock source property changed. (SourceName=Tod1, Priority1=1, Priority2=2, ClockClass=6, ClockAccuracy=20, ClockSourceType=Atomic clock)
日志说明	<p>时钟源属性发生改变，原因包括：</p> <ul style="list-style-type: none"> <li>● 用户通过命令行改变时钟源属性</li> <li>● 接收到了精度更高的外接时钟源</li> </ul>
处理建议	无

## 115.7 PTP\_SRC\_SWITCH

日志内容	In PTP instance [UINT16], PTP clock source switched. (LastClockID=[STRING], CurrentClockID=[STRING])
参数解释	\$1: PTP实例ID (PTP实例的支持情况与设备型号有关, 请以设备实际情况为准) \$2: 原来的时钟源ID \$3: 当前的时钟源ID
日志等级	4
举例	PTP/4/PTP_SRC_SWITCH: In PTP instance 1, PTP clock source switched.(LastSource=000FE2-FFFE-FF0000, CurrentSource=000FE2-FFFE-FF0001)
日志说明	新的更好的时钟源加入PTP域, 设备跟踪的时钟源发生切换
处理建议	无

## 115.8 PTP\_TIME\_LOCK

日志内容	Time resumed to locked state.
参数解释	无
日志等级	3
举例	PTP/3/PTP_TIME_LOCK: Time resumed to locked state.
日志说明	时钟从失锁状态中恢复为正常
处理建议	无

## 115.9 PTP\_TIME\_NOT\_LOCK

日志内容	Time not in locked state.
参数解释	无
日志等级	3
举例	PTP/3/PTP_TIME_NOT_LOCK: Time not in locked state.
日志说明	时钟失锁告警，原因包括： <ul style="list-style-type: none"><li>• 频率失锁</li><li>• 子卡或者时钟扣板故障</li><li>• DSP 收到的时间戳不变或者错误</li></ul>
处理建议	检查PTP Slave接口是否链路故障或接口DOWN： <ul style="list-style-type: none"><li>• 若链路故障或接口 DOWN，排除故障恢复链路</li><li>• 接口正常，则查看 PTP 配置信息是否发生改变<ul style="list-style-type: none"><li>◦ 若 PTP 配置信息发生改变，则恢复配置</li><li>◦ 若 PTP 配置信息未发生改变，则收集告警、日志和配置信息，联系技术支持</li></ul></li></ul>

# 116 PTS

本节介绍 PTS（Platform Trust Services，平台可信服务）模块输出的日志信息。

## 116.1 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）

## 116.2 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

## 116.3 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

## 116.4 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）

## 116.5 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

## 116.6 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

## 116.7 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

## 116.8 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	<ol style="list-style-type: none"><li>1. 依次执行 <b>undo pts</b> 和 <b>pts</b> 命令重启 PTS 服务</li><li>2. 如果问题仍然存在，请联系技术支持</li></ol>

## 116.9 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	<ol style="list-style-type: none"><li>1. 依次执行 <b>undo pts</b> 和 <b>pts</b> 命令重启 PTS 服务</li><li>2. 如果问题仍然存在，请联系技术支持</li></ol>

## 116.10 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

## 116.11 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	<ol style="list-style-type: none"><li>1. 依次执行 <code>undo pts</code> 和 <code>pts</code> 命令重启 PTS 服务</li><li>2. 如果问题仍然存在，请联系技术支持</li></ol>

## 116.12 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	<ol style="list-style-type: none"><li>1. 依次执行 <code>undo pts</code> 和 <code>pts</code> 命令重启 PTS 服务</li><li>2. 如果问题仍然存在，请联系技术支持</li></ol>

## 116.13 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	<ol style="list-style-type: none"><li>1. 依次执行 <code>undo pts</code> 和 <code>pts</code> 命令重启 PTS 服务</li><li>2. 如果问题仍然存在，请联系技术支持</li></ol>

## 116.14 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	<ul style="list-style-type: none"><li>• 请联系技术支持</li><li>• 可以通过 <code>integrity selfverify</code> 命令手动执行可信自检</li></ul>

## 116.15 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	<ol style="list-style-type: none"><li>1. 依次执行 <code>undo pts</code> 和 <code>pts</code> 命令重启 PTS 服务</li><li>2. 如果问题仍然存在，请联系技术支持</li></ol>

## 116.16 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	<ol style="list-style-type: none"><li>1. 依次执行 <code>undo pts</code> 和 <code>pts</code> 命令重启 PTS 服务</li><li>2. 如果问题仍然存在，请联系技术支持</li></ol>



## 116.17 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/lis 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

## 116.18 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	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 <b>display tcsn key name</b> ） 请联系技术支持

## 116.19 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	依次执行 <b>undo pts</b> 和 <b>pts</b> 命令重启PTS服务 如果问题仍然存在，请联系技术支持

## 116.20 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

## 116.21 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

## 116.22 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

## 116.23 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

## 116.24 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 tcsn trusted-computing-chip），确保TPM芯片可用

## 116.25 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	<ol style="list-style-type: none"><li>1. 尝试重新启动可信自检</li><li>2. 如果问题仍然存在，请联系技术支持</li></ol>

## 116.26 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/lis 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

# 117 PWDCTL

本节介绍 Password control 模块输出的日志信息。

## 117.1 PWDCTL\_ADD\_BLACKLIST

日志内容	[STRING] was added to the blacklist for failed login attempts.
参数解释	\$1: 用户名
日志等级	6
举例	PWDCTL/6/PWDCTL_ADD_BLACKLIST: hhh was added to the blacklist for failed login attempts.
日志说明	因为用户输入密码错误, 用户登录设备失败, 被加入密码控制黑名单
处理建议	无

## 117.2 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: <ul style="list-style-type: none"><li>o it was the first login of the account: 用户首次登录</li><li>o the password had expired: 密码已经过期</li><li>o the password was too short: 密码长度过短</li><li>o the password was not complex enough: 密码复杂度不满足要求</li><li>o the password was default password: 密码是缺省密码</li></ul>
日志等级	6
举例	PWDCTL/6/PWDCTL_CHANGE_PASSWORD: hhh changed the password because it was the first login of the account.
日志说明	由于某种原因, 用户改变用户密码。例如该用户的账户第一次登录设备
处理建议	无

## 117.3 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

## 117.4 PWDCTL\_FAILED\_PROCMMSG

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_PROCMMSG: 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

## 117.5 PWDCTL\_FAILED\_TO\_WRITEPWD

日志内容	Failed to write the password records to file.
参数解释	N/A
日志等级	3
举例	PWDCTL/3/PWDCTL_FAILED_TO_WRITEPWD: Failed to write the password records to file.
日志说明	设备无法将用户密码写入密码记录文件
处理建议	请检查设备文件系统存储空间是否充足

## 117.6 PWDCTL\_FAILED\_TO\_OPENFILE

日志内容	Failed to open the password file.
参数解释	N/A
日志等级	3
举例	PWDCTL/3/PWDCTL_FAILED_TO_OPENFILE: Failed to open the password file.
日志说明	因文件系统异常导致创建或打开*.dat文件失败
处理建议	无

## 117.7 PWDCTL\_NOENOUGHSPACE

日志内容	Not enough free space on the storage media where the file is located.
参数解释	N/A
日志等级	3
举例	PWDCTL/3/PWDCTL_NOENOUGHSPACE: Not enough free space on the storage media where the file is located.
日志说明	配置失败，因为*.dat文件所在介质（Flash或CF卡等）存储空间不足
处理建议	请检查设备文件系统存储空间是否充足

## 117.8 PWDCTL\_NOTFOUNDUSER

日志内容	Can't find the username in the file.
参数解释	无
日志等级	3
举例	PWDCTL/3/PWDCTL_NOTFOUNDUSER: Can't find the username in the file.
日志说明	本地用户密码设置失败，因为在*.dat文件中获取不到该用户信息
处理建议	重新创建一个本地用户或关闭Password Control功能后再重新开启Password Control功能

## 117.9 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

## 117.10 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

## 117.11 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

# 118 qos

本节介绍 QoS 模块输出的日志信息。

## 118.1 QOS\_MIRROR\_SYNC\_CFG\_FAIL

日志内容	Failed to restore configuration for monitoring group [UINT32] in [STRING], because [STRING]
参数解释	\$1: 监控组编号 \$2: chassis编号+slot编号或slot编号 \$3: 数据恢复失败的详细原因
日志等级	4
举例	QOS/4/MIRROR_SYNC_CFG_FAIL: Failed to restore configuration for monitoring group 1 in chassis 2 slot 1, because monitoring resources are insufficient.
日志说明	业务板插入设备后，恢复该业务板监控组数据失败。失败原因如下： <ul style="list-style-type: none"><li>• 监控端口总数超过当前监控组支持的最大数量</li><li>• 当前业务板监控资源不足</li><li>• 监控组中端口的类型在当前业务板不支持</li></ul>
处理建议	删除或者修改不支持配置



## 118.2 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
日志等级	4
举例	QOS/4/QOS_CAR_APPLYUSER_FAIL: -MAC=1111-2222-3333-IP=192.168.1.2-SVLAN=100-VPN="N/A"-Port=GigabitEthernet5/1/5; Failed to apply the inbound CAR in user profile a to the user. Reason: The resources are insufficient.
日志说明	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

## 118.3 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

## 118.4 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=1111-2222-3333-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

## 118.5 QOS\_IFA\_CONFIG\_FAIL

日志内容	Failed to configure [STRING].
参数解释	\$1: IFA具体配置，取值为： <ul style="list-style-type: none"><li>the collector: 下发 INT 报文的封装参数命令失败</li><li>the device ID: 下发 INT 设备的设备 ID 命令失败</li><li>packet dorp: 下发开启全局丢弃 INT 报文命令失败</li></ul>
日志等级	4
举例	QOS/4/QOS_IFA_CONFIG_FAIL: -Slot=2; Failed to configure the device ID.
日志说明	在Slot上下发INT配置失败
处理建议	接口板不支持该功能，请勿下发

## 118.6 QOS\_IFA\_REFRESH\_FAIL

日志内容	Failed to refresh IFA action [UINT32] on interface [STRING].
参数解释	\$1: INT动作的编号 \$2: 接口名称
日志等级	4
举例	QOS/4/QOS_IFA_REFRESH_FAIL: Failed to refresh IFA action 1 on interface GigabitEthernet1/0/1.
日志说明	将接口的INT动作下发驱动失败
处理建议	<ul style="list-style-type: none"><li>• 检查 INT 动作引用的 ACL 的配置是否正确</li><li>• 重新配置 INT 动作</li></ul>

## 118.7 QOS\_LR\_APPLYIF\_FAIL

日志内容	Failed to apply the rate limit on interface [STRING]. Reason: [STRING]
参数解释	\$1: 接口名称 \$2: 失败原因 <ul style="list-style-type: none"><li>◦ The operation is not supported.: 操作不支持</li><li>◦ The resources are insufficient.: 资源不足</li></ul>
日志等级	4
举例	QOS/4/QOS_LR_APPLYIF_FAIL: Failed to apply the rate limit on interface GigabitEthernet1/0/1. Reason: The operation is not supported.
日志说明	<ul style="list-style-type: none"><li>• 不支持在接口上配置限速</li><li>• 由于资源不足, 导致在接口上配置限速失败</li></ul>
处理建议	请根据失败原因, 取消接口上的限速配置或者修改接口限速的相关配置

## 118.8 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

## 118.9 QOS\_NOT\_ENOUGH\_NNIBANDWIDTH

日志内容	The total UNI bandwidth is greater than the NNI bandwidth. The total UNI bandwidth is greater than the NNI bandwidth.The bandwidth of [STRING] is changed. The total UNI bandwidth is greater than the NNI bandwidth.[STRING] is created based on [STRING] of the UNI interface.
参数解释	\$1: 接口名称
日志等级	4
举例	QOS/4/ QOS_NOT_ENOUGH_NNIBANDWIDTH: The total UNI bandwidth is greater than the NNI bandwidth. QOS/4/ QOS_NOT_ENOUGH_NNIBANDWIDTH: The total UNI bandwidth is greater than the NNI bandwidth. The bandwidth of GigabitEthernet4/0/1 is changed. QOS/4/ QOS_NOT_ENOUGH_NNIBANDWIDTH: The total UNI bandwidth is greater than the NNI bandwidth. Virtual-Access1 is created based on Virtual-Template1 of the UNI interface.
日志说明	<ul style="list-style-type: none"> <li>当用户增加上行接口带宽或降低下行接口带宽限速后，下行总带宽仍然大于上行带宽</li> <li>接口带宽改变导致下行接口总带宽大于上行接口总带宽</li> <li>新创建的动态子接口导致下行接口总带宽大于上行接口总带宽</li> </ul>
处理建议	增加上行接口带宽或降低下行接口带宽限速

## 118.10 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
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

## 118.11 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

## 118.12 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

## 118.13 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

## 118.14 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 <ul style="list-style-type: none"><li>○ The behavior is empty.: 流行为为空, 未配置任何动作</li><li>○ The card where the interface specified in the class-behavior association resides is not in position.: CB 对中配置的接口所在的单板不在位</li></ul>
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

## 118.15 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

## 118.16 QOS\_POLICY\_APPLYUSER\_FAIL

日志内容	[STRING]; Failed to apply the [STRING] QoS policy [STRING] in user profile [STRING] to the user.Reason: [STRING].
参数解释	\$1: 用户标识信息 \$2: QoS policy应用方向 \$3: QoS policy名称 \$4: User profile名称 \$5: 失败原因
日志等级	4
举例	QOS/4/QOS_POLICY_APPLYUSER_FAIL: -MAC=1111-2222-3333-IP=192.168.1.2/16-CVLAN=100-Port=GigabitEthernet5/1/5; Failed to apply the inbound QoS policy p in user profile a to the user.Reason: The QoS policy is not supported.
日志说明	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

## 118.17 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



## 118.18 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

## 118.19 QOS\_QMPROFILE\_APPLYIF\_FAIL

日志内容	Failed to apply queue management profile [STRING] on interface [STRING]. Reason: [STRING]
参数解释	\$1: 队列调度策略名称 \$2: 接口名称 \$3: 失败原因 <ul style="list-style-type: none"><li>○ The operation is not supported.: 操作不支持</li><li>○ The resources are insufficient.: 资源不足</li></ul>
日志等级	4
举例	QOS/4/QOS_QMPROFILE_APPLYIF_FAIL: Failed to apply queue management profile b on interface GigabitEthernet1/0/1. Reason: The operation is not supported.
日志说明	<ul style="list-style-type: none"><li>● 不支持在接口上应用队列调度策略</li><li>● 由于资源不足，导致在接口上应用队列调度策略失败</li></ul>
处理建议	请根据失败原因，取消队列调度策略在接口上的应用或者修改队列调度策略的相关配置

## 118.20 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=1111-2222-3333-IP=192.168.1.2/16-SVLAN=100-Port=GigabitEthernet5/1/5; Failed to apply queue management profile b in session group profile a to the user. Reason: The QMProfile is not supported.
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

## 118.21 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

## 118.22 QOS\_QUEUE\_APPLYIF\_FAIL

日志内容	Failed to apply queue scheduling on interface [STRING]. Reason: [STRING]
参数解释	\$1: 接口名称 \$2: 失败原因 <ul style="list-style-type: none"><li>The operation is not supported.: 操作不支持</li><li>The resources are insufficient.: 资源不足</li></ul>
日志等级	4
举例	QOS/4/QOS_QUEUE_APPLYIF_FAIL: Failed to apply queue scheduling on interface GigabitEthernet1/0/1. Reason: The operation is not supported.
日志说明	<ul style="list-style-type: none"><li>不支持在接口上进行队列配置</li><li>由于资源不足，导致在接口上进行队列配置失败</li></ul>
处理建议	请根据失败原因，取消接口上的队列配置或者修改队列配置的相关配置

## 118.23 QOS\_UNI\_RESTORE\_FAIL

日志内容	Failed to restore the UNI configuration of [STRING], because the total UNI bandwidth is greater than the NNI bandwidth.
参数解释	\$1: 接口名称
日志等级	4
举例	QOS/4/ QOS_NNIBANDWIDTH_OVERFLOW: Failed to restore the UNI configuration of the interface GigabitEthernet5/1/5, because the total UNI bandwidth is greater than the NNI bandwidth.
日志说明	恢复下行接口时，因下行接口上的CAR限速总和超过上行接口带宽，接口的下行接口功能恢复失败
处理建议	增加上行接口带宽或降低下行接口CAR限速总和后，重新使能下行口功能

## 118.24 QOS\_WRED\_TABLE\_APPLYFABRIC\_FAIL

日志内容	Failed to apply WRED table [STRING] to internal interfaces.Reason: [STRING].
参数解释	\$1: WRED表的名称 \$2: 下发和刷新配置失败的详细原因 <ul style="list-style-type: none"><li>Hardware resources are insufficient.: 业务板上资源不足</li><li>ECN is not supported.: 业务板内接口不支持应用 WRED 表</li></ul>
日志等级	4
举例	QOS/4/QOS_WRED_TABLE_APPLYFABRIC_FAIL: Failed to apply WRED table to internal interfaces.Hardware resources are insufficient.
日志说明	某些WRED配置在部分业务板上不支持或者业务板上资源不足
处理建议	调整业务板资源重新下发配置

## 118.25 QOS\_WRED\_TABLE\_CFG\_FAIL

日志内容	Failed to dynamically modify the configuration of WRED table [STRING], because [STRING].
参数解释	\$1: WRED表的名称 \$2: 配置失败的详细原因
日志等级	4
举例	QOS/4/WRED_TABLE_CFG_FAIL: Failed to dynamically modify the configuration of WRED table a, because ECN is not supported.
日志说明	由于各业务板支持特性不同, 某些配置在部分业务板上不支持
处理建议	无

# 119 RADIUS

本节介绍 RADIUS 模块输出的日志信息。

## 119.1 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	<ol style="list-style-type: none"><li>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。</li><li>2. 执行 <a href="http://localhost:7890/pages/30007870/01/30007870/01/resources/dc_ne_product_manual_v8r9c10/software/nev8r9_vrpv8r15/user/vrp/ping.html">http://localhost:7890/pages/30007870/01/30007870/01/resources/dc_ne_product_manual_v8r9c10/software/nev8r9_vrpv8r15/user/vrp/ping.html</a> 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。</li><li>3. 请收集日志信息和诊断信息, 并联系技术支持。</li></ol>

## 119.2 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

## 119.3 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服务器拒绝了用户的认证请求
处理建议	无

## 119.4 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	<ol style="list-style-type: none"><li>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。</li><li>2. 执行 <a href="http://localhost:7890/pages/30007870/01/30007870/01/resources/dc_ne_product_manual_v8r9c10/software/nev8r9_vrpv8r15/user/vrp/ping.html">http://localhost:7890/pages/30007870/01/30007870/01/resources/dc_ne_product_manual_v8r9c10/software/nev8r9_vrpv8r15/user/vrp/ping.html</a> 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。</li><li>3. 请收集日志信息和诊断信息, 并联系技术支持</li></ol>

## 119.5 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

## 119.6 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

## 119.7 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

# 120 RDDC

本节介绍 RDDC（冗余备份）模块输出的日志信息。

## 120.1 RDDC\_ACTIVENODE\_CHANGE

日志内容	Redundancy group [STRING] active node changed to [STRING], because of [STRING].
参数解释	<p>\$1: 冗余组名称</p> <p>\$2: 激活节点信息</p> <p>\$3: 状态变化原因</p> <ul style="list-style-type: none"><li>○ manual switchover: 表示状态变化由手动切换引起</li><li>○ group's configuration changed: 表示状态变化由冗余组配置变化引起</li><li>○ node's weight changed: 表示状态变化由冗余组节点权重变化引起</li></ul>
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

# 121 RESMON

本节介绍 RESMON（RESOURCE MONITOR，资源监控）模块输出的日志信息。



## 121.1 RESMON\_MINOR

日志内容	-Resource=[STRING]-Total=[STRING]-Used=[STRING]-Free=[STRING]; Free resource decreased to or below minor threshold [STRING]. [STRING].
参数解释	\$1: 资源名称 \$2: 资源总数 \$3: 当前已使用的资源数 \$4: 当前剩余的资源数 \$5: 低级别告警门限值 \$6: 资源的补充描述信息，部分资源可能无该描述信息
日志等级	4
举例	RESMON/4/RESMON_MINOR: -Resource=AA-Total=100%-Used=83%-Free=17%; Free resource decreased to or below minor threshold 20%.
日志说明	当资源剩余值小于或等于低级别告警门限时，资源进入低级别告警状态，并定期输出该日志
处理建议	请根据具体的资源类型操作设备，使资源得到合理分配

## 121.2 RESMON\_MINOR\_RECOVERY

日志内容	-Resource=[STRING]-Total=[STRING]-Used=[STRING]-Free=[STRING]; Free resource increased above minor threshold [STRING]. [STRING].
参数解释	\$1: 资源名称 \$2: 资源总数 \$3: 当前已使用的资源数 \$4: 当前剩余的资源数 \$5: 低级别告警门限值 \$6: 资源的补充描述信息，部分资源可能无该描述信息
日志等级	5
举例	RESMON/5/RESMON_MINOR_RECOVER: -Resource=AA-Total=100%-Used=77%-Free=23%; Free resource increased above minor threshold 20%.
日志说明	当资源处于低级别告警状态，且剩余值大于低级别告警门限，则资源解除低级别告警状态，并输出该日志。资源使用率进入正常范围
处理建议	无

## 121.3 RESMON\_SEVERE

日志内容	-Resource=[STRING]-Total=[STRING]-Used=[STRING]-Free=[STRING]; Free resource decreased to or below severe threshold [STRING]. [STRING].
参数解释	\$1: 资源名称 \$2: 资源总数 \$3: 当前已使用的资源数 \$4: 当前剩余的资源数 \$5: 高级别告警门限值 \$6: 资源的补充描述信息，部分资源可能无该描述信息
日志等级	3
举例	RESMON/3/RESMON_SEVERE: -Resource=AA-Total=100%-Used=93%-Free=7%; Free resource decreased to or below severe threshold 10%.
日志说明	当资源剩余值小于或等于高级别告警门限，且资源没有被使用完，则资源进入高级别告警状态，并定期输出该日志
处理建议	请根据具体的资源类型操作设备，使资源得到合理分配

## 121.4 RESMON\_SEVERE\_RECOVERY

日志内容	-Resource=[STRING]-Total=[STRING]-Used=[STRING]-Free=[STRING]; Free resource increased above severe threshold [STRING]. [STRING].
参数解释	\$1: 资源名称 \$2: 资源总数 \$3: 当前已使用的资源数 \$4: 当前剩余的资源数 \$5: 高级别告警门限值 \$6: 资源的补充描述信息，部分资源可能无该描述信息
日志等级	5
举例	RESMON/5/RESMON_SEVERE_RECOVER: -Resource=AA-Total=100%-Used=83%-Free=17%; Free resource increased above severe threshold 10%.
日志说明	当资源处于高级别告警状态，并且剩余值大于高级别告警门限时，解除高级别告警状态，并输出该日志
处理建议	无

## 121.5 RESMON\_USEDUP

日志内容	-Resource=[STRING]-Total=[STRING]-Used=[STRING]-Free=[STRING]; Resources used up. [STRING].
参数解释	\$1: 资源名称 \$2: 资源总数 \$3: 当前已使用的资源数 \$4: 当前剩余的资源数 \$5: 资源的补充描述信息, 部分资源可能无该描述信息
日志等级	2
举例	RESMON/2/RESMON_USEDUP: -Resource=vlaninterface-Total=2048-Used=2048-Free=0; Resources used up.
日志说明	当资源被使用完时, 资源进入用完状态, 并定期输出该日志
处理建议	请尽快清理资源中不用的数据或者表项, 以免对应业务受影响

## 121.6 RESMON\_USEDUP\_RECOVERY

日志内容	-Resource=[STRING]-Total=[STRING]-Used=[STRING]-Free=[STRING]; The amount of free resources increased from zero to a non-zero value. [STRING].
参数解释	\$1: 资源名称 \$2: 资源总个数, 当以绝对值显示时为INT32数值; 当以百分比显示时为100% \$3: 当前使用的资源个数, 当以绝对值显示时为INT32数值; 当以百分比显示时为xx% \$4: 当前剩余的资源个数, 当以绝对值显示时为INT32数值; 当以百分比显示时为xx% \$5: 产品对资源使用附加信息, 可能为空
日志等级	5
举例	RESMON/5/RESMON_USEDUP_RECOVER: -Resource=vlaninterface-Total=2048-Used=2047-Free=1; The amount of free resources increased from zero to a non-zero value.
日志说明	当资源处于用完状态, 且资源被释放, 则解除用完状态, 并输出该日志
处理建议	无

# 122 RIP

本节介绍 RIP 模块输出的日志信息。

## 122.1 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

## 122.2 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

# 123 RIPNG

本节介绍 RIPng 模块输出的日志信息。

## 123.1 RIPNG\_MEM\_ALERT

日志内容	RIPng 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	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

## 123.2 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

# 124 RM

本节介绍 RM 模块输出的日志信息。

## 124.1 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

## 124.2 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

## 124.3 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

## 124.4 RM\_TOTAL\_THRESHLD\_VALUE\_REACH

日志内容	Threshold value [UINT32] reached for active [STRING] routes in all URTs
参数解释	\$1: 最大激活路由数 \$2: IPv4或IPv6
日志等级	4
举例	RM/4/ RM_TOTAL_THRESHLD_VALUE_REACH: Threshold value 1000 reached for active IPv4 routes in all URTs
日志说明	公网和所有VPN实例的激活路由总数达到了告警值
处理建议	检查路由表确认是否需要进行相关处理

# 125 RPR

本节介绍 RPR 模块输出的日志信息。

## 125.1 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

## 125.2 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

## 125.3 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

## 125.4 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

## 125.5 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



## 125.6 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

## 125.7 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

## 125.8 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

## 125.9 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

## 125.10 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

## 125.11 RPR\_LAGGCONFIG\_INCONSISTENT

日志内容	An inconsistent LAGG configuration is present on the ring corresponding to RPR logical interface [STRING].
参数解释	\$1: RPR逻辑接口名称
日志等级	4
举例	RPR/4/RPR_LAGGCONFIG_INCONSISTENT: An inconsistent LAGG configuration is present on the ring corresponding to RPR logical interface RPR-Router1.
日志说明	RPR环上，本站点与邻居站点的RPR逻辑接口的聚合配置不一致
处理建议	使用 <b>display link-aggregation verbose</b> 命令检查本站点和邻居站点的RPR逻辑接口的聚合配置，确保本站点和邻居站点上的聚合配置保持一致

## 125.12 RPR\_LAGGCONFIG\_INCONSISTENT\_OVER

日志内容	An inconsistent LAGG configuration is cleared on the ring corresponding to RPR logical interface [STRING].
参数解释	\$1: RPR逻辑接口名称
日志等级	5
举例	RPR/5/RPR_LAGGCONFIG_INCONSISTENT: An inconsistent LAGG configuration is cleared on the ring corresponding to RPR logical interface RPR-Router1.
日志说明	RPR环上, 本站点与邻居站点的RPR逻辑接口的聚合配置已经更改为一致
处理建议	无

## 125.13 RPR\_MISCABLING

日志内容	A miscabling defect is present on ringlet0/ringlet1 corresponding to RPR logical interface [STRING].
参数解释	\$1: 接口名称
日志等级	3
举例	RPR/3/RPR_MISCABLING: A miscabling defect is present on ringlet0 corresponding to RPR logical interface RPR-Router1.
日志说明	站点的西向/东向边连接到了其它站点的西向/东向边
处理建议	检查站点与其它站点间的RPR物理端口是否连接错误

## 125.14 RPR\_MISCABLING\_OVER

日志内容	A miscabling defect is cleared on ringlet0/ringlet1 corresponding to RPR logical interface [STRING].
参数解释	\$1: 接口名称
日志等级	5
举例	RPR/5/RPR_MISCABLING_OVER: A miscabling defect is cleared on ringlet0 corresponding to RPR logical interface RPR-Router1.
日志说明	站点与其它站点间的RPR物理端口连接正确
处理建议	无

## 125.15 RPR\_PROTECTION\_INCONSISTENT

日志内容	A protection configuration defect is present on the ring corresponding to RPR logical interface [STRING].
参数解释	\$1: 接口名称
日志等级	3
举例	RPR/3/RPR_PROTECTION_INCONSISTENT: A protection configuration defect is present on the ring corresponding to RPR logical interface RPR-Router1.
日志说明	RPR环上至少两个站点间的保护模式配置不一致
处理建议	找到保护模式配置不一致的站点，并修改其保护模式配置

## 125.16 RPR\_PROTECTION\_INCONSISTENT\_OVER

日志内容	A protection configuration defect is cleared on the ring corresponding to RPR logical interface [STRING].
参数解释	\$1: 接口名称
日志等级	5
举例	RPR/5/RPR_PROTECTION_INCONSISTENT_OVER: A protection configuration defect is cleared on the ring corresponding to RPR logical interface RPR-Router1.
日志说明	RPR环上站点的保护模式配置一致
处理建议	无

## 125.17 RPR\_SEC\_MAC\_DUPLICATE

日志内容	A duplicate secondary MAC addresses defect is present on the ring corresponding to RPR logical interface [STRING].
参数解释	\$1: 接口名称
日志等级	3
举例	RPR/3/RPR_SEC_MAC_DUPLICATE: A duplicate secondary MAC addresses defect is present on the ring corresponding to RPR logical interface RPR-Router1.
日志说明	RPR环上至少两个站点间的次级MAC地址重复
处理建议	找到次级MAC地址相同的站点，并修改其次级MAC地址

## 125.18 RPR\_SEC\_MAC\_DUPLICATE\_OVER

日志内容	A duplicate secondary MAC addresses defect is cleared on the ring corresponding to RPR logical interface [STRING].
参数解释	\$1: 接口名称
日志等级	5
举例	RPR/5/RPR_SEC_MAC_DUPLICATE_OVER: A duplicate secondary MAC addresses defect is cleared on the ring corresponding to RPR logical interface RPR-Router1.
日志说明	RPR环上站点的次级MAC地址不再相同
处理建议	无

## 125.19 RPR\_TOPOLOGY\_INCONSISTENT

日志内容	An inconsistent topology defect is present on the ring corresponding to RPR logical interface [STRING].
参数解释	\$1: 接口名称
日志等级	3
举例	RPR/3/RPR_TOPOLOGY_INCONSISTENT: An inconsistent topology defect is present on the ring corresponding to RPR logical interface RPR-Router1.
日志说明	站点上不同端口收集的拓扑信息不一致
处理建议	在链路上依次执行 <b>shutdown</b> 和 <b>undo shutdown</b> 命令，使站点重新收集拓扑信息

## 125.20 RPR\_TOPOLOGY\_INCONSISTENT\_OVER

日志内容	An inconsistent topology defect is cleared on the ring corresponding to RPR logical interface [STRING].
参数解释	\$1: 接口名称
日志等级	5
举例	RPR/5/RPR_TOPOLOGY_INCONSISTENT_OVER: An inconsistent topology defect is cleared on the ring corresponding to RPR logical interface RPR-Router1.
日志说明	站点上不同端口收集的拓扑信息已一致
处理建议	无

## 125.21 RPR\_TOPOLOGY\_INSTABILITY

日志内容	A topology instability defect is present on the ring corresponding to RPR logical interface [STRING].
参数解释	\$1: 接口名称
日志等级	4
举例	RPR/4/RPR_TOPOLOGY_INSTABILITY: A topology instability defect is present on the ring corresponding to RPR logical interface RPR-Router1.
日志说明	RPR环的拓扑不稳定
处理建议	无

## 125.22 RPR\_TOPOLOGY\_INSTABILITY\_OVER

日志内容	A topology instability defect is cleared on the ring corresponding to RPR logical interface [STRING].
参数解释	\$1: 接口名称
日志等级	5
举例	RPR/5/RPR_TOPOLOGY_INSTABILITY_OVER: A topology instability defect is cleared on the ring corresponding to RPR logical interface RPR-Router1.
日志说明	RPR环的拓扑已稳定
处理建议	无

## 125.23 RPR\_TOPOLOGY\_INVALID

日志内容	A topology invalid defect is present on the ring corresponding to RPR logical interface [STRING].
参数解释	\$1: 接口名称
日志等级	4
举例	RPR/4/RPR_TOPOLOGY_INVALID: A topology invalid defect is present on the ring corresponding to RPR logical interface RPR-Router1.
日志说明	站点收集的拓扑信息无效
处理建议	在链路上依次执行 <b>shutdown</b> 和 <b>undo shutdown</b> 命令，使站点重新收集拓扑信息

## 125.24 RPR\_TOPOLOGY\_INVALID\_OVER

日志内容	A topology invalid defect is cleared on the ring corresponding to RPR logical interface [STRING].
参数解释	\$1: 接口名称
日志等级	5
举例	RPR/5/RPR_TOPOLOGY_INVALID_OVER: A topology invalid defect is cleared on the ring corresponding to RPR logical interface RPR-Router1.
日志说明	站点收集的拓扑信息有效
处理建议	无

# 126 RRPP

本节介绍 RRPP 模块输出的日志信息。

## 126.1 RRPP\_IPP\_CHECK

日志内容	An RRPP port can't be configured as an IPP port.
参数解释	无
日志等级	6
举例	RRPP/6/RRPP_IPP_CHECK: An RRPP port can't be configured as an IPP port.
日志说明	RRPP环端口不支持配置为IPP口
处理建议	无

## 126.2 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

## 126.3 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

# 127 RTM

本节介绍 EAA 的 RTM (Real-Time Management) 模块输出的日志信息。

## 127.1 RTM\_EMAIL\_SUCCESS

日志内容	Succeed in sending an email with the subject [STRING] to [STRING].
参数解释	\$1: 邮件主题 \$2: 邮件接收者
日志等级	6
举例	RTM/6/RTM_EMAIL_SUCCESS: Succeed in sending an email with the subject Interface info to test1@163.com,test2@163.com.
日志说明	EAA自动发送邮件成功
处理建议	无



## 127.2 RTM\_EMAIL\_FAILED

日志内容	Failed to send an email with the subject of [STRING] to [STRING], please check email domain, username password, max size and email server settings.
参数解释	\$1: 邮件主题 \$2: 邮件接收者
日志等级	4
举例	RTM/4/RTM_EMAIL_FAILED: Failed to send an email with subject of Interface info to test1@UNIS.com, please check email domain, username password, max size and email server settings.
日志说明	EAA模块自动发送邮件失败，失败原因可能为： <ul style="list-style-type: none"><li>• 邮件超大</li><li>• 邮件配置不完全</li><li>• 设备与发送端邮件服务器之间路由不可达</li><li>• 发送端邮件服务器上的邮件服务不可用等</li></ul>
处理建议	请确认： <ul style="list-style-type: none"><li>• <code>rtm email max-size</code> 命令配置的邮件大小限制是否合适</li><li>• <code>rtm email domain</code>、<code>rtm email username password</code> 命令的配置是否正确</li><li>• Ping 发送端邮件服务器，确认发送邮件服务器是否路由可达</li><li>• 使用 NQA HTTP 探测发送端邮件服务器上的邮件服务是否可用</li><li>• 发送端邮件服务器上设置的参数是否和设备侧的邮件发送参数匹配</li></ul>

## 127.3 RTM\_ENVIRONMENT

日志内容	Can't find environment variable [STRING].
参数解释	\$1: EAA环境变量的名称
日志等级	4
举例	RTM/4/RTM_ENVIRONMENT: Can't find environment variable eee.
日志说明	CLI监控策略替换环境变量时没有找到对应环境变量，CLI监控策略执行失败
处理建议	请先定义环境变量再使用环境变量

## 127.4 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 test.
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

## 127.5 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

## 127.6 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

# 128 SAVA

本节介绍 SAVA（Source Address Validation Architecture）模块输出的日志信息。

## 128.1 SAVA\_SET\_DRV\_FAILED

日志内容	Failed to set the driver for enabling IPv6 SAVA on interface [STRING].
参数解释	\$1: 接口名称
日志等级	5
举例	SAVA/5/SAVA_SET_DRV_FAILED: Failed to set the driver for enabling IPv6 SAVA on interface GigabitEthernet1/0/1.
日志说明	在接口上开启IPv6 SAVA功能，功能下硬件驱动失败
处理建议	请稍后重新执行一遍本命令

## 128.2 SAVA\_SPOOFING\_DETECTED

日志内容	Spoofing packet detected: Spoofing packet detected : source IP 2000::1, destination IP 3000::2, protocol 6, source port 200, destination port 3000 on interface GigabitEthernet1/0/1.
参数解释	\$1: 仿冒的源IP地址 \$2: 目的IP地址 \$3: IP报文协议号 \$4: 源端口号 \$5: 目的端口号 \$6: 接口名称
日志等级	6
举例	SAVA/6/SAVA_SPOOFING_DETECTED: Spoofing packet detected : source IP 2000::1, destination IP 3000::2, protocol 6, source port 200, destination port 3000 on interface GigabitEthernet1/0/1.
日志说明	设备检测到非法主机仿冒合法用户IP
处理建议	检查报文发送者的合法性

# 129 SAVI

本节介绍 SAVI 模块输出的日志信息。

## 129.1 SAVI\_FILTER\_ENTRY\_ADD

日志内容	Filter entry add with IP address [STRING], MAC [STRING] on interface [STRING] and VLAN [UINT32].
参数解释	\$1: IP 地址 \$2: MAC 地址 \$3: 接口名称 \$4: VLAN ID
日志等级	6
举例	SAVI/6/SAVI_FILTER_ENTRY_ADD: Filter entry add with IP address 3000::22, MAC 0011-0231-4520 on interface GigabitEthernet1/0/1 and VLAN 112.
日志说明	新增SAVI过滤表项
处理建议	无

## 129.2 SAVI\_FILTER\_ENTRY\_DEL

日志内容	Filter entry delete with IP address [STRING], MAC [STRING] on interface [STRING] and VLAN [UINT32].
参数解释	\$1: IP 地址 \$2: MAC 地址 \$3: 接口名称 \$4: VLAN ID
日志等级	6
举例	SAVI/6/SAVI_FILTER_ENTRY_DEL: Filter entry delete with IP address 3000::22, MAC 0011-0231-4520 on interface GigabitEthernet1/0/1 and VLAN 112.
日志说明	删除SAVI过滤表项
处理建议	无

## 129.3 SAVI\_SPOOFING\_DETECTED

日志内容	Spoofing packet detected: source IP [STRING], MAC [STRING], destination IP [STRING], protocol [UINT32], source port [UINT32], destination port [UINT32], incoming interface [STRING], VLAN [UINT32].
参数解释	\$1: 仿冒的源IP地址 \$2: 源MAC地址 \$3: 目的IP地址 \$4: IP报文协议号 \$5: 源端口号 \$6: 目的端口号 \$7: 接口名称 \$8: VLAN ID
日志等级	6
举例	SAVI/6/SAVI_SPOOFING_DETECTED: Spoofing packet detected: source IP 2000::1, MAC 0011-0231-4520, destination IP 3000::2, protocol 6, source port 299, destination port 399, incoming interface GigabitEthernet1/0/1, VLAN 40.
日志说明	设备检测到非法主机仿冒合法用户IP
处理建议	检查报文发送者的合法性

# 130 SCMD

本节介绍 SCMD（服务控制管理）模块输出的日志信息。

## 130.1 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	<p>\$1: 进程名</p> <p>\$2: 进程脚本里定义的服务名</p> <p>\$3: 进程退出码, 取值为:</p> <ul style="list-style-type: none"> <li>○ 数字表示进程退出码</li> <li>○ NA 表示无退出码, 进程被信号关闭</li> </ul> <p>\$4: 关闭进程的信号, 取值为:</p> <ul style="list-style-type: none"> <li>○ 数字表示关闭进程的信号的数值</li> <li>○ NA 表示没有关闭信号, 进程主动退出, 并非被信号关闭</li> </ul> <p>\$5: 进程的创建时间</p> <p>\$6: 进程的关闭时间</p>
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	进程异常退出, 输出进程异常退出的相关参数, 以便定位
处理建议	<ol style="list-style-type: none"> <li>1. 通常情况下, 进程异常退出后, 会立即自动重启。可使用 <code>display process</code> 命令查看进程是否存在。如果进程存在, 则进程已恢复</li> <li>2. 如果进程未恢复, 请搜集以下信息: <ul style="list-style-type: none"> <li>○ 在 <code>probe</code> 视图下, 执行 <code>view /var/log/trace.log &gt; trace.log</code>, 然后将设备存储目录下的 <code>trace.log</code> 文件通过 FTP 或 TFTP 功能, 上传到服务器</li> <li>○ 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</li> </ul> </li> <li>3. 如果进程已恢复, 但仍需要定位进程异常退出的原因, 请执行第二步 当使用FTP功能将文件上传到服务器时, 请使用binary传输模式</li> </ol>

## 130.2 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

## 130.3 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	<ol style="list-style-type: none"><li>1. 请使用 <code>display exception context</code> 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</li><li>2. 通过 <code>display exception filepath</code> 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</li><li>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</li></ol> 当使用FTP功能将文件上传到服务器时,请使用binary传输模式

## 130.4 SCM\_ABNORMAL\_REBOOT

日志内容	Failed to restore process [STRING]. Rebooting [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. Rebooting 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	<ol style="list-style-type: none"><li>1. 等单板重启后,使用 <code>display process</code> 命令查看进程是否恢复</li><li>2. 若多次重启后仍不能恢复,联系工程师解决</li></ol>

## 130.5 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	<ol style="list-style-type: none"><li>1. 等单板重启后, 使用 <code>display process</code> 命令查看进程是否恢复</li><li>2. 若多次重启后仍不能恢复, 联系工程师解决</li></ol>

## 130.6 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	<ol style="list-style-type: none"><li>1. 任意视图下执行 <code>display process log</code> 命令查看进程退出详细信息</li><li>2. 重启异常进程所在单板或 MDC, 尝试恢复</li><li>3. 提供 <code>display process log</code> 命令的显示信息, 联系工程师解决</li></ol>



## 130.7 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 \$2: 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	<ol style="list-style-type: none"><li>1. 重启单板，尝试恢复</li><li>2. 联系工程师解决</li></ol>

## 130.8 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	<ol style="list-style-type: none"><li>1. 重启单板，尝试恢复</li><li>2. 联系工程师解决</li></ol>

## 130.9 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输出该日志的时间 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输出该日志的时间
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	<ol style="list-style-type: none"><li>1. 系统/MDC/Context 稳定后，使用 <code>display process</code> 命令查看进程是否恢复</li><li>2. 联系工程师解决</li></ol>

## 130.10 SCM\_PROCESS\_HEALTHY

日志内容	Process [%s] is healthy.
参数解释	\$1: 进程名
日志等级	6
举例	SCMD/6/SCM_PROCESS_HEALTHY: Process fsd is healthy.
日志说明	进程正常启动，进入健康状态
处理建议	无

## 130.11 SCM\_PROCESS\_STARTING\_TOOLONG

日志内容	<p>形式一： The process [STRING] has not finished starting in [UINT32] hours.</p> <p>形式二： The process [STRING] on [STRING] [UINT16] has not finished starting in [STRING] hours.</p>
参数解释	<p>形式一： \$1: 进程名 \$2: 所用时间</p> <p>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</p>
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	<ol style="list-style-type: none"> <li>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</li> <li>2. 重启单板/MDC/Context，尝试恢复。等单板/MDC/Context 重启后，使用 <code>display process</code> 命令查看进程是否恢复</li> <li>3. 联系工程师解决</li> </ol>

## 130.12 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 [STRING] 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 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

## 130.13 SCM\_PROCESS\_UNHEALTHY

日志内容	Process [%s] is unhealthy.
参数解释	\$1: 进程名
日志等级	4
举例	SCMD/6/SCM_PROCESS_UNHEALTHY: Process fsd is unhealthy.
日志说明	设备/板卡启动过程中，有进程启动超时，进入非健康状态。进程处于非健康状态，会导致设备/板卡一直处于启动状态
处理建议	用户无需干预。系统会自动尝试继续启动进程。如果长时间（六小时后）不能正常启动进程，系统会忽略该进程，继续下一步操作

## 130.14 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	某进程超过6小时未启动完成，系统跳过该进程，继续启动
处理建议	<ol style="list-style-type: none"><li>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</li><li>2. 联系工程师解决</li></ol>

# 131 SCRLSP

本节介绍静态 CRLSP 模块输出的日志信息。

## 131.1 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： <ul style="list-style-type: none"><li>○ 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</li><li>○ 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</li></ul>
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

# 132 SESSION

本节介绍 SESSION 模块输出的日志信息。

## 132.1 SESSION\_IPV4\_FLOW

日志内容	Protocol(1001)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];NATSrcIPAddr(1005)=[IPADDR];NATSrcPort(1006)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];NATDstIPAddr(1009)=[IPADDR];NATDstPort(1010)=[UINT16];InitPktCount(1044)=[UINT32];InitByteCount(1046)=[UINT32];RplyPktCount(1045)=[UINT32];RplyByteCount(1047)=[UINT32];RcvVPNInstance(1042)=[STRING];SndVPNInstance(1043)=[STRING];RcvDSLiteTunnelPeer(1040)=[STRING];SndDSLiteTunnelPeer(1041)=[STRING];BeginTime_e(1013)=[STRING];EndTime_e(1014)=[STRING];Event(1048)=[UINT16][STRING];
参数解释	<p>\$1: 协议类型</p> <p>\$2: 源IP地址</p> <p>\$3: 源端口号</p> <p>\$4: 转换后的源IP地址</p> <p>\$5: 转换后的源端口号</p> <p>\$6: 目的IP地址</p> <p>\$7: 目的端口号</p> <p>\$8: 转换后的目的IP地址</p> <p>\$9: 转换后的目的端口号</p> <p>\$10: 入方向的报文总数</p> <p>\$11: 入方向的字节总数</p> <p>\$12: 出方向的报文总数</p> <p>\$13: 出方向的字节总数</p> <p>\$14: 源VPN名称</p> <p>\$15: 目的VPN名称</p> <p>\$16: 源DS-Lite Tunnel</p> <p>\$17: 目的DS-Lite Tunnel</p> <p>\$18: 创建会话的时间</p> <p>\$19: 会话删除时间</p> <p>\$20: 日志类型</p> <p>\$21: 日志类型描述信息, 包括:</p> <ul style="list-style-type: none"> <li>o Session created: 会话创建日志</li> <li>o Active flow threshold: 流量或时间阈值日志</li> <li>o Normal over: 正常流结束, 会话删除日志</li> <li>o Aged for timeout: 会话老化删除日志</li> <li>o Aged for reset or config-change: 通过配置删除会话日志</li> <li>o Other: 其他原因删除会话日志, 如由其他模块删除</li> </ul>
日志等级	6
举例	SESSION/6/SESSION_IPV4_FLOW: Protocol(1001)=UDP;SrcIPAddr(1003)=10.10.10.1;SrcPort(1004)=1024;NATSrcIPAddr(1005)=10.10.10.1;NATSrcPort(1006)=1024;DstIPAddr(1007)=20.20.20.1;DstPort(1008)=21;NATDstIPAddr(1009)=20.20.20.1;NATDstPort(1010)=21;InitPktCount(1044)=1;InitByteCount(1046)=50;RplyPktCount(1045)=0;RplyByteCount(1047)=0;RcvVPNInstance(1042)=;SndVPNInstance(1043)=;RcvDSLiteTunnelPeer(1040)=;SndDSLiteTunnelPeer(1041)=;BeginTime_e(1013)=03182024082546;EndTime_e(1014)=;Event(1048)=(8)Session created;
日志说明	创建、删除IPv4会话时会发送该日志

日志内容	Protocol(1001)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];NATSrcIPAddr(1005)=[IPADDR];NATSrcPort(1006)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];NATDstIPAddr(1009)=[IPADDR];NATDstPort(1010)=[UINT16];InitPktCount(1044)=[UINT32];InitByteCount(1046)=[UINT32];RplyPktCount(1045)=[UINT32];RplyByteCount(1047)=[UINT32];RcvVPNInstance(1042)=[STRING];SndVPNInstance(1043)=[STRING];RcvDSLiteTunnelPeer(1040)=[STRING];SndDSLiteTunnelPeer(1041)=[STRING];BeginTime_e(1013)=[STRING];EndTime_e(1014)=[STRING];Event(1048)=[UNIT16][STRING];
	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



## 132.2 SESSION\_IPV6\_FLOW

日志内容	Protocol(1001)=[STRING];SrcIPv6Addr(1036)=[IPADDR];SrcPort(1004)=[UINT16];DstIPv6Addr(1037)=[IPADDR];DstPort(1008)=[UINT16];InitPktCount(1044)=[UINT32];InitByteCount(1046)=[UINT32];RplyPktCount(1045)=[UINT32];RplyByteCount(1047)=[UINT32];RcvVPNInstance(1042)=[STRING];SndVPNInstance(1043)=[STRING];BeginTime_e(1013)=[STRING];EndTime_e(1014)=[STRING];Event(1048)=[(UNIT16)][STRING];
参数解释	<p>\$1: 协议类型</p> <p>\$2: 源IPv6地址</p> <p>\$3: 源端口号</p> <p>\$3: 目的IPv6地址</p> <p>\$4: 目的端口号</p> <p>\$5: 入方向的报文总数</p> <p>\$6: 入方向的字节总数</p> <p>\$7: 出方向的报文总数</p> <p>\$8: 出方向的字节总数</p> <p>\$9: 源VPN名称</p> <p>\$10: 目的VPN名称</p> <p>\$11: 创建会话的时间</p> <p>\$12: 会话删除时间</p> <p>\$13: 日志类型</p> <p>\$14: 日志类型描述信息, 包括:</p> <ul style="list-style-type: none"> <li>○ Session created: 会话创建日志</li> <li>○ Active flow threshold: 流量或时间阈值日志</li> <li>○ Normal over: 正常流结束, 会话删除日志</li> <li>○ Aged for timeout: 会话老化删除日志</li> <li>○ Aged for reset or config-change: 通过配置删除会话日志</li> <li>○ Other: 其他原因删除会话日志, 如由其他模块删除</li> </ul>
日志等级	6
举例	SESSION/6/SESSION_IPV6_FLOW: Protocol(1001)=UDP;SrcIPv6Addr(1036)=2001::2;SrcPort(1004)=1024;DstIPv6Addr(1037)=3001::2;DstPort(1008)=53;InitPktCount(1044)=1;InitByteCount(1046)=110;RplyPktCount(1047)=0;RplyByteCount(1047)=0;RcvVPNInstance(1042)=;SndVPNInstance(1043)=;BeginTime_e(1013)=03182024082901;EndTime_e(1014)=;Event(1048)=(8) Session created;
日志说明	<p>创建、删除IPv6会话时会发送该日志</p> <p>IPv6会话过程中会定时发送该日志</p> <p>IPv6会话的流量或时间达到指定的阈值时会发送该日志</p>
处理建议	无

# 133 SFLOW

本节介绍 sFlow 模块输出的日志信息。

## 133.1 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

# 134 SHELL

本节介绍 SHELL 模块输出的日志信息。

## 134.1 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

## 134.2 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

## 134.3 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

## 134.4 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： <ul style="list-style-type: none"><li>在执行 <b>save</b> 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</li><li>在执行 <b>save</b> 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</li><li>在执行 <b>save</b> 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</li></ul>
处理建议	无

## 134.5 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

## 134.6 SHELL\_CMD\_INVALID\_CHARACTER

日志内容	Execution failed for the [STRING] command. Reason: The command contains invalid characters (? or \t).
参数解释	\$1: 要执行的命令行
日志等级	6
举例	SHELL/6/SHELL_CMD_INVALID_CHARACTER: Execution failed for the sysname abc?? command. Reason: The command contains invalid characters (? or \t).
日志说明	当设备使用文本类型的配置文件下发配置时，例如进行配置恢复或配置回滚时，如果配置文件中的命令行里包含无效字符“?”或“\t”，则输出此日志
处理建议	请用户根据需要，将命令行修改为正确形式，进行手动配置

## 134.7 SHELL\_CMD\_MATCHFAIL

日志内容	-User=[STRING]-IPAddr=[STRING]; Command [STRING] in view [STRING] failed to be matched.
参数解释	\$1: 用户名 \$2: IP地址 \$3: 命令字符串 \$4: 当前命令模式
日志等级	4
举例	SHELL/4/SHELL_CMD_MATCHFAIL: -User=-IPAddr=192.168.62.138; Command description 10 in view system failed to be matched.
日志说明	由于命令输入错误，或者当前模式错误等，造成命令匹配错误
处理建议	定位命令匹配失败的具体原因

## 134.8 SHELL\_CMDDENY

日志内容	-Line=[STRING]-IPAddr=[STRING]-User=[STRING]; Command=[STRING] is denied.
参数解释	\$1: 用户线名（如果不涉及该参数，显示为**） \$2: IP地址（如果不涉及该参数，显示为**） \$3: 用户名（如果不涉及该参数，显示为**） \$4: 命令字符串
日志等级	5
举例	SHELL/5/SHELL_CMDDENY: -Line=vty0-IPAddr=192.168.62.138-User=-; Command vlan 10 is permission denied.
日志说明	命令执行失败。用户权限不够
处理建议	无

## 134.9 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

## 134.10 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

## 134.11 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 <b>configuration commit delay</b> 命令延长延长时间

## 134.12 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

## 134.13 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

## 134.14 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

## 134.15 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 <b>configuration commit delay</b> 命令延长长时间

## 134.16 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

## 134.17 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 用户线名为“local”时，表示用户登录到备用主控板自身
处理建议	无



## 134.18 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 用户线名为“local”时，表示用户登录到备用主控板自身
处理建议	无

# 135 SLSP

本节介绍静态 LSP 模块输出的日志信息。

## 135.1 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： <ul style="list-style-type: none"><li>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</li><li>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</li></ul>
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

# 136 SMARTMC

本节介绍 SMARTMC（Smart Management Center，智能管理中心）模块输出的日志信息。

## 136.1 ERROR

日志内容	Failed to set a password for device [UNIT].
参数解释	\$1: 成员设备的ID
日志等级	3
举例	SMARTMC/3/ERROR: Failed to set a password for device 10.
日志说明	执行smartmc tc password命令设置成员设备的密码失败
处理建议	<ul style="list-style-type: none"><li>• 执行 <code>display password-control</code> 命令，查看显示信息中 Password length、Password composition、Password complexity 三个字段的取值，了解密码设置要求，重新设置密码</li><li>• 执行 <code>password-control length</code>、<code>password-control composition</code> 和 <code>password-control complexity</code> 命令修改密码复杂度要求</li></ul>

# 137 SMLK

本节介绍 Smart Link 模块输出的日志信息。

## 137.1 SMLK\_PORT\_INACTIVE

日志内容	Not all the members in smart link group [UINT16] are DR ports. An IPP port can't be a member of a smart link group.
参数解释	\$1: Smart Link组ID
日志等级	4
举例	SMLK/4/SMLK_DRPORT_CHECK: -MDC=1; Not all the members in smart link group 1 are DR ports.
日志说明	Smart Link组成员接口为DR接口与非DR接口或IPP接口，成员接口不生效
处理建议	配置Smart Link组成员接口都为DR接口或非DR接口或非IPP接口

## 137.2 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

# 138 SNMP

本节介绍 SNMP 模块输出的日志信息。

## 138.1 SNMP\_ACL\_RESTRICTION

日志内容	SNMP [STRING] from [STRING] is rejected due to ACL restriction.
参数解释	\$1: SNMP团体名/用户名/组名 \$2: NMS的IP地址
日志等级	3
举例	SNMP/3/SNMP_ACL_RESTRICTION: SNMP community public from 192.168.1.100 is rejected due to ACL restrictions.
日志说明	当SNMP报文因ACL限制被拒绝通过时，打印系统日志
处理建议	检查SNMP agent上的ACL配置，及agent是否被攻击

## 138.2 SNMP\_AUTHENTICATION\_FAILURE

日志内容	Failed to authenticate SNMP message.
参数解释	无
日志等级	4
举例	SNMP/4/SNMP_AUTHENTICATION_FAILURE: Failed to authenticate SNMP message.
日志说明	NMS向Agent发起SNMP请求，当认证失败时，Agent记录此日志信息
处理建议	无

## 138.3 SNMP\_GET

日志内容	-seqNO=[UINT32]-srcIP=[STRING]-op=GET-node=[STRING]-value=[STRING]; The agent received a message.
参数解释	\$1: SNMP操作日志的序列号 \$2: NMS的IP地址 \$3: Get操作的MIB节点名及对应的OID \$4: 请求报文的取值字段
日志等级	6
举例	SNMP/6/SNMP_GET: -seqNO=1-srcIP=192.168.28.28-op=GET-node=sysLocation(1.3.6.1.2.1.1.6.0)-value=; The agent received a message.
日志说明	NMS向Agent发送Get请求报文。如果SNMP日志功能开启，SNMP模块将记录Get请求相关信息
处理建议	无

## 138.4 SNMP\_INFORM\_LOST

日志内容	Inform failed to reach NMS [STRING]: Inform [STRING][STRING].
参数解释	\$1: NMS主机地址及端口号 \$2: 告警名称及对应的OID \$3: 告警携带的MIB节点名称、OID及相应的值 <ul style="list-style-type: none"> <li>○ 如果告警未携带 MIB 节点，此参数部分不会出现</li> <li>○ 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</li> </ul>
日志等级	3
举例	SNMP/3/SNMP_INFORM_LOST: Inform failed to reach NMS 192.168.111.222(163): Inform coldStart(1.3.6.1.6.3.1.1.5.1).
日志说明	设备给NMS发送Inform报文后，未收到NMS的响应报文，则认为NMS不可达。设备会打印该日志方便用户定位 当日志携带多个参数导致日志超长时，系统会自动将当前日志拆分为多条日志发送，且添加定位符标识“-PART=xx”，xx表示拆分后生成的日志的序号
处理建议	检查设备到NMS是否路由可达

## 138.5 SNMP\_NOTIFY

日志内容	Notification [STRING][STRING].
参数解释	<p>\$1: 告警名称及对应的OID</p> <p>\$2: 告警携带的MIB节点名称、OID及相应的值</p> <ul style="list-style-type: none"> <li>○ 如果告警未携带 MIB 节点，此参数部分不会出现</li> <li>○ 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</li> </ul>
日志等级	6
举例	<p>未拆分的日志举例：</p> <p>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.</p> <p>被拆分的日志举例：</p> <p>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.</p> <p>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)=**.</p>
日志说明	<p>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</p> <p>当日志携带多个参数导致日志超长时，系统会自动将当前日志拆分为多条日志发送，且添加定位符标识“-PART=xx”，xx表示拆分后生成的日志的序号</p>
处理建议	无

## 138.6 SNMP\_SET

日志内容	-seqNO=[UINT32]-srcIP=[STRING]-op=SET-errorIndex=[UINT32]-errorStatus=[STRING]-node=[STRING]-value=[STRING]; The agent received a message.
参数解释	\$1: SNMP操作日志的序列号 \$2: NMS的IP地址 \$3: Set操作的差错索引 \$4: Set操作的差错状态 \$5: Set操作的MIB节点名及对应的OID \$6: Set操作设置的MIB节点的值
日志等级	6
举例	SNMP/6/SNMP_SET: -seqNO=3-srcIP=192.168.28.28-op=SET-errorIndex=0-errorStatus=noError-node=sys Location(1.3.6.1.2.1.1.6.0)-value=Hangzhou China; The agent received a message.
日志说明	NMS向Agent发送Set请求。如果SNMP日志功能开启，SNMP模块将记录Set操作
处理建议	无

## 138.7 SNMP\_USM\_NOTINTIMEWINDOW

日志内容	-User=[STRING]-IPAddr=[STRING]; SNMPv3 message is not in the time window.
参数解释	\$1: 用户名 \$2: NMS的IP地址
日志等级	4
举例	SNMP/4/SNMP_USM_NOTINTIMEWINDOW: -User=admin-IPAddr=169.254.0.7; SNMPv3 message is not in the time window.
日志说明	SNMPv3消息不在时间窗
处理建议	无

# 139 SOCKET

本节介绍 SOCKET 模块输出的日志信息。

## 139.1 SOCKET\_TCP\_UNREAD

日志内容	Data stays in the receive buffer for [INTEGER] secs. Owner=[STRING], VRF index=[INTEGER], local address/port=[STRING]/[INTEGER], remote address/port=[STRING]/[INTEGER], buffered sent bytes=[INTEGER], buffered received bytes=[INTEGER].
参数解释	\$1: 时间 \$2: 进程名 \$3: VPN索引 \$4: 本地IP地址 \$5: TCP本地端口 \$6: 对端IP地址 \$7: TCP对端端口 \$8: 发送缓冲区的字节数 \$9: 接收缓冲区的字节数
日志等级	6
举例	SOCKET/6/SOCKET_TCP_UNREAD: Data stays in the receive buffer for 40 secs. Owner=bgpd, VRF=0, local address/port=1.1.1.1/179, remote address/port=1.1.1.2/12345, buffered sent bytes=1000, buffered received bytes=50.
日志说明	TCP数据在接收缓冲区超过40秒未被读取
处理建议	无

# 140 SSHC

本节介绍 SSHC（SSH Client，SSH 客户端）模块输出的日志信息。

## 140.1 SSHC\_ALGORITHM\_MISMATCH

日志内容	The SSH client failed to log in because of [STRING] algorithm mismatch.
参数解释	\$1: 算法类型，取值包括： <ul style="list-style-type: none"><li>• encryption: 加密算法</li><li>• key exchange: 密钥交换算法</li><li>• MAC: HMAC 算法</li><li>• public key: 主机签名算法</li></ul>
日志等级	5
举例	SSHC/5/SSHC_ALGORITHM_MISMATCH: The SSH client 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客户端和服务端使用相同算法

## 140.2 SSHC\_AUTH\_PASSWORD\_FAIL

日志内容	SSH user [STRING] failed to pass password authentication because of invalid username or wrong password.
参数解释	\$1: 用户名
日志等级	5
举例	SSHC/5/SSHC_AUTH_PASSWORD_FAIL: SSH user aaa failed to pass password authentication because of invalid username or wrong password.
日志说明	由于用户名无效或者密码错误导致认证失败
处理建议	检查用户是否存在和密码是否正确

## 140.3 SSHC\_AUTH\_PUBLICKEY\_FAIL

日志内容	SSH user [STRING] failed to pass publickey authentication.
参数解释	\$1: 用户名
日志等级	5
举例	SSHC/5/SSHC_AUTH_PUBLICKEY_FAIL: SSH user abc failed to pass publickey authentication.
日志说明	SSH用户没有通过公钥认证
处理建议	检查服务器上保存的用户公钥与客户端上的公钥是否一致



## 140.4 SSHC\_CERT\_VERIFY\_FAIL

日志内容	Failed to verify the certificate because [STRING].
参数解释	<p>\$1: 失败原因:</p> <ul style="list-style-type: none"> <li>• null certificate: 证书为空</li> <li>• null certificate name: 证书名字为空</li> <li>• unable to get issuer certificate: 获取颁发者证书失败</li> <li>• unable to get certificate CRL: 无法获取证书的 CRL</li> <li>• unable to decrypt CRL's signature: 无法解密 CRL 的签名</li> <li>• certificate signature failure: 证书签名错误</li> <li>• CRL signature failure: CRL 签名失败</li> <li>• unable to decrypt certificate's signature: 解密证书签名失败</li> <li>• certificate is not yet valid: 证书尚未生效</li> <li>• certificate has expired: 证书已失效</li> <li>• CRL is not yet valid: CRL 尚未生效</li> <li>• CRL has expired: CRL 已经失效</li> <li>• format error in certificate's notBefore field: 证书的起始时间格式错误</li> <li>• format error in certificate's notAfter field: 证书的结束时间格式错误</li> <li>• format error in CRL's lastUpdate field: CRL 的上次更新时间格式错误</li> <li>• format error in CRL's nextUpdate field: CRL 的下次更新时间格式错误</li> <li>• out of memory: 内存不足</li> <li>• self signed certificate: 自签名证书</li> <li>• self signed certificate in certificate chain: 证书链中存在自签名证书</li> <li>• unable to verify the first certificate: 验证首个证书失败</li> <li>• certificate chain too long: 证书链过长</li> <li>• certificate revoked: 证书被撤回</li> <li>• invalid CA certificate: 无效的 CA 证书</li> <li>• invalid non-CA certificate (has CA markings): 无效的非 CA 证书</li> <li>• path length constraint exceeded: 超过路径深度约束</li> <li>• proxy path length constraint exceeded: 超过代理路径深度约束</li> <li>• proxy certificates not allowed, please set the appropriate flag: 代理证书不通过, 请设置合适的标记</li> <li>• unsupported certificate purpose: 不支持的证书用途</li> <li>• certificate not trusted: 证书不被信任</li> <li>• certificate rejected: 证书被拒绝</li> <li>• application verification failure: 证书应用验证失败</li> <li>• subject issuer mismatch: 证书主题颁发者不匹配</li> <li>• authority and subject key identifier mismatch: 授权和主题密钥标识不匹配</li> <li>• authority and issuer serial number mismatch: 授权和颁发者序列号不匹配</li> <li>• key usage does not include certificate signing: 密钥用途不包括证书签名</li> <li>• unable to get CRL issuer certificate: 获取 CRL 颁发者证书失败</li> </ul>

日志内容	Failed to verify the certificate because [STRING].
	<ul style="list-style-type: none"> <li>unhandled critical extension: 不受控的决定性的扩展</li> <li>key usage does not include CRL signing: 密钥用途不包括 CRL 签名</li> <li>key usage does not include digital signature: 密钥用途不包括数字签名</li> <li>unhandled critical CRL extension: 不受控的决定性的 CRL 扩展</li> <li>invalid or inconsistent certificate extension: 无效或不一致的证书扩展</li> <li>invalid or inconsistent certificate policy extension: 无效或不一致的证书策略扩展</li> <li>no explicit policy: 不存在明确的策略</li> <li>Different CRL scope: CRL 范围不同</li> <li>CRL path validation error: CRL 路径检验失败</li> <li>unsupported or invalid name syntax: 不支持的或无效的名字语法</li> <li>unsupported or invalid name constraint syntax: 不支持的或无效的名字约束语法</li> <li>Suite B: certificate version invalid: Suite B: 证书版本号无效</li> <li>Suite B: invalid public key algorithm: Suite B: 无效的公钥算法</li> <li>Suite B: invalid ECC curve: Suite B: 无效的 ECC 曲线</li> <li>Suite B: invalid signature algorithm: Suite B: 无效的签名算法</li> <li>Suite B: curve not allowed for this LOS: Suite B: 曲线不被本 LOS 准许</li> <li>Suite B: cannot sign P-384 with P-256: Suite B: 不能使用 P-256 给 P-384 签名</li> <li>Invalid certificate verification context: 无效的证书认证上下文</li> <li>Issuer certificate lookup error: 颁发者证书查找失败</li> <li>proxy subject name violation: 代理主题名称不规范</li> </ul>
日志等级	5
举例	SSHC/5/SSHC_CERT_VERIFY_FAIL: Failed to verify the certificate because null certificate.
日志说明	证书验证失败
处理建议	检查证书有效性

## 140.5 SSHC\_CONNECT\_FAIL

日志内容	The SSH client failed to connect to SSH server [IPADDR] port [UINT32].
参数解释	<p>\$1: SSH服务器端IP地址</p> <p>\$2: SSH服务器的端口号</p>
日志等级	5
举例	SSHC/5/SSHC_CONNECT_FAIL: The SSH client failed to connect to SSH server 1.1.1.1 port 2000.
日志说明	和SSH服务器建立连接失败
处理建议	检查IP地址端口是否正确，SSH服务器端是否开启服务

## 140.6 SSHC\_DECRYPT\_FAIL

日志内容	The SSH client failed to use [STRING] to decrypt the packet received from the SSH server.
参数解释	\$1: 加密算法（比如aes256-cbc）
日志等级	5
举例	SSHC/5/SSHC_DECRYPT_FAIL: The SSH client failed to use aes256-cbc to decrypt the packet received from the SSH server.
日志说明	来自SSH服务器端的报文解密失败
处理建议	请联系技术支持

## 140.7 SSHC\_DISCONNECT

日志内容	The SSH client was disconnected from the SSH server because the network was not available.
参数解释	无
日志等级	5
举例	SSHC/5/SSHC_DISCONNECT: The SSH client was disconnected from the SSH server because the network was not available.
日志说明	SSH客户端与服务器由于网络问题断开连接
处理建议	检查网络

## 140.8 SSHC\_ENCRYPT\_FAIL

日志内容	The SSH client failed to use [STRING] to encrypt the packet sent to the SSH server.
参数解释	\$1: 加密算法（比如aes256-cbc）
日志等级	5
举例	SSHC/5/SSHC_ENCRYPT_FAIL: The SSH client failed to use aes256-cbc to encrypt the packet sent to the SSH server.
日志说明	发往SSH服务器的报文加密失败
处理建议	请联系技术支持

## 140.9 SSHC\_HOST\_NAME\_ERROR

日志内容	The SSH server host name [STRING] is incorrect.
参数解释	\$1: 主机名
日志等级	5
举例	SSHC/5/SSHC_HOST_NAME_ERROR: The SSH server host name AAA is incorrect.
日志说明	服务器主机名错误
处理建议	检查指定的主机名

## 140.10 SSHC\_KEY\_EXCHANGE\_FAIL

日志内容	The SSH client failed to exchange keys with the SSH server.
参数解释	无
日志等级	5
举例	SSHC/5/SSHC_KEY_EXCHANGE_FAIL: The SSH client failed to exchange keys with the SSH server.
日志说明	在密钥交换过程中出现错误
处理建议	检查SSH客户端和服务端的支持的算法类型是否匹配，如不匹配更改SSH客户端支持的算法

## 140.11 SSHC\_MAC\_ERROR

日志内容	The SSH client received from the SSH server a packet with incorrect message authentication code.
参数解释	无
日志等级	5
举例	SSHC/5/SSHC_MAC_ERROR: The SSH client received from the SSH server a packet with incorrect message authentication code.
日志说明	SSH客户端从服务器收到一个MAC错误的报文
处理建议	无

## 140.12 SSHC\_PUBLICKEY\_NOT\_EXIST

日志内容	The public key of the SSH server does not exist.
参数解释	无
日志等级	5
举例	SSHC/5/SSHC_PUBLICKEY_NOT_EXIST: The public key of the SSH server does not exist.
日志说明	用户登录过程中指定的服务器端公钥不存在
处理建议	通过 <b>display public-key peer</b> 命令检查服务器端指定公钥是否存在

## 140.13 SSHC\_VERSION\_MISMATCH

日志内容	The SSH client failed to log in because of version mismatch.
参数解释	无
日志等级	5
举例	SSHC/5/SSHC_VERSION_MISMATCH: The SSH client failed to log in because of version mismatch.
日志说明	版本不匹配，导致SSH客户端登录失败
处理建议	更改SSH客户端的版本号

# 141 SSHS

本节介绍 SSHS（SSH server，SSH 服务器）模块输出的日志信息。

## 141.1 SSHS\_ACL\_DENY

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

## 141.2 SSSH\_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客户端和服务端使用相同算法

## 141.3 SSSH\_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

## 141.4 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: <ul style="list-style-type: none"><li>○ wrong public key algorithm: 公钥算法错误</li><li>○ wrong public key: 公钥错误</li><li>○ wrong digital signature: 数字签名错误</li></ul>
日志等级	6
举例	SSHS/6/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

## 141.5 SSHS\_AUTH\_KBDINT\_FAIL

日志内容	SSH user [STRING] (IP: [STRING]) didn't pass keyboard-interactive authentication.
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_KBDINT_FAIL: SSH user David (IP: 192.168.30.117) didn't pass keyboard-interactive authentication.
日志说明	SSH用户没有通过keyboard-interactive认证
处理建议	请SSH用户重新登录

## 141.6 SSSH\_AUTH\_PWD\_FAIL

日志内容	Authentication failed for user [STRING] from [STRING] port [INT32] because of invalid username or wrong password.
参数解释	\$1: 用户名 \$2: SSH客户端IP地址 \$3: 端口号
日志等级	6
举例	SSHS/6/SSHS_AUTH_PWD_LOG: Authentication failed for user David from 140.1.1.46 port 16266 because of invalid username or wrong password.
日志说明	由于用户名无效或者密码错误导致认证失败
处理建议	检查用户名密码

## 141.7 SSSH\_AUTH\_SUCCESS

日志内容	SSH user [STRING] from [IPADDR] port [INTEGER] passed [STRING] authentication.
参数解释	\$1: 用户名 \$2: 用户IP地址 \$3: TCP源端口 \$4: 认证方法, 取值为keyboard-interactive、password和publickey
日志等级	6
举例	SSHS/6/SSHS_AUTH_SUCCESS: SSH user ABC from 1.1.1.1 port 55361 passed keyboard-interactive authentication.
日志说明	SSH用户认证通过
处理建议	无

## 141.8 SSSH\_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



## 141.9 SSSH\_AUTHOR\_FAIL

日志内容	Authorization failed for user [STRING] from [STRING] port [INT32].
参数解释	\$1: 用户名 \$2: SSH客户端IP地址 \$3: 端口号
日志等级	6
举例	SSHS/6/SSHS_AUTHOR_FAIL: Authorization failed for user David from 140.1.2.46 port 15000.
日志说明	SSH用户授权失败
处理建议	检查本地用户配置或者认证服务器配置

## 141.10 SSHS\_CERT\_VERIFY\_FAIL

日志内容	Failed to verify the certificate because [STRING].
参数解释	<p>\$1: 失败原因:</p> <ul style="list-style-type: none"><li>• null certificate: 证书为空</li><li>• null certificate name: 证书名字为空</li><li>• unable to get issuer certificate: 获取颁发者证书失败</li><li>• unable to get certificate CRL: 无法获取证书的 CRL</li><li>• unable to decrypt CRL's signature: 无法解密 CRL 的签名</li><li>• certificate signature failure: 证书签名错误</li><li>• CRL signature failure: CRL 签名失败</li><li>• unable to decrypt certificate's signature: 解密证书签名失败</li><li>• certificate is not yet valid: 证书尚未生效</li><li>• certificate has expired: 证书已失效</li><li>• CRL is not yet valid: CRL 尚未生效</li><li>• CRL has expired: CRL 已经失效</li><li>• format error in certificate's notBefore field: 证书的起始时间格式错误</li><li>• format error in certificate's notAfter field: 证书的结束时间格式错误</li><li>• format error in CRL's lastUpdate field: CRL 的上次更新时间格式错误</li><li>• format error in CRL's nextUpdate field: CRL 的下次更新时间格式错误</li><li>• out of memory: 内存不足</li><li>• self signed certificate: 自签名证书</li><li>• self signed certificate in certificate chain: 证书链中存在自签名证书</li><li>• unable to verify the first certificate: 验证首个证书失败</li><li>• certificate chain too long: 证书链过长</li><li>• certificate revoked: 证书被撤回</li><li>• invalid CA certificate: 无效的 CA 证书</li><li>• invalid non-CA certificate (has CA markings): 无效的非 CA 证书</li><li>• path length constraint exceeded: 超过路径深度约束</li><li>• proxy path length constraint exceeded: 超过代理路径深度约束</li><li>• proxy certificates not allowed, please set the appropriate flag: 代理证书不通过, 请设置合适的标记</li><li>• unsupported certificate purpose: 不支持的证书用途</li><li>• certificate not trusted: 证书不被信任</li><li>• certificate rejected: 证书被拒绝</li><li>• application verification failure: 证书应用验证失败</li><li>• subject issuer mismatch: 证书主题颁发者不匹配</li><li>• authority and subject key identifier mismatch: 授权和主题密钥标识不匹配</li><li>• authority and issuer serial number mismatch: 授权和颁发者序列号不匹配</li><li>• key usage does not include certificate signing: 密钥用途不包括证书签名</li><li>• unable to get CRL issuer certificate: 获取 CRL 颁发者证书失败</li></ul>

日志内容	Failed to verify the certificate because [STRING].
	<ul style="list-style-type: none"> <li>unhandled critical extension: 不受控的决定性的扩展</li> <li>key usage does not include CRL signing: 密钥用途不包括 CRL 签名</li> <li>key usage does not include digital signature: 密钥用途不包括数字签名</li> <li>unhandled critical CRL extension: 不受控的决定性的 CRL 扩展</li> <li>invalid or inconsistent certificate extension: 无效或不一致的证书扩展</li> <li>invalid or inconsistent certificate policy extension: 无效或不一致的证书策略扩展</li> <li>no explicit policy: 不存在明确的策略</li> <li>Different CRL scope: CRL 范围不同</li> <li>CRL path validation error: CRL 路径检验失败</li> <li>unsupported or invalid name syntax: 不支持的或无效的名字语法</li> <li>unsupported or invalid name constraint syntax: 不支持的或无效的名字约束语法</li> <li>Suite B: certificate version invalid: Suite B: 证书版本号无效</li> <li>Suite B: invalid public key algorithm: Suite B: 无效的公钥算法</li> <li>Suite B: invalid ECC curve: Suite B: 无效的 ECC 曲线</li> <li>Suite B: invalid signature algorithm: Suite B: 无效的签名算法</li> <li>Suite B: curve not allowed for this LOS: Suite B: 曲线不被本 LOS 准许</li> <li>Suite B: cannot sign P-384 with P-256: Suite B: 不能使用 P-256 给 P-384 签名</li> <li>Invalid certificate verification context: 无效的证书认证上下文</li> <li>Issuer certificate lookup error: 颁发者证书查找失败</li> <li>proxy subject name violation: 代理主题名称不规范</li> </ul>
日志等级	5
举例	SSHS/5/SSHS_CERT_VERIFY_FAIL: Failed to verify the certificate because null certificate.
日志说明	证书验证失败
处理建议	检查证书有效性

## 141.11 SSHS\_CONNECT

日志内容	SSH user [STRING] (IP: [STRING]) connected to the server successfully.
参数解释	<p>\$1: 用户名</p> <p>\$2: SSH客户端IP地址</p>
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

## 141.12 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

## 141.13 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

## 141.14 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

## 141.15 SSSH\_LOG

日志内容	Authentication failed for user [STRING] from [STRING] port [INT32] because of invalid username or wrong password. Authorization failed for user [STRING] from [STRING] port [INT32].
参数解释	\$1: 用户名 \$2: SSH客户端IP地址 \$3: 端口号
日志等级	6
举例	SSHS/6/SSHS_LOG: Authentication failed for user David from 140.1.1.46 port 16266 because of invalid username or wrong password. SSHS/6/SSHS_LOG: Authorization failed for user David from 140.1.2.46 port 15000.
日志说明	由于用户名无效或者密码错误导致认证失败 SSH用户授权失败
处理建议	无

## 141.16 SSSH\_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

## 141.17 SSHS\_REACH\_SESSION\_LIMIT

日志内容	SSH client [STRING] failed to log in. The current number of SSH sessions is [NUMBER]. The maximum number allowed is [NUMBER].
参数解释	\$1: SSH客户端IP地址 \$2: 当前的SSH会话数 \$3: 设备允许建立的SSH会话数
日志等级	6
举例	SSHS/6/SSHS_REACH_SESSION_LIMIT: SSH client 192.168.30.117 failed to log in. The current number of SSH sessions is 10. The maximum number allowed is 10.
日志说明	SSH客户端登录失败，SSH会话数达到了最大值
处理建议	无

## 141.18 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

## 141.19 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 <ul style="list-style-type: none"><li>get file "name": 下载名为 name 的文件</li><li>put file "name": 上传名为 name 的文件</li></ul>
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

## 141.20 SSHS\_SFTP\_OPER

日志内容	User [STRING] at [IPADDR] requested operation: [STRING].
参数解释	<p>\$1: 用户名称.</p> <p>\$2: 用户IP地址.</p> <p>\$3: 用户请求内容, 包括文件操作和目录操作等信息</p> <ul style="list-style-type: none"><li>• open dir "<i>path</i>": 打开目录 <i>path</i></li><li>• open "<i>file</i>" (attribute code <i>code</i>) in <i>MODE</i> mode: 在 <i>MODE</i> 模式下, 打开文件 <i>file</i>, 该文件的属性代码为 <i>code</i></li><li>• remove file "<i>path</i>": 删除文件 <i>path</i></li><li>• mkdir "<i>path</i>" (attribute code <i>code</i>): 创建新目录 <i>path</i>, 该目录的属性代码为 <i>code</i></li><li>• rmdir "<i>path</i>": 删除目录 <i>path</i></li><li>• rename old "<i>old-name</i>" to new "<i>new-name</i>": 改变旧文件或文件夹的名称 <i>old-name</i> 为 <i>new-name</i></li></ul>
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

## 141.21 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

## 141.22 SSSH\_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客户端和服务端使用相同SSH版本

# 142 STAMGR

本节介绍 STAMGR 模块输出的日志信息。

## 142.1 STAMGR\_ADD\_FAILVLAN

日志内容	-SSID=[STRING]-UserMAC=[STRING]; Added a user to the Fail VLAN [STRING].
参数解释	\$1: 用户上线的无线服务名称 \$2: 用户的MAC地址 \$3: 用户加入的Fail-VLAN的VLAN ID
日志等级	5
举例	STAMGR/5/STAMGR_ADD_FAILVLAN:-SSID=text-wifi-UserMAC=dc2d-cb16-28cd; Added a user to the Fail VLAN 5.
日志说明	用户认证失败加入Fail-VLAN
处理建议	无

## 142.2 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



## 142.3 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

## 142.4 STAMGR\_AUTHORACL\_FAILURE

日志内容	-SSID=[STRING]-UserMAC=[STRING]; Failed to assign an ACL. Reason: [STRING].
参数解释	<p>\$1: 用户上线的无线服务名称</p> <p>\$2: 用户的MAC地址</p> <p>\$3: 授权ACL失败的原因</p> <ul style="list-style-type: none"><li>• The ACL doesn't exist: 指定的 ACL 不存在</li><li>• ACL type not supported: 不支持指定的 ACL 类型</li><li>• Not enough hardware resources: 内存不足</li><li>• The ACL conflicts with other ACLs: 指定的 ACL 与其他 ACL 冲突</li><li>• The ACL doesn't contain any rules: 指定 ACL 没有包含任何规则</li><li>• Unknown error: 未知错误</li></ul>
日志等级	5
举例	STAMGR/5/STAMGR_AUTHORACL_FAILURE:-SSID=text-wifi-UserMAC=dc2d-cb16-28cd; Failed to assign an ACL.Reason: The ACL doesn't exist.
日志说明	下发ACL失败
处理建议	无

## 142.5 STAMGR\_AUTHORUSERPROFILE\_FAILURE

日志内容	-SSID=[STRING]-UserMAC=[STRING]; Failed to assign a user profile
参数解释	\$1: 用户上线的无线服务名称 \$2: 用户的MAC地址
日志等级	5
举例	STAMGR/5/STAMGR_AUTHORUSERPROFILE_FAILURE:-SSID=text-wifi-UserMAC=dc2d-cb16-28cd; Failed to assign a user profile
日志说明	下发user profile失败
处理建议	无

## 142.6 STAMGR\_CLIENT\_OFFLINE

日志内容	Client [STRING] went offline from BSS [STRING] with [STRING]. State changed to Unauth.
参数解释	\$1: 客户端的MAC地址 \$2: BSSID \$3: 服务模板的SSID
日志等级	6
举例	STAMGR/6/STAMGR_CLIENT_OFFLINE: Client dc2d-cb33-2147 went offline from BSS 0023-12ef-78dc with SSID abc. State changed to Unauth.
日志说明	客户端在BSS下线，状态变为未认证状态
处理建议	<ul style="list-style-type: none"><li>若客户端主动下线，则不用排查问题</li><li>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</li></ul>

## 142.7 STAMGR\_CLIENT\_ONLINE

日志内容	Client [STRING] went online from BSS [STRING] with SSID [STRING]. State changed to Run.
参数解释	\$1: 客户端的MAC地址 \$2: BSSID \$3: 无线服务模板的SSID
日志等级	6
举例	STAMGR/6/STAMGR_CLIENT_ONLINE: Client dc2d-cb33-2147 went online from BSS 0023-12ef-78dc with SSID abc. State changed to Run.
日志说明	客户端在BSS上线，状态变为运行状态
处理建议	无

## 142.8 STAMGR\_DELBAC\_INFO

日志内容	Delete BAS AC [STRING].
参数解释	\$1: BAS AC的MAC地址
日志等级	6
举例	STAMGR/6/STAMGR_DELBAC_INFO: Delete BAS AC dc2d-cb16-28cd.
日志说明	Master AC断开与BAS AC的连接
处理建议	无

## 142.9 STAMGR\_DELSTA\_INFO

日志内容	Delete client [STRING].
参数解释	\$1: 客户端的MAC地址
日志等级	6
举例	STAMGR/6/STAMGR_DELSTA_INFO: Delete client dc2d-cb16-28cd.
日志说明	客户端断开与BAS AC的连接
处理建议	无

## 142.10 STAMGR\_DOT1X\_LOGIN\_FAILURE

日志内容	-Username=[STRING]-UserMAC=[STRING]-SSID=[STRING]-VLANID=[STRING]; A user failed 802.1X authentication.
参数解释	\$1: 用户名 \$2: 用户的MAC地址 \$3: 用户上线的无线服务名称 \$4: 用户上线的VLAN ID
日志等级	5
举例	STAMGR/5/STAMGR_DOT1X_LOGIN_FAILURE:-Username=Dot1X-UserMAC=dc2d-cb16-28cd-SSID=text-wifi-VLANID=11; A user failed 802.1X authentication.
日志说明	用户802.1X认证失败。触发该日志的原因可能有：AAA服务器不可用、用户名或密码设置不正确
处理建议	<ul style="list-style-type: none"><li>• 检查设备与 AAA 服务器的网络连接是否正常</li><li>• 检查 AAA 服务器是否正常工作</li><li>• 检查用户名和密码设置是否和 AAA 服务器上的设置一致</li></ul>

## 142.11 STAMGR\_DOT1X\_LOGIN\_SUCC

日志内容	-Username=[STRING]-UserMAC=[STRING]-SSID=[STRING]-VLANID=[STRING]; A user passed 802.1X authentication and came online.
参数解释	\$1: 用户名 \$2: 用户的MAC地址 \$3: 用户上线的无线服务名称 \$4: 用户上线的VLAN ID
日志等级	6
举例	STAMGR/6/STAMGR_DOT1X_LOGIN_SUCC:-Username=Dot1X-UserMAC=dc2d-cb16-28cd-SSID=text-wifi-VLANID=11; A user passed 802.1X authentication and came online.
日志说明	用户通过802.1X认证
处理建议	无

## 142.12 STAMGR\_DOT1X\_LOGOFF

日志内容	Username=[STRING]-UserMAC=[STRING]-SSID=[STRING]-VLANID=[STRING]; Session for an 802.1X user was terminated.
参数解释	\$1: 用户名 \$2: 用户的MAC地址 \$3: 用户上线的无线服务名称 \$4: 用户上线的VLAN ID
日志等级	6
举例	STAMGR/6/STAMGR_DOT1X_LOGOFF:-Username=Dot1X-UserMAC=dc2d-cb16-28cd-SSID=text-wifi-VLANID=11; Session for an 802.1X user was terminated.
日志说明	802.1X用户下线
处理建议	无

## 142.13 STAMGR\_MACA\_LOGIN\_FAILURE

日志内容	-Username=[STRING]-UserMAC=[STRING]-SSID=[STRING]-VLANID=[STRING]-UsernameFormat=[STRING]; A user failed MAC authentication.
参数解释	\$1: 用户名 \$2: 用户的MAC地址 \$3: 用户上线的无线服务名称 \$4: 用户上线的VLAN ID \$5: 用户名格式 <ul style="list-style-type: none"><li>fixed: 固定用户名格式</li><li>MAC address: MAC 地址格式</li></ul>
日志等级	5
举例	STAMGR/5/STAMGR_MACA_LOGIN_FAILURE:-Username=MAC-UserMAC=dc2d-cb16-28cd-SSID=text-wifi-VLANID=11-UsernameFormat=fixed; A user failed MAC authentication.
日志说明	用户MAC地址认证失败。触发该日志的原因可能有：AAA服务器不可用、用户名或密码设置不正确
处理建议	<ul style="list-style-type: none"><li>检查设备与 AAA 服务器的网络连接是否正常</li><li>检查 AAA 服务器是否正常工作</li><li>检查用户名和密码设置是否和 AAA 服务器上的设置一致</li></ul>

## 142.14 STAMGR\_MACA\_LOGIN\_SUCC

日志内容	-Username=[STRING]-UserMAC=[STRING]-SSID=[STRING]-VLANID=[STRING]-UsernameFormat=[STRING]; A user passed MAC authentication and came online.
参数解释	\$1: 用户名 \$2: 用户的MAC地址 \$3: 用户上线的无线服务名称 \$4: 用户上线的VLAN ID \$5: 用户名格式 <ul style="list-style-type: none"><li>fixed: 固定用户名格式</li><li>MAC address: MAC 地址格式</li></ul>
日志等级	6
举例	STAMGR/6/STAMGR_MACA_LOGIN_SUCC:-Username=MAC-UserMAC=dc2d-cb16-28cd-SSID=text-wifi-VLANID=11-UsernameFormat=fixed; A user passed MAC authentication and came online.
日志说明	用户通过MAC地址认证
处理建议	无

## 142.15 STAMGR\_MACA\_LOGOFF

日志内容	-Username=[STRING]-UserMAC=[STRING]-SSID=[STRING]-VLANID=[STRING]-UsernameFormat=[STRING]; Session for a MAC authentication user was terminated.
参数解释	\$1: 用户名 \$2: 用户的MAC地址 \$3: 用户上线的无线服务名称 \$4: 用户上线的VLAN ID \$5: 用户名格式 <ul style="list-style-type: none"><li>fixed: 固定用户名格式</li><li>MAC address: MAC 地址格式</li></ul>
日志等级	6
举例	STAMGR/6/STAMGR_MACA_LOGOFF:-Username=MAC-UserMAC=dc2d-cb16-28cd-SSID=text-wifi-VLANID=11-UsernameFormat=fixed; Session for a MAC authentication user was terminated.
日志说明	用户下线
处理建议	无

## 142.16 STAMGR\_STAIPCHANGE\_INFO

日志内容	IP address of client [STRING] changed to [STRING].
参数解释	\$1: 客户端的MAC地址 \$2: 客户端更新的IP地址
日志等级	6
举例	STAMGR/6/STAMGR_STAIPCHANGE_INFO: IP address of client 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

## 142.17 STAMGR\_TRIGGER\_IP

日志内容	-SSID=[STRING]-UserMAC=[STRING]-VLANID=[STRING]; Intrusion protection triggered. Action: [STRING].
参数解释	\$1: 用户上线的无线服务名称 \$2: 用户的MAC地址 \$3: 用户上线的VLAN ID \$4: 入侵检测模式 <ul style="list-style-type: none"><li>Added the user to the blocked MAC address list: 将用户加入 Block-MAC 表中</li><li>Closed the user's BSS temporarily: 关闭用户所在 BSS 一段时间</li><li>Closed the user's BSS permanently: 永久关闭用户所在的 BSS</li></ul>
日志等级	5
举例	STAMGR/5/STAMGR_TRIGGER_IP:-SSID=text-wifi-UserMAC=dc2d-cb16-28cd-VLANID=11; Intrusion protection triggered, the intrusion protection action: added a user to the list of Block-MAC.
日志说明	触发入侵检测，并显示入侵检测模式
处理建议	无

# 143 STM

本节介绍 STM（IRF）模块输出的日志信息。

## 143.1 STM\_AUTO\_UPDATE\_FAILED

日志内容	<p>形式一： Slot [UINT32] auto-update failed. Reason: [STRING].</p> <p>形式二： Chassis [UINT32] slot [UINT32] auto-update failed. Reason: [STRING].</p>
参数解释	<p>形式一：</p> <p><b>\$1:</b> 成员设备编号</p> <p><b>\$2:</b> 失败原因：</p> <ul style="list-style-type: none"> <li>○ Timeout when loading: 加载超时</li> <li>○ 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</li> <li>○ Disk full when writing to disk: 存储介质上的空间不够</li> </ul> <p>形式二：</p> <p><b>\$1:</b> 成员设备编号</p> <p><b>\$2:</b> 主控板槽位号</p> <p><b>\$3:</b> 失败原因：</p> <ul style="list-style-type: none"> <li>○ Timeout when loading: 加载超时</li> <li>○ 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</li> <li>○ Disk full when writing to disk: 主控板存储介质上的空间不够</li> </ul>
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	<p>形式一： 在加入IRF时，从设备从主设备自动加载启动软件包失败</p> <p>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</p>
处理建议	<ol style="list-style-type: none"> <li>1. 如果失败原因为 Timeout when loading，请检查 IRF 链路是否畅通</li> <li>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</li> <li>3. 如果失败原因为 Disk full when writing to disk，请先清理设备的存储介质，删除一些暂时不用的文件</li> <li>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</li> </ol>



## 143.2 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

## 143.3 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

## 143.4 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线程发包时间间隔超过10秒，记录发包超时时间
处理建议	执行 <b>display cpu-usage</b> 查看系统是不是暂时的CPU利用率增高，例如受到攻击或者处理其他较耗费CPU资源的任务。如果不能定位原因请联系技术支持。需要注意的是，如果Hello报文发包时间超过心跳超时时间会造成IRF分裂

## 143.5 STM\_HELLOPKT\_NOTRCV

日志内容	Hello thread hasn't received packets for [UINT] 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线程收包时间超过10秒，记录收包超时的时间
处理建议	执行 <b>display cpu-usage</b> 查看系统是不是暂时的CPU利用率增高，例如受到攻击或者处理其他较耗费CPU资源的任务。如果不能定位原因请联系技术支持。需要注意的是，如果长时间收不到Hello报文会导致IRF分裂

## 143.6 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

## 143.7 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

## 143.8 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

## 143.9 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

## 143.10 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 <b>reboot</b> 命令重启本IRF

## 143.11 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

## 143.12 STM\_PHY\_DOWN

日志内容	Physical interface [STRING] of IRF port [UINT32] went down.
参数解释	\$1: IRF物理端口名 \$2: IRF端口名
日志等级	3
举例	STM/3/STM_PHY_DOWN: Physical interface Ten-GigabitEthernet1/0/1 of IRF port 1 went down.
日志说明	IRF物理端口状态变为down
处理建议	请检查IRF物理端口线缆连接情况

## 143.13 STM\_PHY\_UP

日志内容	Physical interface [STRING] of IRF port [UINT32] came up.
参数解释	\$1: IRF物理端口名 \$2: IRF端口名
日志等级	6
举例	STM/6/STM_PHY_UP: Physical interface Ten-GigabitEthernet1/0/1 of IRF port 1 came up.
日志说明	IRF物理端口状态变为UP
处理建议	无

## 143.14 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

## 143.15 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： <ul style="list-style-type: none"><li>设备型号是否允许组成 IRF</li><li>IRF 配置是否正确</li></ul> 要获取更多信息，请参见该型号设备的IRF配置指导

# 144 STP

本节介绍生成树模块输出的日志信息。

## 144.1 STP\_BPDU\_PROTECTION

日志内容	BPDU-Protection port [STRING] received BPDUs.
参数解释	\$1: 接口名
日志等级	4
举例	STP/4/STP_BPDU_PROTECTION: BPDU-Protection port GigabitEthernet1/0/1 received BPDUs.
日志说明	使能了BPDU保护功能的接口收到BPDU报文
处理建议	检查下行设备是否是用户终端，是否存在恶意攻击

## 144.2 STP\_BPDU\_RECEIVE\_EXPIRY

日志内容	Instance [UINT32]'s port [STRING] received no BPDU within the rcvdInfoWhile interval. Information of the port aged out.
参数解释	\$1: 生成树实例编号 \$2: 接口名
日志等级	5
举例	STP/5/STP_BPDU_RECEIVE_EXPIRY: Instance 0's port GigabitEthernet1/0/1 received no BPDU within the rcvdInfoWhile interval. Information of the port aged out.
日志说明	非指定端口因在BPDU超时之前没有收到任何BPDU报文，端口状态发生改变
处理建议	检查上行设备的STP状态及是否存在恶意攻击

## 144.3 STP\_CONSISTENCY\_CHECK

日志内容	DR role assignment finished. Please verify that the local device and the peer device have consistent global and DR-interface-specific STP settings.
参数解释	N/A
日志等级	5
举例	STP/5/STP_CONSISTENCY_CHECK: DR role assignment finished. Please verify that the local device and the peer device have consistent global and DR-interface-specific STP settings.
日志说明	确保分布式聚合系统中两台DR设备上生成树全局和DR口上的配置一致
处理建议	无

## 144.4 STP\_CONSISTENCY\_RESTORE

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_RESTORE: Consistency restored on VLAN 10's port GigabitEthernet1/0/1.
日志说明	接口类型不一致或者PVID不一致的保护状态解除
处理建议	无

## 144.5 STP\_DETECTED\_TC

日志内容	[STRING] [UINT32]'s port [STRING] detected a topology change.
参数解释	\$1: 生成树实例或VLAN \$2: 生成树实例编号或VLAN ID \$3: 接口名
日志等级	6
举例	STP/6/STP_DETECTED_TC: Instance 0's port GigabitEthernet1/0/1 detected a topology change.
日志说明	接口所在生成树实例或VLAN拓扑发生变化，本端设备检测到拓扑变化
处理建议	检查拓扑变化的原因。如果有链路down了，就恢复此故障链路

## 144.6 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

## 144.7 STP\_DISCARDING

日志内容	Instance [UINT32]'s port [STRING] has been set to discarding state.
参数解释	\$1: 生成树实例编号 \$2: 接口名
日志等级	6
举例	STP/6/STP_DISCARDING: Instance 0's port GigabitEthernet1/0/1 has been set to discarding state.
日志说明	MSTP在计算实例内端口状态，该接口被置为discarding状态
处理建议	无

## 144.8 STP\_DISPUTE

日志内容	[STRING] [UINT32]'s port [STRING] received an inferior BPDU from a designated port which is in forwarding or learning state.
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	4
举例	STP/4/STP_DISPUTE: Instance 0's port GigabitEthernet1/0/2 received an inferior BPDU from a designated port which is in forwarding or learning state.
日志说明	在生成树实例或VLAN内，端口收到了指定端口发出的低优先级BPDU报文，且发送端口处于Forwarding或Learning状态
处理建议	通过 <b>display stp abnormal-port</b> 命令查看处于Dispute保护的阻塞端口信息。检查链路上是否存在对端接收不到本端所发报文的单通故障。确保两端的端口VLAN配置一致后，可以尝试down/up链路恢复或更换连线

## 144.9 STP\_DISPUTE\_RESTORATION

日志内容	[STRING] [UINT32]'s port [STRING] exited the dispute state.
参数解释	\$1: 生成树实例或VLAN \$2: 生成树实例编号或VLAN ID \$3: 接口名称
日志等级	6
举例	STP/6/STP_DISPUTE_RESTORATION: Instance 0's port GigabitEthernet1/0/2 exited the dispute state.
日志说明	在生成树实例或VLAN内，端口从dispute状态恢复
处理建议	无



## 144.10 STP\_EDGEPORT\_INACTIVE

日志内容	Port [STRING] became a non-edge port after receiving a BPDU.
参数解释	\$1: 接口名称
日志等级	4
举例	STP/4/STP_EDGEPORT_INACTIVE: Port GigabitEthernet1/0/1 became a non-edge port after receiving a BPDU.
日志说明	边缘端口收到了STP报文，成为了非边缘端口
处理建议	检查是否有恶意用户伪造BPDU攻击网络

## 144.11 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

## 144.12 STP\_FORWARDING

日志内容	Instance [UINT32]'s port [STRING] has been set to forwarding state.
参数解释	\$1: 生成树实例编号 \$2: 接口名
日志等级	6
举例	STP/6/STP_FORWARDING: Instance 0's port GigabitEthernet1/0/1 has been set to forwarding state.
日志说明	STP在计算实例内端口状态，该接口被置为forwarding状态
处理建议	无

## 144.13 STP\_LOOP\_PROTECTION

日志内容	Instance [UINT32]'s LOOP-Protection port [STRING] failed to receive configuration BPDUs.
参数解释	\$1: 生成树实例编号 \$2: 接口名
日志等级	4
举例	STP/4/STP_LOOP_PROTECTION: Instance 0's LOOP-Protection port GigabitEthernet1/0/1 failed to receive configuration BPDUs.
日志说明	使能了环路保护功能的接口不能接受BPDU配置报文
处理建议	检查上行设备的STP状态及是否存在恶意攻击

## 144.14 STP\_LOOPBACK\_PROTECTION

日志内容	[STRING] [UINT32]'s port [STRING] received its own BPDU.
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	4
举例	STP/4/STP_LOOPBACK_PROTECTION: Instance 0's port GigabitEthernet1/0/2 received its own BPDU.
日志说明	在生成树实例或VLAN中，端口收到自己发出的BPDU报文
处理建议	检查是否有恶意用户伪造BPDU攻击网络或者网络中是否存在环路

## 144.15 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

## 144.16 STP\_NOTIFIED\_TC

日志内容	[STRING] [UINT32]'s port [STRING] was notified a topology change.
参数解释	\$1: 生成树实例或VLAN \$2: 生成树实例编号或VLAN ID \$3: 接口名
日志等级	6
举例	STP/6/STP_NOTIFIED_TC: Instance 0's port GigabitEthernet1/0/1 was notified a topology change.
日志说明	远端相连设备通知本设备某接口所在生成树实例或VLAN的拓扑发生变化
处理建议	检查拓扑变化的原因。如果是有链路down了，就恢复此故障链路

## 144.17 STP\_PORT\_TYPE\_INCONSISTENCY

日志内容	Access port [STRING] in VLAN [UINT32] received PVST BPDUs from a trunk or hybrid port.
参数解释	\$1: 接口名 \$2: VLAN ID
日志等级	4
举例	STP/4/STP_PORT_TYPE_INCONSISTENCY: Access port GigabitEthernet1/0/1 in VLAN 10 received PVST BPDUs from a trunk or hybrid port.
日志说明	Access接口收到了对端Trunk或Hybrid接口发出的PVST报文
处理建议	检查两端的接口类型配置是否一致

## 144.18 STP\_PVID\_INCONSISTENCY

日志内容	Port [STRING] with PVID [UINT32] received PVST BPDUs from a port with PVID [UINT32].
参数解释	\$1: 接口名 \$2: VLAN ID \$3: VLAN ID
日志等级	4
举例	STP/4/STP_PVID_INCONSISTENCY: Port GigabitEthernet1/0/1 with PVID 10 received PVST BPDUs from a port with PVID 20.
日志说明	接口收到了PVID不一致的报文
处理建议	检查两端的接口PVID配置是否一致

## 144.19 STP\_PVST\_BPDU\_PROTECTION

日志内容	PVST BPDUs were received on port [STRING], which is enabled with PVST BPDU protection.
参数解释	\$1: 接口名
日志等级	4
举例	STP/4/STP_PVST_BPDU_PROTECTION: PVST BPDUs were received on port GigabitEthernet1/0/1, which is enabled with PVST BPDU protection.
日志说明	在MSTP模式下，设备上使能了PVST报文保护功能的端口收到了PVST报文
处理建议	检查其他设备是否发出了PVST BPDU

## 144.20 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 GigabitEthernet1/0/1 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

## 144.21 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

# 145 SYSEVENT

本节介绍系统事件模块输出的日志信息。

## 145.1 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 <i>MDC-ID</i> 或Context <i>Context-ID</i>
日志等级	6
举例	SYSEVENT/6/EVENT_TIMEOUT: -MDC=1; Module 0x1140000's processing for event 0x20000010 timed out. SYSEVENT/6/EVENT_TIMEOUT: -Context=1; Module 0x33c0000's processing for event 0x20000010 on Context 16 timed out.
日志说明	应用模块处理事件超时 非缺省MDC/Context上打印的日志信息不包含MDC <i>MDC-ID</i> 或Context <i>Context-ID</i> 缺省MDC/Context上打印的本MDC/Context的日志信息不包含MDC <i>MDC-ID</i> 或Context <i>Context-ID</i> 缺省MDC/Context上打印的其它MDC/Context的日志信息包含MDC <i>MDC-ID</i> 或Context <i>Context-ID</i>
处理建议	无

# 146 SYSLOG

本节包含 syslog（信息中心）模块输出的日志消息。

## 146.1 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	请重启设备或者联系技术支持人员

## 146.2 SYSLOG\_LOGFILE\_CREATE

日志内容	Going to create new logfile [%s].
参数解释	\$1: 日志文件的名称
日志等级	6
举例	SYSLOG/6/SYSLOG_LOGFILE_CREATE: Going to create new logfile flash:/logfile/logfile2.log.
日志说明	设备将创建日志文件用于存储新的日志
处理建议	无

## 146.3 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

## 146.4 SYSLOG\_LOGFILE\_OVERWRITE

日志内容	The logfile [%s] will be overwritten.
参数解释	\$1: 日志文件的名称
日志等级	6
举例	SYSLOG/6/SYSLOG_LOGFILE_OVERWRITE: The logfile flash:/logfile/logfile.log will be overwritten.
日志说明	日志文件已经写满，设备存储下一条日志时，将对日志文件进行覆盖操作
处理建议	请备份日志文件，以免旧日志被新日志覆盖

## 146.5 SYSLOG\_NO\_SPACE

日志内容	Failed to save log file due to lack of space resources.
参数解释	无
日志等级	4
举例	SYSLOG/4/SYSLOG_NO_SPACE: -MDC=1; Failed to save log file due to lack of space resources.
日志说明	存储介质空间不足，将日志保存到日志文件失败
处理建议	请定期清理存储介质的存储空间，以免影响日志文件功能

## 146.6 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

## 146.7 SYSLOG\_RTM\_EVENT\_BUFFER\_FULL

日志内容	In the last minute, [STRING] syslog logs were not monitored because the buffer was full.
参数解释	\$1: 过去1分钟内SYSLOG模块没有发送给EAA模块的日志的条数
日志等级	5
举例	SYSLOG/5/SYSLOG_RTM_EVENT_BUFFER_FULL: In the last minute, 100 syslog logs were not monitored because the buffer was full.
日志说明	设备在短时间内产生大量日志，导致EAA监控的日志缓冲区被占满，有多条日志没来得及匹配便被丢弃了
处理建议	<ul style="list-style-type: none"><li>找到日志的来源，减少日志的生成</li><li>使用 <code>rtm event syslog buffer-size</code> 命令增大 EAA 监控的日志缓冲区的大小</li></ul>

## 146.8 SYSLOG\_START

日志内容	System started -- [STRING] Software.
参数解释	\$1: 公司名称
日志等级	6
举例	SYSLOG/6/SYSLOG_START: System started -- XXXX Software
日志说明	系统启动完成（本日志的支持情况与设备的型号有关，请以设备的实际情况为准）
处理建议	无

# 147 TACACS

本节介绍 TACACS 模块输出的日志信息。

## 147.1 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	<ol style="list-style-type: none"><li>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。</li><li>2. 执行 <a href="http://localhost:7890/pages/30007870/01/30007870/01/resources/dc_ne_product_manual_v8r9c10/software/nev8r9_vrpv8r15/user/vrp/ping.html">http://localhost:7890/pages/30007870/01/30007870/01/resources/dc_ne_product_manual_v8r9c10/software/nev8r9_vrpv8r15/user/vrp/ping.html</a> 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。</li><li>3. 请收集日志信息和诊断信息，并联系技术支持</li></ol>



## 147.2 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

## 147.3 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 服务器拒绝了用户的认证请求
处理建议	无

## 147.4 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	<ol style="list-style-type: none"><li>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。</li><li>2. 执行 <a href="http://localhost:7890/pages/30007870/01/30007870/01/resources/dc_ne_product_manual_v8r9c10/software/nev8r9_vrpv8r15/user/vrp/ping.html">http://localhost:7890/pages/30007870/01/30007870/01/resources/dc_ne_product_manual_v8r9c10/software/nev8r9_vrpv8r15/user/vrp/ping.html</a> 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。</li><li>3. 请收集日志信息和诊断信息, 并联系技术支持</li></ol>

## 147.5 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

## 147.6 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

## 147.7 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	<ol style="list-style-type: none"><li>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。</li><li>2. 执行 <a href="http://localhost:7890/pages/30007870/01/30007870/01/resources/dc_ne_product_manual_v8r9c10/software/nev8r9_vrpv8r15/user/vrp/ping.html">http://localhost:7890/pages/30007870/01/30007870/01/resources/dc_ne_product_manual_v8r9c10/software/nev8r9_vrpv8r15/user/vrp/ping.html</a> 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。</li><li>3. 请收集日志信息和诊断信息, 并联系技术支持</li></ol>

## 147.8 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

## 147.9 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

# 148 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。

## 148.1 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	<ol style="list-style-type: none"><li>1. 建议更换存储介质</li><li>2. 通过管理端为设备的 TCSM 密钥重新签发证书</li><li>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</li></ol>

## 148.2 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	<ol style="list-style-type: none"><li>1. 如果该密钥还存在，删除该密钥（相关命令为 key destroy）</li><li>2. 建议更换存储介质</li><li>3. 如果丢失/损坏的是系统预置密钥，请联系技术支持</li></ol>

## 148.3 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	<ol style="list-style-type: none"><li>1. 删除该密钥及其上层密钥（相关命令为 key destroy）</li><li>2. 建议更换存储介质</li></ol>

## 148.4 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

## 148.5 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

# 149 TELNETD

本节介绍 TELNETD（Telnet Daemon）模块输出的日志信息。

## 149.1 TELNETD\_ACL\_DENY

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

## 149.2 TELNETD\_REACH\_SESSION\_LIMIT

日志内容	Telnet client [STRING] failed to log in. The current number of Telnet sessions is [NUMBER]. The maximum number allowed is ([NUMBER]).
参数解释	\$1: Telnet客户端IP地址 \$2: 当前的Telnet会话数 \$3: 设备允许建立的Telnet会话数
日志等级	6
举例	TELNETD/6/TELNETD_REACH_SESSION_LIMIT: Telnet client 1.1.1.1 failed to log in. The current number of Telnet sessions is 10. The maximum number allowed is (10).
日志说明	Telnet登录用户达到上限。该日志在Telnet服务端检测到登录客户端数达到上限时输出
处理建议	请根据需要使用命令 <code>aaa session-limit</code> 配置允许的Telnet最大登录用户数

# 150 TRACK

本节介绍 TRACK 模块输出的日志信息。

## 150.1 TRACK\_STATE\_CHANGE

日志内容	The state of track entry [UINT32] changed from [STRING] to [STRING].
参数解释	\$1: Track项的序号，取值范围为1~1024 \$2: 先前状态，取值为Positive、Negative和NotReady \$3: 当前状态，取值为Positive、Negative和NotReady
日志等级	6
举例	TRACK/6/TRACK_STATE_CHANGE: -MDC=1; The state of track entry 1 changed from Negative to Positive.
日志说明	Track项的状态： <ul style="list-style-type: none"><li>如果监测结果为监测对象工作正常（如接口处于 up 状态、网络可达），则对应 Track 项的状态为 Positive</li><li>如果监测结果为监测对象出现异常（如接口处于 down 状态、网络不可达），则对应 Track 项的状态为 Negative</li><li>如果监测结果无效（如 NQA 作为监测模块时，与 Track 项关联的 NQA 测试组不存在），则对应 Track 项的状态为 NotReady</li></ul>
处理建议	检查监测模块运行是否正常

# 151 TRILL

本节介绍 TRILL 模块输出的日志信息。

## 151.1 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： <ul style="list-style-type: none"><li>• 为本地 RBridge 和远端 RBridge 分配了相同的 System ID</li><li>• 本地 RBridge 收到了一个自己产生、携带了旧的 Nickname 的 LSP PDU</li></ul>
处理建议	检查TRILL网络中上RBridge的System ID

## 151.2 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



### 151.3 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	3
举例	TRILL/3/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	请更换有效的License

### 151.4 TRILL\_LICENSE\_EXPIRED\_TIME

日志内容	The TRILL feature will be disabled in [ULONG] days.
参数解释	\$1: 功能还可使用的天数
日志等级	5
举例	TRILL/5/TRILL_LICENSE_EXPIRED_TIME: The TRILL feature will be disabled in 2 days.
日志说明	TRILL的License不可用，TRILL功能将在2天后失效  说明 主备倒换后新的主控板上没有可用的 TRILL License。会启动 30 天临时可用定时器
处理建议	若要继续使用TRILL功能，请准备新的License

### 151.5 TRILL\_LICENSE\_UNAVAILABLE

日志内容	The TRILL feature has no available license.
参数解释	无
日志等级	3
举例	TRILL/3/TRILL_LICENSE_UNAVAILABLE: The TRILL feature has no available license.
日志说明	进程启动时，没有找到TRILL对应的License
处理建议	请为TRILL安装有效的License

## 151.6 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

## 151.7 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 <ul style="list-style-type: none"><li>○ up: 表示邻居关系已建立, 可以正常工作</li><li>○ initializing: 表示初始状态</li><li>○ down: 表示邻居关系结束</li></ul>
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

# 152 VCF

本节介绍 VCF Fabric 模块输出的日志信息。

## 152.1 VCF\_AGGR\_CREAT

日志内容	Phase [STRING], Device [STRING] created Layer 2 aggregation group [INT32]: member ports=[STRING].
参数解释	\$1: 阶段 \$2: 设备MAC地址 \$3: 二层聚合组ID \$4: 二层聚合组成员端接口列表
日志等级	6
举例	VCF/6/VCF_AGGR_CREAT: Phase 2.0.5, Device 0000-0000-0000 created Layer 2 aggregation group 10: member ports=Ten-GigabitEthernet1/0/2, Ten-GigabitEthernet1/0/10.
日志说明	创建二层聚合组，并将端口加入对应的聚合组
处理建议	无

## 152.2 VCF\_AGGR\_DELETE

日志内容	Phase [STRING], Device [STRING] deleted Layer 2 aggregation group [INT32].
参数解释	\$1: 阶段 \$2: 设备MAC地址 \$3: 二层聚合组ID
日志等级	6
举例	VCF/6/VCF_AGGR_DELETE: Phase 2.0.6, Device 0000-0000-0000 deleted Layer 2 aggregation group 10.
日志说明	二层聚合组中仅包含一条Up状态的链路时，删除聚合组
处理建议	无

## 152.3 VCF\_AGGR\_FAILED

日志内容	Phase [STRING], Device [STRING] failed to create Layer 2 aggregation group [INT32].
参数解释	\$1: 阶段 \$2: 设备MAC地址 \$3: 聚合组ID
日志等级	3
举例	VCF/3/ VCF_AGGR_FAILED: Phase 2.0.7, Device 0000-0000-0000 failed to create Layer 2 aggregation group 10.
日志说明	创建聚合组失败
处理建议	请管理员排查是否因为资源不足等原因造成聚合组创建失败

## 152.4 VCF\_AUTO\_ANALYZE\_USERDEF

日志内容	Phase [STRING], Device [STRING] started to parse template file.
参数解释	\$1: 阶段 \$2: 设备的MAC地址
日志等级	6
举例	VCF/6/VCF_AUTO_ANALYZE_USERDEF: Phase 1.2.2, Device 0000-0000-0000 started to parse template file.
日志说明	开始解析模板文件中的用户自定义配置
处理建议	无

## 152.5 VCF\_AUTO\_NO\_USERDEF

日志内容	Phase [STRING], Device [STRING] found undefined variable [STRING] in command [STRING] on line [INTEGER].
参数解释	\$1: 阶段 \$2: 设备的MAC地址 \$3: 未定义的用户变量 \$4: 出错的命令行 \$5: 出错的命令行行号
日志等级	3
举例	VCF/3/VCF_AUTO_NO_USERDEF: Phase 1.2.3, Device 0000-0000-0000 found undefined variable \$\$_ABC in command interface \$\$_ABC on line 192.
日志说明	解析模板文件过程中，若模板文件中存在无法识别的用户定义变量时，输出此日志信息，提示未找到用户定义的变量。若存在多个无法识别的用户定义变量，则打印多条此日志信息
处理建议	需管理员确认模板文件中定义的变量是否正确，修改后重新部署

## 152.6 VCF\_AUTO\_START

日志内容	Phase [STRING], Device [STRING] (Role [STRING]) started VCF automated deployment.
参数解释	\$1: 阶段 \$2: 设备的MAC地址 \$3: 设备的角色，spine、leaf或access
日志等级	5
举例	VCF/5/VCF_AUTO_START: Phase 1.0.1, Device 0000-0000-0000 (Role leaf) started VCF automated deployment.
日志说明	自动化部署开始
处理建议	无

## 152.7 VCF\_AUTO\_STATIC\_CMD

日志内容	Phase [STRING], Device [STRING] automatically executed static commands.
参数解释	\$1: 阶段 \$2: 设备的MAC地址
日志等级	6
举例	VCF/6/VCF_AUTO_STATIC_CMD: Phase 1.2.4, Device 0000-0000-0000 automatically executed static commands.
日志说明	执行模板中的静态配置命令，静态配置命令是指与VCF拓扑等动态信息无关的配置命令
处理建议	无

## 152.8 VCF\_BGP

日志内容	Phase [STRING], Device [STRING] established a BGP session with peer [STRING] in AS [INT32]. Phase [STRING], Device [STRING] established a BGP session with peers [[STRING]] in AS [INT32].
参数解释	\$1: 阶段 \$2: 设备的MAC地址 \$3: peer地址（三层组网时，主Spine节点可能一次为设备配置多个peer，不同peer地址之间用逗号分隔） \$4: BGP的AS号
日志等级	6
举例	VCF/6/VCF_BGP: Phase 3.0.5, Device 0000-0000-0000 established a BGP session with peer 1.1.1.1 in AS 100. VCF/6/VCF_BGP: Phase 3.0.5, Device 0000-0000-0000 established a BGP session with peers ['1.1.1.1', '1.1.1.2'] in AS 100.
日志说明	VCF成功与对等体建立BGP会话 在三层组网中，仅主Spine节点上会记录该日志信息
处理建议	无

## 152.9 VCF\_DOWN\_LINK

日志内容	Phase [STRING], Device [STRING] discovered downlink interface [STRING].
参数解释	\$1: 阶段 \$2: 设备MAC地址 \$3: 下行接口名
日志等级	6
举例	VCF/6/VCF_DOWN_LINK: Phase 2.0.8, Device 0000-0000-0000 discovered downlink interface Ten-GigabitEthernet1/0/1.
日志说明	VCF发现下行接口（Spine设备上连接Leaf的接口或leaf设备连接下游接入设备的接口），并下发配置
处理建议	无

## 152.10 VCF\_DRIVER\_INIT

日志内容	Phase [STRING], failed to find driver [STRING]. Driver initialization failed.
参数解释	\$1: 阶段 \$2: 驱动名称
日志等级	3
举例	VCF/3/VCF_DRIVER_INIT: Phase 3.0.8, failed to find driver 6820. Driver initialization failed.
日志说明	设备驱动不存在时，提示驱动初始化失败。
处理建议	请检查模板对应驱动名称是否正确，联系开发人员确认VCF是否支持该驱动

## 152.11 VCF\_FAILED\_ADD\_IRFPORT

日志内容	Phase [STRING], failed to bind IRF physical interface [STRING] on device with MAC address [STRING] to an IRF port three times.
参数解释	\$1: 阶段 \$2: IRF物理端口 \$3: MAC地址
日志等级	4
举例	VCF/4/VCF_FAILED_ADD_IRFPORT: Phase 2.0.10, failed to bind IRF physical interface [STRING] on device with MAC address 4c85-5206-0100 to an IRF port three times.
日志说明	设备自动化上线时，如果指定IRF物理端口绑定IRF端口失败三次，则VCF不再尝试将该IRF物理端口与IRF端口绑定，同时打印此日志
处理建议	建议检查IRF连线

## 152.12 VCF\_GET\_IMAGE

日志内容	Phase [STRING], Device [STRING] obtained information about update startup image file [STRING]: new version=[STRING], current version=[STRING].
参数解释	\$1: 阶段 \$2: 设备的MAC地址 \$3: 新版本文件名 \$4: 新版本的产品外部版本号 \$5: 设备当前产品外部版本号
日志等级	6
举例	VCF/6/VCF_GET_IMAGE: Phase 1.3.1, Device 0000-0000-0000 obtained information about update startup image file s6800.ipe: new version=V300R009B01D002, current version=V300R009B01D001.
日志说明	通过模板文件获取新版本的文件名和版本号
处理建议	无

## 152.13 VCF\_GET\_TEMPLATE

日志内容	Phase [STRING], Device [STRING] downloaded template file [STRING].
参数解释	\$1: 阶段 \$2: 设备的MAC地址 \$3: 模板文件名
日志等级	6
举例	VCF/6/VCF_GET_TEMPLATE: Phase 1.2.1, Device 0000-0000-0000 downloaded template file /mnt/flash/vxlan_spine.template.
日志说明	将自动部署的模板文件下载到本地设备
处理建议	无



## 152.14 VCF\_INSTALL\_IMAGE

日志内容	Phase [STRING], Device [STRING] started to install the [STRING] version of startup image.
参数解释	\$1: 阶段 \$2: 设备的MAC地址 \$3: 设备的版本号
日志等级	6
举例	VCF/6/VCF_INSTALL_IMAGE: Phase 1.3.3, Device 0000-0000-0000 started to install the V700R001B70D001 version of startup image.
日志说明	设备开始安装新版本
处理建议	无

## 152.15 VCF\_IRF\_FINISH

日志内容	Phase [STRING], Device [STRING] finished IRF configuration: result=[INT32].
参数解释	\$1: 阶段 \$2: 本设备的MAC地址 \$3: 执行IRF配置的结果 (成功=0, 失败=-1)
日志等级	5
举例	VCF/5/VCF_IRF_FINISH: Phase 2.0.3, Device 0000-0000-0000 finished IRF configuration: result=0.
日志说明	完成IRF配置下发
处理建议	如果配置下发失败, 请联系用服工程师解决

## 152.16 VCF\_IRF\_FOUND

日志内容	Phase [STRING], Device [STRING] (Role [STRING]) found a peer ([STRING]) with the same role, IRF stackability check result: [INT32].
参数解释	\$1: 阶段 \$2: 本设备的MAC地址 \$3: 角色名字 \$4: 对端设备的MAC地址 \$5: 检查结果, 取值包括: <ul style="list-style-type: none"><li>0: 表示可配置 IRF</li><li>1: 表示 MAC 地址冲突</li></ul>
日志等级	5
举例	VCF/5/VCF_IRF_FOUND: Phase 2.0.1, Device 0000-0000-0000 (Role leaf) found a peer with the same role, IRF stackability check result: 0.
日志说明	VCF通过拓扑变化发现对端需要搭建IRF的设备, 检查是否能够开始进行IRF配置
处理建议	无

## 152.17 VCF\_IRF\_START

日志内容	Phase [STRING], Device [STRING] started IRF configuration: current member ID=[INT32], new member ID=[INT32], priority=[INT32], IRF-port 1's member ports=[STRING], IRF-port 2's member ports=[STRING].
参数解释	\$1: 阶段 \$2: 本设备的MAC地址 \$3: 设备当前的成员编号 \$4: 设备新的成员编号 \$5: 设备新的优先级 \$6: 设备IRF-Port1绑定的物理端口列表, 没有为none \$7: 设备IRF-Port2绑定的物理端口列表, 没有为none
日志等级	5
举例	VCF/5/VCF_IRF_START: Phase 2.0.2, Device 0000-0000-0000 started IRF configuration: current member ID=2, new member ID=1, priority=2, IRF-port 1's member ports=GigabitEthernet1/0/1, IRF-port 2's member ports=none.
日志说明	开始下发IRF配置
处理建议	无

## 152.18 VCF\_LOOPBACK\_START

日志内容	Phase [STRING], IP address assignment started for [STRING] on other nodes.
参数解释	\$1: 阶段 \$2: 接口名称
日志等级	5
举例	VCF/5/VCF_LOOPBACK_START: Phase 3.0.1, IP address assignment started for Loopback0 on other nodes.
日志说明	VCF主节点开始为其他节点的接口分配IP地址
处理建议	无

## 152.19 VCF\_LOOPBACK\_START\_FAILED

日志内容	Phase [STRING], failed to assign IP addresses to [STRING] on other nodes: reason=[STRING].
参数解释	\$1: 阶段 \$2: 接口名称 \$3: 启动失败的原因 <ul style="list-style-type: none"><li>○ -1: 表示没有指定 IP 范围</li><li>○ -2: 表示 IP 地址无效</li></ul>
日志等级	5
举例	VCF/5/VCF_LOOPBACK_START_FAILED: Phase 3.0.1, failed to assign IP addresses to Loopback0 on other nodes: reason=-1.
日志说明	VCF Fabric组网中，由于以下原因之一，主节点没能开始为其他节点的接口分配IP地址： <ul style="list-style-type: none"><li>○ 没有指定 IP 范围</li><li>○ IP 地址无效</li></ul>
处理建议	管理员检查模板中IP范围是否有问题

## 152.20 VCF\_LOOPBACK\_ALLOC

日志内容	Phase [STRING], assigned IP [STRING] to [STRING] on Device [STRING]: result=[INT32].
参数解释	\$1: 为Loopback接口分配的IP地址 \$2: 设备的MAC地址 \$3: 接口名称 \$4: IP地址分配的状态, 取值包括: <ul style="list-style-type: none"><li>○ 0: 表示成功</li><li>○ -1: 表示 netconf 下发失败</li><li>○ -2: 表示 netconf 处理异常</li><li>○ -3: 表示 netconf 初始化失败</li></ul>
日志等级	5
举例	VCF/5/VCF_LOOPBACK_ALLOC: Phase 3.0.2, assigned IP 10.100.1.1 to Loopback0 on Device 0000-0000-0000: result=0.
日志说明	VCF主节点为指定设备的接口分配IP地址
处理建议	管理员根据结果查找失败原因

## 152.21 VCF\_LOOPBACK\_NO\_FREE\_IP

日志内容	Phase [STRING], no IP addresses available for Device [STRING].
参数解释	\$1: 阶段 \$2: 设备的MAC地址
日志等级	4
举例	VCF/4/VCF_LOOPBACK_NO_FREE_IP: Phase 3.0.4, no IP addresses available for Device 0000-0000-0000.
日志说明	VCF主节点上没有可用的IP地址, 无法为指定设备的接口分配IP地址
处理建议	请用户确认IP预留范围是否准确

## 152.22 VCF\_LOOPBACK\_RECLAIM

日志内容	Phase [STRING], reclaimed IP [STRING] from [STRING] on Device [STRING]: reason=[INT32].
参数解释	\$1: 阶段 \$2: 收回的Loopback接口IP地址 \$3: 接口名称 \$4: 收回IP地址的设备的MAC地址 \$5: 收回原因, 取值 <ul style="list-style-type: none"><li>1: 表示设备 DOWN</li></ul>
日志等级	5
举例	VCF/5/VCF_LOOPBACK_RECLAIM: Phase 3.0.3, reclaimed IP 10.10.10.1 from Loopback0 on Device 0000-0000-0000: reason=1.
日志说明	VCF收回已经分配出去的接口的IP地址
处理建议	无

## 152.23 VCF\_REBOOT

日志内容	Phase [STRING], Device [STRING] will reboot. Reason: [STRING].
参数解释	\$1: 阶段 \$2: 设备的MAC地址 \$3: 重启原因, 取值为: <ul style="list-style-type: none"><li>Hardware resource mode change: 硬件资源模式修改</li><li>Version upgrade success: 版本升级成功</li><li>IRF member ID change: 自动化上线时修改成员 ID</li><li>IRF fabric setup success: IRF 成功建立</li><li>Change of the maximum number of ECMP routes: 最大等价路由条数修改</li><li>Standalone-to-IRF mode switchover: 设备由独立运行模式切换为 IRF 模式</li></ul>
日志等级	5
举例	VCF/5/VCF_REBOOT: Phase 1.2.3, Device dc2d-cb20-6304 will reboot. Reason: IRF member ID change.
日志说明	完成新版本升级、IRF成员编号变更等操作后, 设备自动重启
处理建议	无

## 152.24 VCF\_SKIP\_INSTALL

日志内容	Phase [STRING], Device [STRING] skipped automatic version update.
参数解释	\$1: 阶段 \$2: 设备的MAC地址
日志等级	5
举例	VCF/5/VCF_SKIP_INSTALL: Phase 1.3.2, Device 0000-0000-0000 skipped automatic version update.
日志说明	设备当前运版本与通过模板文件获取的版本一致时，跳过自动更新版本
处理建议	无

## 152.25 VCF\_STATIC\_CMD\_ERROR

日志内容	Phase [STRING], Device [STRING] failed to automatically execute static command '[STRING]' in context '[STRING]'.
参数解释	\$1: 阶段 \$2: 设备的MAC地址 \$3: 自动配置执行失败的命令 \$4: 执行失败的命令所在的完整片段
日志等级	4
举例	VCF/4/VCF_STATIC_CMD_ERROR: Phase 1.2.5, Device 0000-0000-0000 failed to automatically execute static command 'port link bridge' in context 'interface ten-gigabitethernet1/0/1; port link bridge'.
日志说明	自动部署过程中执行失败的静态命令
处理建议	管理员查找错误原因，修改错误后需要重新部署

## 152.26 VCF\_UP\_LINK

日志内容	Phase [STRING], Device [STRING] discovered uplink interface [STRING].
参数解释	\$1: 阶段 \$2: 设备MAC地址 \$3: 上行接口名
日志等级	6
举例	VCF/6/VCF_UP_LINK: Phase 2.0.9, Device 0000-0000-0000 discovered uplink interface Ten-GigabitEthernet1/0/1.
日志说明	VCF发现上行接口（Leaf设备上连接Spine的接口），并下发配置
处理建议	无

## 152.27 VCF\_WHITE\_LIST\_CHECK

日志内容	Phase [STRING], Device [STRING] failed whitelist check and automated undelay network deployment stopped.
参数解释	\$1: 阶段 \$2: 本设备的MAC地址, 格式为xxxx-xxxx-xxxx
日志等级	5
举例	VCF/5/VCF_WHITE_LIST_CHECK: Phase 1.0.1, Device dc2d-cb20-6304 failed whitelist check and automated undelay network deployment stopped.
日志说明	VCF模块提示白名单检查失败, Underlay自动化配置下发停止。
处理建议	无

# 153 VLAN

本节介绍接口 VLAN 模块输出的日志信息。

## 153.1 VLAN\_CREATEFAIL

日志内容	Failed to create VLAN [STRING]. The maximum number of VLANs has been reached.
参数解释	\$1: VLAN ID
日志等级	4
举例	VLAN/4/VLAN_CREATEFAIL: Failed to create VLAN 1025-4094. The maximum number of VLANs has been reached.
日志说明	因为VLAN硬件资源不足, 导致创建VLAN失败
处理建议	无

## 153.2 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

### 153.3 VLAN\_QINQETHTYPE\_FAILED

日志内容	Failed to set the TPID value in CVLAN tags to [UINT32] (hexadecimal). The operation is not supported.
参数解释	\$1: 内层VLAN Tag的TPID值
日志等级	4
举例	VLAN/5/VLAN_QINQETHTYPE_FAILED: Failed to set the TPID value in CVLAN tags to 8200 (hexadecimal). The operation is not supported.
日志说明	在IRF3.1组网环境中, CB支持配置内层VLAN Tag的TPID值但PEX不支持的情况下, 在CB上执行 <b>qinq ethernet-type customer-tag</b> 命令后打印, 提示配置未成功
处理建议	确认组网中的PEX设备是否支持配置内层VLAN Tag的TPID值

### 153.4 VLAN\_VLANMAPPING\_FAILED

日志内容	The configuration failed because of resource insufficiency or conflicts on [STRING].
参数解释	\$1: 接口名称
日志等级	4
举例	VLAN/4/VLAN_VLANMAPPING_FAILED: The configuration failed because of resource insufficiency or conflicts on Ethernet0/0.
日志说明	因本接口硬件资源不足或者接口加入或离开二层聚合组, 所以部分或全部VLAN映射配置丢失
处理建议	无

### 153.5 VLAN\_VLANTRANSPARENT\_FAILED

日志内容	The configuration failed because of resource insufficiency or conflicts on [STRING].
参数解释	\$1: 接口名称
日志等级	4
举例	VLAN/4/VLAN_VLANTRANSPARENT_FAILED: The configuration failed because of resource insufficiency or conflicts on Ethernet0/0.
日志说明	因本接口硬件资源不足或者接口加入或离开二层聚合组, 所以部分或全部VLAN透传配置丢失
处理建议	无

## 154 VRRP

本节介绍 VRRP 模块输出的日志信息。



## 154.1 VRRP\_STATUS\_CHANGE

日志内容	The status of [STRING] virtual router [UINT32] (configured on [STRING]) changed from [STRING] to [STRING]: [STRING].
参数解释	<p>\$1: VRRP协议版本</p> <p>\$2: VRRP备份组号</p> <p>\$3: VRRP备份组所在接口的名称</p> <p>\$4: 先前状态</p> <p>\$5: 当前状态</p> <p>\$6: 状态变化原因:</p> <ul style="list-style-type: none"> <li>• Interface event received: 收到接口事件</li> <li>• IP address deleted: 虚地址删除</li> <li>• The status of the tracked object changed: Track 对象状态变化</li> <li>• VRRP packet received: 收到 VRRP 报文</li> <li>• Current device has changed to IP address owner: 当前设备成为地址拥有者</li> <li>• Master-down-timer expired: Master down 定时器超时</li> <li>• Zero priority packet received: 收到 0 优先级的报文</li> <li>• Preempt: 发生了抢占</li> <li>• Master group drove: 管理备份组驱动</li> </ul>
日志等级	6
举例	VRRP/6/VRRP_STATUS_CHANGE: The status of IPv4 virtual router 10 (configured on Ethernet0/0) changed (from Backup to Master): Master-down-timer expired.
日志说明	VRRP备份组中的Master或Backup路由器状态发生变化。可能的原因包括: 收到接口事件、虚地址删除、Track对象状态变化、收到VRRP报文、当前设备成为地址拥有者、Master down定时器超时、收到0优先级的报文、发生了抢占或者管理备份组驱动
处理建议	检查VRRP备份组中的Master或Backup路由器状态, 确保备份组工作正常

## 154.2 VRRP\_VF\_STATUS\_CHANGE

日志内容	The [STRING] virtual router [UINT32] (configured on [STRING]) virtual forwarder [UINT32] detected status change (from [STRING] to [STRING]): [STRING].
参数解释	\$1: VRRP协议版本 \$2: VRRP备份组号 \$3: VRRP备份组所在接口的名称 \$4: VF ID \$5: VF先前状态 \$6: VF当前状态 \$7: 状态变化原因
日志等级	6
举例	VRRP/6/VRRP_VF_STATUS_CHANGE: The IPv4 virtual router 10 (configured on GigabitEthernet5/1) virtual forwarder 2 detected status change (from Active to Initialize): Weight changed.
日志说明	虚拟转发器状态发生改变。可能的原因包括权重变化、定时器超时、VRRP备份组Down
处理建议	检查Track项的状态

## 154.3 VRRP\_VMAC\_INEFFECTIVE

日志内容	The [STRING] virtual router [UINT32] (configured on [STRING]) failed to add virtual MAC: [STRING].
参数解释	\$1: VRRP协议版本 \$2: VRRP备份组号 \$3: VRRP备份组所在接口的名称 \$4: 出现错误的原因
日志等级	3
举例	VRRP/3/VRRP_VMAC_INEFFECTIVE: The IPv4 virtual router 10 (configured on Ethernet0/0) failed to add virtual MAC: Insufficient hardware resources.
日志说明	添加虚拟MAC地址失败
处理建议	确定操作失败的根因并解决

# 155 VSRP

本节介绍 VSRP 模块输出的日志信息。

## 155.1 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

# 156 VXLAN

本节介绍 VXLAN 模块输出的日志信息。

## 156.1 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

# 157 WEB

本节介绍 WEB 模块输出的普通日志信息。

## 157.1 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

## 157.2 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

## 157.3 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

# 158 WIPS

本节介绍 WIPS 模块输出的日志信息。

## 158.1 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

## 158.2 AP\_CHANNEL\_CHANGE

日志内容	-VSD=[STRING]-SrcMAC=[MAC]; Channel change detected.
参数解释	\$1: VSD名字 \$2: AP的地址
日志等级	5
举例	WIPS/5/AP_CHANNEL_CHANGE: -VSD=home-SrcMAC=1122-3344-5566; Channel change detected.
日志说明	指定VSD内检测到指定AP信道改变时触发日志
处理建议	检查AP信道改变是否正常

## 158.3 ASSOCIATEOVERFLOW

日志内容	-VSD=[STRING]-SrcMAC=[MAC]; Association/Reassociation DoS attack detected.
参数解释	\$1: VSD名字 \$2: AP的地址
日志等级	5
举例	WIPS/5/ASSOCIATEOVERFLOW: -VSD=home-SrcMAC=1122-3344-5566; Association/Reassociation DoS attack detected.
日志说明	指定VSD内检测到指定AP回应status code为17的关联回应帧时触发日志
处理建议	检查AP是否受到攻击

## 158.4 HONEYPOT

日志内容	-VSD=[STRING]-SrcMAC=[MAC]; Honeypot AP detected.
参数解释	\$1: VSD名字 \$2: AP的地址
日志等级	5
举例	WIPS/5/HONEYPOT: -VSD=home-SrcMAC=1122-3344-5566; Honeypot AP detected.
日志说明	指定VSD内检测到指定AP为蜜罐时触发日志
处理建议	检查是否存在攻击

## 158.5 HTGREENMODE

日志内容	-VSD=[STRING]-SrcMAC=[MAC]; HT-Greenfield AP detected.
参数解释	\$1: VSD名字 \$2: AP的地址
日志等级	5
举例	WIPS/5/HTGREENMODE: -VSD=home-SrcMAC=1122-3344-5566; HT-Greenfield AP detected.
日志说明	指定VSD内检测到指定AP携带绿野模式时触发日志
处理建议	检查是否受到攻击

## 158.6 MAN\_IN\_MIDDLE

日志内容	-VSD=[STRING]-SrcMAC=[MAC]; Man-in-the-middle attack detected.
参数解释	\$1: VSD名字 \$2: client的地址
日志等级	5
举例	WIPS/5/MAN_IN_MIDDLE: -VSD=home-SrcMAC=1122-3344-5566; Man-in-the-middle attack detected.
日志说明	指定VSD内检测到指定client受到中间人攻击时触发日志
处理建议	检查client是否受到中间人攻击

## 158.7 WIPS\_DOS

日志内容	-VSD=[STRING]; [STRING] rate attack detected.
参数解释	<p>\$1: VSD名字</p> <p>\$2: 设备类型</p> <ul style="list-style-type: none"> <li>○ AP: AP</li> <li>○ Client: 客户端</li> </ul>
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

## 158.8 WIPS\_FLOOD

日志内容	-VSD=[STRING]-SrcMAC=[MAC]; [STRING] flood detected.
参数解释	<p>\$1: VSD名字</p> <p>\$2: Flood攻击的MAC地址</p> <p>\$3: Flood帧类型</p> <ul style="list-style-type: none"> <li>● Association request: Association 帧</li> <li>● Authentication: Authentication 帧</li> <li>● Disassociation: Disassociation 帧</li> <li>● Reassociation request: Reassociation request 帧</li> <li>● Deauthentication: Deauthentication 帧</li> <li>● Null data: Null data 帧</li> <li>● Beacon: Beacon 帧</li> <li>● Probe request: Probe request 帧</li> <li>● BlockAck: BlockAck 帧</li> <li>● CTS: CTS 帧</li> <li>● RTS: RTS 帧</li> <li>● EAPOL start: EAPOL start 帧</li> </ul>
日志等级	5
举例	WIPS/5/WIPS_FLOOD: -VSD=home-SrcMAC=1122-3344-5566; Association request flood detected.
日志说明	一定时间内在指定VSD内检测到同一类型的报文超过阈值时触发日志
处理建议	检查报文发送者的合法性

## 158.9 WIPS\_MALF

日志内容	-VSD=[STRING]-SrcMAC=[MAC]; Error detected: [STRING].
参数解释	<p>\$1: VSD名字</p> <p>\$2: 发送者的MAC地址</p> <p>\$3: 畸形报文类型</p> <ul style="list-style-type: none"> <li>• invalid ie length: 非法 IE 长度</li> <li>• duplicated ie: 重复 IE</li> <li>• redundant ie: 冗余 IE</li> <li>• invalid pkt length: 报文长度无效</li> <li>• illegal ibss ess: 不合法 IBSS ESS</li> <li>• invalid source addr: 无效源 MAC</li> <li>• overflow eapol key: EAPOL-Key 帧畸形</li> <li>• malf auth: 畸形认证</li> <li>• malf assoc req: 畸形关联请求</li> <li>• malf ht ie: HT IE 畸形</li> <li>• large duration: large duration 畸形</li> <li>• null probe resp: null probe resp 畸形</li> <li>• invalid deauth code: Deauthentication 畸形</li> <li>• invalid disassoc code: 解除关联码畸形</li> <li>• over flow ssid: Overflow-ssid 畸形</li> <li>• fata jack: fata jack 畸形</li> </ul>
日志等级	5
举例	WIPS/5/WIPS_MALF: -VSD=home-SrcMAC=1122-3344-5566; Error detected: fata jack.
日志说明	指定VSD内检测到指定类型的畸形报文时触发日志
处理建议	检查报文发送者的合法性



## 158.10 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 <ul style="list-style-type: none"><li>• AP spoofing AP: AP 仿冒为 AP</li><li>• AP spoofing client: AP 仿冒为 client</li><li>• AP spoofing ad-hoc: AP 仿冒为 ad-hoc</li><li>• Ad-hoc spoofing AP: Ad-hoc 仿冒为 AP</li><li>• Client spoofing AP: Client 仿冒为 AP</li></ul>
日志等级	5
举例	WIPS/5/WIPS_SPOOF: -VSD=home-SrcMAC=1122-3344-5566; AP spoofing AP detected.
日志说明	指定VSD内检测到设备仿冒时触发日志
处理建议	检查报文发送者的合法性

## 158.11 WIPS\_WEAKIV

日志内容	-VSD=[STRING]-SrcMAC=[MAC]; Weak IV detected.
参数解释	\$1: VSD名字 \$2: 发送者的MAC地址
日志等级	5
举例	WIPS/5/WIPS_WEAKIV: -VSD=home-SrcMAC=1122-3344-5566; Weak IV detected.
日志说明	指定VSD内检测到采用weak IV加密的报文
处理建议	使用安全级别更高的加密方法加密报文

## 158.12 WIRELESSBRIDGE

日志内容	-VSD=[STRING]-AP1=[MAC]-AP2=[MAC]]; Wireless bridge detected.
参数解释	\$1: VSD名字 \$2: AP的地址 \$3: AP的地址
日志等级	5
举例	WIPS/5/WIRELESSBRIDGE: -VSD=home-AP1=1122-3344-5566-AP2=7788-9966-5544; Wireless bridge detected.
日志说明	指定VSD内检测到AP1和AP2建立无线网桥时触发日志
处理建议	检查无线网桥是否合法